2001년 한국정보처리학회 추계 학술발표논문집 제8권 제2호

TPMACA의 트리 구성에 관한 연구

조성진*, 최언숙*, 김한두**, 김석태***, 이석기***
*부경대학교 수리과학부
**인제대학교 컴퓨터 응용과학부
***부경대학교 전자컴퓨터정보통신공학부
e-mail:sjcho@pknu.ac.kr

Construction of Trees in Linear TPMACA

Sung-Jin Cho*, Un-Sook Choi*, Han-Doo Kim**, Seok-Tae Kim***and Seok-Ki Lee***
*Division of Mathematical Sciences, Pukyong National University
**School of Computer Aided Science, Inje University
***Division of Electronic, Computer and Telecommunication Engineering

요약

셀의 상태가 2가지인 3-이웃 CA의 행동에 관한 분석은 그 응용분야가 넓어지면서 활발히 연구되고 있다. 본 논문에서는 2개의 직전자를 가지는 1차원 선형 다중 끌개를 갖는 셀룰라오타마타의 효율적인 트리 구성 방법을 제안한다.

I. Introduction

Cellular Automata(abbreviately, CA) have been introduced by Von Neumann and Ulam as models of self-organizing and self-reproducing behaviors[9]. A CA is a discrete time dynamical system, which consists of a uniform array of memories called cells. The states of cells in the array are updated according to a rule : the state of a cell at a given time depends only on its own state and the states of its nearby neighbors at the previous step.

A CA is necessary in many application areas such as test pattern generation, pseudo-random number generation, cryptography, error correcting codes and signature analysis. The analysis of the state transition behavior of group CA was studied by many researchers[2,6].

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. The characteristic matrix of group CA is nonsingular. But the characteristic matrix of nongroup CA is singular. However some properties of nongroup CA have been employed in several applications[4, 5, 7, 8]. In this paper, we construct the 0-tree from the 0-basic path and also construct the other trees in a given

* 본 연구는 정보통신부 2001년도 대학기초연구지원 사업에 의하여 수행되었음. (#2001-050-2).

two-predecessor MACA. Moreover we present the more effective methods of construction of trees in one dimensional MACA C having two predecessor and complemented cellular automata derived from C by replacing the XORs with XNORs at some(or all) of the value of each cells.

Section 2 provides the CA preliminaries. Section 3 deals with the general characterization of nongroup CA.

Ⅱ. Cellular Automata Preliminaries

A one-dimensional CA(1-D CA) consists of a number of interconnected cells arranged spatially in a regular manner. In the present work, we use a 3-neighbourhood 1-D CA with the cells arranged linearly on GF(2).

The following definitions are well-known.

Definition 2.1. a) If the rule of a CA cell involves only XOR logic, then it is called a linear rule. A CA with all the cells having linear rules is called a *linear CA*.

b) If the rule of a CA cell involves only XNOR logic then it is called a complemented rule. A CA with some cells having complemented rules is called a *complemented CA*.

c) If all the CA cells obey the same rule, then the CA is said to be a *uniform CA* ; otherwise, it is a *hybrid CA*.

d) If the characteristic matrix is nonsingular, then the CA is a *group CA* ; otherwise, it is a *nongroup CA*.

Definition 2.2. a) A state with a self-loop in the state transition diagram of nongroup CA are referred to as an *attractor*[1].

b) The *depth* of a CA is defined to be the minimum number of clock cycle required to reach the cyclic state from any nonreachable state in the state transition diagram of the CA[1].

c) A state y at level l(l< 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 $T^l y=\alpha$)[2].

d) A state w of an n-cell CA is an r-predecessor($1\le r\le 2^n-1$) of a state y if $T^r w=y$, where T is the characteristic matrix of the CA[2].

Definition 2.3.[1] The nongroup CA for which the state transition diagram consists of a set of disjoint components forming(inverted) tree-like structures rooted at attractors are referred to as *multiple-attractor CA(MACA)*.

Remark A. i) In case the number of attractors is one we call *single-attractor CA(SACA)*. ii) If a reachable cell of MACA has two predecessors, then the MACA is called *two-predecessor MACA(TPMACA)*. iii) The rank of T is $n-1$ where T is the characteristic matrix of the n-cell TPMACA. iv) The minimal polynomial of the n-cell MACA is $x^d(x+1)$ where $d(<n)$ is the depth of a tree.

Definition 2.4. Let C be a linear TPMACA with depth d and let T be a state-transition matrix of C. Then $x\rightarrow Tx\cdots\rightarrow T^d x(=\alpha)$ is called the α-basic path of the α-tree in C.

Ⅲ. Construction of Trees of Linear TPMACA

In this section, we present the method of more effective construction of trees in one dimensional linear TPMACA by using the basic path in the 0-tree.

Lemma 3.1. [3] Let X_m and X_n be level i states in the α-tree of a TPMACA C. If $j=\min\{k \mid T^k X_m = T^k X_n\}$, then $X_m \oplus X_n$ is one of level j states in the 0-tree of C.

Corollary 3.2. The sum of different predecessors of any reachable state is a nonzero predecessor of the state 0.

Theorem 3.3. Let C be a linear TPMACA. If the states of the state-transition diagram of C are labeled such that $S_{l,k}$ be the $(k+1)$-th state in the l-th ($l \geq 2$) level of the 0-tree of C, then the following hold:

(1) $\sum_{k=0}^{2^{l-1}-1} S_{l,k} = 2^{l-1} S_{l,0}$
$\oplus 2^{l-2}(S_{l,0} \oplus S_{2,0} \oplus \cdots \oplus S_{l-1,0})$

for all l($l \leq$depth) where kS denotes $S \oplus \cdots \oplus S$(k summands).

(2) For each level l($l \leq$depth),

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

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.

Remark B. In Theorem 3.3 (1) if $l=2$, then $\sum_{k=0}^{2^{l-1}-1} S_{l,k} = S_{l,0}$. And if $l > 2$, then $\sum_{k=0}^{2^{l-1}-1} S_{l,k} = 0$.

Definition 3.4. Let C be a linear TPMACA and the depth of C be d. Let β be a nonrechable state of the α-tree of C. Then we call the path

$$\beta \rightarrow T\beta \rightarrow \cdots \rightarrow T^d\beta (= \alpha)$$

a α-basic path of the α-tree in C.

Remark C. Let C be a linear TPMACA in Theorem 3.3 with depth d. Then

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

is a 0-basic path of the 0-tree in C.

Lemma 3.5. Let C be a linear TPMACA. Let $\alpha_{i,j}$(resp. $\beta_{i,j}$) be the $(j+1)$-th state in the i-th level of the α-tree(resp. β-tree) in C. Then

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

As a corollary we obtain the following result which is a α-basic path of the α-tree using 0-basic path of the 0-tree in linear TPMACA.

Corollary 3.6. Let C be a linear TPMACA with depth d and T be the characteristic matrix of C. If

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

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

$$(S_{d,0} \oplus \alpha) \rightarrow (S_{d-1,0} \oplus \alpha) \rightarrow \cdots \rightarrow (S_{1,0} \oplus \alpha) \rightarrow \alpha$$

is a α-basic path of the α-tree of C.

Example 3.7. Let C be a five-cell linear nongroup CA with the rule <204, 240, 240, 240, 240>. Then the characteristic matrix T is the following.

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

The minimal polynomial $m(x)$ of T is $m(x) = x^4(x+1)$ and attractors are 0 and 31. The state-transition diagram is in Fig. 1. (8-4-2-1-0) is a 0-basic path in the 0-tree. The 31-basic path in the 31-tree corresponding to the 0-basic path is (23-27-29-30-31).

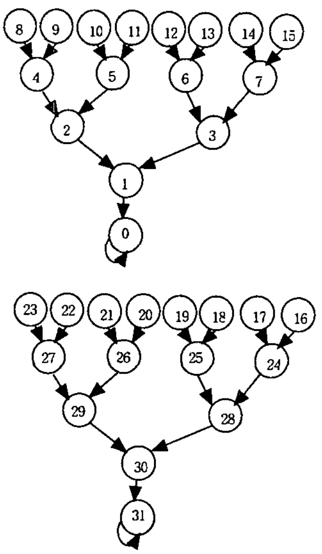

Fig. 1 The state-transition diagram

The following theorem is an extension of Theorem 3.3.

Theorem 3.8. Let C be a linear TPMACA with depth d. If the states of the state-transition diagram of C are labeled such that $S^{a}_{l,k}$(resp. $S_{l,k}$) be the $(k+1)$-th state in the l-th level of the a-tree(resp. 0-tree) in C and $S^{a}_{l,k} = S_{l,0} + a$, then the following hold:

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

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

References

[1] T.L. Booth, *Sequential Machines and Automata Theory*, John Wiely & Sons, London, 1967.

[2] Kevin Cattell and Jon C. Muzio, "Synthesis of One-Dimensional Linear Hybrid Cellular Automata", *IEEE Trans. Computer-Aided Design*, Vol. 15, 1996.

[3] S.J. Cho, U.S. Choi and H.D. Kim,, "Some properties of one dimensional linear nongroup cellular automata over GF(2)", *J. Korean Multimedia Soc.*, Vol.4, pp. 91-94, 2001.

[4] T. Damarla and A. Sathaye, "Application of one-dimensional cellular automata and linear feedback shift registers for pseudo exhaustive testing", *IEEE. Trans. Computer-Aided Design*, Vol. 12, pp. 1580-1591, 1993.

[5] A.K. Das, A. Ganguly, A. Dasgupta, S. Bhawmik and P.P. Chaudhuri, " Efficient characterization of cellular automata" *Proc. IEE(Part E)*, Vol. 137, pp. 81-87, 1990.

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

[7] D.M. Miller, J.C. Muzio, M. Serra, X. Sun, S. Zhang and R.D. McLeod "Cellular automata techniques for compaction based BIST", *Proc. IEEE Int. Symp. Circuits Syst.*, pp. 1893-1896, 1991.

[8] D.M. Miller and S. Zhang, "A study of the fault coverage of LFSR and CA pseudo-random test pattern generators", *Proc. 5th Technical Workshop New Directions IC Testing*, 1991.

[9] J. Von Neumann, *Theory of self-reproducing automata*, University of Illinois Press, Urbana, 1966.