선형 TPMACA의 0-tree의 0이 아닌 상태를 여원벡터로 갖는 CA

CA with complemented vector as a nonzero state in the 0-tree of the linear TPMACA

조성진*, 김한두**, 최언숙*, 고귀자*
부경대학교 수리과학부*, 인제대학교 컴퓨터응용과학부

Sung Jin Cho*, Han Doo Kim**, Un Sook Choi*, Gwi Ja Ko*
Pukyong National University*, Inje University**
E-mail : sjcho@dolphin.pknu.ac.kr

ABSTRACT

본 논문에서는 선형 TPMACA C 의 0-tree에서 0이 아닌 상태를 여원벡터로 갖는 CA C′를 분석하여 C 의 모든 상태가 C′의 어느 곳에 있는지를 밝혔으며 또한 C 의 상태전이 그래프에서 한 경로만 알면 나머지 상태를 알 수 있음을 밝혔다.

Keywords : Cellular automata, TPMACA, 여원벡터, 여원CA, tree

Ⅰ. 서 론

Group CA의 상태전이 행동의 분석은 그동안 많은 연구가 이루어졌다([1], [8], [10], [12]). 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, 논리회로의 test 등에 응용이 되면서 관심을 받기 시작하였다([6], [7], [9], [11]). 특히 multiple-attractor CA는 효과적인 해시함수 생성기임이 입증되었으며[8] 또한 두 개의 직전자를 갖는 single-attractor CA는 CA를 기반으로 한 완전해쉬함수(perfect hash function) 생성에 사용되어왔다. 본 논문에서는 셀들에 XOR 논리 대신 XNOR 논리를 적용함으로써 여원벡터(complement vector)를 갖는 CA의 행동에 대한 자세한 분석을 제시한다. 또한 multiple-attractor CA(이하 MACA)의 셀들의 상태전이 함수를 전도함으로써 유도되는 여원을 갖는 CA의 상태전이 행동의 특징을 살펴본다. 특히 여원벡터 F가 0-tree에서 0이 아닌 상태일 경우의 여원을 갖는 CA의 행동을 밝히도록 한다. 2절에서는 선형 nongroup CA([3], [4], [5])의 정의와 간단한 성질들을 밝히고 3절에서는 선형 CA로부터 유도된 여원을 갖는 CA의 행동을 분석하고 4절에서 결론을 맺는다.

Ⅱ. 본 론

1. 선형 Nongroup CA의 정의 및 성질

이 절에서는 선형 nongroup CA의 정의와 2절에서 필요한 용어의 정의를 기술한다.

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

• ***Attractor*** : Nongroup CA의 상태전이 그래프에서 순환상태(cyclic state)들 중 사이클(cycle)의 길이가 1인 상태를 말한다.

• ***Multiple-attractor CA(MACA)***: 상태전이 그래프가 각 attractor를 root로 하는 서로 분리된 tree들로 구성된 nongroup CA를 multiple-attractor CA(이하 MACA)라 한다. 특히 직전자의 수가 2인 MACA를 TPMACA라 부른다.

참고1> attractor의 개수가 1인 MACA를 single-attractor CA(이하 SACA)라 부르며 특히 직전자의 수가 2인 SACA를 TPSACA라 부

른다.

• *α-tree* : 순환상태 α를 root로 하는 tree이다.

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

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

• ***r-predecessor*** : $T^r Y = X$을 만족하는 상태 Y를 상태 X의 r-predecessor라 한다. ($1 \leq r \leq 2^n - 1$)

2. 선형 CA로부터 유도된 여원을 갖는 CA의 행동

정리1> LNCA의 전이행렬이 T이고 그에 대응하는 여원을 갖는 CA에서 연산자 $\overline{T}$를 p번 적용한 연산자를 $\overline{T}^p$라 하자. 그러면

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

이다. 여기서 $[F(x)]$는 XOR 논리를 적용한 후 전도를 취한 n차원 벡터(n은 셀의 개수)이다. $F(x)$는 XNOR 논리가 적용된 CA 셀의 위치의 성분이 1이다.
(단, $\oplus$는 bitwise 덧셈연산이다)

정리2> C는 depth가 d인 TPMACA이고, C에서 0-tree의 level i ($0 < i \leq d$)에 있는 상태 F를 여원벡터로 택하자. 그러면 $\overline{T}^{i-1} F$는 C에 대응하는 여원을 갖는 CA C′에서 attractor이다.

정리3> TPMACA C에 대응하는 여원을 갖는 CA C′의 상태전이 그래프에서 임의의 도달가능한 상태의 서로 다른 두 직전자의 합은 C의 상태 0의 0이 아닌 직전자이다.

정리4> C가 TPMACA이고 C에 대응하는 여원을 갖는 CA를 C′이라 하자. 여원벡터 F를 C의 0-tree의 level l에 있는 비순환 상태로 택하자. 그러면 다음이 성립한다.

(a) C에서 l보다 더 큰 level에 있는 모든 상태는 C′에서 변하지 않는다.

(b) C에서 level l에 있는 모든 상태는 C′에서 l보다 작은 level에 배열된다.

(c) C에서 l보다 작은 level에 있는 모든 상태는 C′에서 level l에 배열된다.

(d) 상태 F는 C′에서 level $l-1$에 배열된다.

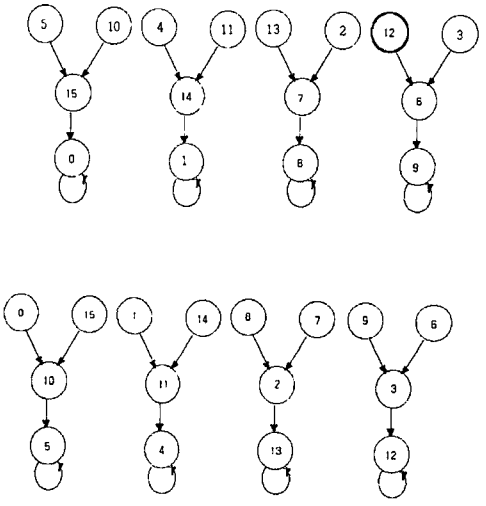

그림1:C와 C′의 상태전이 그래프

그림 1은 TPMACA의 예이다. 4개의 셀로 이루어진 CA에 적용된 rule이 <102, 102, 60, 60>이고 전이행렬 T는 다음과 같다.

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

이때 최소다항식은 $m(x) = x^2(x+1)$이고 attractor는 0, 1, 8 그리고 9이다. 여원벡터를 level 2에 있는 비순환상태 $F = (1010)^T$로 택하면 $\overline{T}F$는 C'에서 attractor이다(정리 2). C에서 level 2에 있는 모든 상태는 C'에서 2보다 작은 level에 배열되었고(정리 4의 b), C에서 2보다 작은 level에 있는 모든 상태는 C'에서 level 2에 배열되었으며(정리 4의 c), 상태 F는 C'에서 level 1에 배열되었다(정리 4

의 d). 한편, C'에서 상태 2의 두 직전자 8과 7의 합은 C의 상태 0의 0이 아닌 직전자인 15 이다(정리 3).

정리5> C 를 TPSACA라 하자. C 의 상태전이 그래프에서 $S_{l,k}$를 level l에서 $(k+1)$번째 상태라 하면 다음 식이 성립한다:

$$S_{l,k} = S_{l,0} \oplus \sum_{i=1}^{l} b_i S_{i,0}$$

여기서 $b_{l-1} b_{l-2} \cdots b_1$ 은 k의 이진법 표현이고 k의 최대값은 $2^{l-1}-1$ 이다.

정의 1> C 가 TPMACA이고 C 의 depth 는 d라 하자. β를 C 에서 α-tree의 도달불가능한 상태라 하자. 그러면

$\beta \rightarrow T\beta \rightarrow \cdots \rightarrow \alpha$

를 C 에서 α-tree의 α-기본경로(α-basic tree)라 부른다.

정리6> 상태 0의 직전자 수가 r일 때, $P_{i,j}$를 0-tree의 level i의 j번째 상태라 하고, R_i를 상태 X의 cyclic i-predecessor라 하자. 그리고 $X_{i,j}$를 X-tree의 level i의 j번째 상태라 하면 $X_{i,j}$는 다음을 만족한다.

$X_{i,j} = R_i \oplus P_{ij}$

(단, $\oplus$는 bitwise 덧셈연산, $1 \le i \le$ depth, $j = 1, \cdots, (r-1)r^{i-1}$)

정리7> C 를 TPMACA라 하자. $\alpha_{i,j}$ ($\beta_{i,j}$)를 C 에서 α-tree(β-tree)의 level i에 있는 j번째 상태라 하면

$\alpha_{i,j} \oplus \beta_{i,j} = \alpha \oplus \beta$

가 성립한다.

다음 정리는 정리 5>의 확장이다.

정리8> C 를 두 개의 직전자를 갖는 MACA라 하자. C 의 상태전이 그래프에서 $S^{\alpha}_{l,k}$ ($S_{l,k}$)를 C 에서 α-tree(0-tree)의 level l에서 $(k+1)$번째 상태라 하면 다음 식이 성립한다:

$$S^{\alpha}_{l,k} = S^{\alpha}_{l,0} \oplus \sum_{i=1}^{l} b_i S_{i,0}$$

여기서 $b_{l-1} b_{l-2} \cdots b_1$ 은 k의 이진법 표현이고 k의 최대값은 $2^{l-1}-1$ 이다.

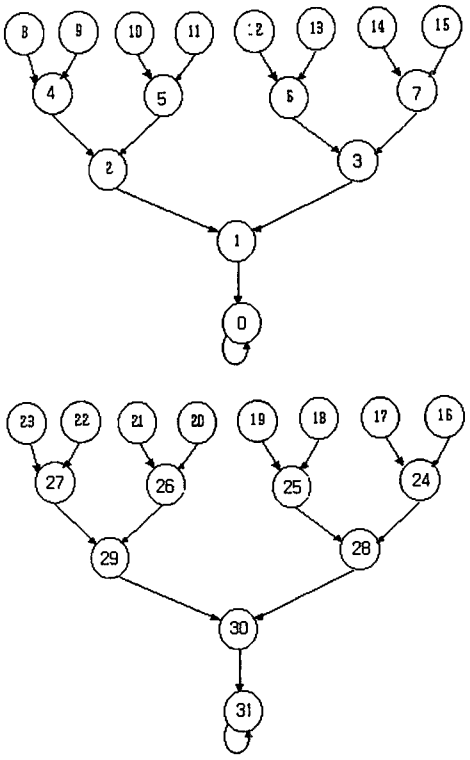

그림 2 : C 의 상태전이 그래프

그림 2는 TPMACA의 예이다. 5개의 셀로 이루어진 CA에 적용된 rule이 <204, 240, 240, 240, 240>이고 전이행렬 T는 다음과 같다.

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

이때 최소다항식은 $m(x) = x^4(x+1)$이고 attractor는 0과 31이다. 여기서 $8 \rightarrow 4 \rightarrow 2 \rightarrow 1 \rightarrow 0$ 은 0-기본경로이고, 이 0-기본경로에 대응하는 31-기본경로는 $23 \rightarrow 27 \rightarrow 29 \rightarrow 30 \rightarrow 31$ 이다. 또한 정리8>에 의하여 31-기본경로로부터 31-tree의 나머지 상태들을 알 수 있어서 31-tree를 구할 수 있다.

III. 결 론

선형 TPMACA C 의 0-tree에서 0이 아닌 상태를 여원벡터로 갖는 CA C′를 분석하여 C 의 모든 상태가 C′의 어느 곳에 있는지를 밝혔으며 또한 C 의 상태전이 그래프에서 0-tree

의 기본경로만 알면 나머지 $\alpha(\neq 0)$-tree의 기본경로를 알 수 있으며 $\alpha(\neq 0)$-tree의 기본경로를 이용하여 $\alpha(\neq 0)$-tree를 얻을 수 있음을 보였다. 본 연구결과는 완전해시함수(perfect hash function) 생성에 관한 연구에 도움이 되리라 사료된다.

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

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

[9] 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.

[10] 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.

[11] 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.

[12] 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.