J. KSIAM **Vol.5**, No.1, 1-10, 2001

The relationship between the 0-tree and other trees in a linear nongroup cellular automata [*][†]

Sung-Jin Cho

Abstract

We investigate the relationship between the 0-tree and other trees in linear nongroup cellular automata. And we show that given a 0-basic path of 0-tree and a nonzero attractor α of a multiple attractor linear cellulara automata with two predecessor we construct an α-tree of that multiple attractor linear cellular automata.

1 Introduction

An analysis of the state-transition behavior of group cellular automata(abbreviately, CA) was studied by many researchers ([1], [4], [7], [9]). 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. However some properties of nonsingular CA have been employed in several applications ([5], [8], [9]). In this paper, we investigate the relationship between the 0-tree and other trees in linear nongroup cellular automata. Especially given a 0-basic path of 0-tree and all attractors of a multiple attractor linear CA (abbreviately, MALCA) with two predecessor we construct all trees of that MALCA.

2 Linear nongroup CA

In the rest of this paper, unless specified otherwise, a null boundary CA [7] is simply referred to as a CA.

[*] 1991 Mathematics Subject Classification: 94

[†] Key words and phrases: Nongroup cellular automata, singular matrix, multiple-attractor linear cellular automata, depth, tree.

Definition 2.1. *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 nongroup CA are not attractors.*

Definition 2.3. *[3] 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 linear CA(MALCA).*

Remark 2.4. *In case the number of attractors is one we call MALCA single-attractor linear CA(SALCA).*

The tree rooted at a cyclic state α is denoted as α-*tree*.

Definition 2.5. *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.*

Lemma 2.6. *The state 0 in a linear nongroup CA $\mathbb{C}$ is an attractor.*

Proof. Let T be the characteristic matrix of $\mathbb{C}$. Then $T0 = 0$. Hence 0 is an attractor in $\mathbb{C}$. □

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.

Lemma 2.7. *If d is the dimension of the null space $N(T)$ of the characteristic matrix T of a nongroup CA $\mathbb{C}$, the total number of 1-predecessors of the state 0 is 2^d.*

Proof. Let X be a predecessor of the state 0 in $\mathbb{C}$. Then $TX = 0$. Since $dimN(T) = d$, $TX = 0$ has d free variables on $GF(2)$. Hence the total number of 1-predecessors of the state 0 is 2^d. □

Theorem 2.8. *The number of predecessors of a reachable state and those of the state 0 in a linear nongroup CA $\mathbb{C}$ are equal.*

Proof. Let T be the characteristic matrix of $\mathbb{C}$ and α be a reachable state in $\mathbb{C}$. Also let X be a state in the α-tree. Then the equation $TX = \alpha$ has at least one solution. Therefore $|\{Y|TY = \alpha\}| = |\{X|TX = 0\}|$. Hence the proof is completed. □

Definition 2.9. *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 2.10. *A state Y of an n-cell CA is an i-predecessor $(1 \leq i \leq 2^n - 1)$ of a state X if $T^i Y = X$, where T is the characteristic matrix of the CA. A state X_i in a cycle of length l is called by the cyclic r-predecessor $(r < l)$ of the state X_i (written by X_{i-r}) if $T^r X_{i-r} = X_i$.*

From the following theorem we obtain the relation between the minimal polynomial of the characteristic matrix of a CA and the depth of the state-transition diagram of the CA.

Theorem 2.11. *Let k be the largest integer such that x^k divides the minimal polynomial of the characteristic matrix of an n-cell CA $\mathbb{C}$. Then the depth of the state-transition diagram of the CA $\mathbb{C}$ is k.*

Proof. Let the characteristic matrix of $\mathbb{C}$ be T. And let $m(x)$ (the minimal polynomial of T) be written as

$$m(x) = x^k \phi(x)$$

where k is the largest integer for which x^k is one of its factors and $\phi(x)$ is a polynomial not divisible by x. Since x^k and $\phi(x)$ are co-prime polynomials, the whole space S corresponding to T is decomposed into two invariant subspaces as

$$S = R_1 + R_2$$

where R_1 is the invariant subspace with x^k as the minimal polynomial and R_2 is the invariant subspace with $\phi(x)$ as the minimal polynomial [6]. Thus there exists at least one nonzero vector y in R_1 which has x^k as its minimal polynomial. Therefore $T^k y = 0$ for the minimum value of k. Hence the depth of the state-transition diagram of $\mathbb{C}$ is k. □

Example 2.12. *Let $\mathbb{C}$ be a four-cell linear nongroup CA with the rule $< 102, 102, 60, 60 >$. Then*

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

Now $m(x) = x^2(x^2+1)$, $S = \{0, 1, \cdots, 15\}$, $R_1 = \{0, 5, 10, 15\}$ and $R_2 = \{0, 1, 8, 9\}$. Hence the depth of the state-transition diagram of $\mathbb{C}$ is 2.

Lemma 2.13. *The number of r-predecessors($r > 0$) of any cyclic state is the same as that of the state 0.*

Proof. Let S_r be the set of all r-predecessors of the state 0 ($l > 0$). Then

$$S_r = \{Y | T^r Y = 0\}$$

Let X_0 be a nonzero cyclic state in the state-transition diagram and let A_r be the set of all r-predecessors of the state X_0. Then

$$A_r = \{Z | T^r Z = X_0\}$$

Since $A_r \neq \emptyset$,

$$|A_r| = |S_r|$$

This completes the proof. □

3 The relationship between 0-tree and other $\alpha(\neq 0)$-tree in linear nongroup CA

In this section we show that there are interesting relationships between the states in an α-tree corresponding to each level state in the 0-tree.

Lemma 3.1. *Let X_l and X_m be level i states in an α-tree. If there exists $j(\leq i)$ such that $j = min\{k | T^k X_l = T^k X_m\}$, then $X_l \oplus X_m$ is one of level j states in the 0-tree.*

Proof. Since $T^j X_l = T^j X_m$, $T^j(X_l \oplus X_m) = 0$. Thus $X_l \oplus X_m$ is one of j-predecessors of the state 0. Suppose that $X_l \oplus X_m$ is a level $p(< j)$ state in the 0-tree. Then $T^p(X_l \oplus X_m) = 0$. Thus $T^p X_l = T^p X_m$. This is a contradiction. Hence $X_l \oplus X_m$ is one of level j states in the 0-tree. □

From Lemma 3.1 we obtain the following corollary.

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

Theorem 3.3. *The sum of two states lying at different levels* p *and* $q (p > q)$ *of the* α*-tree is a state at level* p *of the* 0*-tree.*

Proof. Let X_p be a level p state of the α-tree, X_q a level q state of the α-tree and $X_0 = \alpha$ the attractor of the α-tree. Then $T^p X_p = X_0$. Since

$$\begin{aligned} T^p X_q &= T^{p-q}(T^q X_q) \\ &= T^{p-q} X_0 \\ &= X_0 \end{aligned}$$

Thus $T^p(X_p \oplus X_q) = 0$ and therefore $X_p \oplus X_q$ is a p-predecessor of the state 0. Since X_p is a level p state of the α-tree, $T^{p-1}X_p$ is a nonzero predecessor of the state α, i.e., $T^{p-1}X_p$ is a level 1 state of the α-tree and $T^{p-1}X_q = X_0$. Therefore $T^{p-1}(X_p \oplus X_q) = X_1 \oplus X_0$. Since X_1 and X_0 are different predecessors of the α-tree, by Corollary 3.2 $X_1 \oplus X_0$ is a nonzero predecessor of the state 0. Hence $X_p \oplus X_q$ is a state at level p of the 0-tree. □

Theorem 3.4. *Let the number of* 1*-predecessors of the state* 0 *in a linear nongroup CA be* n*. If* $U_i = \{P_1, P_2, \cdots, P_{n^i}\}$ *is the set of the* i*-predecessors with respect to the state* 0 *(with* $P_1 = 0$*) and* X_1 *is one of the* i*-predecessors with respect to a nonzero cyclic state* X*, then the set of the* i*-predecessors with respect to* X *is* $\{X_1 \oplus P_k |\ k = 1, 2, \cdots, n^i\}$*.*

Proof. We know that $U_i = \{Y |\ T^i Y = 0\}$. And let $V_i = \{Z |\ T^i Z = X\}$. Since $X_1 \in V_i, V_i \neq \emptyset$. Thus $|V_i| = |U_i| = n^i$. Since $T^i(X_1 \oplus P_k) = T^i X_1 \oplus T^i P_k = T^i X_1 \oplus 0 = X, X_1 \oplus P_k$ is a i-predecessor of the state X where $k = 1, 2, \cdots, n^i$. Thus the set of the i-predecessors with respect to X is $\{X_1 \oplus P_k |\ k = 1, 2, \cdots, n^i\}$. □

Theorem 3.5. *Let* r *be the number of* 1*-predecessors of the state* 0 *in a linear nongroup CA,* $P_{ij} (j = 1, 2, \cdots, (r-1)r^{i-1})$ *be the level* i *states of the* 0*-tree and* R_i *the cyclic* i*-predecessor of a cyclic state* X*. And let* $X_{ij} (j = 1, 2, \cdots, (r-1)r^{i-1})$ *be the level* i *states of the* X*-tree. Then*

$$(*)\ X_{ij} = R_i \oplus P_{ij} \ \textit{where}\ 1 \leq i \leq \textit{depth},\ j = 1, 2, \cdots, (r-1)r^{i-1}$$

Proof. We prove $(*)$ by mathematical induction. The case where $i = 1$ is trivial by Theorem 3.4. Assume that $X_{kj} = R_k \oplus P_{kj} (j = 1, 2, \cdots, (r-1)r^{k-1})$. Then $TR_{k+1} = R_k$. Since $T(X_{k+1j} \oplus R_{k+1}) = X_{kj} \oplus R_k = P_{kj}, X_{k+1j} \oplus R_{k+1} = P_{k+1j}$ for some P_{k+1j} such that P_{k+1j} is a level $k+1$ state of the 0-tree. Thus $X_{k+1j} = R_{k+1} \oplus P_{k+1j} (j = 1, 2, \cdots, (r-1)r^k)$. Therefore $(*)$ holds for $i = k+1$. Hence the proof is completed. □

From the above theorem we obtain the following corollary.

Corollary 3.6. *Let $\mathbb{C}$ be a nongroup linear CA. Let r be the number of 1-predecessors of the state 0, $P_{ij}(j = 1, 2, \cdots, (r-1)r^{i-1})$ be the level i states of the 0-tree and α an attractor of $\mathbb{C}$. And let $X_{ij}(j = 1, 2, \cdots, (r-1)r^{i-1})$ be the level i states of the X-tree. Then*

$$X_{ij} = \alpha \oplus P_{ij} \text{ where } 1 \le i \le depth,\ \ j = 1, 2, \cdots, (r-1)r^{i-1}$$

Example 3.7. *Let $\mathbb{C}$ be a four-cell linear nongroup CA with the rule $< 102, 102, 102, 60 >$. Then*

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

Now $m(x) = x^2(x^2+1)$, $rank = 3$ and $depth = 2$. The number of predecessors is equal to 2 and cyclic states are $\{0\}, \{4, 12\}$ and $\{8\}$. Thus attractors are 0 and 8. We get the states of each nonzero tree as the following:

(i) In 4-tree, $14 = 10 \oplus 4$, $1 = 5 \oplus 4$ and $3 = 15 \oplus 12$.

(ii) In 12-tree, $6 = 10 \oplus 12$, $9 = 5 \oplus 12$ and $11 = 15 \oplus 4$.

(iii) In 8-tree, since state 8 is an attractor, the cyclic r-predecessor is always state 8.

Thus $13 = 5 \oplus 8$, $2 = 10 \oplus 8$ and $7 = 15 \oplus 8$.
The state-transition diagram is as the following:

Lemma 3.8. *Given a linear nongroup CA $\mathbb{C}$, let T be the characteristic matrix of $\mathbb{C}$. Let d be the depth of the 0-tree of $\mathbb{C}$ and let $dimN(T) = r$. Then the number of states in the 0-tree is 2^{rd}.*

Proof. Since $dimN(T) = r$, the number of 1-predecessors of any reachable state is 2^r by Lemma 2.7. Let a_i be the number of level i states in the 0-tree. Then $a_{i+1} = 2^r a_i$. Therefore the number of level i states of the 0-tree is $(2^r)^{i-1}(2^r - 1)$. Thus the number of states in the 0-tree is

$$1 + (2^r - 1) + 2^r(2^r - 1) + \cdots + (2^r)^{d-1}(2^r - 1) = 2^{rd}$$

□

Theorem 3.9. *Let $\mathbb{C}$, T, d and r be in Lemma 3.8. Let $m(x)$ be the minimal polynomial of T. If $|T + xI| = x^d(x + 1)^{n-d}$ and $m(x) = x^d(x + 1)$, then the following hold:*

(i) The number of states in the 0-tree is 2^{rd}.

(ii) The number of attractors is 2^{n-rd}.

Proof. (i) By Lemma 2.7 the number of predecessors of the state 0 is 2^r. And since $m(x) = x^d(x + 1)$, the depth of the 0-tree is d. Hence by Lemma 3.8 the number of states in the 0-tree is 2^{rd}.

(ii) By Lemma 2.13 the number of states in each attractor tree is the same as the number of states in the 0-tree. Therefore by (i) the number of attractors is $2^n/2^{rd} = 2^{n-rd}$. □

From Theorem 3.9 we obtain the following two corollaries.

Corollary 3.10. *The number of states in each attractor tree is 2^{rd}.*

Corollary 3.11. *Given a linear nongroup CA $\mathbb{C}$, let T be the characteristic matrix of $\mathbb{C}$. Let d be the depth of the 0-tree of $\mathbb{C}$ and let $dimN(T) = r$. Then the number of states in the 0-tree is 2^{rd}.*

Theorem 3.12. *[2] Let $\mathbb{C}$ be SALCA having two-predecessor. If the states of the state-transition diagram of $\mathbb{C}$ are labeled such that $S_{l,k}$ be the $(k+1)$-th state in the l-th level, then the following relation holds good:*

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

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

Definition 3.13. *Let $\mathbb{C}$ be MALCA with two-predecessor and the depth of $\mathbb{C}$ be d. Let β be a nonreachable state of the α-tree of $\mathbb{C}$. Then we call the $\beta \to T\beta \to \cdots \to \alpha$ a α-basic path of the α-tree of $\mathbb{C}$.*

Remark 3.14. *Let $\mathbb{C}$ be the SALCA in Theorem 3.12 with the depth d. Then $S_{d,0} \to S_{d-1,0} \to \cdots \to S_{1,0} \to 0$ is a 0-basic path of the 0-tree of $\mathbb{C}$.*

Example 3.15. *Let $\mathbb{C}$ be a five-cell linear nongroup CA with the rule $< 204, 240, 240, 240, 240 >$. Then*

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

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 as the following:

Figure 1: The state-transition diagram of $\mathbb{C}$

$8 \to 4 \to 2 \to 1 \to 0$ *is a* 0*-basic path. The 31-basic path corresponding to the* 0*-basic path is* $23 \to 27 \to 29 \to 30 \to 31$.

Lemma 3.16. *Let $\mathbb{C}$ be MALCA with two-predecessor and let α_{ij} be the $(j+1)$-th state at level i of the α-tree of $\mathbb{C}$ and β_{ij} be the $(j+1)$-th state at level i of the β-tree of $\mathbb{C}$. Then $\alpha_{ij} \oplus \beta_{ij} = \alpha \oplus \beta$.*

Proof. Let P_{ij} be the $(j+1)$-th state at level i of the 0-tree. Then $\alpha_{ij} = P_{ij} \oplus \alpha$ and $\beta_{ij} = P_{ij} \oplus \beta$ by Corollary 3.6. Thus $\alpha_{ij} \oplus \beta_{ij} = P_{ij} \oplus \alpha \oplus P_{ij} \oplus \beta = \alpha \oplus \beta$. Therefore $\alpha_{ij} \oplus \beta_{ij} = \alpha \oplus \beta$. □

Corollary 3.17. *Let $\mathbb{C}$ be MALCA with two-predecessor (depth $= d$) and T be the characteristic polynomial of $\mathbb{C}$. If $S_{d,0} \longrightarrow S_{d-1,0} \longrightarrow \cdots \longrightarrow S_{1,0}$ is a* 0*-basic path of the* 0*-tree of $\mathbb{C}$, then $(S_{d,0} \oplus \alpha) \to (S_{d-1,0} \oplus \alpha) \to \cdots \to (S_{1,0} \oplus \alpha) \to \alpha$ is a α-basic path of the α-tree of $\mathbb{C}$.*

Proof. The proof follows from Lemma 3.16. □

The following theorem is an extension of Theorem 3.12.

Theorem 3.18. *Let $\mathbb{C}$ be MALCA having two-predecessor. If the states of the state-transition diagram of $\mathbb{C}$ are labeled such that $S^{\alpha}_{l,k}$(resp. $S_{l,k}$) be the $(k+1)$-th state in* *the l-th level of the α-tree (resp. 0-tree) in $\mathbb{C}$ and $S^{\alpha}_{l,0} = S_{l,0} \oplus \alpha$, then the following hold:*

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

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

Proof. Since $S^{\alpha}_{l,k} = S_{l,k} \oplus \alpha$ by Lemma 3.16,

$$\begin{aligned} S^{\alpha}_{l,k} &= S_{l,k} \oplus \alpha \\ &= (S_{l,0} \oplus \sum_{i=1}^{l-1} b_i S_{i,0}) \oplus \alpha \qquad by\ Theorem\ 3.12 \\ &= (S_{l,0} \oplus \alpha) \oplus \sum_{i=1}^{l-1} b_i S_{i,0} \\ &= S^{\alpha}_{l,0} \oplus \sum_{i=1}^{l-1} b_i S_{i,0} \end{aligned}$$

□

From Theorem 3.18 we obtain the following corollary.

Corollary 3.19. *Let $\mathbb{C}$ be a MALCA with two-predecessor. Given a 0-basic path of the 0-tree of $\mathbb{C}$ and the set of attractors, we can construct the state-transition diagram 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. Chowdhury, P.P. Chaudhuri, "An efficient endoding algorithm for image compression hardware based on Cellular Automata", *High Performance Computing* , Proc. 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] A.K. Das and P.P. Chaudhuri, "Efficient characterization of cellular automata", *Proc. IEE(Part E)*, **Vol. 137, No. 1**, 1990, pp. 81-87.

[5] 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.

[6] F.R. Gantmatcher, *The Theory of Matrices*, **Vol. 1**, Chelsea Publishing Co., New York, 1959.

[7] 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.

[8] 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.

[9] 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.

Department of Applied Mathematics
Pukyong National University
Pusan 608-737
KOREA
e-mail: sjcho@dolphin.pknu.ac.kr