J. KSIAM **Vol.6**, No.2, 53-62, 2002

BEHAVIOR OF TWO-PREDECESSOR MULTIPLE ATTRACTOR CELLULAR AUTOMATA

SUNG-JIN CHO AND UN-SOOK CHOI

Abstract. In this paper we analyze the behavior of linear multiple attractor cellular automata having two-predecessors.

1. Introduction

Cellular automata(abbreviately, CA) have been introduced by Von Neumann and Ulam as models of self-organizing and self-reproducing behaviors ([11], [14]). 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 a necessity in many application areas such as test pattern generation, pseudorandom number generation, cryptography, error correcting codes and signature analysis([1], [3], [7], [9], [12], [13]). The analysis of the state transition behavior of group CA was studied by many researchers ([1], [2], [4], [8]). 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. Recently some interesting properties of nongroup CA have been employed in several applications([4],[5], [8], [10], [12]). In this paper, we analyze the behavior of linear multiple attractor cellular automata having two-predecessors.

1991 Mathematics Subject Classification: 94
Key words and phrases: Cellular automata, state transition diagram, level, tree, depth
This research was supported by the Research Fund of Pukyong National University, 2001

2. CA Preliminaries

A CA consists of a number of interconnected cells arranged spatially in a regular manner [14], where the state-transitions of each cell depends 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 [14].

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	(rule 150)

The top row gives all eight possible states of the three neighboring cells (the left neighbor of the ith cell, 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, 150, 204 and 240 result in the following logic functions, where $\oplus$ denotes 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:	$q_i(t+1) = q_{i-1}(t) \oplus q_i(t)$
rule 90:	$q_i(t+1) = q_{i-1}(t) \oplus q_{i+1}(t)$
rule 102:	$q_i(t+1) = q_i(t) \oplus q_{i+1}(t)$
rule 150:	$q_i(t+1) = q_{i-1}(t) \oplus q_i(t) \oplus q_{i+1}(t)$
rule 204:	$q_i(t+1) = q_i(t)$
rule 240:	$q_i(t+1) = q_{i-1}(t)$

Definition 2.1. [6] i) *Linear CA*: If the next-state generating logic employs only XOR logic, then the CA is called an *linear* CA; otherwise it is called a *non-linear* CA.

ii) *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*.

iii) *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*.

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

v) *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.

vi) *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.

vii) *Multiple-attractor CA(MACA)*: The non-group 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*.

viii) *TPMACA*: *TPMACA* is a MACA such that every reachable state in the state-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.

ix) α*-tree*: The tree rooted at a cyclic state α is called the α*-tree*.

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 2.2. [5] The number of predecessors of a reachable state and the number of predecessors of the state 0 in a linear nongroup CA are equal.

Fig. 1 displays the state-transition diagram of a TPMACA.

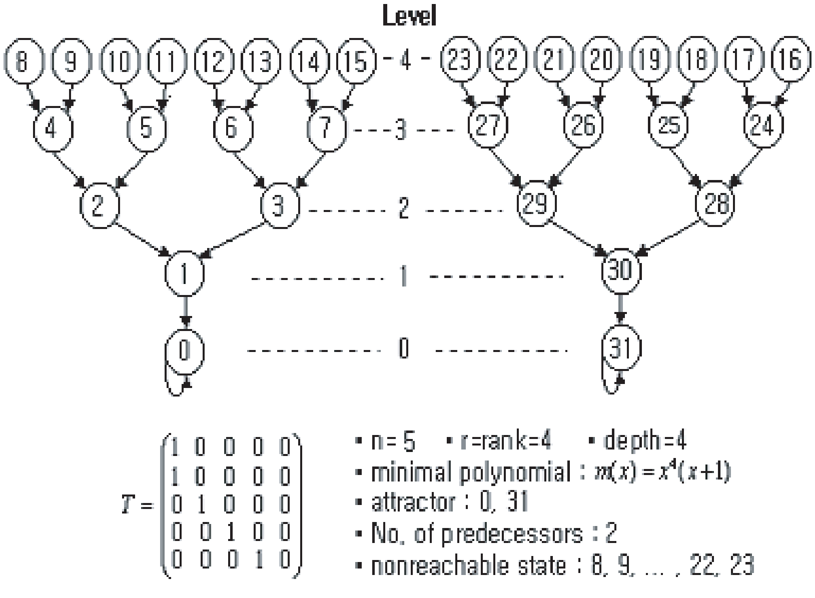

Figure 1. Structure and state-transition diagram of TPMACA

3. 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. First, we note

Lemma 3.1. [5] *Let X_m and X_n be level i states in the α-tree of a TPMACA $\mathbb{C}$. If there exist $j(\leq i)$ such that $j = \min\{k|T^k X_m = T^k X_n\}$, then $X_m \oplus X_n$ is one of level j states in the* 0*-tree of* $\mathbb{C}$.

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

Theorem 3.3. *Let $\mathbb{C}$ be a linear TPMACA. 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 $(l \geq 2)$ level of the* 0*-tree of $\mathbb{C}$, then the following hold:*
(1)

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

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 $2^{l-1}-1$.

Proof. (1) The proof will be by induction on l. For the case $l = 1$, the level 1 state is only $S_{1,0}$. For the case $l = 2$, since $S_{2,0} \oplus S_{2,1} = S_{1,0}$ by Lemma 3.1

$$\sum_{k=0}^{1} S_{2,k} = 2S_{2,0} \oplus S_{1,0}$$

Hence the statement is true for $l = 2$. Now as inductive hypothesis, assume that the statement is true for $l = m$:

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

Note that the number of states at the level m of the 0-tree of $\mathbb{C}$ is 2^{m-1}. If k is an integer, $2^r \leq k \leq 2^{r+1}-1$, then $\min\{k|T^k S_{m+1,k} = T^k S_{m+1,0}\} = r$. Therefore $S_{m+1,0} \oplus S_{m+1,k}$ $(2^r \leq k \leq 2^{r+1}-1)$ is one of level r states in the 0-tree of $\mathbb{C}$ by Lemma

3.1. Also

$$\begin{aligned}
& (S_{m+1,0} \oplus S_{m+1,2^r}) \oplus (S_{m+1,0} \oplus S_{m+1,2^r+1}) \oplus \cdots \oplus (S_{m+1,0} \oplus S_{m+1,2^{r+1}-1}) \\
= \;& (S_{m+1,0} \oplus \cdots \oplus S_{m+1,0}) \oplus (S_{m+1,2^r} \oplus S_{m+1,2^r+1} \oplus \cdots \oplus S_{m+1,2^{r+1}-1}) \\
& \qquad\qquad (the\ number\ of\ S_{m+1,0}{}'s\ is\ 2^r) \\
= \;& S_{m+1,2^r} \oplus S_{m+1,2^r+1} \oplus \cdots \oplus S_{m+1,2^{r+1}-1}
\end{aligned}$$

Hence

$$\begin{aligned}
& \sum_{k=0}^{2^m-1} S_{m+1,k} \\
= \;& (S_{m+1,0} \oplus S_{m+1,1}) \oplus (S_{m+1,2} \oplus S_{m+1,2^2-1}) \oplus (S_{m+1,2^2} \oplus \cdots \oplus S_{m+1,2^3-1}) \oplus \cdots \\
& \oplus (S_{m+1,2^{m-1}} \oplus \cdots \oplus S_{m+1,2^m-1}) \\
= \;& S_{1,0} \oplus (S_{2,0} \oplus S_{2,1}) \oplus (S_{3,0} \oplus S_{3,1} \oplus \cdots \oplus S_{3,2^2-1}) \\
& \oplus \cdots \oplus (S_{m,0} \oplus S_{m,1} \oplus \cdots \oplus S_{m,2^{m-1}-1}) \\
= \;& S_{1,0} \oplus \{2^{2-1}S_{2,0} \oplus 2^{2-2}S_{1,0}\} \oplus \{2^{3-1}S_{3,0} \oplus 2^{3-2}(S_{1,0} \oplus S_{2,0})\} \\
& \oplus \{2^{4-1}S_{4,0} \oplus 2^{4-2}(S_{1,0} \oplus S_{2,0} \oplus S_{3,0})\} \\
& \oplus \cdots \oplus \{2^{m-2}S_{m-1,0} \oplus 2^{m-3}(S_{1,0} \oplus \cdots \oplus S_{m-2,0})\} \\
& \oplus \{2^{m-1}S_{m,0} \oplus 2^{m-2}(S_{1,0} \oplus S_{2,0} \oplus \cdots \oplus S_{m-1,0})\} \\
= \;& (1 + 2^{2-2} + 2^{3-2} + 2^{4-2} + \cdots + 2^{m-3} + 2^{m-2})S_{1,0} \\
& \oplus (2^{2-1} + 2^{3-2} + 2^{4-2} + \cdots + 2^{m-3} + 2^{m-2})S_{2,0} \\
& \oplus (2^{3-1} + 2^{4-2} + \cdots + 2^{m-3} + 2^{m-2})S_{3,0} \oplus \cdots \\
& \oplus (2^{(m-1)-1} + 2^{m-2})S_{m-1,0} \oplus 2^{m-1}S_{m,0} \\
= \;& (1 + \frac{2^{m-1}-1}{2-1})S_{1,0} \oplus (2^1 + \frac{2^1(2^{m-2}-1)}{2-1})S_{2,0} \\
& \oplus (2^{3-1} + \frac{2^2(2^{m-3}-1)}{2-1})S_{3,0} \oplus \cdots \oplus (2^{m-2} + 2^{m-2})S_{m-1,0} \oplus 2^{m-1}S_{m,0} \\
= \;& 2^{m-1}S_{1,0} \oplus 2^{m-1}S_{2,0} \oplus \cdots \oplus 2^{m-1}S_{m,0} \\
= \;& 2^{m-1}(S_{1,0} \oplus \cdots \oplus S_{m,0}) \\
= \;& 2^m S_{m+1,0} \oplus 2^{m-1}(S_{1,0} \oplus \cdots \oplus S_{m,0}) \quad (because\ 2^m\ is\ even)
\end{aligned}$$

Hence the statement is true for $l = m + 1$, to complete the induction.
(2) For the case level is $l(l \leq depth)$, the proof will be by induction on k that

$$S_{l,k} \;=\; S_{l,0} \;\oplus\; \sum_{i=1}^{l-1} b_i S_{i,0} \quad (0 \leq k \leq 2^{l-1} - 1)$$

holds. For the case $k = 1$ since $S_{l,1} \oplus S_{l,0} = S_{1,0}$ by Lemma 3.1 $S_{l,1} = S_{l,0} \oplus S_{1,0}$. Hence the statement is true for $k = 1$. Now as inductive hypothesis, assume that the statement is true for $k = n$:

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

Now consider the case $k = n + 1$.
(a) For the case $n + 1$ is odd:
Let b_i^n be the i-th bit value in the binary representation of n. Since n is even, $b_1^n = 0$. Also since $n + 1$ is odd, $b_1^{n+1} = 1$. Therefore $b_1^{n+1} \oplus b_1^n = 1$. Also since n is even, $b_j^{n+1} = b_j^n$ for all j $(2 \le j \le l - 1)$. Since $TS_{l,n} = TS_{l,n+1}$, $T(S_{l,n} \oplus S_{l,n+1}) = 0$. Therefore $S_{l,n} \oplus S_{l,n+1} = S_{1,0}$. Thus

$$\begin{aligned}
S_{l,n+1} &= S_{l,n} \oplus S_{1,0} \\
&= (S_{l,0} \;\oplus\; \sum_{i=1}^{l-1} b_i^n S_{i,0}) \oplus S_{1,0} \quad (\textit{by inductive hypothesis}) \\
&= S_{l,0} \oplus b_{l-1}^n S_{l-1,0} \oplus \cdots \oplus b_2^n S_{2,0} \oplus S_{1,0} \quad (\textit{because } b_1^n = 0) \\
&= S_{l,0} \oplus b_{l-1}^{n+1} S_{l-1,0} \oplus \cdots \oplus b_2^{n+1} S_{2,0} \oplus b_1^{n+1} S_{1,0} \\
&\qquad [\textit{because } b_1^{n+1} = 0 \textit{ and } b_j^{n+1} = b_j^n \textit{ for all } j \ (2 \le j \le l-1)] \\
&= S_{l,0} \oplus \sum_{i=1}^{l-1} b_i^{n+1} S_{i,0}
\end{aligned}$$

(b) For the case $n + 1$ is even:
If $\min\{p \mid T^p S_{l,n+1} = T^p S_{l,n}\} = r,\ 2 \le r \le l - 1$, then $S_{l,n+1} \oplus S_{l,n}$ is one of level r states in the 0-tree of $\mathbb{C}$ by Lemma 3.1. Also since

$$b_i^{n+1} \oplus b_i^n = \begin{cases} 1 & \text{if} 1 \le i \le r \\ 0 & \text{if} r + 1 \le i \le l - 1 \end{cases}$$

, $S_{l,n+1} \oplus S_{l,n} = S_{r,2^{r-1}-1}$. Thus

$$\begin{aligned}
S_{l,n+1} &= S_{l,n} \oplus S_{r,2^{r-1}-1} \\
&= (S_{l,0} \oplus \sum_{i=1}^{l-1} b_i^n S_{i,0}) \oplus (S_{r,0} \oplus \sum_{i=1}^{r-1} b_i^{2^{r-1}-1} S_{i,0}) \quad (\textit{by inductive hypothesis}) \\
&= (S_{l,0} \oplus \sum_{i=1}^{l-1} b_i^n S_{i,0}) \oplus (S_{r,0} \oplus S_{r-1,0} \oplus \cdots \oplus S_{1,0}) \\
&= S_{l,0} \oplus \sum_{i=1}^{r} (b_i^n + 1) S_{i,0} \oplus \sum_{i=r+1}^{l-1} b_i^n S_{i,0} \\
&= S_{l,0} \oplus \sum_{i=1}^{r} b_i^{n+1} S_{i,0} \oplus \sum_{i=r+1}^{l-1} b_i^{n+1} S_{i,0} \quad (\because\ b_i^{n+1} = b_i^n \ \textit{for all}\ i, r+1 \leq i \leq l-1) \\
&= S_{l,0} \oplus \sum_{i=1}^{l-1} b_i^{n+1} S_{i,0}
\end{aligned}$$

Hence by (a) and (b) the statement is true for $k = n+1$, to complete the induction. □

Remark 3.4. *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 3.5. *Let $\mathbb{C}$ be a linear TPMACA 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 path*

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

a α-basic path of the α-tree in $\mathbb{C}$.

Remark 3.6. *Let $\mathbb{C}$ be a linear TPMACA in Theorem 3.3 with 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 in $\mathbb{C}$.

Lemma 3.7. *Let $\mathbb{C}$ 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 $\mathbb{C}$. Then*

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

Proof. Let $P_{i,j}$ be the $(j+1)$-th state in the i-th level of the 0-tree. Then by Theorem 4 [5] $\alpha_{i,j} = P_{i,j} \oplus \alpha$ and $\beta_{i,j} = P_{i,j} \oplus \beta$.
Therefore

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

Hence

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

□

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 3.8. *Let $\mathbb{C}$ be a linear TPMACA(depth = d) and T be the characteristic matrix of $\mathbb{C}$. 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, 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 $\mathbb{C}$.*

Example 3.9. *Let $\mathbb{C}$ be a five-cell linear nongroup CA with the rule $< 204, 240, 240, 240, 240 >$. Then the characteristic matrix T is as 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 Figure 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).

The following theorem is an extension of Theorem 3.3.

Theorem 3.10. *Let $\mathbb{C}$ be a linear TPMACA with depth d. 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 $S^{\alpha}_{l,k} = S_{l,0} \oplus \alpha$, 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 $2^{l-1} - 1$.

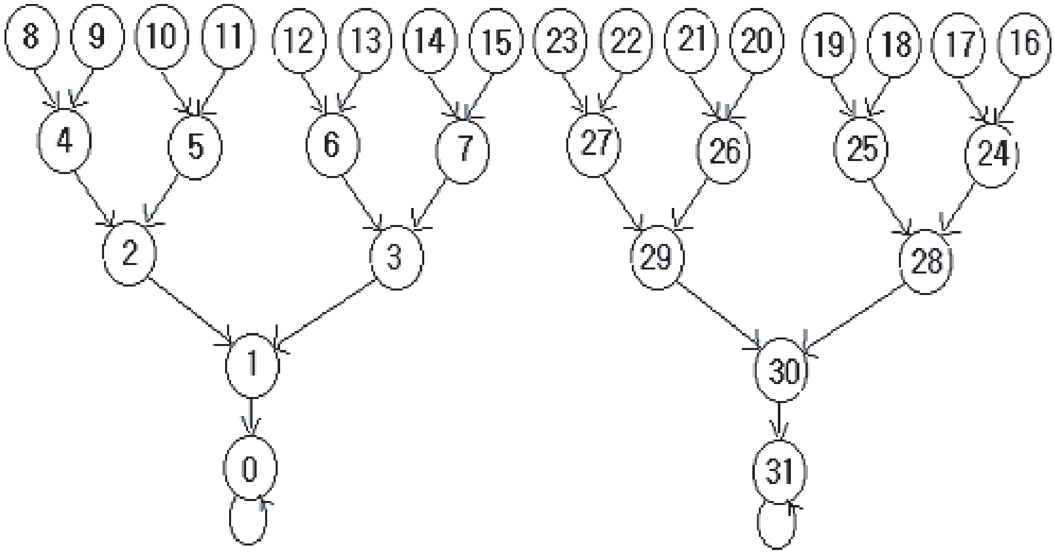

FIGURE 2. The state transition diagram of $\mathbb{C}$

Proof. Since $S^{\alpha}_{l,k} = S_{l,k} \oplus \alpha$ by Lemma 3.7,

$$\begin{aligned} S^{\alpha}_{l,k} &= (S_{l,0} \oplus \sum_{i=1}^{l-1} b_i S_{i,0}) \oplus \alpha \quad \textit{by Theorem } 3.3(2) \\ &= (S_{l,0} \oplus \alpha) \oplus \sum_{i=1}^{l-1} b_i S_{i,0} \\ &= S^{\alpha}_{l,0} \oplus \sum_{i=1}^{l-1} b_i S_{i,0} \quad \textit{by Lemma } 3.7 \end{aligned}$$

□

REFERENCES

[1] P.H. Bardell, "Analysis of cellular automata used as pseudorandom pattern generators", *Proc. IEEE int. Test. Conf.*, 1990, pp. 762-767.

[2] Kevin Cattell and Jon C. Muzio, "Analysis of one-dimensional linear hybrid cellular automata over $GF(q)$", *IEEE Trans. Computers*, **Vol. 45, No. 7**, 1996, pp. 782-792.

[3] D.R. Chowdhury, S. Basu, I. S. Gupta and P.P. Chaudhuri "Design of CAUCC-cellular automata based error correcting code", *IEEE Trans. Comput.*, **Vol. 43**, 1994, pp. 759-764.

[4] S.J. Cho, U.S. Choi and H.D. Kim, "Analysis of complemented CA derived from a linear TPMACA", Computers and Math. Appl., **(Accepted)**.

[5] 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**, 2001, pp. 91-94.

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

[7] D.R. Chowdhury, P. Subbarao and P.P. Chaudhuri "Characterization of two dimensional cellular automata using matrix algebra", *Information Sciences*, **Vol. 71**, 1993, pp. 289-314.

[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] P.D. Hortensius, R.D. McLeod and H.C. Card, "Cellular automata based signature analysis for built-in self-test", *IEEE Trans. Comput.*, **Vol. 39**, 1990, pp. 1273-1283.

[10] 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.*, 1991, pp. 1893-1896.

[11] J. Von Neumann, *Theory of self-reproducing automata*, **University of Illinois Press, Urbana**, 1996.

[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.

[13] P. Tsalides, T.A. York and A. Thanailakis, "Pseudorandom number generators for systems based on linear cellular automata", *IEE Proc(Part E) Computers Digital Techniques*, **Vol. 138**, 1991, pp. 241-249.

[14] S. Wolfram, *Statistical mechanics of cellular automata, Rev. Modern Physics*, **Vol. 55, No. 3**, 1983.

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