J. Appl. Math. & Informatics Vol. **34***(2016), No. 3 - 4, pp. 239 - 247*
http://dx.doi.org/10.14317/jami.2016.239

ANALYSIS OF COMPLEMENTED GROUP CA DERIVED FROM 90/150 GROUP CA

MIN-JEONG KWON, SUNG-JIN CHO*, HAN-DOO KIM, UN-SOOK CHOI AND GIL-TAK KONG

Abstract. In recent years, CA has been applied to image security due to its simple and regular structure, local interaction and random-like behavior. Since the initial state is regenerated after some iterations in the group CA, the receiver is able to decrypt by the same CA. Pries et al. showed that the all lengths of the cycles in the complemented group CA **C** with rules 195, 153, and 51 are equal to the order of **C**. Nandi et al. reported the encryption technique using **C**. These results can be made efficient use in cryptosystem by expanding the Nandi's key space. In this paper, we analyze the order of the complemented group CA derived from 90/150 group CA and show that all the lengths of the cycles in the complemented CA are equal to the order of the complemented CA.

AMS Mathematics Subject Classification : 97N70, 11G25, 94A55, 68Q87.
Key words and phrases : Cellular Automata, complement vector, order, complemented group CA, length of cycle.

1. Introduction

The concept of cellular automata(henceforth CA) was originally discovered in the 1940s by Ulam and von Neumann who suggested using a discrete system for creating a reductionist model of self-replication [10, 13]. In 1960s, CA were studied as a particular type of dynamical system and the connection with the mathematical field of symbolic dynamics [6]. In 1980s, Wolfram engaged in a systematic study of one-dimensional CA and claimed that CA have applications in many fields of science. These include computer processors and cryptography [14]. Applications of CA in various fields have been proposed in [8, 11].

In recent years, CA has also been applied to image security due to its simple and regular structure, local interaction and random-like behavior [1, 7]. In the case of the group CA, information is preserved during the iteration. With this

Received December 9, 2015. Revised February 27, 2016. Accepted March 4, 2016.
*Corresponding author.

property, group CA can be made full use in cryptosystem. The CA rule is the key and the final configuration which is obtained by forward iteration of the CA for fixed time steps is an encrypted image.

In the group CA, since the initial state is regenerated after some iterations, the receiver is able to decrypt by the same CA. It was already known that the complemented CA derived from a group CA is also a group CA.

Pries et al.[11] showed that the all lengths of the cycles in the complemented group CA $\mathbf{C}$ with rules 195, 153, and 51 are equal to the order of $\mathbf{C}$. And Nandi et al. reported the encryption technique using $\mathbf{C}$ in [9]. They also used $F = (11\cdots1)^t$ as the complement vector to derive the complemented CA.

But if we use the rules 90 and 150 to generate the next state of each cell, the randomness is more strong since the dependency of the next state to its neighbor of the present state is higher than the dependency by the rules 60, 102, and 204. And we can use the results of Cho et al. to synthesize the CA according to the minimal polynomial [2, 3, 4].

In this paper, we analyze the order of the complemented group CA derived from 90/150 group CA and find the complement vectors F such that the all lengths of cycles are equal to the order of the complemented group CA derived from 90/150 group CA and F.

2. Preliminaries

CA consist of cells on a line where each cell has two possible values 0 or 1. Each configuration of CA evolves in discrete time steps and the next state is decided by the cell to its left, the cell itself, and the cell to its right, according to the combinational logic known as a rule. The next state transition function can be expressed as follows;

$$x_i(t+1) = f(x_{i-1}(t), x_i(t), x_{i+1}(t)),$$

where $x_i(t)$ is the ith cell at the tth time step and f is a rule of the CA. Since there are 2^3 possible states for the three cells neighboring a given cell, there are 2^{2^3} distinct mappings from all these neighborhood configurations to the next state, each of which can be indexed with an 8-bit binary number. For example,

$x_{i-1}(t)x_i(t)x_{i+1}(t)$	:	111	110	101	100	011	010	001	000	
$x_i(t+1)$	:	0	1	0	1	1	0	1	0	(Rule 90)
$x_i(t+1)$	:	1	0	0	1	0	1	1	0	(Rule 150)

The corresponding logic for rule 90 is $x_i(t+1) = x_{i-1}(t) \oplus x_{i+1}(t)$ and for rule 150 is $x_i(t+1) = x_{i-1}(t) \oplus x_i(t) \oplus x_{i+1}(t)$.

A CA having only XOR logic is called a linear CA and the corresponding rule is called a linear rule. In the case of the rules involving XNOR logic, the CA is called a complemented CA and the corresponding rule is called a complemented rule. In this paper, we will employ the rule 90, rule 150 and the null boundary conditions in which the boundary of the extreme cells is imposed as all 0(henceforth NBCA).

An n-cell linear CA is specified by $n \times n$ state transition matrix operating over GF(2) which can be represented as the following tridiagonal matrix[5].

$$\begin{pmatrix} d_1 & a_{1,2} & 0 & \cdots & 0 & 0 \\ a_{2,1} & d_2 & a_{2,3} & \cdots & 0 & 0 \\ 0 & a_{3,2} & d_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a_{n,n-1} & d_n \end{pmatrix}$$

In the matrix, the principal diagonal specifies the self-dependency if the next state of the ith cell depends on its present state. The other two diagonals specify the dependency of the corresponding cell on its left and right neighbors. Since all the entries in the other two diagonals of the state transition matrix are 1 for the rules 90 and 150, we abbreviate the matrix T as $T_n = \langle d_1, d_2, d_3, \cdots, d_n \rangle$, where each d_i is 0 or 1. That is, if the rule for the ith cell is rule 150, then $d_i = 1$. Similarly $d_i = 0$ represents the rule 90 for the rule of the ith cell. So T_n can also represent the rule vector for the CA. If $X(t)$ stands for the state of the CA at the tth instant of time, then the state $X(t+1)$ at the next time instant can be represented as $X(t+1) = TX(t)$. Since the XNOR logic cannot be represented in the multiplicative notation, the state transition funcion for the complemented CA is symbolically represented as $\bar{T}$ for the state transition matrix T of the corresponding CA with XOR logic only. Thus the next state of the complemented CA is $X(t+1) = TX(t) \oplus F$, where F is the complement vector which has significant entries in places of the cell positions where the inversion is required.

Lemma 2.1 ([5]). *If $\bar{T}^p$ denotes p times application of the complemented CA operator $\bar{T}$, then $\bar{T}^p X(t) = \left(I \oplus T \oplus T^2 \oplus \cdots \oplus T^{p-1}\right) F \oplus T^p X(t)$, where F is the complement vector.*

The characteristic polynomial of a matrix T is given by $|T \oplus xI|$ and the minimal polynomial of T is the minimum degree factor of the characteristic polynomial that is annihilated by T. In general, the characteristic polynomial is different from the minimal polynomial for a matrix. However for the state transition matrix T of the rules 90 and 150, the two polynomials are identical [12].

Definition 2.2. A CA is called a group CA if $det(T) = 1$, where T is the state transition matrix for the CA and $det(T)$ is the determinant of T. In a group CA, all states of the CA form cycles. And for a positive integer m, $T^m = I$ where I is the identity matrix.

Das et al. [5] reported that the complement of a group CA is also a group CA. And Pries et al. [11] investigated the order of the complemented group CA derived from the group CA with rules 195, 153, and 51. We analyze the relation between the orders of the complemented CA and the corresponding non-complemented 90/150 group NBCA. And we show the structure of the cycles in the complemented group CA.

Theorem 2.3 ([2]). *For the* 90/150 *k-cell group CA, let* $T_k = \langle d_1, d_2, \cdots, d_k \rangle$ *be the rule vector for the CA, where* $d_i = 0$ *for the rule* 90 *and* $d_i = 1$ *for the rule* 150 *at the ith cell. Then the followings hold :*

(1) $\langle d_1, d_2, \cdots, d_k \oplus 1, d_k \oplus 1, \cdots, d_2, d_1 \rangle$ *is a* $2k$*-cell group CA with the minimal polynomial* $(x+1)^{2k}$.
(2) $\langle d_1, d_2, \cdots, d_k, 1, d_k, \cdots, d_2, d_1 \rangle$ *is a* $2k+1$*-cell group CA with the minimal polynomial* $(x+1)^{2k+1}$.

3. The Structure of the Complemented CA

Lemma 3.1. *For the state transition matrix* T *of the* n*-cell group NBCA* $\mathbf{C}$ *with the minimal polynomial* $m_T(x) = (1+x)^n, 2^{r-1} < n \leq 2^r$ $(r = 2, 3, 4, \cdots)$, *let* $\bar{T}$ *be the state transition function of the complemented group CA* $\bar{\mathbf{C}}$ *derived from* $\mathbf{C}$ *and the complement vector* $F = (f_1 f_2 \cdots f_n)^t$, $f_i = 0$ *or* 1 $(1 \leq i \leq n)$. *Then* $ord(T) \leq ord(\bar{T})$, *where ord(T) is the order of T.*

Proof. If $ord(T) = p$ and $ord(\bar{T}) = k$, then $p = 2^r$ from $2^{r-1} < n \leq 2^r$. Suppose that $k = \frac{p}{2}$, then $k = 2^{r-1}$ and for all the states $\mathbf{X}$ in $\mathbf{C}$, $\bar{T}^k \mathbf{X} = \mathbf{X}$. So $\bar{T}^k \mathbf{X} = \left(I \oplus T \oplus T^2 \oplus \cdots \oplus T^{k-1}\right) F \oplus T^k \mathbf{X}$. Then $\left(I \oplus T \oplus T^2 \oplus \cdots \oplus T^{k-1}\right) F = (I \oplus T)^{k-1} F = \left(I \oplus T^k\right) \mathbf{X} = (I \oplus T)^k \mathbf{X}$.

Since $rank\left((I \oplus T)^k\right) = n - k$, $dim N\left((I \oplus T)^k\right) = k$ and thus $N\left((I \oplus T)^{k-1}\right) \subset N\left((I \oplus T)^k\right)$, where $N(A)$ is the null space of A.

(i) If $F \in N\left((I \oplus T)^{k-1}\right)$, then $(I \oplus T)^{k-1} F = \mathbf{0}$ but $(I \oplus T)^k \mathbf{X} \neq \mathbf{0}$ for $X \notin N\left((I \oplus T)^k\right)$. This is a contradiction.

(ii) If $F \in N\left((I \oplus T)^k\right) \setminus N\left((I \oplus T)^{k-1}\right)$, then $(I \oplus T)^{k-1} F \neq \mathbf{0}$ but $(I \oplus T)^k \mathbf{X} = \mathbf{0}$ for $\mathbf{X} = F$. This is a contradiction.

(iii) If $F \notin N\left((I \oplus T)^k\right)$, then $(I \oplus T)^{k-1} F \neq \mathbf{0}$ but $(I \oplus T)^k \mathbf{X} = \mathbf{0}$ for $\mathbf{X} \in N\left((I \oplus T)^{k-1}\right)$. This is a contradiction.

By (i), (ii) and (iii), $(I \oplus T)^{k-1} F \neq (I \oplus T)^k \mathbf{X}$. So $ord(\bar{T}) > \frac{p}{2}$ and thus $ord(\bar{T}) \geq p$. □

The following lemma can be proved by Lemma 3.1 and the proof of Lemma 4.5.1 in [5].

Lemma 3.2. *For the state transition matrix* T *of the* n*-cell group NBCA* $\mathbf{C}$ *with the minimal polynomial* $(1+x)^n$, $2^{r-1} < n \leq 2^r$ $(r = 2, 3, 4, \cdots)$, *let* $\bar{T}$ *be the state transition function of the complemented group CA* $\bar{\mathbf{C}}$ *derived from* $\mathbf{C}$ *with the complement vector* $F = (f_1 f_2 f_3 \cdots f_n)^t$, $f_i = 0$ *or* 1 $(1 \leq i \leq n)$. *If* $ord(T) = p$, *then* $ord(\bar{T}) = p$ *or* $ord(\bar{T}) = 2p$.

The following theorem is very important for the results in this paper.

Theorem 3.3. *For the state transition matrix T_n of the n-cell 90/150 group NBCA* $\mathbf{C}$ *with the minimal polynomial* $(1+x)^n$, $n = 2, 3, \cdots$, *let* $S_n = (I \oplus T_n)^{n-1}$. *Then the matrices* S_{2n} *and* S_{2n+1} *can be obtained from* S_n *as followings;*

$$S_{2n} = \begin{pmatrix} S_n & S_n \\ S_n & S_n \end{pmatrix} \text{ and } S_{2n+1} = \begin{pmatrix} S_n & \mathbf{0}_n & S_n \\ {\mathbf{0}_n}^t & 0 & {\mathbf{0}_n}^t \\ S_n & \mathbf{0}_n & S_n \end{pmatrix},$$

where $\mathbf{0_n}$ *is the* $n \times 1$ *zero matrix.*

Proof. For the case of $n = 2$, we can easily confirm the theorem.

For the case of $n = k$, let $\langle r_1, r_2, \cdots, r_k \rangle$ be the rule vector of $I \oplus T_k$. Then $\langle r_1, \cdots, r_{k-1}, \bar{r_k}, \bar{r_k}, r_{k-1}, \cdots, r_1 \rangle$ is the rule vector of $I \oplus T_{2k}$ by Theorem 2.3. Let $S_k = \begin{pmatrix} A_1 \\ A_2 \\ \vdots \\ A_k \end{pmatrix}$ and $S_{2k} = \begin{pmatrix} B_1 \\ B_2 \\ \vdots \\ B_{2k} \end{pmatrix}$, where $A_i\,(resp.B_i)$ is the ith row of $S_k\,(resp.S_{2k})$ for $1 \le i \le k$. Since $(I \oplus T_k)\,S_k = O_k$ and $(I \oplus T_{2k})\,S_{2k} = O_{2k}$,

$$\begin{cases} r_1 A_1 + A_2 = O, \\ A_1 + r_2 A_2 + A_3 = O, \\ \quad \vdots \\ A_{k-2} + r_{k-1} A_{k-1} + A_k = O \end{cases} \tag{3.1}$$

and

$$\begin{cases} r_1 B_1 + B_2 = O, \\ B_1 + r_2 B_2 + B_3 = O, \\ \quad \vdots \\ B_{k-2} + r_{k-1} B_{k-1} + B_k = O, \\ B_{k-1} + \bar{r_k} B_k + B_{k+1} = O, \\ B_k + \bar{r_k} B_{k+1} + B_{k+2} = O, \\ \quad \vdots \\ B_{2k-1} + r_1 B_{2k} = O \end{cases} \tag{3.2}$$

Since $rank\,(I \oplus T_k) = k - 1$, the relation of $A_i\,(i = 1, 2, \cdots, k)$ is determined by the first $(k-1)$ equations of (3.1). Thus the relation of $B_i\,(i = 1, 2, \cdots, k)$ is determined by the first $(k-1)$ equations of (3.2).

Let $S_k = (U_1 U_2 \cdots U_k)$ and $S_{2k} = (V_1 V_2 \cdots V_{2k})$. Since $S_k\,(I \oplus T_k) = O_k$ and $S_{2k}\,(I \oplus T_{2k}) = O_{2k}$, we can show that the relation of V_i is equal to the relation of U_i by the similar method for $i = 1, 2, \cdots, k$. Let $S_{2k} = \begin{pmatrix} W_1 & W_2 \\ W_3 & W_4 \end{pmatrix}$, where W_i is a $k \times k$ submatrix. Then $W_1 = S_k$. By the same reason, we obtain $W_4 = S_k$. From $rank\,(S_k) = 1$, we obtain $W_2 = W_3 = S_k$. Hence $S_{2k} = \begin{pmatrix} S_k & S_k \\ S_k & S_k \end{pmatrix}$.

In the case of $S_{2k+1} = (I \oplus T_{2k+1})^{2k}$, the rule vector of $I \oplus T_{2k+1}$ is $\langle r_1, \cdots, r_{k-1}, r_k, 0, r_k, r_{k-1}, \cdots, r_1 \rangle$ from Theorem 2.3. If Y_i is the ith row of S_{2k+1} for $1 \le i \le k$, then $Y_l = Y_{k+l+1}$ for $1 \le l \le k$, since $\langle r_1, \cdots, r_{k-1}, r_k, 0, r_k, r_{k-1}, \cdots, r_1 \rangle$

is symmetric with respect to the center and $(I \oplus T_{2k+1})\, S_{2k+1} = O_{2k+1}$. Moreover the first k entries of Y_i and the last k entries of Y_{k+1+i} are equal to the first k entries of the ith row of S_k for $1 \le i \le k$.

Since $rank\,(I \oplus T_k) = k-1$, the kth row of $I \oplus T_{2k+1}$ is changed to $(0\ 0 \cdots 0 \overset{(k+1)th}{1}\ 0 \cdots 0\ 0)$ by the elementary row operation. Thus the $(k+1)$th row of $(I \oplus T_{2k+1})\, S_{2k+1}$ is Y_{k+1}. Therefore Y_{k+1} is the zero vector. With the same reason, the $(k+1)$th column of S_{2k+1} should be the zero column. Hence

$$S_{2k+1} = \begin{pmatrix} S_k & \mathbf{0}_k & S_k \\ {\mathbf{0}_k}^t & 0 & {\mathbf{0}_k}^t \\ S_k & \mathbf{0}_k & S_k \end{pmatrix}.$$

□

Corollary 3.4. *Let T_n be the state transition matrix of the n-cell 90/150 group NBCA with the minimal polynomial $(1+x)^n$, where $n = 2^r$, $r = 1, 2, \cdots$. Then*

$$(I \oplus T_n)^{n-1} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix}$$

Proof. Since T_2 is $\langle 0, 0\rangle$, $(I \oplus T_2)^1 = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$. By Theorem 3.3, we obtain $(I \oplus T_n)^{n-1}$ consisting of all columns with entries 1s. □

Example 3.5. For $T_3 = \langle 1, 1, 1\rangle$, $S_3 = (I \oplus T_3)^2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}$. Then

$$S_6 = (I \oplus T_6)^5 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} S_3 & S_3 \\ S_3 & S_3 \end{pmatrix},$$

$$S_7 = (I \oplus T_7)^6 = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} S_3 & \mathbf{0_3} & S_3 \\ {\mathbf{0_3}}^t & 0 & {\mathbf{0_3}}^t \\ S_3 & \mathbf{0_3} & S_3 \end{pmatrix},$$

where $\mathbf{0_3}$ is the 3×1 zero matrix.

The following two theorems are main results in this paper.

Theorem 3.6. *Let* $\mathbf{C}$ *be the* n*-cell* 90/150 *group NBCA with the minimal polynomial* $(1+x)^n$, $2^{r-1} < n \leq 2^r$ $(r = 2, 3, 4, \cdots)$. *And let* $\bar{\mathbf{C}}$ *be the complemented CA derived from* $\mathbf{C}$ *with the complement vector* $F = (f_1 f_2 \cdots f_n)^t$ *with* $f_i = 0$ *or* 1, $1 \leq i \leq n$. *If* $ord(T) = p$ *for the state transition matrix* T *of* $\mathbf{C}$, *then* $ord(\bar{T})$ *for the state transition function* $\bar{T}$ *of* $\bar{\mathbf{C}}$ *satisfies the following;*

$$ord(\bar{T}) = \begin{cases} 2^r, & 2^{r-1} < n < 2^r, \\ 2^{r+1}, & n = 2^r and \sum_{i=1}^{n} f_i \equiv 1 \,(mod 2)\,, \\ 2^r, & n = 2^r and \sum_{i=1}^{n} f_i \equiv 0 \,(mod 2)\,. \end{cases}$$

Proof. For $ord(T) = p$, let $ord(\bar{T}) = k$ for some positive integer k.

(i) In case of $2^{r-1} < n < 2^r$:

From $T^{2^r} = I$, we obtain $p = 2^r$ and $\bar{T}^p\mathbf{X} = \left(I \oplus T \oplus T^2 \oplus \cdots \oplus T^{p-1}\right) F \oplus T^p\mathbf{X} = (I \oplus T)^{p-1} F \oplus \mathbf{X}$. Since $(I \oplus T)^n = O$ and $n \leq p-1$, $(I \oplus T)^{p-1} F = \mathbf{0}$. So $\bar{T}^p\mathbf{X} = \mathbf{X}$ and thus $k|p$. Therefore $k = p = 2^r$ by Lemma 3.2.

(ii) In case of $n = 2^r$:

Since $\bar{T}^p\mathbf{X} = (I \oplus T)^{p-1}F \oplus T^p\mathbf{X}$ and $(I \oplus T_p)^{p-1} = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 1 \end{pmatrix}$ by Corollary 3.4, $(I \oplus T)^{p-1}F \neq \mathbf{0}$ for the complement vector $F = (f_1 f_2 f_3 \cdots f_n)^t$ with $\sum_{i=1}^{n} f_i \equiv 1 \,(mod 2)$. Therefore $k > p$ and thus $k = 2p = 2^{r+1}$ by Lemma 3.2. But $(I \oplus T)^{p-1}F = \mathbf{0}$ for the complement vector $F = (f_1 f_2 f_3 \cdots f_n)^t$ with $\sum_{i=1}^{n} f_i \equiv 0 \,(mod 2)$, so $\bar{T}^p\mathbf{X} = (I \oplus T)^{p-1}F \oplus T^p\mathbf{X} = \mathbf{X}$ and thus $k = p = 2^r$. □

Theorem 3.7. *Let* $\mathbf{C}$ *be the* n*-cell* 90/150 *group NBCA with the minimal polynomial* $(1+x)^n$, $n = 2, 3, 4, \cdots$. *And let* $\mathbf{C}'$ *be the complemented CA derived from* $\mathbf{C}$ *with the complement vector* $F = (f_1 f_2 \cdots f_n)^t$ *such that* $(I \oplus T)^{n-1}F \neq \mathbf{0}$, *where* T *is the state transition matrix of* $\mathbf{C}$ *and* $f_i = 0$ *or* 1, $1 \leq i \leq n$. *Then all the lengths of the cycles are equal to* $ord(\bar{T})$ *in the state transition graph of* $\mathbf{C}'$.

Proof. Let $\bar{T}$ be $ord(\bar{T}) = k$. Then $k = 2^r$ or $k = 2^{r+1}$ by Lemma 3.2. Assume that there exists a cycle of length l such that $l < k$. Then l can be $l = \frac{k}{2}$. Since there exists a cycle of length l, there is a nonzero state $\mathbf{X}$ such that $\bar{T}^l\mathbf{X} = \mathbf{X}$. Then $\bar{T}^l\mathbf{X} = (I \oplus T)^{l-1}F \oplus T^l\mathbf{X} = \mathbf{X}$. Thus

$$(I \oplus T)^{l-1}F = (I \oplus T)^l\mathbf{X} \tag{3.3}$$

By multiplying $(I \oplus T)^{n-l}$ to the both sides of (3.3), we obtain $\mathbf{0} \neq (I \oplus T)^{n-1}F = (I \oplus T)^n\mathbf{X} = \mathbf{0}$. This is a contradiction. So there does not exist any cycle with length l such that $l < k$. Hence all cycles in $\mathbf{C}'$ have the same length $k = ord(\bar{T})$. □

To find the CA in which all the lengths of cycles are equal to $ord\left(\bar{T}\right)$, it is sufficient to find F such that $(I \oplus T_n)^{n-1}F \neq \mathbf{0}$. F can be obtained from the form of $(I \oplus T_n)^{n-1}$. If we try to find the $S_n = (I \oplus T_n)^{n-1}$ from the state transition

matrix $T_n =< d_1, d_2, \cdots, d_n >$, the time complexity is $O(n)$. By Theorem 3.3, we can easily derive $(I \oplus T_n)^{n-1}$ from $(I \oplus T_{\lfloor \frac{n}{2} \rfloor})^{\lfloor \frac{n}{2} \rfloor - 1}$. And thus we can find the complement vector F such that $(I \oplus T_n)^{n-1} F \neq \mathbf{0}$ within the time complexity $O(log_2 n)$.

4. Conclusion

In this paper, we analyzed the order of the complemented group CA derived from 90/150 group CA and showed that all the lengths of the cycles in the complemented CA are equal to the order of the complemented CA. Especially, the order of the complemented group CA $\bar{\mathbf{C}}$ derived from 90/150 group CA $\mathbf{C}$ is equal to or twice the order of $\mathbf{C}$. And we showed that all the cycles in $\bar{\mathbf{C}}$ has the same length cycle with the order of $\bar{\mathbf{C}}$. Also we showed that the time complexity to find the complement vector F such that $(I \oplus T_n)^{n-1} F \neq \mathbf{0}$ is $O(log_2 n)$. So it is even more efficient than direct computation whose time complexity is $O(n)$.

References

1. A.A. Abdo, S. Lian, I.A. Ismail, M. Amin and H. Diab, *A cryptosystem based on elementary cellular automata*, Communications in Nonlinear Science and Numerical Simulation **18** (2013), 136-147.
2. U.S. Choi, S.J. Cho and G.T. Kong, *Analysis of characteristic polynomial of cellular automata with symmetrical transition rules*, Proc. Jangjeon Math. Soc. **18** (2015), 85-93.
3. S.J. Cho, U.S. Choi, H.D. Kim, Y.H. Hwang and J.G. Kim, *Analysis of* 90/150 *two predecessor nongroup cellular automata*, In Cellular Automata, Springer Berlin Heidelberg (2008), 128-135.
4. 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 Transactions on Computer-Aided Design of Integrated Circuits and Systems **26** (2007), 1720-1724.
5. A.K. Das, *Additive Cellular Automata: Theory and Application as a Built-in Self-Test Structure*, Ph.D. Thesis, I.I.T., 1990.
6. G.A. Hedlund, *Endomorphisms and automorphisms of the shift dynamical system*, Theory of Computing Systems **3** (1969), 320-375.
7. J. Jin, *An image encryption based on elementary cellular automata*, Optics and Lasers in Engineering **50** (2012), 1836-1843.
8. S. Nandi, B.K. Kar and P.P. Chaudhuri, *Theory and Applications of Cellular Automata in Cryptography*, IEEE Transactions on Computers **43** (1994), 1346-1357.
9. S. Nandi, S. Roy, S. Nath, S. Chakraborty, W. Ben Abdessalem Karaa and N. Dey, *1-D Group Cellular Automata based Image Encryption Technique*, In Control, Instrumentation, Communication and Computational Technologies (ICCICCT), 2014 IEEE International Conference (2014), 521-526.
10. J.V. Neumann, *Theory of self-reproducing automata*, University of Illinois, Urbana, 1966.
11. W. Pries, A. Thanailakis and H.C. Card, *Group properties of Cellular Automata and VLSI Applications*, IEEE Transactions on Computers **100** (1986), 1013-1024.
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 Transactions on Computer-Aided Design of Integrated Circuits and Systems **9** (1990), 767-778.
13. S. Ulam, *Random processes and transformations*, Proceedings of the International Congress on Mathematics **2** (1952), 264-275.

14. S. Wolfram, *Statistical mechanics of cellular automata*, Reviews of modern physics **55** (1983), 601-644.

Min-Jeong Kwon received the Ph.D. degree at Pukyong National University. She is currently a teacher of the KSA of Kaist since 2014. Her research interests include finite field theory, discrete mathematics and cellular automata.

Department of Mathematics and Computer science, Korea Science Academy of Kaist, Busan 47162, Korea.
e-mail: mjblack02@hanmail.net

Sung-Jin Cho received the Ph.D. degree at Korea University. He is currently a professor at Pukyong University since 1988. His research interests include finite field theory, discrete mathematics and cellular automata.

Department of Applied Mathematics, Pukyong National University, Busan 48513, Korea.
e-mail: sjcho@pknu.ac.kr

Han-Doo Kim received the Ph.D. degree at Korea University. He is currently a professor at Inje University since 1989. His research interests include cryptography, cellular automata and its applications.

Institute of Basic Science, Department of Applied Mathematics, Inje University, Kyeongnam 50834, Korea.
e-mail: mathkhd@inje.ac.kr

Un-Sook Choi received the Ph.D. degree at Pukyong National University. She is currently a professor at Tongmyong University since 2006. Her research interests include crytography, cellular automata and its applications.

Department of Information and Communications Engineering, Tongmyong University, Busan 48520, Korea.
e-mail: choies@tu.ac.kr

Gil-Tak Kong received the MS degree at Pukyong National University. His research interests include cellular automata.

Department of Applied Mathematics, Pukyong National University, Busan 48513, Korea.
e-mail: dieze@naver.com