J. Appl. Math. & Informatics Vol. **27***(2009), No. 5 - 6, pp. 1331 - 1342*
Website: http://www.kcam.biz

ALGORITHM FOR THE CONSTRUCTION OF THE STATE TRANSITION DIAGRAM OF A SACA OVER $GF(2^p)$

UN-SOOK CHOI AND SUNG-JIN CHO*

ABSTRACT. In this paper, we analyze the behavior of the state transition of nongroup CA with a single attractor over $GF(2^p)(p > 1)$, and propose the algorithm for the construction of the state transition diagram of a Single Attractor CA(SACA) over $GF(2^p)$ which is very different from the construction algorithm for the state transition diagram of $GF(2)$ SACA.

AMS Mathematics Subject Classification : 68Q80
Key words and phrases : Cellular automata, basic path, complemented $GF(2^p)$ cellular automata, tree construction algorithm

1. Introduction

Biological self-reproduction was first investigated in terms of von Neumann's cellular automaton capable of universal computation and construction [10]. Cellular Automata(CA) are mathematical idealizations of physical systems in which space and time are discrete, and each cell assume the value either 0 or 1. The cells evolve in discrete time steps according to some deterministic rule that depends only on logical neighborhood. For the simplest case, Wolfram [17] suggested the use of a simple two-state, 3-neighborhood one-dimensional CA with cells arranged linearly in one dimension. Each cell is essentially comprised of a memory element and a combinatorial logic that generates the next-state of the cell from the present-state of its neighboring cells(left, right and self).

Das et al. [8], [9] developed a matrix algebraic tool capable of characterizing CA. CA have been employed in several applications [11] $\sim$ [16]. Cho et al. [5], [6] analyzed CA to study hash function, data storage, cryptography and so on. In particular, they proposed an algorithm for the construction of state transition

Received July 28, 2008. Revised April 6, 2009. Accepted April 18, 2009. *Corresponding author. This work was supported by the Korea Research Foundation Grant funded by the Korean Government (KRF-2009-371-B00008).

© 2009 Korean SIGCAM and KSCAM .

diagram of two predecessor multiple attractor CA over $GF(2)$ by using the concept of basic path. Also they analyzed the behavior of the state transition of the complemented nongroup $GF(2)$ CA corresponding to two predecessor linear nongroup $GF(2)$ CA.

Also, CA has been used as modeling and computing paradigm for a long time. CA has been used to model many physical systems. While studying the models of such systems, it is seen that as the complexity of the physical system increase, the $GF(2)$ CA based model becomes very complex and becomes to difficult to track analytically. Also such models fail to recognize the presence of inherent hierarchical nature of a physical system. Sikdar et al. [13], [14] and Cho et al. [4] studied hierarchical CA to overcome these problems. Sikdar et al. [14] used group CA over $GF(2^p)$ with hierarchical structure [13] for a test pattern generation. Also they used $GF(2^p)$ multiple attractor CA for the diagnosis of the defect of VLSI circuits.

In this paper, we characterize SACA over $GF(2^p)$ and propose the algorithm of the effective construction of the state transition diagram of $GF(2^p)$ SACA which is very different from the construction algorithm for the state transition diagram of $GF(2)$ SACA which is in [2]. This algorithm reduce the time-complexity by changing multiplications of matrices into additions of vectors. These results will be helpful to study data-storage, hashing by $GF(2^p)$ SACA and so on.

2. $GF(2^p)$ CA preliminaries

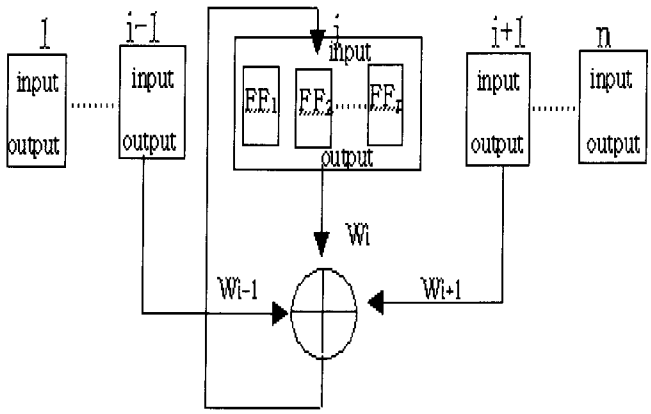

FIGURE 1. General structure of a $GF(2^p)$ CA

A $GF(2^p)$ CA can be viewed as an extension of $GF(2)$ CA. It consists of an array of cells, spatially interconnected in a regular manner, each cell being capable of storing an element of $GF(2^p)$.

Under three neighborhood restriction, the next state of the ith cell is given by a function of the weighted combination of the present states of the $(i-1)$th, ith and $(i+1)$th cells, the weights being elements of $GF(2^p)$. Thus if $q_i(t)$ is the state of the ith cell at the tth instant, then

$$q_i(t+1) = \phi\Big(w_{i-1}q_{i-1}(t), w_iq_i(t), w_{i+1}q_{i+1}(t)\Big)$$

where ϕ denotes the local transition function of the ith cell and w_{i-1}, w_i and $w_{i+1} \in GF(2^p)$ which specify the weights of interconnections as in Figure 1.

The rule for a three-neighborhood $GF(2^p)$ CA cell is represented by the vector of length 3, $< w_{i-1}, w_i, w_{i+1} >$ $\Big(w_{i-1}, w_i, w_{i+1} \in GF(2^p)\Big)$. Here w_{i-1} indicates the weight of dependence of the cell on its left neighborhood, while w_i and w_{i+1} indicate the weighted dependence on itself and its right neighborhood respectively. If the same rule vector is applied to all the cells of a $GF(2^p)$ CA, the CA is called the *uniform* $GF(2^p)$ CA, otherwise it is called the *hybrid* $GF(2^p)$ CA.

The **addition** and **multiplication** operations follow the additive and multiplicative rules of the underlying $GF(2^p)$. The polynomial which generates $GF(2^p)$ is called the *generator polynomial.*

For example, let T be the state transition matrix of a 3-cell $GF(2^2)$ CA as the following.

$$T = \begin{pmatrix} 0 & \alpha & 0 \\ \alpha & 0 & \alpha \\ 0 & \alpha^2 & 0 \end{pmatrix}$$

, where α is the generator which generates $GF(2^2)$. The elements of $GF(2^2)$ are 0, 1, α and α^2 and α is a solution of the generator polynomial $g(x) = x^2 + x + 1$. For a present state X of an n-cell $GF(2^p)$ CA, the next state Y of X is given by $Y = TX$.

Let M be a matrix whose characteristic polynomial is the generator polynomial of $GF(2^p)$. Then M is called the *generator matrix.* In the above example, the generator matrix of $g(x)$ is as the following.

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

Each state of an n-cell $GF(2^p)$ CA can be expressed as the vector which consists of n elements $\alpha^i \in GF(2^p)$. For the addition and multiplication operations over $GF(2^p)$, let α^i be the last column vector of M^i. In the above example, each α^i is given by

$$\alpha = (10)^t = 2, \quad \alpha^2 = (11)^t = 3, \quad \alpha^3 = (01)^t = 1.$$

The addition and multiplication over $GF(2^2)$ are given in Table 1.

[Table 1] Addition and multiplication over $GF(2^2)$

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Now we give the following definition which is needed in this paper.

Definition 2.1. i) Linear $GF(2^p)$ CA: If the next-state generating logic employs only XOR logic, then the $GF(2^p)$ CA is called a *linear* $GF(2^p)$ CA; otherwise it is called a *non-linear* $GF(2^p)$ CA.

ii) Complemented $GF(2^p)$ CA: *Complemented* $GF(2^p)$ CA employ XNOR logic for one or more cells of $GF(2^p)$ CA.

iii) Group $GF(2^p)$ CA: $GF(2^p)$ CA is called a *group* $GF(2^p)$ *CA* if all the states in its state transition diagram lie on cycles, otherwise it is referred to as a *non-group* $GF(2^p)$ *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 state 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 minimum number of clock cycles required to reach the nearest cyclic state from any nonreachable state in the CA state transition diagram is defined as the *depth* of the non-group CA.

viii) Level: *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.

ix) $GF(2^p)$ Single Attractor CA(SACA): The non-group $GF(2^p)$ CA for which the state transition diagram consists of a set of disjoint components forming (inverted) tree-like structures rooted at the only attractor is referred to as $GF(2^p)$ *Single Attractor CA*.

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

xi) Predecessor, Immediate predecessor: Let $X, Y \in GF(2^p)$ be states in the state transition diagram of the state transition matrix T of a given $GF(2^p)$ SACA. If $Y = T^n X$ for some $n \in \mathbb{N}$, then Y is called the predecessor of X. If $Y = TX$, then Y is called the immediate predecessor of X.

Complemented $GF(2^p)$ SACA $\mathbb{C}'$ employs XNOR logic for some cell. The use of XNOR logic implies that the next state of a particular cell is to be inverted after evaluation of its state with XOR logic. We call the inverting vector F as the *complement vector*, where non zero entries are presented in those cell positions whose transition function is dependent on XNOR logic. We call $\mathbb{C}'$ *the complemented* $GF(2^p)$ *SACA derived from* $\mathbb{C}$ *with the complement vector* F.

Define $\overline{T}$ by $\overline{T}X = TX+F$, where $X, F \in GF(2^p)$ and T is the state transition matrix of a linear $GF(2^p)$ SACA.

Then we obtain

$$\overline{T}^k X = T^k X + \left(T^{k-1} + T^{k-2} + \cdots + T + I\right)F, \ k = 1, 2, \cdots$$

3. Linear $GF(2^p)$ SACA

Let $\mathbb{C}$ be a linear n-cell $GF(2^p)$ SACA. Then $\mathbb{C}$ is a non-group $GF(2^p)$ CA and the state transition matrix T of $\mathbb{C}$ is singular. In this case the attractor is the only zero state and the depth of the state transition diagram of $\mathbb{C}$ is n. The number of all states of $\mathbb{C}$ is $(2^p)^n$ and the number of all immediate predecessors of any reachable state is 2^p by the definition of an n-cell $GF(2^p)$ SACA.

The following theorem shows the properties of the state transition matrix of a linear n-cell $GF(2^p)$ SACA.

Theorem 3.1. *Let T be the state transition matrix of a linear n-cell $GF(2^p)$ SACA $\mathbb{C}$. Then T satisfies the following properties.*

(1) The rank of T ($rank(T)$) is $n-1$.

(2) The rank of $T+I$ ($rank(T+I)$) is n.

(3) The characteristic polynomial and the minimal polynomial of T are x^n respectively.

Proof. (1) The set of all immediate predecessors of the zero state is $\left\{X \in GF(2^p) | TX = 0\right\}$. Since the number of all immediate predecessors of the zero state in the state transition diagram of $\mathbb{C}$ is $\left|\left\{X \in GF(2^p) | TX = 0\right\}\right| = 2^p$, the number of free variable of the matrix equation $TX = 0$ is one. Therefore the dimension of the null space of T ($dimN(T)$) is 1 and thus $rank(T) = n-1$.

(2) Since the attractor is the only zero state in the state transition diagram of $\mathbb{C}$,

$$N(T+I) = \{X \in GF(2^p) | (T+I)X = 0\} = \{X \in GF(2^p) | TX = X\} = \{0\}.$$

Thus $dimN(T+I)$ is zero. Hence $rank(T+I) = n$.

(3) Since the depth of the state transition diagram of $\mathbb{C}$ is n, $T^n Y = 0$ for all states $Y \in GF(2^p)$. Therefore $T^n = 0$. Hence the characteristic polynomial and minimal polynomial of T is x^n. □

Theorem 3.2. *Let $\mathbb{C}$ be a linear n-cell $GF(2^p)$ SACA. Then the sum of distinct two immediate predecessors of any reachable state in $\mathbb{C}$ is a nonzero immediate predecessor of the zero state.*

Proof. Let $X \in GF(2^p)$ be a reachable state and let $Y, Z \in GF(2^p)$ be distinct immediate predecessors of X. Then $TY = TZ = X$. Therefore $T(Y+Z) = 0$ and hence $Y+Z$ is an immediate predecessor of the zero state. Furthermore

$Y + Z \neq 0$ because $Y \neq Z$. Hence $Y + Z$ is the nonzero immediate predecessor of the zero state. □

Example 3.3. Consider the following state transition diagram of a 3-cell $GF(2^2)$ SACA with the state transition matrix

$$T = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 3 \end{pmatrix}.$$

Figure 2 shows the state transition diagram of the given $GF(2^2)$ SACA. In this figure, the sum of immediate predecessors $(333)^t$ and $(210)^t$ of $(231)^t$ is $(123)^t$, that is the nonzero immediate predecessor of the zero state.

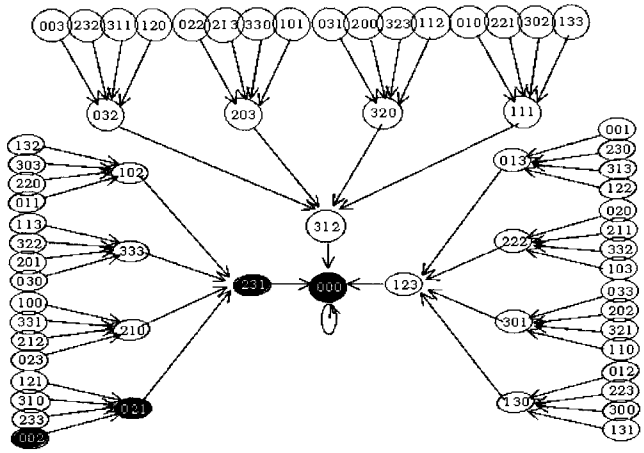

FIGURE 2. State transition diagram of a 3-cell $GF(2^2)$ SACA

Definition 3.4. Let $\mathbb{C}$ be a linear $GF(2^p)$ SACA with depth d and let T be the state transition matrix of $\mathbb{C}$. Then we call

$$X \to TX \to \cdots \to T^d X (= 0)$$

a *basic path* of the 0-tree in $\mathbb{C}$, where X is a nonreachable state of the 0-tree in $\mathbb{C}$.

Theorem 3.5. *Let $\mathbb{C}$ be a linear n-cell $GF(2^p)$ SACA. Let the kth state $S_{l,k}$ at level l in the state transition diagram of $\mathbb{C}$ be*

$$S_{l,k} = (b_l + 1)S_{l,0} + \sum_{i=1}^{l-1} b_i S_{i,0}$$

where $k = b_l b_{l-1} \cdots b_{1(2^p)}$ $\left(0 \leq k \leq (2^p)^{l-1}(2^p - 1) \right)$ is the base 2^p expansion of k. If we know a basic path of the 0-tree in $\mathbb{C}$, every state of the remaining part can be expressed as the sum of the states which lie on the basic path.

Proof. Let X be a nonreachable state in the state transition diagram of $\mathbb{C}$. Then we get the following basic path of the 0-tree.

$$X \to TX \to \cdots \to T^n X(=0)$$

Let $S_{l,0} = T^{n-l-1}X$. Then the number of the states from level 1 to level n is

$$\sum_{l=1}^{n} (2^p)^{l-1}(2^p - 1) = (2^p)^n - 1$$

Therefore the number of all states of the state transition diagram of $\mathbb{C}$ including the attractor is $\{(2^p)^n - 1\} + 1 = 2^{pn}$ which is the number of all states of n-cell $GF(2^p)$ CA. Also we get

$$\begin{aligned} TS_{l,k} &= T\left((b_l + 1)S_{l,0} + \sum_{i=1}^{l-1} b_i S_{i,0}\right) \\ &= (b_l + 1)TS_{l,0} + \sum_{i=1}^{l-1} b_i TS_{i,0} \\ &= (b_l + 1)S_{l-1,0} + b_{l-1}S_{l-2,0} + \cdots + b_2 S_{1,0} + b_1 S_{0,0} \end{aligned}$$

where $S_{0,0} = 0$. Let $k' = \left\lfloor \frac{k}{2^p} \right\rfloor$ and $k = b_l b_{l-1} \cdots b_{1_{(2^p)}}$. Then $k' = b_l b_{l-1} \cdots b_{2_{(2^p)}}$. If we put $b'_i = b_{i+1} (i = 1, 2, \cdots, l-1)$, then $k' = b'_{l-1} \cdots b'_{1_{(2^p)}}$. Therefore we obtain

$$TS_{l,k} = (b'_{l-1} + 1)S_{l-1,0} + \sum_{i=1}^{l-2} b'_i S_{i,0} = S_{l-1,k'}.$$

□

Example 3.6. In Figure 2 if we take $< 002 > \to < 021 > \to < 231 > \to < 000 >$ as the basic path of the 0-tree, then the 9th state $S_{3,9}$ at the level 3 is given by

$$S_{3,9} = 1 < 002 > +2 < 021 > +1 < 231 > = < 201 > .$$

Definition 3.7. The tree obtained by Theorem 3.5 is called *the standard tree of* $\mathbb{C}$.

4. Complemented $GF(2^p)$ SACA

The next-state function of the complemented $GF(2^p)$ SACA is given by $Y = \overline{T}X = TX + F$. For example, consider the 4-cell $GF(2^2)$ SACA $\mathbb{C}$ with the following state transition matrix T.

$$T = \begin{pmatrix} 2 & 2 & 0 & 0 \\ 2 & 0 & 2 & 0 \\ 0 & 2 & 0 & 2 \\ 0 & 0 & 2 & 2 \end{pmatrix}$$

If we take the complement vector $F = (3201)^t$, then the next state Y of the current state $X = (1203)^t$ is $Y = \overline{T}X = (2020)^t$.

Lemma 4.1. *Let $\mathbb{C}$ be a linear n-cell $GF(2^p)$ SACA and let $\mathbb{C}'$ be the complemented $GF(2^p)$ SACA derived from $\mathbb{C}$ with the complement vector F whose level is $l(1 \leq l \leq n)$ in the state transition diagram of $\mathbb{C}$. Then $\overline{T}^{l-1}F$ is the attractor of $\mathbb{C}'$.*

Proof. Since F lies at the level l in $\mathbb{C}$, $T^lF = 0$ and thus

$$\begin{aligned}\overline{T}\left(\overline{T}^{l-1}F\right) &= \overline{T}\left[T^{l-1}F + (T^{l-2} + \cdots + T + I)F\right] \\ &= T\left[(T^{l-1} + T^{l-2} + \cdots + T + I)F\right] + F \\ &= T^lF + \overline{T}^{l-1}F = \overline{T}^{l-1}F.\end{aligned}$$

Hence $\overline{T}^{l-1}F$ is the attractor of $\mathbb{C}'$. □

Theorem 4.2. *Let $\mathbb{C}$ be a linear n-cell $GF(2^p)$ SACA and let $\mathbb{C}'$ be the complemented $GF(2^p)$ SACA derived from $\mathbb{C}$ with the complement vector F whose level is $l(1 \leq l \leq n)$. Then, in the state transition diagram of $\mathbb{C}'$,*

(a) all states at levels higher than l in the state transition diagram of $\mathbb{C}$ remain unaltered,

(b) all states at levels up to $(l-1)$ in the state transition diagram of $\mathbb{C}$ are located in level l,

(c) some states at level l of $\mathbb{C}$ are rearranged in levels lower than l and the other states at level l are located in the remaining part of level l,

(d) F lies at the level $(l-1)$.

Proof. (a) By Lemma 4.1, $\overline{T}^{l-1}F$ is the attractor of $\mathbb{C}'$ and thus $\overline{T}^{k-1}F = \overline{T}^{k-2}F = \cdots = \overline{T}^{l-1}F$ for $k > l$. Let X be a state at level $k(> l)$ of $\mathbb{C}$. Then

$$\begin{aligned}\overline{T}^kX &= T^kX + \left(T^{k-1} + \cdots + I\right)F \\ &= \overline{T}^{k-1}F(\text{ because } T^kX = 0) \\ &= \overline{T}^{l-1}F.\end{aligned}$$

Thus the level of X is at most k in $\mathbb{C}'$. And

$$\begin{aligned}\overline{T}^{k-1}X &= T^{k-1}X + \left(T^{k-2} + \cdots + T + I\right)F \\ &= T^{k-1}X + \overline{T}^{k-2}F \\ &= T^{k-1}X + \overline{T}^{l-1}F \\ &\neq \overline{T}^{l-1}F \text{ because } T^{k-1}X \neq 0.\end{aligned}$$

Hence X lies at level k in $\mathbb{C}'$.

(b) Let W be a state at level $i(< l)$ of $\mathbb{C}$. Then

$$T^iW = T^{i+1}W = \cdots = T^lW = 0$$

And thus

$$\overline{T}^lW = T^lW + \Big(T^{l-1} + \cdots + I\Big)F = \overline{T}^{l-1}F$$

But

$$\begin{aligned}\overline{T}^{l-1}W &= T^{l-1}W + \Big(T^{l-1} + \cdots + I\Big)F \\ &= T^{l-1}W + \overline{T}^{l-2}F \\ &= \overline{T}^{l-2}F \neq \overline{T}^{l-1}F\end{aligned}$$

Since $\overline{T}^{l-1}F$ is the attractor of $\mathbb{C}'$ by Lemma 4.1, W is on the level l of $\mathbb{C}'$

(c) Since the number of all states at levels up to $l-1$ is

$$1 + (2^p - 1) + 2^p(2^p - 1) + \cdots + (2^p)^{l-2}(2^p - 1) = (2^p)^{l-1}$$

the number of level l states which are remained unaltered in $\mathbb{C}'$ is $(2^p)^{l-1}(2^p - 1)$. Hence the results of (c) are obtained from (a) and (b).

(d) By (b) the state 0 is the level l state in $\mathbb{C}$. Since $\overline{T}0 = T0 + F = F$, F lies on the level $l-1$. □

The following Table 2 shows the alteration of states of a linear SACA over $GF(2^p)$.

[Table 2] Alteration of the states of a linear $GF(2^p)$ SACA

Linear $GF(2^p)$ SACA	Complemented $GF(2^p)$ SACA
States at levels higher than level l	The level is unchanged
States at levels lower than level l	Rearranged at level l
Complement vector F	F lies at level $(l-1)$
States at level l	Rearranged at levels lower than or equal to l

Theorem 4.3. *Let $\mathbb{C}$ be a linear n-cell $GF(2^p)$ SACA and $\mathbb{C}'$ be the complemented SACA derived from $\mathbb{C}$ with the given complement vector. Let $S_{n,0} \to S_{n-1,0} \to \cdots \to S_{0,0}(= 0)$ be the basic path in the standard tree of $\mathbb{C}$ and let $\overline{S}_{n,0} \to \overline{S}_{n-1,0} \to \cdots \to \overline{S}_{0,0}$ be a basic path in $\mathbb{C}'$. Then every state of the remaining part can be expressed as the sum of the states which lie on the basic path of $\mathbb{C}'$.*

Proof. Let $S_{n,0} \to S_{n-1,0} \to \cdots \to S_{0,0}(= 0)$ be the basic path in the standard tree of $\mathbb{C}$ and let $\overline{S}_{n,0} \to \overline{S}_{n-1,0} \to \cdots \to \overline{S}_{0,0}$ be a basic path in $\mathbb{C}'$. In the state transition diagram of $\mathbb{C}$ the kth state at the level l is

$$S_{l,k} = (b_l + 1)S_{l,0} + \sum_{i=1}^{l-1} b_i S_{i,0},$$

where $k = b_l b_{l-1} \cdots b_{1(2^p)}$, $0 \leq k \leq (2^p)^{l-1}(2^p - 1)$ by Theorem 3.5.

Then the number of all states from level 1 to level n is given by

$$\sum_{l=1}^{n}(2^p)^{l-1}(2^p-1) = (2^p)^n - 1.$$

Thus the number of all states of the state transition diagram in $\mathbb{C}'$ including the attractor is $(2^p)^n - 1 + 1 = 2^{pn}$. This is equal to the number of all states in $\mathbb{C}'$. Let

$$\overline{S}_{l,k} = \overline{S}_{l-1,0} + (b_l + 1)S_{l,0} + \sum_{i=1}^{l-1} b_i S_{i,0}.$$

Then we get

$$\begin{aligned}
\overline{T}\,\overline{S}_{l,k} &= T(\overline{S}_{l,k}) + F \\
&= T\left(\overline{S}_{l-1,0} + (b_l+1)S_{l,0} + \sum_{i=1}^{l-1} b_i S_{i,0}\right) + F \\
&= T\overline{S}_{l-1,0} + F + (b_l+1)S_{l-1,0} + \sum_{i=1}^{l-2} b_{i+1}S_{i,0} \\
&= \overline{S}_{l-2,0} + (b'_{l-1}+1)S_{l-1,0} + \sum_{i=1}^{l-2} b'_i S_{i,0} \\
&= \overline{S}_{l-1,k},
\end{aligned}$$

where $k' = \left\lfloor \frac{k}{2^p} \right\rfloor = b_l b_{l-1}\cdots b_{2(2^p)} = b'_{l-1}\cdots b'_{1(2^p)}$.

Hence we can get the state transition diagram of $\mathbb{C}'$. □

5. Algorithm for the tree construction of $GF(2^p)$ SACA

From Theorems 3.5, 4.2 and 4.3, we propose the following algorithm for the construction of the state transition diagrams of $GF(2^p)$ SACA $\mathbb{C}$ and $GF(2^p)$ SACA $\mathbb{C}'$ derived from $\mathbb{C}$ with a given complement vector F. This algorithm does not hold for $p = 1$. This means that the construction algorithms for the state transition diagram of the $GF(2^p)(p > 1)$ SACA $\mathbb{C}$ and the state transition diagram of the $GF(2^p)(p > 1)$ SACA $\mathbb{C}'$ are different from the construction algorithms for the state transition diagram of the $GF(2)$ SACA $\mathbb{C}$ and the state transition diagram of the $GF(2)$ SACA $\mathbb{C}'$ derived from a $\mathbb{C}$ with some complement vector.

Tree_Construction_Algorithm

/* Tree construction of a linear $GF(2^p)$ SACA $\mathbb{C}$ */

Step 1. Find a nonreachable state X in the 0-tree satisfying
$T^n X = 0$ and $T^{n-1}X \neq 0$, For the state transition matrix T of $\mathbb{C}$

Step 2. Find the following basic path of $\mathbb{C}$ by using X.

$$X(=S_{n,0}) \to TX(=S_{n-1,0}) \to \cdots \to 0$$

Step 3. Construct the 0-tree by the equation

$$S_{l,k} = (b_l + 1)S_{l,0} + \sum_{i=1}^{l-1} b_i S_{i,0}.$$

/* Tree construction of the complemented $GF(2^p)$ SACA $\mathbb{C}'$ derived from $\mathbb{C}$ with the complement vector F */

Step 4. Find the basic path of $\mathbb{C}'$ derived from $\mathbb{C}$ with complement vector F.

If the complement vector F is a nonreachable state of $\mathbb{C}$, **then** the basic path of $\mathbb{C}'$ is given by

$$0(=\overline{S}_{n,0}) \to \overline{T}0(=\overline{S}_{n-1,0}) \to \cdots \to \overline{T}^n 0(=\overline{S}_{0,0});$$

else the basic path of $\mathbb{C}'$ is given by

$$X(=\overline{S}_{n,0}) \to \overline{T}X(=\overline{S}_{n-1,0}) \to \cdots \to \overline{T}^n X(=\overline{S}_{0,0}),$$

where X is a nonreachable state in Step 1.

Step 5. Construct the tree of $\mathbb{C}'$ by using the equation

$$\overline{S}_{l,k} = \overline{S}_{l-1,0} + (b_l + 1)S_{l,0} + \sum_{i=1}^{l-1} b_i S_{i,0}.$$

6. Conclusion

In this paper we analyzed the behavior of the state transition of the complemented $GF(2^p)$ SACA derived from a linear $GF(2^p)$ SACA.

And we proposed the algorithm for the construction of the state transition diagram of $GF(2^p)$ SACA by using the basic paths of a linear $GF(2^p)$ SACA $\mathbb{C}$ and the complemented $GF(2^p)$ $\mathbb{C}'$ SACA derived from $\mathbb{C}$ with some complement vector. This algorithm reduced the time-complexity by changing multiplications of matrices into additions of vectors. This work will be helpful for the generation of CA based hashing functions by using a $GF(2^p)$ SACA.

References

1. C. Chattopadhyay, Some studies on theory and applications of additive Cellular Automata, Ph. D. Thesis, I.I.T., Kharagpur, India, (2002).
2. S.J. Cho, U.S. Choi and H.D. Kim, *Analysis of complemented CA derived from a linear TPMACA,* Computers and Mathematics with Applications **45** Issues 4-5 (2003) 689-698.
3. S.J. Cho, U.S. Choi and H.D. Kim, *Behavior of complemented CA whose complement vector is acyclic in a linear TPMACA,* Mathematical and Computer Modelling **36** Issues 9-10 (2002), 979-986.

4. S.J. Cho, U.S. Choi, Y.H. Hwang, H.D. Kim and H.H. Choi, Behaviors of single attractor cellular automata over Galois field $GF(2^p)$, In *Proc. ACRI 2006 LNCS* **4173** (2006), 232-237.
5. S.J. Cho, U.S. Choi, H.D. Kim, Y.H. Hwang, J.G. Kim and S.H. Heo, *New synthesis of one-dimensional 90/150 linear hybrid group cellular automata, IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.* **26** (9) (2007) 1720-1724.
6. S.J. Cho, U.S. Choi, Y.H. Hwang, Y.S. Pyo, H.D. Kim and S.H. Heo, Computing Phase Shifts of Maximum-Length 90/150 Cellular Automata Sequences, *Lecture Notes in computer Science* **3305** (2004), 31-39.
7. A.K. Das, *Additive Cellular Automata: Theory and Applications as a Built-In Self-Test Structure,* Ph. D. Thesis, I.I.T. Kharagpur, India, (1990).
8. A.K. Das and P.P. Chaudhuri, Efficient characterization of cellular automata, *Proc. IEE(Part E)* **137** (1) (1990), 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.* **42** (1993), 340-352.
10. J. Von Neumann, *Theory of self-reproducing automata,* University of Illinois Press Urbana, IL, (1966).
11. S. Nandi, B.K. Kar and P.P. Chaudhuri, Theory and applications of cellular automata in cryptography, *IEEE Trans. Computers* **43** (1994), 1346-1357.
12. K. Paul, Theory and Application of $GF(2^p)$ Cellular Automata, Ph. D. Thesis, B.E. College (Deemed University), Howrah, India, (2002).
13. B.K. Sikdar, N. Ganguly, P. Majumder and P.P. Chaudhuri, *Design of Multiple Attractor $GF(2^p)$ Cellular Automata for Diagnosis of VLSI Circuits,* VLSI Design, Fourteenth International Conference on 2001 (2001), 454-459.
14. B.K. Sikdar, P. Majumder, M. Mukherjee, N. Ganguly, D.K. Das and P.P. Chaudhuri, *Hierarchical Cellular Automata as an On-Chip Test Pattern Generator,* VLSI Design, Fourteenth International Conference on 2001 (2001), 403-408.
15. S. Sen, C. Shaw, D.R. Chowdhury, N. Ganguly and P.P. Chaudhuri, Cellular automata based cryptosystem, *Proc. ICICS* (2002), 303-314.
16. P. Tsalides, T.A. York and A. Thanailakis, Pseudo-random number generators for VLSI systems based on linear cellular automata, *IEE Proc. E. Comput. Digit. Tech.* **138** (1991), 241-249.
17. S. Wolfram, Statistical mechanics of cellular automata, *Rev. Modern Physics,* **55** (3) (1983), 601-644.

Un-Sook Choi received her Ph.D at Pukyong National University. Since 2006 she has been at the Tongmyoung University. Her research interests center on Cellular Automata, Cryptography and Coding Theory.

Department of Multimedia Engineering, Tongmyoung University, Busan 608-711, Korea
e-mail: choies@@pknu.ac.kr

Sung-Jin Cho received his Ph.D at Korea University. Since 1988 he has been at the Pukyong National University. His research interests center on Cellular Automata, Cryptography and Coding Theory.

Division of Mathematical Sciences, Pukyong National University, Busan 608-737, Korea
e-mail: sjcho@@pknu.ac.kr