Complemented CA derived from a linear Two-Predecessor MACA

조성진* · 김석태** · 최언숙*

Sung-Jin Cho*, Seok-Tae Kim** and Un-Sook Choi*

요 약

선형 TPMACA로부터 유도되는 여원 CA중 여원벡터가 0이 아닌 attractor인 경우의 여원 CA의 행동들을 분석하고, 선형 TPMACA의 0-트리의 한 개의 기본 경로를 이용하여 여원 CA의 상태전이그래프를 구성하는 알고리즘을 제안한다.

ABSTRACT

In this paper, we analyze behavior of complemented CA derived from a linear Two-Predecessor MACA(TPMACA) and obtain the state-transition diagram of complemented CA by using a basic path in the 0-tree of a linear TPMACA.

I. Introduction

An analysis of the state-transition behavior of group cellular automata(briefly, CA) was studied by many researchers ([1], [8], [10], [12]). The characteristic matrix of group CA is nonsingular. But the characteristic matrix of nongroup CA is singular. Although the study of nonsingular linear machines has received considerable attention from researchers, the study of the class of machines with singular characteristic matrix has not received due attention. Cho and Kim [6] and others [4,5] studied nonsingular linear machines. Some properties of nonsingular CA have been employed in several applications ([5], [9], [11], [12]). In this paper, by using basic paths in the 0-tree of a linear multiple-attractor CA with two predecessors(briefly, TPMACA) C we obtain the state-transition diagram of complemented CA C′ derived from C such that the complement vector is a nonzero attractor of C. Also we analyze the behavior of C′. We call C′ the CA corresponding to C. Especially we investigate the behavior of the complemented CA which the complement vector is taken as a nonzero attractor of C.

* 부경대학교 수리과학부(sjcho@pknu.ac.kr)

**부경대학교 전자컴퓨터정보통신공학부 (setakim@pknu.ac.kr)

II. Preliminaries

Definition 2.1[2]. A state with a self-loop in the state-transition diagram of a nongroup CA are referred to as an attractor.

Remark 2.2. The cycles with length $l(\geq 2)$ in the state-transition diagram of a nongroup CA are not attractors.

Definition 2.3[2]. The nongroup CA for which the state-transition diagram consists of a set of disjoint components forming (inverted) tree-like structures at attractors are referred to as MACA.

Remark 2.4. (1) In case the number of attractors is one we call single-attractor CA (SACA). (2) A MACA with two predecessors is called a TPMACA.

The tree rooted at a cyclic state α is called an α-tree.

Definition 2.5[2]. The depth of a CA is defined to be the minimum number of clock cycles required to reach the cyclic state from any nonreachable state in the state-transition diagram of the CA.

Since the 0-tree and another tree rooted at a nonzero cyclic state have very interesting relationships, the study of the 0-tree is necessary and very important.

Theorem 2.6[7]. The number of predecessors of a reachable state and the number of predecessors of the state 0 in a linear nongroup CA are equal.

Definition 2.7[3]. A state X at level l($l \leq$ *depth*) of the α-tree is a state lying on that tree and it evolves to the state α exactly after l-cycles (l is the smallest possible integer for which $T^l X = \alpha$).

Definition 2.8[3]. A state Y of an n-cell CA is an r-predecessor ($1 \leq r \leq 2^n - 1$) of a state X if $T^r Y = X$, where T is the characteristic matrix of the CA.

Lemma 2.9[11]. Let $\overline{T}^p$ denote p times application of the complemented CA operator $\overline{T}$. Then,

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

where T is the characteristic matrix of the corresponding noncomplemented rule vector and [F(x)] is an n-dimensional vector (n=number of cells) responsible for inversion after XNORing. F(x) has '1' entries (i.e., nonzero entries) for CA cell positions where XNOR function is employed.

III. The Behavior of complemented CA derived from a linear TPMACA

By using basic paths in the 0-tree of a linear TPMACA C we obtain the stat-transition diagram of complemented CA C′ derived from C such that the complement vector is a nonzero attractor of C. Also we analyze the behavior of C′.

Lemma 3.1. Let C be a linear TPMACA with depth d and F be a nonzero attractor in C as a complement vector. Then the state 0 is a cyclic state in the complemented CA C′ corresponding to C. Also the cycle length becomes two.

Lemma 3.2. Let C be a linear TPMACA

and α be a nonzero attractor in C as a complement vector. Then α lies on the two-length cycle including the state 0 of C′ corresponding to C.

Theorem 3.3. Let C be a linear TPMACA and α be a nonzero attractor in C as a complement vector. Then the following hold:

(1) If β is an attractor of C, then $\beta \oplus \alpha$ is also an attractor of C.

(2) If β is an attractor of C, then β and $\beta \oplus \alpha$ are coalesced to form a two-length cycle, and thus β and $\beta \oplus \alpha$ lie on the same two-length cycle in the complemented CA C′ corresponding to C.

Theorem 3.4. Let C be a linear TPMACA. Let α be a nonzero attractor in C as a complement vector. If x is a state at the level 2m in the β-tree of C, then x is a state at the level 2m in the β-tree of C′ corresponding to C.

Theorem 3.5. Let C be a linear TPMACA. Let α be a nonzero attractor in C as a complement vector. If y is a state at the level (2m-1) in the β-tree of C, then y is rearranged at the level (2m-1) in the ($\beta \oplus \alpha$)-tree of C′ corresponding to C.

Now we construct the state-transition diagram of the complemented CA corresponding to a linear TPMACA.

Definition 3.6. Let C be a linear TPMACA and the depth of C be d. Let β be a nonreachable state of the α-tree of C. Then we call the path $\beta \rightarrow T\beta \rightarrow \cdots \rightarrow \alpha$ a α-basic path of the α-tree of C.

Remark 3.7. Let C be a linear TPMACA with depth d. Then

$$S_{d,0} \rightarrow S_{d-1,0} \rightarrow \dots \rightarrow S_{1,0} \rightarrow 0$$

is a 0-basic path of the 0-tree of C, where

$$TS_{i+1,0} = S_{i,0} \ (1 \le i \le d-1)$$

and $S_{i,0}$ is the leftmost state of level i of the 0-tree of C.

Theorem 3.8[7]. Let C be a linear TPMACA. Given a 0-basic path of the 0-tree of C′ corresponding to C we can construct the state-transition diagram of the 0-tree of C′ as the following : If the states of the state-transition diagram of C (resp. C′) are labeled such that $S_{l,k}$ (resp. $\overline{S}_{l,k}$) be the (k+1)-th state in the l-th level, then

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

where $b_{l-1}\, b_{l-2} \cdots b_1$ is the binary representation of k and the maximum value of k is $2^{l-1}-1$.

The next theorem deals with rearrangements of the tree-structures between a linear TPMACA C and its complemented CA C′.

Theorem 3.9. Let C be a linear TPMACA and the depth of C be d. Let α be a nonzero attractor in C as a complement vector. Given a 0-basic path $S_{d,0} \rightarrow S_{d-1} \rightarrow \cdots \rightarrow 0$ of the 0-tree of C, we can construct a 0-basic path $\overline{S}_{d,0} \rightarrow \overline{S}_{d-1} \rightarrow \cdots \rightarrow 0$ of the 0-tree of the complemented CA C′ corresponding to C as the following:

$$\overline{S}_{l,0} = \begin{cases} S_{l,0} & \text{if } l \text{ is even} \\ S_{l,0} \oplus \beta & \text{if } l \text{ is odd} \end{cases}$$

Lemma 3.10. Let C be a linear TPMACA.

The states lying at the i-th level of the β-tree of C′ corresponding to C satisfy the following:

$$\overline{B}_{i,k} = \overline{S}_{i,k} \oplus \beta \quad (k = 0, \cdots, 2^{i-1}-1)$$

where $\overline{B}_{i,k}$ is the (k+1)-th state in the i-th level of the β-tree of C′ and $\overline{S}_{i,k}$ is in Theorem 3.8.

Theorem 3.11. Let C be a linear TPMACA with depth d. A β-basic path of the β-tree of C′ corresponding to C is

$\overline{B}_{d,0} \rightarrow \overline{B}_{d-1,0} \rightarrow \cdots \rightarrow \beta$ where $\overline{B}_{l,0}$ is the state in Lemma 3.10 and $\overline{S}_{l,0}$ is in Theorem 3.8 $(1 \le i \le d)$.

Theorem 3.12. Let C be a linear TPMACA. The (k+1)-th state lying at the l-th level of the β-tree of C′ corresponding to C satisfies the following:

If $\overline{B}_{l,k}$ is the state in Lemma 3.10, then

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

where $b_{l-1} \, b_{l-2} \cdots b_1$ is the binary representation of k and the maximum value of k is $2^{l-1}-1$.

Example 3.13. Let C be a five-cell linear TPMACA with the rule <102, 102, 60, 240, 204>.

Then

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

Now the characteristic polynomial of T is $c(x) = x^3 (1+x)^4$ and the minimal polynomial of T is $m(x) = x^3(1+x)$. The state-transition diagram of C is as the following:

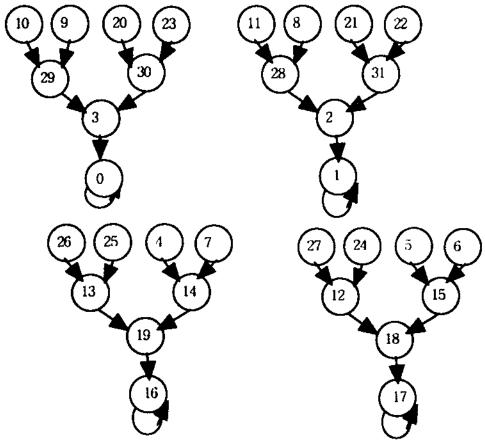

Figure 1 : The state-transition diagram of C

For the case $F =$ (00001) ^{T} is the complement vector, the state-transition diagram of C′ is as the following:

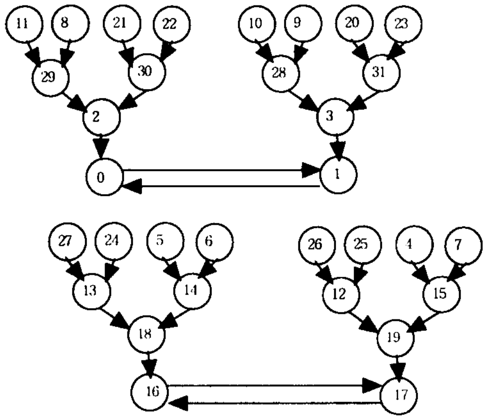

Figure 2 : The state-transition diagram of C′

The 0-tree and the 1-tree of C are closed in C'. Also the state at the even levels of the 0-tree and the 1-tree of C remain unaltered in C' whereas the states at the odd levels of C get interchanged between the trees in C'.

IV. Conclusion

By using a basic path in the 0-tree of TPMACA, we obtain the state-transition diagram of complemented CA derived from CA such that the complement vector is a nonzero attractor of given TPMACA. Also we analyze the behavior of complemented CA. Especially we investigate the behavior of the complemented CA which the complement vector is taken as a nonzero attractor of given TPMACA.

References

[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, 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.

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

[4] 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, 769-781.

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

[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, 2001, pp. 91-95.

[7] U.S. Choi, S.J. Cho and H.D. Kim, "Construction of a state-transition diagram using the basic-paths" (Submitted).

[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.

조성진(Sung-Jin Cho)
1979년 강원대학 수학교육과(이학사)
1981년 고려대학교 수학과 대학원(이학석사)
1988년 고려대학교 수학과 대학원(이학박사)
1988~현재 부경대학교 자연과학대학 수리과학부 재직(교수)
※관심분야: Cellular Automata론, ATM, Queueing론

김석태(Seok-Tae Kim)
1983년 광운대학 전자공학과(공학사)
1988년 Kyoto Institute of Technology, 전자공학과(공학석사)
1991년 Osaka대학, 통신공학과(공학박사)
1991년-현재 부경대학교 공과대학 전자컴퓨터정보통신공학부 재직(부교수)
※관심분야: 화상처리, 패턴인식, Cellular Automata론

최언숙(Un-Sook Choi)
1992년 성균관대학교 산업공학과(공학사)
2000년 부경대학교 자연과학대학 응용수학과 대학원(이학석사)
2000년~현재 부경대학교 자연과학대학 응용수학과 대학원 박사과정 재학중
※관심분야: Cellular Automata론, ATM, Queueing론