최대 동일 길이를 갖는 여원 HGCA 구성

조성진* · 최언숙** · 황윤희* · 김진경* · 표용수* · 김한두***

Construction of Complemented Hybrid Group Cellular Automata with Maximum Equal Lengths

S.J. Cho* · U.S. Choi** · Y.H. Hwang* · J.G. Kim* · Y.S. Pyo* · H.D. Kim***

요 약

최근 무선 통신의 출현과 PDA, 스마트 카드와 같은 휴대용 장치의 발전으로 인해, 이에 대한 보안과 개인 정보 보호에 대한 필요성이 대두되면서 암호학의 적용에 관심이 높아지고 있다. CA는 암 · 복호화를 공유할 수 있는 하드웨어 구현이 용이하다. 본 논문에서는 전이규칙 60, 102 또는 204를 갖는 선형 하이브리드 셀룰라 오토마타가 그룹 셀룰라 오토마타가 되는 조건을 제안하고 이 셀룰라 오토마타로부터 유도된 여원 하이브리드 그룹 CA의 상태 전이그래프에서 모든 사이클의 주기가 동일하고 가능한 최대 길이를 갖는 CA가 되기 위한 여원벡터의 조건을 제시한다. 또한 여원 하이브리드 그룹 셀룰라 오토마타의 사이클들 간의 관계를 분석한다. 이는 Mukhopadhyay의 결과의 일반화이다.

ABSTRACT

Recently with the ever increasing growth of data communication, the need for security and privacy has become a necessity. The advent of wireless communication and other handheld devices like Personal Digital Assistants and smart cards have made the implementation of cryptosystems a major issue. The Cellular Automata(CA) can be programmed to implement hardware sharing between the encryption and decryption. In this paper, we give conditions for a linear hybrid cellular automata with 60, 102 or 204 to be a linear hybrid group cellular automata C. And we present the conditions which the complemented hybrid group cellular automata C' with complement vectors derived from C has maximum equal lengths in the state transition diagram of C'. Also we analyze the relationship among cycles of C'. These results generalize Mukhopadhyay's results.

키워드

셀룰라 오토마타, 선형 하이브리드 그룹 CA, 여원 CA, 전이규칙, 상태전이행렬, 여원벡터, 주기, 최소다항식

Ⅰ. 서 론

셀룰라 오토마타(이하, CA)는 셀이라 불리는 간단한 메모리의 배열로서 각 셀들의 상태가 국소적인 상호작용에 의해서 동시에 갱신되는 시스템이다. CA는 간단하고, 규칙적이며 작은 단위로 확장연결이 가능하여 전용의 하드웨어를 사용하지 않고 실행 가능하도록 프로그램화 될 수 있다. 최근 무선 통신의 출현과 PDA, 스마트 카드와 같은 휴대용 장치의 발전으로 인해, 이에 대한 보안과 개인 정보 보호에 대한 필요성이 대두되면서 암호학의 적용에

* 부경대학교
** 동명대학교, 교신저자
*** 인제대학교

접수일자 : 2006. 4. 13

관심이 높아지고 있다. 특히, 암·복호화를 공유할 수 있는 하드웨어 구현에 관심이 모아지고 있는데, 여기에 CA가 이용가능하다.

Mukhopadhyay 등은 전이규칙 102를 사용하는 uniform CA로부터 셀 상태가 모두 1인 여원벡터에 의하여 유도된 여원 uniform 그룹 CA를 분석하고, 이러한 성질을 이용하여 키 공유 프로토콜에 적용하였다[1].

본 논문에서는 전이규칙 60, 102 또는 204를 갖는 선형 하이브리드 셀룰라 오토마타가 그룹 셀룰라 오토마타가 되는 조건을 제안하고, 이 셀룰라 오토마타로부터 유도된 여원 하이브리드 그룹 CA(Hybrid Group CA: 이하 HGCA)의 상태전이그래프에서 모든 사이클의 주기가 동일하고 가능한 최대 길이를 갖는 CA가 되도록 하는 여원벡터의 조건을 제시한다. 또한 여원 HGCA의 사이클들 간의 관계를 분석한다. 이 결과들은 Mukhopadhyay의 결과의 일반화이다.

Ⅱ. 셀룰라 오토마타

이산 시간의 동적 시스템으로 셀이라는 기본 단위 메모리의 배열로 이루어진 CA는 간단하고 규칙적이며 작은 단위로 확장 연결이 가능하여 VLSI 하드웨어 구현이 용이하여, 패턴 생성, 의사 난수열 생성기, 오류 정정 부호, 신호 분석기, 암호 등에 많이 응용되고 있다[2-8]. Cattell 등에 의하여 LFSR에 대응하는 CA에 대한 연구가 이뤄졌으며, 최대 길이를 갖는 CA를 찾는 연구가 수행되었다[9,10]. 또, Cho 등은 비그룹 CA의 특성에 관한 연구를 하였다[11-13].

본 논문에서 다루는 1차원 3-이웃(linear 3-neighbourhood) CA는 모든 셀이 선형으로 배열되어 있고, 국소적 상호작용이 자신과 인접한 두 셀에 의하여 이루어지는 CA이다. CA에 대한 상태전이함수(state transition function)는

$$x_i^{t+1} = f(x_{i-1}^t, x_i^t, x_{i+1}^t)$$

과 같이 나타낸다. 여기서 x_i^t는 시간 t에서 i번째 셀의 상태를 나타낸다. 그리고 이러한 f는 2^{2^3}개가 있으며 이것을 CA의 전이규칙이라 한다. 본 논문에서 사용되는 전이규칙 60, 102 와 204는 다음과 같다.

전이규칙 60 : $x_i^{t+1} = x_{i-1}^t \oplus x_i^t$

전이규칙 102 : $x_i^{t+1} = x_i^t \oplus x_{i+1}^t$

전이규칙 204 : $x_i^{t+1} = x_i^t$

모든 CA의 셀이 같은 전이규칙을 따르는 CA를 uniform CA라 하고, 2가지 이상의 서로 다른 규칙이 적용된 CA를 하이브리드 CA라 한다. 선형 n-셀 CA의 상태전이함수는 $n \times n$ 행렬로 나타낼 수 있으며, 이를 상태전이행렬(state transition matrix)이라고 한다. 주어진 n-셀 CA의 상태전이행렬 T의 특성다항식(characteristic polynomial) $c(x)$는 $GF(2)$위에서 $c(x)=|T \oplus xI|$이다. 여기서, I는 n차 단위행렬이다. 또, 특성다항식의 인수 중 T를 근으로 갖는 차수가 가장 낮은 다항식을 최소다항식(minimal polynomial)이라 한다. 그룹 CA의 상태전이그래프에서 사이클의 구조는 CA의 최소다항식에 의하여 특성화된다. 특히, $GF(2)$ 위에서 기약다항식 $p(x)$의 주기(order)가 k라면, $[p(x)]^j$ 의 주기는 $k \cdot 2^r$이다. 여기서 $2^{r-1} < j \le 2^r$이다[14].

상태전이행렬 T를 갖는 CA로부터 여원벡터 F에 의하여 유도된 CA의 연산자를 $\overline{T}$라 하면 X의 p번째 다음 상태는

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

이다.

보조정리 2.1[15]> C를 전이규칙 60(102)을 갖는 n-셀 선형 uniform 그룹 CA라 하고, T와 S를 C의 상태전이행렬이라 하자($2^{k-1} < n \le 2^k$). 그러면 $T^{2^{k-1}} = (t_{ij})$과 $S^{2^{k-1}} = (s_{ij})$ 은 다음과 같다.

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

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

보조정리 2.2[15]> C를 전이규칙 60 또는 102를 갖는 n-셀 선형 uniform 그룹 CA라 하고, T를 C의 상태전이행렬이라 하면 C의 임의의 상태 $X = (x_1, \cdots, x_n)^t$에 대하여 다음이 성립한다.

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

Ⅲ. 최대 동일 길이를 갖는 여원 HGCA

3절에서는 전이규칙 60, 102 또는 204를 가지는 선형 HGCA로부터 유도된 여원 CA를 분석한다.

정리 3.1> C를 전이규칙 60, 102 또는 204를 갖는 상태전이행렬이 T인 n-셀 선형 HGCA라 하자. C가 선형 HGCA일 필요충분조건은 전이규칙 60이 전이규칙 102의 바로 다음에 위치하지 않는 것이다.

<증명>

$$T(=T_n)=\begin{pmatrix} 1 & u_1 & 0 & 0 & \cdots & 0 \\ l_2 & 1 & u_2 & 0 & \cdots & 0 \\ 0 & l_3 & 1 & u_3 & \cdots & 0 \\ & & \vdots & & & \\ 0 & 0 & \cdots & l_{n-1} & 1 & u_{n-1} \\ 0 & 0 & 0 & \cdots & l_n & 1 \end{pmatrix}$$

라 하면 $i\neq 1$에 대하여 $l_iu_{i-1}\neq 1$이므로 $|T_n|=|T_{n-1}|=|T_{n-2}|=\cdots=|T_1|=1$ 이다. 따라서 C는 그룹 CA이므로 C는 선형 HGCA이다. 역으로, 전이규칙이 i번째가 102이고, $i+1$번째가 60이라면 T의 i번째 행과 $i+1$번째 행은 같으므로 $|T|=0$이고, 따라서 C는 그룹 CA가 아니다. □

정리 3.2> C를 전이규칙 60, 102 또는 204를 갖는 상태전이행렬이 T인 n-셀 선형 HGCA라 하면 T의 특성다항식은 $c(x)=(x+1)^n$ 이다.

<증명> T가 정리 3.1의 증명에 있는 T와 같다고 하자. 그러면 $l_iu_i\neq 1$ 이다. 전이규칙 60이 전이규칙 102의 바로 다음에 위치하지 않으므로, $l_iu_{i-1}=0$ $(i=2,3,\cdots,n)$이다. 그러므로
$c(x)=|T\oplus xI|=(x+1)^n$ 이다.

정리 3.1에 의하여 전이규칙 60, 102 또는 204를 갖는 선형 HGCA는 다음에 제시된 룰 벡터(Rule Vector) $RV_i(i=1,2,3,4,5)$의 조합으로만 이루어진다.

$$RV_1=<60,\cdots,60,102,\cdots,102>$$
$$RV_2=<60,\cdots,60,204,60,\cdots,60>$$
$$RV_3=<60,\cdots,60,204,102,\cdots,102>$$
$$RV_4=<102,\cdots,102,204,60,\cdots,60>$$
$$RV_5=<102,\cdots,102,204,102,\cdots,102>$$

정리 3.3> C를 n-셀 선형 HGCA라 하고, $m(x)$를 C의 상태전이행렬 T의 최소다항식이라 하자. 다음 각각의 $RV_i(i=1,2,3,4,5)$에 대하여 $m(x)=(x+1)^p$이다.

(1) $RV_1=<\overbrace{60,\cdots,60}^{a개},\overbrace{102,\cdots,102}^{b개}>$
$p=\max\{a,b\}$

(2) $RV_2=<\overbrace{60,\cdots,60}^{a개},204,\overbrace{60,\cdots,60}^{b개}>$
$p=\max\{a,b+1\}$

(3) $RV_3=<\overbrace{60,\cdots,60}^{a개},204,\overbrace{102,\cdots,102}^{b개}>$
$p=\max\{a,b\}$

(4) $RV_4=<\overbrace{102,\cdots,102}^{a개},204,\overbrace{60,\cdots,60}^{b개}>$
$p=\max\{a+1,b+1\}$

(5) $RV_5=<\overbrace{102,\cdots,102}^{a개},204,\overbrace{102,\cdots,102}^{b개}>$
$p=\max\{a+1,b\}$

<증명> (1) $RV_1=<\overbrace{60,\cdots,60}^{a개},\overbrace{102,\cdots,102}^{b개}>$의 상태전이행렬은 $T=\begin{pmatrix} T_1 & O \\ O & T_2 \end{pmatrix}$이다. 여기서 T_1은 $a\times a$ 행렬이고, T_2는 $b\times b$ 행렬이며, O는 영행렬이다. 따라서, T의 특성다항식은 정리 3.2에 의하여 $c(x)=(x+1)^n$ 이므로 최소다항식은 $m(x)=(x+1)^p(p\leq n)$이고, 여기서, p는 [14]에 의하여 $p=\max\{a,b\}$이다.

(2)-(5)의 증명은 (4)의 증명과 유사하므로 (4)만 증명하

기로 한다.

① $a+1 \geq b+1$인 경우 : $T \oplus I$는 $T \oplus I = \begin{pmatrix} S_1 & O \\ A & S_2 \end{pmatrix} = (a_{ij})$이다. 여기서, S_1은 $(a+1)\times(a+1)$ 행렬이고 S_2는 $b \times b$ 행렬이며

$a_{ij} = \begin{cases} 1, & (i=j-1, i<a+1) \\ & \text{또는 } (i=j+1,\ i>a+1), \\ 0, & o/w \end{cases}$ 이므로

$(T \oplus I)^q = \begin{pmatrix} S_1^q & O \\ S_2^{q-1}A & S_2^q \end{pmatrix}$이다. 또한

$S_1^{a+1} = O$, $S_1^j \neq O (j < a+1)$, $S_2^b = O$이고

$S_2^{q-1}A = (b_{ij})$이다. 여기서

$b_{ij} = \begin{cases} 1, & i=q,\ j=a+1, \\ 0, & o/w \end{cases}$ 이므로 $i \leq q \leq b$에 대하여

$S_2^{b-1}A = O$이다. 따라서 $(T \oplus I)^{a+1} = O$이고

$(T \oplus I)^j \neq O\ (j < a+1)$이다.

② $a+1 < b+1$인 경우 : $T \oplus I$은

$T \oplus I = \begin{pmatrix} H_1 & B \\ O & H_2 \end{pmatrix} = (c_{ij})$이다. 여기서, H_1는 $a \times a$ 행렬이고 H_2는 $(b+1)\times(b+1)$ 행렬이며

$c_{ij} = \begin{cases} 1, & (j=i+1, j<a+2) \\ & \text{또는 } (j=i-1, j>a), \\ 0, & o/w \end{cases}$ 이므로

$(T \oplus I)^q = \begin{pmatrix} H_1^q & H_1^{q-1}B \\ O & H_2^q \end{pmatrix}$이다. 또한 $H_1^a = O$,

$H_2^{b+1} = O$이고 $H_2^j \neq O (j < b+1)$이며

$H_1^{q-1}B = (d_{ij})$이다. 여기서 $1 \leq q \leq a$에 대하여

$d_{ij} = \begin{cases} 1, & i=a+1-q, j=1, \\ 0, & o/w \end{cases}$ 이고 $H_1^a B = O$ 이므로,

$(T \oplus I)^{b+1} = O$이고

$(T \oplus I)^j \neq O\ (j < b+1)$ 이다.

①과 ②에 의하여 $m(x)=(x+1)^p$이고, 여기서 $p = \max\{a+1, b+1\}$이다. □

다음 정리는 정리 3.3의 $RV_i (i=1,2,3,4,5)$를 갖는 선형 HGCA를 이용하여 최대 동일 길이를 갖는 여원 HGCA를 구성할 수 있음을 보인다.

정리 3.4> C를 $RV_i (i=1,2,3,4,5)$를 갖는 n-셀 선형 HGCA라 하고, T를 C의 상태전이행렬로 최소다항식이 $m(x)=(x+1)^p$라 하자. C'를 다음과 같이 각각의 여원벡터 $F_i (i=1,2,3,4,5)$에 대응하여 C에서 유도된 여원 HGCA라 하자.

(1) RV_1 :

$$F_1 = \begin{cases} (1, f_2, \cdots, f_n)^t, & a \geq b \\ (f_1, \cdots, f_{n-1}, 1)^t, & a < b \end{cases}$$

(2) RV_2 :

$$F_2 = \begin{cases} (1, f_2, \cdots, f_n)^t, & a \geq b+1 \\ (f_1, \cdots, f_a, 1, f_{a+2}, \cdots, f_n)^t, & a < b+1 \end{cases}$$

(3) RV_3 :

$$F_3 = \begin{cases} (1, f_2, \cdots, f_n)^t, & a \geq b \\ (f_1, \cdots, f_{n-1}, 1)^t, & a < b \end{cases}$$

(4) RV_4 :

$$F_4 = \begin{cases} (f_1, \cdots, f_a, 1, f_{a+2}, \cdots, f_n)^t, & a+1 \geq b+1 \\ (f_1, \cdots, f_a, 1, f_{a+2}, \cdots, f_n)^t, & a+1 < b+1 \end{cases}$$

(5) RV_5 :

$$F_5 = \begin{cases} (f_1, \cdots, f_a, 1, f_{a+2}, \cdots, f_n)^t, & a \geq b+1 \\ (f_1, \cdots, f_n, 1)^t, & a < b+1 \end{cases}$$

이때 $\mathrm{ord}(T) = 2^d$이라면 다음이 성립한다.

(1) C'에 있는 모든 사이클의 길이는 같다.

(2) $\mathrm{ord}(\overline{T}) = \begin{cases} 2^d, & 2^{d-1} < p < 2d, \\ 2^{d+1}, & p = 2^d. \end{cases}$

<증명> 전이규칙 벡터 RV_2를 갖고 $a \geq b+1$인 경우에 대해서만 증명하기로 한다.

C'의 임의의 상태를 $X = (x_1, \cdots, x_n)^t$라 하면

$$\begin{aligned} \overline{T}^{2^{d+1}} X &= T^{2^{d+1}} X \oplus (T^{2^{d+1}-1} \oplus \cdots \oplus T \oplus I) F \\ &= X \oplus \{ T^{2^d} (T^{2^d-1} \oplus \cdots \oplus T \oplus I) \\ &\qquad \oplus (T^{2^d-1} \oplus \cdots \oplus T \oplus I) \} F \\ &= X \end{aligned}$$

이므로 $\mathrm{ord}(\overline{T})(:=p)$는 2^{d+1}의 약수이다. 임의의 X에 대하여 $X = \overline{T}^p X = T^p X \oplus (T^{p-1} \oplus \cdots \oplus T \oplus I) F$이므로 $T^p X = X$이고 $(T^{p-1} \oplus \cdots \oplus T \oplus I) F = O$이다. 따라서 $\mathrm{ord}(T)$는 p의 약수이므로 $p = 2^d$이거나 $p = 2^{d+1}$이다.

① $p=2^d$ 인 경우:

$(T\oplus I)^{2^d-1}=(a_{ij})$이고 여기서

$a_{ij}=\begin{cases}1, (i=a,\ j=1),\\ 0, \quad o/w\end{cases}$이므로 임의의 X에 대하여

$$\overline{T}^{2^d}X=T^{2^d}X\oplus(T\oplus I)^{2^d-1}F$$
$$=X\oplus(0,\cdots,0,\overset{a^{th}}{1}0,\cdots,0)^t\neq X$$

이다. 따라서 $ord(\overline{T})=2^{d+1}$이고, C'에서 모든 사이클의 길이는 같다.

② $2^{d-1}<p<2^d$인 경우:

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

$(T\oplus I)^{2^d-1}F=X$이다. 따라서 $ord(\overline{T})=2^d$이다. C'의 모든 사이클들의 길이가 같음을 보이기 위하여 $X=(x_1,\cdots,x_n)^t$를 C'에서 길이가 $2^c(c<d)$인 사이클에 놓인 상태라 하면

$\overline{T}^{2^c}X=\overline{T}^{2^{c+1}}X=\cdots=\overline{T}^{2^{d-1}}X=\overline{T}^{2^d}X=X$

이고 다음이 성립한다.

$$(T\oplus I)^{2^{d-1}-1}F=(0,\cdots,0,\overset{(2^{d-1})^{th}}{1},\cdots)^t$$

먼저 X 가 C에서 길이가 2^d 보다 작은 사이클에 놓인다면

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

이므로 모순이다.

다음으로 X 가 C에서 길이가 2^d 인 사이클에 놓인다면 T는 $T=\begin{pmatrix}T_1 & O\\ O & T_2\end{pmatrix}$이다. 여기서 T_1, T_2는 각각 전이규칙 60과 102를 갖는 uniform 그룹 CA의 상태전이행렬이다. 보조정리 2.1과 2.2에 의하여

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

$$=(\cdots,\overset{(2^{d-1})^{th}}{\underset{2^{d-1}}{x}},\cdots)^t\oplus(\cdots,\overset{(2^{d-1})^{th}}{1},\cdots)^t$$
$$\neq X$$
$$=\begin{pmatrix}T_1^{2^{d-1}} & O\\ O & T_2^{2^{d-1}}\end{pmatrix}X$$
$$\oplus\begin{pmatrix}(T_1\oplus I)^{2^{d-1}-1} & O\\ O & (T_2\oplus I)^{2^{d-1}-1}\end{pmatrix}F$$

이므로 모순이다. 따라서 C'의 모든 사이클들의 길이는 같다. □

C가 $RV_i(i=1,2,3,4,5)$를 갖는 n-셀 선형 HGCA이고, T가 C의 상태전이행렬이며, C'를 각각의 여원벡터 $F_i(i=1,2,3,4,5)$에 대응하여 상태전이연산자가 $\overline{T}$인 C에서 유도된 여원 CA라 하자. 최소다항식이 $m(x)=(x+1)^p$ $(p=2^d)$이고 $ord(T)=2^d$라 하면, $ord(\overline{T})=2^d(\neq 2^{d+1})$인 여원벡터 F가 존재한다. 예를 들어 C가 $RV_2(a\geq b+1)$를 갖는 n-셀 선형 HGCA이고, 여원벡터가 $F=(0,f_2,\cdots,f_n)^t$, $p=2^d$라 하자. 그러면 C'의 모든 사이클의 길이는 $\overline{T}^{2^d}X=X\oplus O=X$ 이므로 2^d로 같다.

Ⅳ. 여원 HGCA의 사이클들간의 관계

Mukhopadhyay 등은 전이규칙 102를 사용하는 uniform CA로부터 셀 상태가 모두 1인 여원벡터에 의하여 유도된 여원 uniform 그룹 CA를 이용하여 키 공유 프로토콜에 사용가능한 두 함수 R_1과 R_2를 구성하였고, 이들의 관계를 분석하였다[1]. 4절에서는 전이규칙 102, 60, 204등의 다양한 전이규칙을 갖는 선형 HGCA로부터 유도된 다양한 여원 HGCA중 RV_4를 이용하여 키 공유 프로토콜에 사용가능한 다양한 함수를 제안하고, 이들의 관계를 분석한다.

수학적 귀납법에 의하여 다음 보조정리를 증명할 수 있다.

보조정리 4.1> C를 $RV_4(a+1\geq b+1)$를 갖는 n-셀 선형 HGCA라 하고, T를 C의 상태전이행렬이라 하자. C'를 $a+1$번째 성분만 1인 여원벡터 $F=(0,\cdots,0,1,0,\cdots 0)^t$에 의하여 C에서 유도된 여원 CA라 하자. 양의 정수 a에 대하여 C의 각 상태 X는 다음과 같다.

$$\overline{T}^k X=\begin{pmatrix} \vdots \\ {}_kC_0x_a\oplus_kC_1x_{a+1}\oplus_kC_2 \\ {}_kC_0x_{a+1}\oplus_kC_1 \\ {}_kC_1x_{a+1}\oplus_kC_0x_{a+2}\oplus_kC_2 \\ {}_kC_2x_{a+1}\oplus_kC_1x_{a+2}\oplus_kC_0x_{a+3}\oplus_kC_3 \\ \vdots \end{pmatrix}^{(a+1)^{th}}$$

정리 4.2> C를 $RV_4(a+1\geq b+1)$를 갖는 n-셀 선형 HGCA라 하고, T를 C의 상태전이행렬이라 하자. C'를 $a+1$ 번째 성분만 1인 여원벡터 $F=(0,\cdots,0,1,0,\cdots 0)^t$에 의하여 C에서 유도된 여원 CA라 하자. C'의 각 상태 X와 다음 상태들은 각각 다른 사이클에 놓인다.

(1) $X\oplus \overline{T}X\oplus \overline{T}^2X$

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

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

(4) $X\oplus \overline{T}^4X\oplus \overline{T}^5X$

(5) $X\oplus \overline{T}X\oplus \overline{T}^5X$

<증명> (2)-(5)의 증명은 (1)과 유사하므로 (1)만 증명하기로 한다.

T는 $T=\begin{pmatrix} T_1 & O \\ P & T_2 \end{pmatrix}$이다. 여기서 T_1는 $(a+1)\times(a+1)$ 행렬이고 T_2는 $b\times b$행렬이다. 또한 T_1은 전이규칙 102를 갖는 $(a+1)$-셀 uniform CA의 상태전이행렬이고, T_2는 전이규칙 60을 갖는 b-셀 uniform CA의 상태전이행렬이며 P는 1행의 마지막 열의 성분만 1인 행렬이다. $X=(x_1,x_2,\cdots,x_n)^t$이고, $A=X\oplus \overline{T}X\oplus \overline{T}^2X$라 두면

$$A=(I\oplus T\oplus T^2)X\oplus TF$$
$$=\begin{pmatrix} \vdots \\ \overline{x_a\oplus x_{a+1}} \\ \overline{x_{a+1}} \\ \overline{x_{a+1}\oplus x_{a+2}} \\ \vdots \end{pmatrix}^{(a+1)^{th}}$$

이다. $\overline{T}^kX=A$인 정수 k가 존재한다고 가정하자.

보조정리 4.1에 의하여 k가 짝수인 경우,

$$A=(\cdots,\overline{x_{a+1}}^{(a+1)^{th}},\cdots)^t,\ \overline{T}^kX=(\cdots,x_{a+1}^{(a+1)^{th}},\cdots)$$

이므로 $\overline{T}^aX\neq A$이다.

k가 홀수인 경우, $k=4n+1$이라면

$$A=(\cdots,\overline{x_{a+1}\oplus x_{a+2}}^{(a+2)^{th}},\cdots)^t,$$

$$\overline{T}^kX=(\cdots,x_{a+1}\oplus x_{a+2}^{(a+2)^{th}},\cdots)$$

이므로 $\overline{T}^aX\neq A$이다. 또한 $k=4n+3$이라면,

$$A=(\cdots,x_{a+1}\oplus\overline{x_{a+2}\oplus x_{a+3}}^{(a+3)^{th}},\cdots)^t,$$

$$\overline{T}^kX=(\cdots,\overline{x_{a+1}\oplus x_{a+2}\oplus x_{a+3}}^{(a+3)^{th}},\cdots)$$

이므로 $\overline{T}^aX\neq A$이다. 따라서 X와 $X\oplus \overline{T}X\oplus \overline{T}^2X$는 다른 사이클에 놓인다. □

연산자 R_i를 다음과 같이 정의하자.

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

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

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

$$\begin{aligned}&\overline{T}(X_1\oplus X_2\oplus\cdots\oplus X_{2n-1})\\&=T(X_1\oplus X_2\oplus\cdots\oplus X_{2n-1})\oplus F\\&=(TX_1\oplus F)\oplus(TX_2\oplus F)\oplus\cdots\oplus(TX_{2n-1}\oplus F)\\&=\overline{T}X_1\oplus\overline{T}X_2\oplus\cdots\oplus\overline{T}X_{2n-1}\end{aligned}$$

이므로 $\overline{T}$는 홀수 개의 상태들의 합에 대하여 선형 연산자와 같은 성질을 가진다. 이러한 $\overline{T}$의 성질을 이용하여 다음 보조정리를 증명할 수 있다.

보조정리 4.3> C를 $RV_4(a+1\geq b+1)$를 갖는 n-셀 선형 HGCA라 하고, T를 C의 상태전이행렬이라 하자. C'를 $a+1$ 번째 성분만 1인 여원벡터 $F=(0,\cdots,0,1,0,\cdots 0)^t$에 의하여 C에서 유도된 여원 CA라 하면 각 $i,j=1,2,3$에 대하여 다음이 각각 성립한다.

(1) $\overline{T}^a(R_iR_j(\overline{T}^b(X)))=\overline{T}^b(R_jR_i(\overline{T}^a(X)))$

(2) $R_i(X_1\oplus\cdots\oplus X_{2n-1})$
$=R_i(X_1)\oplus\cdots\oplus R_i(X_{2n-1})$

보조정리 4.4> C를 $RV_4(a+1 \geq b+1)$를 갖는 n-셀 선형 HGCA라 하고, T를 C의 상태전이행렬이라 하자. C'를 $a+1$ 번째 성분만 1인 여원벡터 $F=(0,\cdots,0,1,0,\cdots 0)^t$에 의하여 C에서 유도된 여원 CA라 하면 양의 정수 a와 각 $i(=1,2,3)$에 대해 다음이 성립한다.

$$\begin{aligned}&\overline{T}^{i\cdot 2^a}R_i^{2^a}(X)\\&=\{(T\oplus I)^{3\cdot 2^a}(T^i\oplus T\oplus I)^{2^a}\oplus I\}X\\&\qquad\oplus(T\oplus I)^{3\cdot 2^a-1}(T^i\oplus T\oplus I)^{2^a}F\end{aligned}$$

<증명> $i=2,3$의 증명은 $i=1$인 경우의 증명과 유사하므로 a에 대한 수학적 귀납법으로 $i=1$인 경우만 증명하기로 한다. $a=0$일 때

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

이므로 성립한다. $a=k$일 때 성립한다고 가정하자. 보조정리 4.3에 의하여

$$\begin{aligned}&\overline{T}^{2^{k+1}}R_1^{2^{k+1}}(X)\\&=\overline{T}^{2^k}R_1^{2^k}(\overline{T}^{2^k}R_1^{2^k}(X))\\&=\overline{T}^{2^k}R_1^{2^k}[\{(T\oplus I)^{3\cdot 2^k}\oplus I\}X\oplus(T\oplus I)^{3\cdot 2^k-1}F]\\&=\{(T\oplus I)^{3\cdot 2^k}\oplus I\}[\{(T\oplus I)^{3\cdot 2^k}\oplus I\}X\\&\qquad\oplus(T\oplus I)^{3\cdot 2^k-1}F]\\&=\{(T\oplus I)^{3\cdot 2^{k+1}}\oplus I\}X\oplus(T\oplus I)^{3\cdot 2^{k+1}-1}F\end{aligned}$$

이므로 $a=k+1$ 일 때 성립한다. □

다음 정리는 보조정리 4.3과 4.4에 의해 증명할 수 있다.

정리 4.5> C를 $RV_4(a+1 \geq b+1)$를 갖는 n-셀 선형 HGCA라 하고, T를 C의 상태전이행렬이라 하자. C'를 $a+1$ 번째 성분만 1인 여원벡터 $F=(0,\cdots,0,1,0,\cdots 0)^t$에 의하여 C에서 유도된 여원 CA라 하면 각 $i,j=1,2,3$에 대하여 다음이 각각 성립한다.

(1) $\overline{T}^{i\cdot 2^a}R_i^{2^a}(X)=X$

(2) $\overline{T}^{(i+j)\cdot 2^a}(R_iR_j)^{2^a}(X)=X \quad (i\neq j)$

(3) $\overline{T}^{6\cdot 2^a}(R_1R_2R_3)^{2^a}(X)=X$

여기서, $i,j=1,2,3$ 이고 a는 $3\cdot 2^{a-1}\leq k<3\cdot 2^a$ 을 만족하는 음이 아닌 정수이다.

V. 결 론

본 논문에서는 전이규칙 60(102)를 갖는 uniform 셀룰라 오토마타의 성질을 이용하여 전이규칙 60, 102 또는 204와 같은 다양한 전이규칙을 갖는 선형 하이브리드 셀룰라 오토마타가 그룹 셀룰라 오토마타가 되는 조건을 제안하였고 이 셀룰라 오토마타로부터 유도된 여원 하이브리드 그룹 CA가 상태전이그래프에서 모든 사이클의 주기가 동일하고 가능한 최대 길이를 갖는 CA가 되도록 하는 여원벡터의 조건을 제시하였다. 또한 여원 하이브리드 그룹 셀룰라 오토마타의 사이클들 간의 관계를 분석하였다. 이 결과들은 Mukhopadhyay의 결과의 일반화이다.

참고문헌

[1] D. Mukhopadhyay and D.R. Chowdhury, Characterization of a Class of Complemented Group Cellular Automata, LNCS, Vol. 3305, 2004, pp. 775-784.

[2] 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.

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

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

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

[6] 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, Vol. 45, 1996, pp. 769-781.

[7] S. Nandi and P.P. Chaudhuri, Analysis of periodic and

intermediate boundary 90/150 cellular automata, IEEE Trans. Computers, Vol. 45, 1996, pp. 1-12.

[8] 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, Vol. 3305, 2004, pp. 31-39.

[9] K. Cattell and J. Muzio, Analysis of one-dimensional linear hybrid cellular automata over $GF(q)$, IEEE Transactions of Computers, Vol. 45, 1996, pp. 782-792.

[10] K. Cattell and J. Muzio, Synthesis of one-dimensional linear hybrid cellular automata, IEEE Transactions on Computer-Aided Design of Integrated Circuit and Systems, Vol. 15, 1996, pp. 325-335.

[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, Vol. 45, 2003, pp. 689-698.

[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, Vol. 36, 2002, pp. 979-986.

[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. Info. Security and Cryptology, Vol. 15, 2005, pp. 105-111.

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

[15] S.J. Cho, U.S. Choi, H.D. Kim and Y.H. Hwang, Characterization of a class of the Complemented CA Derived from Linear Uniform Group CA, Submitted.

저자소개

조 성 진(Sung-Jin Cho)

1979년 강원대학교 수학교육과 학사
1981년 고려대학교 수학과 석사
1988년 고려대학교 수학과 박사
1988년~현재 부경대학교 수리과학부 정교수
※관심분야 : 셀룰라 오토마타론, 정보보호, 부호이론, 컴퓨터 구조론

최 언 숙(Un-Sook Choi)

1992년 성균관대학교 산업공학과 학사
2000년 부경대학교 응용수학과 석사
2004년 부경대학교 응용수학과 박사
2004년~2006년 영산대학교 자유전공학부 단임교수
2006년~현재 동명대학교 멀티미디어공학과 전임강사
※관심분야 : 셀룰라 오토마타론, 정보보호, 부호이론, 컴퓨터 구조론

황 윤 희(Yoon-Hee Hwang)

2002년 부경대학교 통계학과 학사
2004년 부경대학교 응용수학과 석사
2004년 ~현재 부경대학교 정보보호학과 박사과정
※관심분야 : 셀룰라 오토마타론, 정보보호, 유한체, 컴퓨터 구조론

김 진 경(Jin-Gyoung Kim)

2006년 ~ 현재 부경대학교 응용수학과 석사과정
※관심분야 : 셀룰라 오토마타론, 유한체, 행렬이론

표 용 수(Yong-Soo Pyo)

1980년 계명대학교 수학과 학사
1982년 계명대학교 수학과 석사
1987년 계명대학교 수학과 박사
1983~현재 부경대학교 수리과학부 정교수
※ 관심분야 : 셀룰라 오토마타론, 전산수학

김 한 두(Han-Doo Kim)

1982년 고려대학교 수학과 학사
1984년 고려대학교 수학과 석사
1988년 고려대학교 수학과 박사
1989년 ~ 현재 : 인제대학교 컴퓨터응용과학부 정교수
※관심분야 : 전산수학, 셀룰라 오토마타론, 컴퓨터 구조론