2001년 한국정보처리학회 춘계 학술발표논문집 제8권 제1호

선형 MACA와 그에 대응하는 여원을 갖는 CA의 트리 구성에 관한 연구

°김광석*, 최언숙**, 이경현***
부경대학교 전산정보학과*
부경대학교 수리과학부**
부경대학교 전자컴퓨터정보통신공학부***
e-mail:jacob@ns.kosinmed.or.kr

A Tree Construction Algorithm of Linear Multiple-Attractor CA and its Complemented CA

°Kwang-Seok Kim*, Un-Sook Choi**, Kyung-Hyune Rhee***
*Dept. of Computer & Information Science, Pukyong National Univ.
**Division of Mathematical Sciences, Pukyong National University
***Division of Electronic, Computer and Telecommunications Engineering, Pukyong National University

요약

본 논문에서는 선형 MACA의 0-트리의 한 경로를 기본 경로로 하여 나머지 다른 트리를 구성하고 여원벡터를 선형 MACA의 하나의 상태로 해석하였을 때 상태전이그래프에서 놓이는 위치에 따라 선형 MACA로부터 유도된 여원을 갖는 CA의 모든 트리를 구성하는 알고리즘을 제안한다. 주어진 전이행렬과 여원벡터를 가지는 additive CA의 트리를 구성함에 있어 보다 빠르게 구성할 수 있는 알고리즘을 제시한다.

1. 서론

셀룰라 오토마타(Cellular Automata, 이하 CA)란 동역학계를 해석하는 한 방법으로 공간과 시간을 이산적으로 다루고 셀룰라 공간(Cellular Space)의 기본 단위인 각 셀(Cell)이 취할 수 있는 상태를 이산적이며 유한하게 처리하며, 각 셀의 상태는 셀들 간의 국소적인 상호작용에 의해서 동시에 갱신되는 시스템이다. CA는 난수성과 좋은 수열들을 발생시키는 성질을 가지고 있어서 혼돈과 확산이 뛰어나 최근 LFSR의 대안으로 제안되었다. CA는 이미지 처리, 패턴 생성, 에러 정정 부호, 등 많은 분야에서 응용되고 있다. Group CA의 상태전이 행동의 분석은 그동안 많은 연구([1], [5], [7], [9], [11])가 이루어졌으나, nongroup CA에 대한 연구는 활발하지 못하였다. 그러나 최근 해쉬함수 생성이나 암호 알고리즘, 부울 방정식의 해법, 논리회로의 테스트 등에 응용되면서 관심을 받기 시작하였다([6], [8], [10]).

본 논문에서는 2개의 직전자를 가지는 선형 multiple-attractor linear CA(이하 MACA)의 트리 구성과 이 MACA로부터 유도된 여원벡터(Complement Vector)를 갖는 CA의 트리를 구성하는 알고리즘을 제안한다. 2절에서는 additive nongroup CA([3], [4], [5])의 정의 분류 및 간단한 성질들을 밝히고 3절에서는 제안한 알고리즘에 의해 2개의 직전자를 가지는 선형 MACA의 트리 구성과 그로부터 유도된 여원을 갖는 CA의 트리를 구성하고 4절에서 결론 및 향후 연구과제를 제시한다.

2. Additive Nongroup CA

Nongroup CA는 group CA가 아닌 CA로 상태전이 그래프가 트리 구조를 가진다. 즉, 임의의 상태에 대한 직전자가 없거나 2개 이상이 되며, 현재 상태에서 이전 상태를 정확히 찾을 수 없다. Additive CA는 선형 CA와 여원을 갖는 CA로 나뉘는데, 선형 CA는 다음 상태를 결정짓는 상태전이 함수가 XOR논리로만

이루어진 CA로 이 함수는 행렬로 표현할 수 있다. 이 전이행렬을 T 라 하고 시간 t에서 CA의 상태를 s^t라 하면 이 CA의 $t+1$에서의 상태는 $s^{t+1}=Ts^t$ 이다. 여원을 갖는 CA는 다음 상태를 결정짓는 상태전이 함수가 XOR논리와 XNOR논리로 이루어진 CA로 선형 CA의 셀의 상태를 역으로 바꾸는 여원벡터를 F 라 할때 이 CA의 $t+1$에서의 상태는 $s^{t+1}=Ts^t \oplus F$ 이다. 본 논문에서는 additive CA중 2개의 직전자를 가지는 nongroup CA에 관하여 연구한다.

다음은 본 논문의 전개에 필요한 몇가지 기본적인 용어 및 정리를 서술한다.

- α-**트리** : 순환상태(cyclic state) α를 root로 하는 트리
- **Attractor** : Nongroup CA의 상태전이 그래프에서 순환상태들 중 사이클(cycle)의 길이가 1인 상태
- **Multiple-Attractor CA(MACA)** : 상태전이 그래프가 각 attractor를 root로 하는 서로 분리된 트리들로 구성되는 CA
- **Depth** : Nongroup CA의 상태 전이 그래프에서 임의의 한 도달 불가능한 상태에서 가장 가까운 순환상태로 가는데 걸리는 최소 단계수
- **Level** : 어떤 상태 x가 α-트리의 level k(k≤depth)에 있다는 것은 상태 x가 정확히 k단계후 상태 α가 되는 위치에 있다는 것이다. 즉, $T^p x=\alpha$가 되는 p값 중 최소값이 k이다.

<정리1> depth가 d인 선형 MACA의 전이행렬 T에 대한 최소다항식은 $x^d(x+1)$이다.

<정리2[4]> 선형 MACA의 attractor x는 $(T \oplus I)x=0$를 만족한다.

3. Nongroup CA의 상태전이 그래프의 트리구성

CA는 LFSR보다 난수성이 강하므로 암호화에 있어 보다 효율적으로 혼돈과 확산이 이루어진다. 그러나 이를 분석함에 있어서는 상당한 어려움이 따른다. 주어진 CA의 행동을 분석하기 위해서는 CA의 상태전이 그래프를 구성하는 것은 필수적이다. 이 절에서는 선형 MACA의 0-트리의 한 경로를 기본 경로로 하여 나머지 다른 트리를 구성하고 여원벡터를 선형 MACA의 하나의 상태로 해석하였을 때 상태전이그래프에서 놓이는 위치에 따라 선형 MACA로부터 유도된 여원을 갖는 CA의 모든 트리를 구성하는 알고리즘을 제안한다.

3.1 선형 MACA의 트리 구성

두 개의 직전자를 가지고 depth가 d인 선형 MACA C에서 α-트리의 도달 불가능한 상태 x는 d단계 후 그 상태가 α가 된다. 이때의 상태변화단계 즉, $x \to Tx \to \cdots \to T^d x(=\alpha)$를 α-트리의 α-기본경로(α-basic path)라 한다. 선형 MACA C의 상태전이 그래프에서 0-트리의 각 level l 에서 첫 번째 상태들을 $S_{l,0}$라 하면 $S_{d,0} \to S_{d-1,0} \to \cdots \to S_{1,0} \to 0$는 C의 0-트리의 0-기본경로이다. 이 0-기본경로로부터 나머지 0-트리를 구성할 수 있다. $S_{l,k}$를 0-트리의 level l 의 $(k+1)$번째라 하면 $S_{l,k}$는 다음을 만족한다[2].

$$S_{l,k}=S_{l,0}+\sum_{i=1}^{k} b_i S_{i,0} \qquad (1)$$

여기서 b_i는 k를 이진수로 표현했을 때 각 bit의 값이다. 0-기본경로와 식(1)을 이용하여 0-트리의 나머지 부분을 구성할 수 있다. C의 0이 아닌 α-트리를 구성하기 위하여 0-트리의 각 level의 첫 번째 상태인 $S_{l,0}$로부터 α-트리의 각 level의 첫 번째 상태인 $S^{\alpha}_{l,0}$를 구하고 이 $S^{\alpha}_{d,0} \to S^{\alpha}_{d-1,0} \to \cdots \to S^{\alpha}_{1,0} \to \alpha$를 0-기본경로에 대응하는 α-기본경로라 한다. 식(2)는 $S^{\alpha}_{l,0}$를 구하는 식이다[12]. 또한 식 (3)에 의해 α-트리의 level l 의 $(k+1)$번째 상태인 $S^{\alpha}_{l,k}$ 를 구한다[12]. 식(3)에서 b_i는 식 (1)에서와 같다.

$$S^{\alpha}_{l,0} = S_{l,0} \oplus \alpha \qquad (2)$$

$$S^{\alpha}_{l,k} = S^{\alpha}_{l,0} + \sum_{i=1}^{k} b_i S_{i,0} \qquad (3)$$

3.2 선형 MACA로부터 유도되는 여원을 갖는 CA의 트리 구성

n셀 선형 MACA C의 각 셀의 상태를 역으로 바꾸는 여원벡터를 F라 할 때, 이 F는 n차원 벡터이며 선형 CA의 셀 값을 역으로 취하고자 하는 셀의 위치 성분이 1이다. 이 여원벡터를 C의 한 상태로 보았을 때 이 상태가 상태전이 그래프에서 위치한 곳에 따라 (i) F가 0-트리의 비순환 상태일 때 (ii) F가 0이 아닌 α-트리의 비순환 상태일 때 (iii) F가 0이 아닌 attractor일때로 나눌 수 있다. 각각의 경우 여원을 갖는 CA의 트리는 각기 다른 방법에 의해 그 트리를 구성한다. 본 논문에서는 (i)과 (iii)경우에 대하여 기본경로를 구하는 방법과 트리를 구성하는 식을 제시한다.

3.2.1 F가 0-트리의 비순환 상태일 때

선형 MACA로부터 유도되는 여원을 갖는 CA를 C'라 하고, 여원벡터 F가 0-트리의 level i의 비순환상태인 경우 C'는 또 하나의 MACA가 된다. C'의 기본경로는 다음과 같이 구한다. 우선 level i보다 상위 level은 C와 C'가 같으므로 C의 0-트리에서 도달불가능상태 중 F에 도달하는 하나의 경로를 선택하고 level i부터 $0 \rightarrow \overline{T}0 (=F) \rightarrow \cdots \rightarrow \overline{T}^{i-1}F$ 를 계산한다. <그림 1>에서 F를 6이라 하면 C'의 4-트리의 4-기본경로는 12→0→6→5→4 이다.

($\overline{T}^{i-1}F$)-트리의 각 level의 $(k+1)$번째 상태 $\overline{S_{l,k}}$들은 식 (4)을 이용하여 구한다. 식(4)에서 $\overline{S_{l,0}}$는 C'의 상태0이 속한 트리의 기본경로로부터 얻은 각 level l의 첫 번째 상태이다.

$$\overline{S_{l,k}} = \overline{S_{l,0}} + \sum_{i=1}^{(-)} b_i S_{i,0} \qquad (4)$$

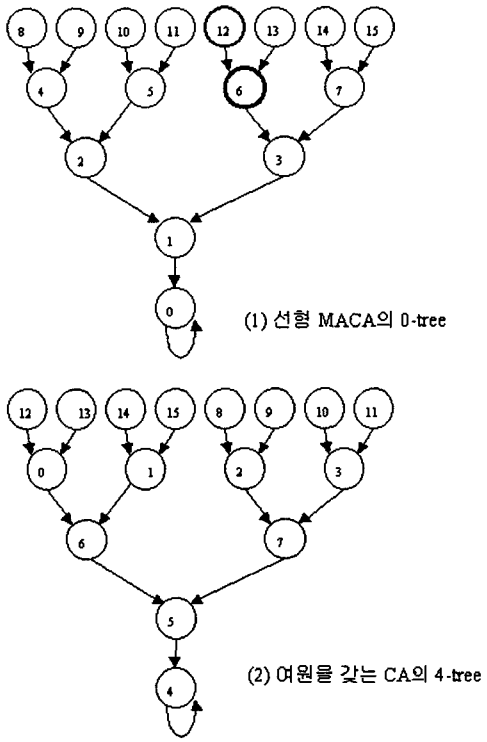
α가 2개의 직전자를 가지는 선형 MACA C의 attractor이고 여원벡터 F가 C의 0-트리의 비순환상태이면 $\overline{T}^{i-1}F \oplus \alpha$는 여원을 갖는 CA의 attractor이다. ($\overline{T}^{i-1}F \oplus \alpha$)-트리를 구성하기 위하여 이 트리의 기본경로인 $\overline{S^{\alpha}_{l,0}}$를 $\overline{S_{l,0}}$로부터 구한다. 식 (5)와 식 (6)은 각각 $\overline{S^{\alpha}_{l,0}}$와 $\overline{S^{\alpha}_{l,k}}$를 구하는 식이다.

$$\overline{S^{\alpha}_{l,0}} = \overline{S_{l,0}} \oplus \alpha \qquad (5)$$

$$\overline{S^{\alpha}_{l,k}} = \overline{S^{\alpha}_{l,0}} + \sum_{i=1}^{(-)} b_i S_{i,0} \qquad (6)$$

3.2.2 F가 0이 아닌 attractor일 때

선형 MACA의 상태가 0이 아닌 attractor를 여원벡터 F로 하여 유도되는 CA는 F가 0-트리의 비순환상태인 경우와 달리 각 트리의 순환상태는 변하지 않으나 트리가 두 개씩 결합이 된다. 0이 아닌 attractor β가 F라 하자. 이때 여원을 갖는 CA C'는 0-트리와 β-트리가 결합하고 나머지 트리들도 두 attractor의 합(bitwise 덧셈)이 β가 되는 트리끼리 결합이 된다. C'의 각 트리를 구성하기 위하여 먼저 0-트리의 0-기본경로를 식 (7)에 의하여 얻는다. 식(7)에서 $S_{l,0}$는 C'이 유도되는 선형 MACA C의 0-기본경로이다.



<그림 1> 선형 MACA와 그로부터 유도된 여원벡터가 6인 CA

$$\overline{S_{l,0}} = \begin{cases} S_{l,0} & l: \text{짝수} \\ S_{l,0} \oplus \beta & l: \text{홀수} \end{cases} \qquad (7)$$

0-트리의 0-기본경로와 식(4)를 이용하여 0-트리의 나머지를 구성한다. 다음으로 나머지 0이 아닌 순환상태 α-트리를 구성하기 위하여 α-트리의 α-기본경로 $\overline{S^{\alpha}_{l,0}}$는 식(5)에서와 같이 식(7)에서 구한 $\overline{S_{l,0}}$에 α를 더하여 얻고 $\overline{S^{\alpha}_{l,k}}$는 식(6)을 이용하여 구하여 나머지 트리를 구성할 수 있다.

3.3 선형 MACA C의 트리구성과 C로부터 유도된 여원벡터를 갖는 CA C'의 트리구성 알고리즘

Step 1. 주어진 전이행렬이 T일 때 $(T \oplus I)x = 0$ 을 만족하는 attractor x를 찾는다.

Step 2. T의 최소다항식 $m(x)$를 나누는 x^k중 최대정수 k를 찾아 CA의 depth d를 구한다.

Step 3. $T^d y = 0$이고 $T^{d-1} y \neq 0$인 0-트리의 도달불가능상태 y하나를 찾는다.

Step 4. y를 시작으로 하는 0-트리의 0-기본경로 $y \rightarrow Ty \rightarrow \cdots \rightarrow 0$를 찾는다.

Step 5. $S_{l,k} = S_{l,0} + \sum_{i=1}^{l} b_i S_{i,0}$에 의하여 0-트리를 구성.

Step 6. $S^{\alpha}_{l,0} = S_{l,0} \oplus \alpha$에 의하여 α-트리의 α-기본경로를 찾는다.

Step 7. $S^{\alpha}_{l,k} = S^{\alpha}_{l,0} + \sum_{i=1}^{l} b_i S_{i,0}$에 의하여 나머지 α-트리를 구성한다.

/* 여원을 갖는 CA C' 트리의 구성*/

Step 8. 여원벡터 F가 0이 아닌 attractor이면 C'의 0-기본경로를 $\overline{S_{l,0}} = \begin{cases} S_{l,0} & l: \text{짝수} \\ S_{l,0} \oplus \beta & l: \text{홀수} \end{cases}$ 에 의하여 구하고 Go To Step 10.

Step 9. 여원벡터 F가 C의 0-트리의 level i의 비순환 상태이면 C에서 도달불가능상태에서 F에 도달하는 한 경로를 $\overline{S_{l,0}}$ $(l > i)$로 $\overline{S_{i,0}} = 0$, level i보다 하위 level의 기본경로는 0에 $\overline{T}$를 연속적으로 연산하여 얻는다. 즉, $\overline{S_{l,0}} = \overline{T}^{i-l-1} \cdot F$이다.

Step 10. $\overline{S_{l,k}} = \overline{S_{l,0}} + \sum_{i=1}^{l} b_i S_{i,0}$에 의하여 상태 0이 속한 트리를 구성한다.

Step 11. $\overline{S^{\alpha}_{l,0}} = \overline{S_{l,0}} \oplus \alpha$에 의하여 또 다른 트리의 기본경로를 구성한다.

Step 12. $\overline{S^{\alpha}_{l,k}} = \overline{S^{\alpha}_{l,0}} + \sum_{i=1}^{l} b_i S_{i,0}$에 의하여 트리의 나머지 부분을 구성한다.

4. 결론

CA는 LFSR과 비교하여 랜덤성이 우수하다는 것이 알려지면서 최근 LFSR의 대안으로 의사 랜덤 패턴 생성기, 해쉬 함수, 스트림 암호 알고리즘 등의 고속화 응용에 많이 활용되고 있다. 그러나 현재까지 CA에 대한 안전성 분석이 제대로 이루어져 있지 않아 암호학적 응용에 다소 어려움이 따르고 있다. 주어진 CA의 행위 분석을 위해서는 CA의 상태전이 그래프를 구성하는 것이 우선되어야 한다. 따라서 본 논문에서 상태전이그래프 생성을 위한 트리 구성 알고리즘을 제안함으로써 CA의 안전성 분석에 일조 할 것으로 기대된다.

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. Chowdhury, 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, S. 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, P.P.Chaudhuri, *"Theory and application of nongroup cellular automata for synthesis of easily testable finite state machines"*, IEEE Trans. Computers, Vol. 45, No. 7, 1996, pp. 769-781.

[6] 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 (To appear).

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

[8] 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.

[9] 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.

[10] S. Nandi, B.K. Kar and P.P. Chaudhuri, *"Theory and Application of Cellular Automata"*, IEEE Trans. Computers., Vol. 43, 1994, pp.1346-1357.

[11] 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.

[12] S.J. Cho, H.D. Kim and U.S. Choi, *"Behavior of complemented cellular automata derived from a linear cellular automata"* (Submitted).