선형 TPNCA의 0-트리의 0이 아닌 상태를 여원벡터로 갖는 여원 TPNCA의 행동분석

Analysis of the behavior of complemented TPNCA with complement vector as nonzero state in the 0-tree of the linear TPNCA

조성진*, 김한두**, 최언숙*, 허성훈***, 고귀자*, 황윤희*
*부경대학교 수리과학부, **인제대학교 컴퓨터응용과학부,
***부경대학교 정보보호협동과정

Sung-Jin Cho*, Han-Doo Kim**, Un-Sook Choi*, Seong-Hun Heo***,
Gwi-Ja Ko* and Yoon-Hee Hwang*
*Division of Mathematical Science, Pukyong National University,
**School of Computer Aided Science, Inje University,
***Interdisciplinary Program of Information Security, Pukyong Nat'l University
E-mail : sjcho@pknu.ac.kr

ABSTRACT

LFSR보다 CA가 랜덤성이 우수한 패턴들을 효율적으로 생성함이 알려지면서 그 응용분야가 점차적으로 확대되어가고 있다. Nongroup CA는 해쉬함수의 생성, 암호알고리즘, 이미지 압축 등에 응용되고 있다. 그러나 CA가 생성하는 패턴의 분석이 용이하지 못하였다. 본 논문에서는 선형 nongroup CA의 일반적인 성질과 여원 벡터가 선형 nongroup CA의 0-트리의 0이 아닌 상태인 경우 이로부터 유도되는 여원 TPNCA의 상태들의 행동을 분석하였다.

Keywords : 셀룰라 오토마타, 선형 Nongroup CA, 여원벡터, 여원CA, 트리, TPNCA, 상태전이 그래프

Ⅰ. 서 론

셀룰라 오토마타(이하 CA)란 동역학계(dynamical system)를 해석하는 한 방법으로 공간과 시간을 이산적으로 다루고, 이산적인 공간을 셀룰라 공간(cellular space)의 기본단위인 각 셀이 취할 수 있는 상태를 유한하게 처리하며, 각 셀들의 상태가 국소적인 상호작용에 의해서 동시에 갱신되는 시스템이다. Group CA의 상태전이 행동의 분석은 그동안 많은 연구가 이루어졌다([1], [10], [12], [14]). Group CA의 전이행렬은 역행렬이 존재하지만 nongroup CA의 전이행렬은 역행렬이 존재하지 않는다.

Group CA에 비하여 nongroup CA에 대한 연구는 그리 활발하지는 못하였으나 최근 해시함수 생성이나 암호, 부울 방정식의 해법, 논리회로 검사 등에 응용이 되면서 관심을 받기 시작하였다([2], [6], [8], [9], [11], [13]).

본 논문에서는 선형 TPNCA의 상태전이 그래프를 0-트리의 한 기본 경로와 사이클 구조를 이용하여 상태전이 그래프를 구성하고 각 셀들에 XOR 논리 대신 XNOR 논리를 적용함으로써 여원벡터(complement vector)를 갖는 여원 CA의 특징을 살펴보고, 특히 여원벡터 F가 0-트리에서 0이 아닌 상태일 경우의 여원 TPNCA의 행동에 대하여 분석한다. 2절에서는 선형 TPNCA([3], [4], [5])의 정의와 간단한 성질들을 밝히고 3절에서는 선형 TPNCA로부터 유도된 여원 CA의 행동을 분석하고 4절에서 결론을 맺는다.

*본 논문은 2001 정보통신부 대학기초연구지원사업으로 수행되었음.

II. 선형 Nongroup CA

이 절에서는 선형 nongroup CA의 정의와 본 논문의 전개에 필요한 용어의 정의를 기술하고 선형 nongroup CA의 일반적인 성질을 밝힌다.

• ***선형 nongroup CA*** : Nongroup CA에서 다음 상태를 결정짓는 상태전이 함수가 XOR 논리로만 이루어져 있어서 이 함수를 행렬로 표현할 수 있다. 이러한 CA를 선형 nongroup CA라 한다.

• ***Attractor*** : Nongroup CA의 상태전이 그래프에서 순환상태들 중 사이클의 길이가 1인 상태를 말한다.

• ***직전자*** : 임의의 도달가능한 상태 x에 대하여 x에 대한 이전상태를 말하며 선형 CA에서 전이행렬을 T라 할 때 $Ty=x$를 만족하는 상태 y를 나타낸다.

• ***TPNCA(Two-Predecessor Nongroup CA)*** : 임의의 도달가능한 상태에 대한 직전자의 수가 2개인 nongroup CA를 TPNCA라 한다.

• ***a-트리*** : 순환상태 a를 root로 하는 트리이다.

• ***Depth*** : Nongroup CA의 상태전이 그래프에서 임의의 도달불가능한 상태에서 가장 가까운 순환상태로 가는데 걸리는 최소의 단계 수를 말한다.

• ***Level*** : 어떤 상태 x가 a-트리의 level l($l \le$ depth)에 있다는 것은 상태 x가 정확히 l단계 후 상태 a가 되는 위치에 있다는 것이다. 즉, $T^p x = a$가 되는 p값 중 최소값이 l이다.

• ***r-직전자*** : 임의의 도달가능한 상태 x에 대하여 $T^r y = x$을 만족하는 상태 y를 상태 x의 r-직전자라 한다. ($1 \le r \le 2^n - 1$)

선형 nongroup CA의 각 셀의 다음 상태는 자기 자신을 포함하여 자신의 왼쪽과 오른쪽 이웃의 상태를 XOR함으로써 얻어지는데 영향을 주는 이웃의 수는 각 셀에 적용되는 rule에 따라 1개에서 3개까지이다. 아래 <표 2.1>은 선형 CA에서 사용되는 rule이다. rule에 따라 이웃의 의존도를 3차원 벡터를 이용하여 표현한다. 첫 번째 성분은 왼쪽 이웃에 대한 의존도이고, 두 번째 성분은 자신에 대한 의존도이며 마지막 성분은 오른쪽 이웃에 대한 의존도를 나타낸다. 만약 주어진 위치의 이웃의 상태가 셀의 다음 상태에 영향을 준다면 '1'로, 영향을 주지 않는다면 '0'으로 그 의존도를 나타낸다. 예를 들어 XOR하는 이웃의 수가 3개인 경우 즉 자신, 왼쪽, 오른쪽 상태들의 XOR로 결정되는 상태전이 함수는 rule 150이다.

Rule	이웃 의존도	Rule	이웃 의존도
60	<110>	170	<001>
90	<101>	204	<010>
102	<011>	240	<100>
150	<111>		

<표 2.1> 선형 CA의 rule

선형 nongroup CA의 상태전이 함수는 행렬로 표현할 수 있고 이 행렬을 전이행렬이라 한다. CA의 전이행렬 T에 대하여 $(T \oplus xI)$의 행렬식 값을 CA의 특성다항식이라 하고, 특성다항식의 인수 중 T를 근으로 갖는 차수가 가장 낮은 다항식을 최소다항식이라 한다

정리1> 선형 nongroup CA의 최소다항식은 $x^d \Phi(x)$이다. 여기서 d는 이 CA의 depth가 되고, $\Phi(x)$에 의하여 순환상태들의 사이클 구조가 결정된다. □

정리 2> n-셀 TPNCA의 전이행렬의 계수(rank)는 $n-1$이다. □

정리 3[8]> 선형 TPNCA의 상태전이 그래프에서 $O_{i,j}$($X_{i,j}$)를 0-트리(X-트리)의 level i의 ($j+1$)번째 상태라 하고 U_i를 상태 X의 순환하는 i-직전자라 하면 $X_{i,j} = U_i \oplus O_{i,j}$이다.□

상태 X가 attractor이면 순환하는 i-직전자는 항상 X이므로 $X_{i,j} = X \oplus O_{i,j}$이다. 또한 선형 TPNCA의 0-트리의 한 기본경로를 $O_{d,0} \to O_{d-1,0} \to \cdots \to O_{1,0} \to 0$이라 하면 0-트리의 기본경로에 대응되는 순환상태 X를 root로 하는 X-트리의 기본경로의 level i 상태 $X_{i,0}$는 다음과 같다.

$$X_{i,0} = U_i \oplus O_{i,0} \qquad (2.1)$$

X-트리의 기본경로를 식 (2.1)에 의하여 구하면 X-트리의 나머지 부분은 0-트리의 기본경로와 X-트리의 기본경로를 이용하여 다음 정리를 통해 구할 수 있다.

정리 4> 선형 TPNCA의 상태전이 그래프에서 $O_{i,0}$를 0-트리의 기본 경로라 하고 $X_{i,0}$을 X-트리의 기본 경로라 하면 X-트리의 level i의 $(j+1)$ 상태를 $X_{i,j}$라 하면 다음을 만족한다.

$$X_{i,j} = O_{i,0} \oplus U_i \oplus \sum_{k=1}^{i-1} b_k O_{k,0} \qquad (2.2)$$

여기서 $b_{i-1}b_{i-2}\cdots b_1$는 k의 이진법 표현의 수이며 최대값은 $2^{i-1}-1$이고 U_i는 상태 X의 순환하는 i-직전자이다. □

정리 5> 선형 TPNCA에서 $R_1 \to R_2 \to \cdots \to R_n \to R_1$이 길이가 n인 사이클이고 β가 attractor이면 $R_1 \oplus \beta \to R_2 \oplus \beta \to \cdots \to R_n \oplus \beta \to R_1 \oplus \beta$도 길이가 n인 사이클이다. □

<예1> Rule이 <150, 60, 90, 60, 60>인 5-셀 선형 CA의 전이행렬 T는 아래와 같다.

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

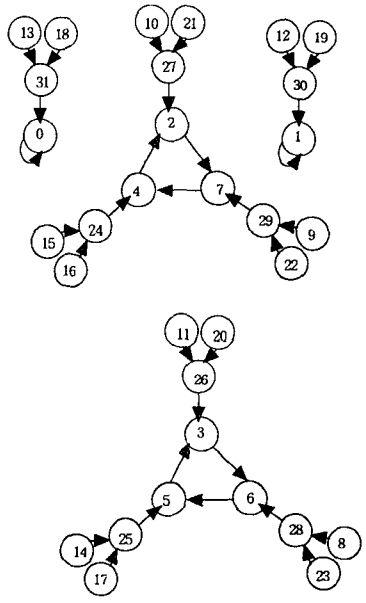
또한 특성다항식 $c(x)$과 최소다항식 $m(x)$은 $c(x) = m(x) = x^2(x^3+1)$이다. <그림 2.1>은 이 선형 TPNCA의 상태전이 그래프이다. 여기서 13→31→0을 0-트리의 기본경로라 하면 상태 18은 $13 \oplus 31$에 의하여 구한다[2]. 또한 1-트리의 기본경로는 0-트리의 기본경로에 각각 1을 더하여 12→30→1을 구하고 19는 $12 \oplus 31$을 계산하여 얻는다[6]. 순환상태 2를 root로 하는 2-트리의 기본경로를 구하기 위하여 2가 속한 사이클의 구조로부터 2의 순환하는 직전자 4와 순환하는 2-직전자 7을 구한다. 2-트리의 기본경로 10→27→2는 다음과 같이 얻는다. $10=13 \oplus 7$, $27=31 \oplus 4$. 또한 2-트리의 level 2의 2번째 상태는 2-트리 기본경로와 0-트리의 기본경로로부터 $21=10 \oplus 31$임을 정확히 알 수 있다. 다음으로 정리 5에서 언급한 사이클 구조를 살펴보면 2→7→4→2가 사이클을 이루고, 상태 1이 attractor이므로 각 순환상태에 1을 더한 3→6→5→3 도 사이클을 이룬다.

III. 여원 Nongrup CA

CA의 각 셀에 적용되는 rule이 XOR논리로만 이루어진 CA를 선형 n-셀 CA라 하는 반면 XOR논리와 XNOR논리의 조합으로 표현되는 CA를 여원 CA라 한다. 여원 CA에 사용되는 rule은 <표 3.1>과 같다. 예를 들어 rule 195는 셀에 rule 60을 적용하여 그 결과값을 역으로 취하는 것이다.

여원 CA의 다음 상태를 구하는 연산자를 $\overline{T}$라 하면 이를 선형 n-셀 CA와 관련지어 다음 상태를 구하는 식으로 유도할 수 있다. 여원 rule에 대응하는 선형 rule로 표현한 전이행렬을 T라 하고, XNOR논리가 적용된 셀의 결과값을 역으로 취하기 위하여 여원 rule이 적용된 셀의 위치성분은 1로, 나머지는 0인 n차원 벡터 F를 여원벡터라 하고 이를 이용하여 CA의 다음 상태 S_{t+1}를 아래와 같이 구한다.

$$S_{t+1} = \overline{T} S_t = T S_t \oplus F \qquad (3.1)$$



<그림 2.1> 5-셀 선형 TPNCA

Rule	이웃 의존도	Rule	이웃 의존도
195	$<\overline{110}>$	85	$<\overline{001}>$
165	$<\overline{101}>$	51	$<\overline{010}>$
153	$<\overline{011}>$	15	$<\overline{100}>$
105	$<\overline{111}>$		

<표 3.1> 여원 CA의 rule

여원벡터 F는 CA의 크기와 같은 n차원 벡터이다. 그러므로 이 벡터의 종류는 모든 성분이 0인 **0** 벡터를 제외한 2^n-1가지를 만들 수 있고 이것은 CA의 가능한 상태와 일대일 대응시킬 수 있다. 따라서 여원벡터를 CA의 상태로 해석한다면 이 벡터가 동일한 전이행렬 T를 따르는 선형 CA의 상태전이 그래프에 놓이는 위치에 따라 CA의 상태변화가 여러 가지 행동패턴을 보인다. 이 절에서는 선형 TPNCA로부터 유도되는 여원 TPNCA의 행동을 분석한다. 특별히 여원 벡터가 이에 대응하는 선형 TPNCA의 상태전이 그래프에서 0-트리의 비순환상태인 경우에 대하여 분석한다.

정리 6[7]> C는 depth가 d인 선형 TPNCA이고, C에서 0-트리의 level i $(0 < i \le d)$에 있는 한 상태를 여원벡터 F로 택하면 $\overline{T}^{i-1}F$ 는 C에 대응하는 여원 CA C′에서 attractor이다. □

정리7> C는 depth가 d인 선형 TPNCA이고, C에서 0-트리의 level i $(0 < i \le d)$에 있는 한 상태를 여원벡터 F로 택할 때, β가 선형 TPNCA의 attractor라면 $\overline{T}^{i-1}F\oplus\beta$ 는 C에 대응하는 여원 TPNCA C′에서 attractor이다. □

정리 8> C가 선형 TPNCA이고 C에 대응하는 여원 CA를 C′이라 하자. 여원벡터 F를 C의 0-트리의 level i에 있는 비순환상태로 택하자. 그러면 다음이 성립한다.

(a) C에서 i보다 상위 level에 있는 모든 상태는 C′에서 level이 변하지 않는다.

(b) C에서 level i에 있는 모든 상태는 C′에서 i보다 하위 level에 배열된다.

(c) C에서 i보다 하위 level에 있는 모든 상태는 C′에서 level i에 배열된다.

(d) 상태 F는 C′에서 level $i-1$에 배열된다. □

정리 9> 선형 TPNCA C에서 $R_1\to R_2\to\cdots\to R_n\to R_1$가 길이가 n인 사이클을 이루고 여원벡터 F를 C의 0-트리의 level i에 있는 비순환상태라 하면 C′에서 $\overline{T}^{i-1}F\oplus R_1\to\overline{T}^{i-1}F\oplus R_2\to\cdots\to\overline{T}^{i-1}F\oplus R_n\to\overline{T}^{i-1}F\oplus R_1$ 은 길이가 n인 사이클을 이룬다. □

정리 10> 여원 TPNCA에서 $R_1'\to R_2'\to\cdots\to R_n'\to R_1'$가 길이가 n인 사이클을 이루고 β가 attractor이며 여원벡터 F를 C의 0-트리의 level i에 있는 비순환상태라 하면 C′에서 $R_1'\oplus\beta\to R_2'\oplus\beta\to\cdots\to R_n'\oplus\beta\to R_1'\oplus\beta$ 은 길이가 n인 한 사이클이다. □

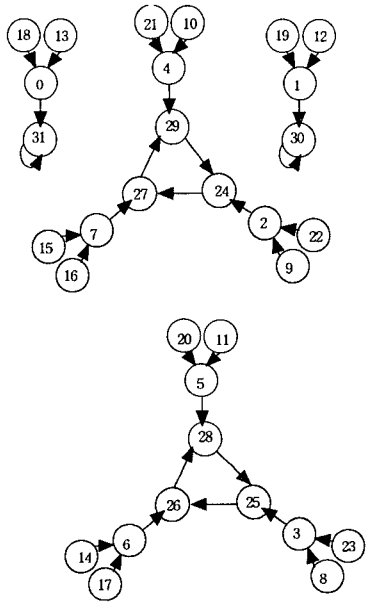
정리 11> 선형 TPNCA를 C라 하고 C로부터 유도된 여원 TPNCA를 C′라 하자. 이때 여원벡터는 C에서 0-트리의 level i의 비순환상태이다. $O_{j,0}$를 C의 0-트리의 기본경로의 level j 상태라 하고 $X'_{j,0}$를 C′에서 X'-트리의 기본경로의 level j 상태라 하면 X'-트리의 level j의 $(k+1)$번째 상태 $X'_{j,k}$는 다음을 만족한다.

$$\begin{aligned} X'_{j,k} &= X'_{j,0}\oplus\sum_{k=1}^{i-1} b_k\, O_{k,0} \\ &= O_{j,0}\oplus U'_j\oplus\sum_{k=1}^{i-1} b_k\, O_{k,0} \end{aligned} \tag{3.2}$$

여기서 $b_{i-1}b_{i-2}\cdots b_1$는 k의 이진법 표현의 수이며 최대값은 $2^{i-1}-1$이고 U_j는 X'의 순환하는 j-직전자이다. □

<예2> <예1>의 5-셀 선형 TPNCA에서 여원벡터 F가 0-트리의 level 1 의 상태 31인 여원 TPNCA의 상태전이 그래프는 <그림 3.1>과 같다. $\overline{T}^{i-1}F=\overline{T}^{0}F=31$이 상태 0가 속한 트리의 attractor가 되고 상태 1이 선형 TPNCA C에서 attractor이므로 $31\oplus1=30$이 C′에서 attractor가 된다. C의 사이클이 $2\to7\to4\to2$이므로 2, 7, 4, 2에 $\overline{T}^{i-1}F=\overline{T}^{0}F=31$를 더한 $2\oplus31\to7\oplus31\to4\oplus31\to2\oplus31$ 즉, $29\to24\to27\to29$가 C′에서 사이클을 이루고 또 $29\to24\to27\to29$의 각 상태에 C의 attractor인 상태 1을 더해서 얻은 사이클 $29\oplus1\to24\oplus1\to27\oplus1\to29\oplus1$ 즉, $28\to26\to25\to28$도 C′에서 또 하나의 사이클을 이룬다. 순환상태 29를 root로 하는 29-트리를 구성하기 위하여 먼저 29-트리의 기본경로를

C의 0-트리의 기본경로와 상태 29의 i-직전자를 이용하여 얻는다. 29-트리의 기본경로의 level 2의 상태는 13⊕24=21이고, 29-트리의 기본경로의 level 1의 상태는 31⊕27 =4 이다. 그러므로 29-트리의 기본경로는 21→4→29 이다. 29-트리의 나머지 상태인 level 2의 두 번째 상태는 식 (3.2)를 이용하여 21⊕31=10로 얻는다.



<그림 3.1> 5-셀 여원 TPNCA

Ⅳ. 결론

본 논문에서는 선형 TPNCA C의 0-트리의 비순환상태를 여원벡터로 갖는 여원 TPNCA C′은 C와 그 구조가 동형임을 밝혔다. 또한 C에서 사이클 구조와 0-트리의 기본경로를 이용하여 나머지 상태들의 위치를 정확히 파악하고, $\overline{T}^{i-1}F$값과 C의 0-트리의 기본경로와 순환상태들을 이용하여 C로부터 유도되는 C′의 상태전이 그래프를 정확히 구성할 수 있음을 보였다. 이는 CA의 다음 상태를 구하는데 있어 셀의 크기가 커질수록 기하급수적으로 늘어나는 행렬의 곱셈 연산을 덧셈 연산으로 대체함으로써 CA의 시간 복잡도를 줄였다. 본 연구결과는 CA를 이용한 암호알고리즘 생성에 관한 연구에 도움이 되리라 사료된다.

Ⅴ. 참고문헌

[1] P.H. Bardell, "Analysis of cellular automata used as pseudorandom pattern generators", Proc. IEEE int. Test. Conf., 1990, pp. 762~767.

[2] S. Bhattacharjee, U.Raghavendra, D.R. cowdhury, P.P. Chaudhuri, "An efficient encoding algorithm for image compression hardware based on Cellular Automata", High Performance computing 1996, Proc. IEEE 3rd International conf., 1996, pp. 239~244.

[3] S. Bhattacharjee, S. Sinha, C. Chattopadhyay, P.P. Chaudhuri "Cellular automata based scheme for solution of Boolean equations", IEEE Proc.-Comput. Digit. Tech., Vol. 143, No. 3, 1996, pp. 174~180.

[4] S. Chattopadhyay, Some studies on Theory and Applications of Additive Cellular Automata, Ph.D. Thesis, I.I.T., Kharagpur, India, 1996.

[5] S. Chakraborty, D.R. Chowdhury, Chaudhuri, "Theory and Application of nongroup cellular automata for synthesis of easily testable finite state machines", IEEE. Trans. Computers, Vol. 45, No. 7, 1996, p.p. 769~781.

[6] S.J. Cho, H.D. Kim and U.S. Choi, "Analysis of complemented CA derived from a Linear TPMACA", To appear in Comput. & Math. Appl..

[7] S.J. Cho, H.D. Kim and U.S. Choi, "Cellular Automata with a Complemented Vector as a Non-zero State in the 0-tree of a Linear TPMACA", J. Korea Multimedia Soc., Vol. 4, No. 4, 2001, pp. 356~361.

[8] S.J. Cho, U.S. Choi and H.D. Kim, "Linear nongroup one-dimensional cellular

automata characterization on GF(2)", J. Korea Multimedia Soc., Vol. 4, No. 1, 2001, pp. 91~95.

[9] P.P. Chaudhuri, D.R. Chowdhury, S. Nandy and Chattopadhyay, Additive Cellular Automata Theory and Application, 1, IEEE Computer Society Press, California, 1997.

[10] A.K. Das and P.P. Chaudhuri, "Efficient characterization of cellular automata", Proc. IEE(Part E), Vol. 137, No. 1, 1990, pp. 81~87.

[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., Vol. 42, 1993, pp. 340~352.

[12] S. Nandi and P.P. Chaudhuri, "Analysis of Periodic and Intermediate Boundary 90/150 Cellular automata", IEEE Trans. Computers, Vol. 45, No 1, 1996, pp. 1~12.

[13] S. Nandi, B.K. Kar and P.P. Chaudhuri, "Theory and Application of Cellular Automata in Cryptography", IEEE Trans. Computers, Vol. 43, 1994, pp. 1346~1357.

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