여원벡터가 비순환적인 CA의 구조에 관한 연구

조성진*, 최언숙*, 고귀자*, 김한두**, 허성훈**, 김석태***
*부경대학교 수리과학부
**인제대학교 컴퓨터 응용과학부
***부경대학교 전자컴퓨터정보통신공학부

Structure of CA which the complement vector is acyclic

Sung-Jin Cho*, Un-Sook Choi*, Gwi-Ja Ko*, Han-Doo Kim**, Seong-Hun Heo**, Seok-Tae Kim***
*Division of Mathematical Sciences, Pukyong National University
**School of Computer Aided Science, Inje University
***Division of Electronic, Computer and Telecommunication Engineering

요 약

본 논문에서는 2개의 직전자를 가지는 선형 MACA부터 유도된 여원CA의 행동에 대한 분석을 한다.

1. Introduction

An analysis of the state-transition behavior of group cellular automata(briefly CA) was studied by many researchers ([1], [5], [7], [9], [11]). The characteristic matrix of group CA is nonsingular. But the characteristic matrix of nongroup CA is singular. Although the study of the class of machines with singular characteristic matrix has not received due attention. However some properties of nonsingular CA have been employed in several applications ([6], [8], [10], [11]).

In this paper, e present a detailed analysis of the behavior of complemented CA derived from a linear multiple-attractor CA with two predecessor(briefly TPMACA) by replacing the XORs at some (or all) of the cells. Also, we give the specific features displayed in the state-transition behavior of the complemented CA C' resulting from inversion of next-state logic of some(or all) of the cells of a TPMACA C. We call C' the CA corresponding to C. Especially we investigate the behavior of the complemented CA which the complement vector is an acyclic state lying on some nonzero-tree as the complement vector of a linear TPMACA.

† 본 연구는 정보통신부 2001년도 대학기초연구지원사업에 의하여 수행되었음. (#2001-050-2)

2. Background

A CA consists of a number of interconnected cells arranged spatially in a regular manner [2], where the state-transitions of each cell depend on the states of its neighbors. The CA structure investigated by Wolfram can be viewed as a discrete lattice of sites(cells), where each cell can assume either the value 0 or 1. The next state of a cell is assumed to depend on itself and on its two neighbors (3-neighbourhood dependency). The cells evolve in discrete time steps according to some deterministic rule that depends only on logical neighbourhood. In effect, each cell consists of a storage element (D flip-flop) and a combinatorial logic implementing the next state function.

If the next-state function of a cell is expressed in the form of a truth table, then the decimal equivalent of the output is conventionally called the rule number for the cell [2].

Neighbourhood state:	111	110	101	100	011	010	001	000	
Next state:	0	1	0	1	1	0	1	0	(rule 90)
Next state:	1	0	0	1	0	1	1	0	(rule150)

The top row gives all eight possible states of the three neighboring cells (the left neighbor of the ith ell, the ith cell itself, and its right neighbor) at the time instant t. The second and third rows give the corresponding states of the ith cell at time instant $t+1$ for two illustrative CA rules. On minimization, the truth tables for the rules 60, 90, 102, 10, 204 and 240 result in the following logic functions, where $\oplus$ enotes XOR logic and $q_i(t)$ denotes the state of the ith CA cell at the ith time instant, $q_{i-1}(t)$ and $q_{i+1}(t)$ refer to the state of its left and right neighbors.

rule 60: $q_{i+1}(t) = q_{i+1}(t) \oplus q_i(t)$

rule 90: $q_{i+1}(t) = q_{i+1}(t) \oplus q_{i+1}(t)$

rule102: $q_{i+1}(t) = q_i(t) \oplus q_{i+1}(t)$

rule150: $q_{i+1}(t) = q_{i-1}(t) \oplus q_{i(t)} \oplus q_{i+1}(t)$

rule204: $q_{i+1}(t) = q_i(t)$

rule240: $q_{i+1}(t) = q_{i-1}(t)$

Definition 2.1. [17] i) Linear CA: if the next-state generating logic employs only XOR logic, then the CA is called a linear CA: otherwise it is called a non-linear CA.

ii) Complemented CA: Complemented CA employs XNOR logic for one or more CA cells.

iii) Group CA: A CA is called a group CA if all the states in its state-transition diagram lie on cycles, otherwise it is referred to as a non-group CA.

iv) Reachable state: In the state-transition diagram of a non-group CA, a state having at least one in-degree is called a reachable state, while a state with no in-degree is called a non-reachable state.

v) Cyclic state: Reachable states which lie on cycles are called cyclic states.

vi) Attractor: A tate having a self-loop is referred to as an attractor. An attractor can be viewed as a cyclic state with unit cycle length.

vii) Depth: The maximum number of state transitions required to reach the nearest cyclic state from any non-reachable state in the CA state-transition diagram is defined as the depth of the non-group CA.

viii) Level and Predecessor: Level of a state S_i is defined as the minimum number of time steps required to reach a cyclic state starting from S_i. The state S_i can be viewed as i-level

predecessor o the cyclic state.

ix) Multiple-attractor CA(MACA): The non-group CA for which the state-transition diagram consists of a set of disjoint components forming I(inverted) tree-like structures rooted at attractors are referred to as multiple-attractor CA. In case the number of attractor is one we call the CA single-attractor CA(SACA).

x) TPMACA: TPMACA is a MACA such that every reachable state in the stat-transition diagram has only two predecessors. TPSACA is a SACA such that every reachable state in the state-transition diagram has only two predecessors. The rank of T is $n-1$ where T is the characteristic matrix of the TPSACA.

xi) α-tree: The tree rooted at a cyclic of the TPSACA.

Theorem 2.2. [15] The number of predecessors of a reachable state and the number of predecessors of the state 0 in a linear nongroup CA are equal.

Lemma 2.3. [18] Let $\overline{T}^P$ denote p times application of the complemented CA operator $\overline{T}$. Then

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

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 and $f(x)$ is the current state assignment of the cells.

3. Behavior of complemented CA derived from a linear TPMACA

In this section we present the behavior of complemented CA derived from a linear TPMACA. Especially we investigate the behavior of complemented CA derived from a linear TPMACA C which the complement vector is an acyclic state lying on some nonzero tree of C.

Lemma 3.1. Let F be a level i state in the $\alpha(\neq 0)$-tree of a linear TPMACA C and β be an attractor of C. Then $(\beta \oplus \overline{T}^{i-1}F)$ lies on a cycle of length 2 of the complemented CA C′ corresponding to C.

Theorem 3.2. Let F be a level i state in the $\alpha(\neq 0)$-tree of a linear TPMACA C and β be an attractor of C. Then $(\beta \oplus \alpha \oplus \overline{T}^{i-1}F)$ and $\beta \oplus \overline{T}^{i-1}F$ lie on the same cycle of length 2 of C′, where C′is in Lemma 3.1.

Corollary 3.3. Let F be a level i state in the $\alpha(\neq 0)$-tree of a linear TPMACA C and β be an attractor of C. Then the sum of two different cyclic states which lie on the same cycle of length 2 of C′ is always α.

Lemma 3.4. Let C be a linear TPMACA with depth d and F be a state at the level $i\,(0 < i \leq d)$ of a non-zero tree in C as a complemented vector. Then $\overline{T}^{i-1}F$ lies on a cycle of length 2 in the complemented CA C′ Corresponding to C.

Lemma 3.5. Let C be a linear TPMACA with depth d and F be a state at the level $i\,(0 < i \leq d)$ in the $\alpha(\neq 0)$-tree

of $\mathbb{C}$ as a complemented vector. Then $\alpha \oplus \overline{T}^{i-1}F$ lies on a cycle of length 2 in the complemented CA $\mathbb{C}'$ Corresponding to $\mathbb{C}$.

Theorem 3.6. Let F be a state at the level i ($0 < i <$ *depth*) in the $\alpha(\neq 0)$-tree of a linear TPMACA $\mathbb{C}$ as a complemented vector. Also let $\mathbb{C}'$ be the complemented CA Corresponding to $\mathbb{C}$. Then the following hold:

(a) If x is a state at level ($i + 1$) in the α-tee of $\mathbb{C}$, then x is also a level ($i + 1$) state in the $\overline{T}^{i-1}F$-tree of $\mathbb{C}'$.

(b) If y is a state at level ($i + 2$) in the α-tee of $\mathbb{C}$, then y is also a level ($i + 2$) state in the ($\alpha \oplus \overline{T}^{i-1}F$)-tree of $\mathbb{C}'$.

(c) The state 0 of $\mathbb{C}$ is rearranged at level i in the $\overline{T}^{i-1}F$ -tree of $\mathbb{C}'$.

(d) The state F is a level ($i - 1$) state in the $\overline{T}^{i-1}F$ -tree of $\mathbb{C}'$.

Theorem 3.7. Let F be a state at the level i ($0 < i <$ *depth*) in the $\alpha(\neq 0)$-tree of a linear TPMACA $\mathbb{C}$ as a complemented vector. Then following hold:

(a) If x is a state at level ($i + j$) in the α-tee of $\mathbb{C}$, then x is also a level ($i + j$) state in the $\overline{T}^{i-1}F$-tree of $\mathbb{C}'$, where j is an odd number such that $i + j \leq$ *depth*.

(b) If y is a state at level ($i + j$) in the α-tee of $\mathbb{C}$, then y is also a level ($i + j$) state in the $\alpha \oplus \overline{T}^{i-1}F$-tree of $\mathbb{C}'$, where j is an even number such that $i + j \leq$ *depth*.

Lemma 3.8. Let x and y be the level 1 states in the α-tree and β-tree of a linear TPMACA $\mathbb{C}$ Respectively. Then $x \oplus y = \alpha \oplus \beta$.

Theorem 3.9. Let F be a state at the level i in the $\alpha(\neq 0)$-tree of a linear TPMACA $\mathbb{C}$ as a complemented vector. Then the following hold:

(a) If x is a state at level ($i + j$) in the $\beta(\neq \alpha)$-tee of $\mathbb{C}$, then x is also a level ($i + j$) state in the $\beta \oplus \alpha \oplus \overline{T}^{i-1}F$-tree of $\mathbb{C}'$, where j is an odd number such that $i + j \leq$ *depth*.

(b) If y is a state at level ($i + j$) in the $\beta(\neq \alpha)$-tee of $\mathbb{C}$, then y is also a level ($i + j$) state in the $\beta \oplus \overline{T}^{i-1}F$ -tree of $\mathbb{C}'$, where j is an even number such that $i + j \leq$ *depth*.

(C) If w is a state in the $\beta(\neq \alpha)$-tee of $\mathbb{C}$ such that the level of w is lower than i, then w get rearranged at level i in the $\beta \oplus \overline{T}^{i-1}F$-tree of $\mathbb{C}'$.

(d) The states at level i of $\mathbb{C}$ get rearranged at level up to ($i - 1$) of $\mathbb{C}'$.

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, 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. 23 9~244.

[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] 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 in Cryptography", *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.