Thesis for the Degree of Master of Engineering
of Doctor of Philosophy

Analysis of Behaviors of Additive Group Cellular Automata

by

Yoon Hee Hwang

Interdisciplinary Program of Information Security

The Graduate School

Pukyong National University

August 2008

Analysis of Behaviors of Additive Group Cellular Automata

가산 그룹 셀룰라 오토마타의 행동 분석

Advisor : Prof. Sung Jin Cho

by

Yoon Hee Hwang

A thesis submitted in partial fulfillment of the requirements
for the degree of

Master of Engineering of Doctor of Philosophy

in Interdisciplinary Program of Information Security, Graduate School,
Pukyong National University

August 2008

Analysis of Behaviors of Additive Group Cellular Automata

A dissertation

by

Yoon Hee Hwang

Approved by:

(Chairman) Kyung-Hyune Rhee

(Member) Ki-Ryong Kwon

(Member) Sang-Uk Shin

(Member) Weon Shin

(Member) Sung-Jin Cho

August 2008

Contents

List of Figures

List of Tables

가산 그룹 셀룰라 오토마타의 행동 분석

황윤희

부경대학교 대학원 정보보호학협동과정

요약

VLSI시대는 선형 기계와 특히 국소적인 이웃을 갖는 셀룰라 오토마타(Cellular Automata, 이하 CA)의 연구에 새로운 국면을 예고하였다. VLSI 구현은 국소적으로 상호 연결된 간단하고 규칙적이며 모듈러하고 작은 단위로 확장 연결이 가능한 구조가 적합한데, 이는 그러한 성질을 가진 CA가 적합하다. 또한 CA는 선형 상태 함수들의 여원에 의하여 구성된 기계의 한 유형이라는 것과 LFSR보다 속도와 응용 면에서 뛰어나다는 장점을 가지고 있다. 이러한 CA는 Von Neumann에 의하여 자체 재생산이 가능한 모델로 소개되었으며 여러 학문 분야에서 응용되고 있다. Wolfram은 CA의 가장 간단한 구조로 $GF(2)$에서의 1차원 CA를 제안하였으며, 이후 Das등에 의하여 행렬 대수에 의하여 이를 체계화하였다. 오늘날 LFSR의 대안으로 제안된 CA는 LFSR과 달리 분석이 어려워 이에 대한 분석과 이를 바탕으로 해쉬, 패턴 생성, 키교환과 암호학 등에서 널리 응용되어지고 있다. 본 논문에서는 CA에 대한 기본 개념과 성질을 살펴보고, 룰 60 또는 102를 갖는 선형 유니폼 group CA(Linear Uniform Group CA, LUGCA)로부터 유도된 각 여원 벡터에 대응하는 여원 CA가 가능한 최대 동일 길이의 사이클로 나누어지는 성질을 분석하고, Das의 추측이 사실임을 보인다. 또한 가능한 최대 동일 길이로 사이클이 나누어지는 룰 60 ,102 또는 204를 갖는 선형 하이브리드 group CA(Linear Hybrid Group CA, LHGCA)로부터 유도된 각 여원 벡터에 대응하는 여원 CA를 분석한다. 또한 LUGCA와 LHGCA에서 키 교환 프로토콜에 유용한 여러 함수를 구성하고 이러한 함수와 여원 연산자간의 관계를 분석한다. 그리고 룰 90 또는 150을 갖고 최대 길이 수열을 생성하는 CA(Maximum-Length CA, MLCA)로부터 생성된 수열을 분석하고, 90/150 MLCA에서 나타나는 각 열의 위상이동차에 대한 성질을 분석한다. 이를 이용하여 90/150 MLCA의 위상이동차를 구하는 알고리즘을 제안한다. 또한 LFSR에 기반한 CCSG(Clock-controlled shrinking generator)를 분석하고 이에 대응하는 비대칭인 최소 차수의 선형 CA를 모델링한다. 마지막으로 $GF(2)$의 확장체인 $GF(2^p)$에서의 그룹 CA의 구조와 특성 다항식을 분석한다.

Chapter 1

Introduction

The VLSI era has ushered in a new phase of activities into the research of linear machines, and specially the local neighborhood **Cellular Automata** (CA) structures. The VLSI design community prefer simple, regular, modular and cascadable structures with local interconnections. The CA provide a wonderful solution in all these respect ([1]). Also another advantage of CA is a class of machines constructed by inverting the linear state functions. CA have the characters of simplicity of basic components, locality of CA interactions, massive parallelism of information processing, and exhibit complex global properties. These ensure that CA have higher speed and more potential applications than LFSR. The locality of signal path of CA contributes more higher speed than LFSR. So in the form of VLSI implementation, CA have more speed advantages than LFSR ([2]). Such a CA were originally proposed by Von Neumann ([3]) as formal and good computational models of self-reproducing organisms and computation capable to simulate complex physical, biological and environmental phenomena. Research of CA was initiated as early as 1950. Wolfram ([4]) suggested a simplified structure, each CA cell, arranged linearly in one dimension, having only two state(0 or 1), with uniform three-neighborhood interconnection. Each cell is essentially composed of a memory element and a combinatorial logic that generates the next states of the cell from present states of neighboring cells(left, right and self). Various researchers([5]-[8]) have accomplished far-reaching study in the modeling of CA and finding out better applications of automata. Later Das et al. ([9]-[11]) developed a multipurpose matrix algebraic tool capable of characterizing state transition of CA with linear next-state function. CA have been employed in several applications ([12]-[15]). Cho et al. ([16]-[18]) and many researchers ([19]-[26]) analyzed CA to study hash function, data storage, cryptography and so on. The state-transition matrix of a group CA is nonsingluar. Furthermore group CA can be divided into two classes : maximum-length and nonmaximum-length. All $(2^n - 1)$ nonzero states of a linear n-cell maximum-length group CA form a single cycle. Such a group CA has been projected as a generator of pseudorandom patterns of high quality. The CA-based scheme for generation of pseudoexhaustive patterns has reported in ([10], [27]-[30]) and so on. The states of a nonmaximum-length group CA form multiple cycles. Das conjectured that if the order of uniform group CA $\mathbb{C}$ is m, then the order of complemented group CA $\mathbb{C}'$ derived from $\mathbb{C}$ is m or $2m$. Mukhopadhyay ([13]) investigated the state spaces of the fundamental transformations of a group CA and proved new properties which relate the state spaces of the CA for the development of new encryption and key distribution protocols. And he asserted that an essential requirement is that the cycle length of a group CA has to be small, so that ciphering (or deciphering) is performed at the expense of few clock cycles. Moreover the length of the machines has to be equal so that the number of cycles required to encrypt or decrypt is predicted.

In ([31]) , they represented an encryption system implemented on a structure of HACA(Hybrid Additive CA) used for securing the medical data sent over the internet.

The phase shift analysis of 90/150 CA ([4], [17], [18]), whose characterisitc polynomials are primitive, has been investigated by Bardell ([27]). But the phase shift with respect to a given cell position is not uniquely determined by the characteristic polynomial. Nandi and Chaudhuri ([32]) proposed a method for the study of phase shift analysis based on matrix algebra. Nandi and Chaudhuri ([32]) showed that every cell position of a maximum-length 90/150 Null Boundary CA(NBCA) generates the same Pseudo-Noise (PN) sequence corresponding to the characterisitc polynomial of the CA with a phase shift.

Clock-controlled LFSRs have become important building blocks for keystream generators in stream cipher applications, because they are known to produce sequences of long period and high linear complexity ([33], [34]).

In ([35]), they showed that CCSGs can be described in terms of linear CA configurations by using mirror image and the Cattell and Muzio synthesis algorithm ([36]).

CA has been used as modeling and computing paradigm for a long time. And 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 CA based model becomes very complex and difficult to track analytically. Also such models fail to recognize the presence of inherent hierarchical nature of a physical system.

To overcome these problems Sikdar et al. [37] and Cho et al. [38] studied $GF(2^p)$ CA.

The outline of the thesis is as follows: Chapter 2 provides a comprehensive survey on CA and the analysis of 90/150 Two Predecessor nongroup CA(TPNCA). We analyze several complemented CA derived from a Linear Uniform Group CA(LUGCA) with rule 60 or 102 according to the complement vector and investigate some properties of these CA and show that Das's conjecture is true in chapter 3. Also in chapter 3, the order of the state transition operator of the complemented CA derived from a LUGCA with rule 60 or 102 is characterized explicitly. We analyze a Linear Hybrid Group CA(LHGCA) $\mathbb{C}$ with rules 60, 102 and 204 and the complemented CA $\mathbb{C}'$ derived from $\mathbb{C}$. And we give the conditions for the complement vectors which determine the state transition of the CA dividing the entire state space into smaller spaces of equal maximum cycle lengths in chapter 4. In chapter 5, we study the sequences obtained from a 90/150 Maximum-Length CA(MLCA) algebraically. And we apply these to phase shifting of sequences generated by a 90/150 MLCA. From these applications we give an improved method to compute phase shifts, which is different from those methods of Bardell's ([27]), Nandi and Chaudhuri's ([32]) , and Sarkar's ([29]). In chapter 6, we analyze the period of CCSGs based on LFSR and propose a new method of modelling linear CA with the minimum stage corresponding to CCSGs based on LFSR using the analyzed period and the Cho et al.'s synthesis algorithm([38]). By using the results in ([36], [40]) we analyze the transition rule, the characteristic polynomial and the cycle structure of $GF(2^p)$ CA in chapter 7. The work is concluded in chapter 8.

Chapter 2

CA Preliminaries

In this chapter, we provide a survey on $GF(2)$ CA.

CA is a collection of interconnected cells arranged spatially in a regular manner([4]). CA can be classified according to four properties:

a. the structure of the arrangement of cells

b. neighborhood's influence

c. the number of values per cell

d. the rules to compute next states

The CA structure investigated by Wolfram ([4]) can be viewed as a discrete lattice of cells, where each cell can assume either the state 0 or 1. The simplest CA are binary and 1-dimensional(1-D) array of cells, with two possible states per cell and a cell's neighborhoods defined as the cell on either side of it. These were called elementary cellular automata by Wolfram, who studied extensivly their properties([41]). The cells evolve in discrete time steps according to some deterministic rule that depends only on logical neighborhood(Figure 1).

2.1 Rule

In effect, each cell consists of a storage element (D flip-flop) and a combinatorial logic implementing the next-state function(Figure 2).

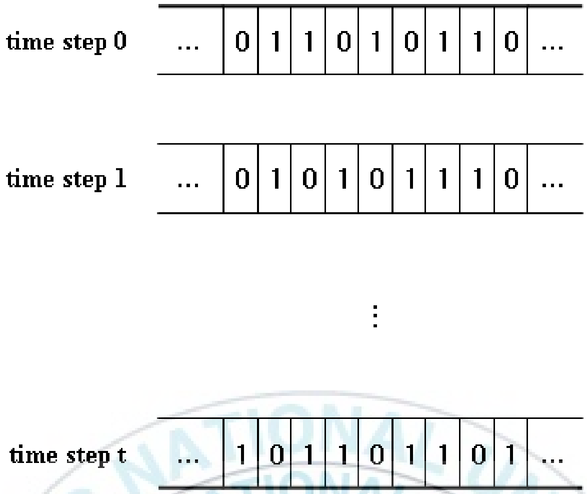

Figure 1: **Evolution of an 1-D CA**

If $q_i(t)$ denotes the state of the ith CA cell at the tth time instant, the next-state function for a 3-neighborhood CA cell can be represented as follows:

$$q_i(t+1) = f[q_{i-1}(t), q_i(t), q_{i+1}(t)]$$

where f denotes the local transition function realized with a combinational logic, and is known as a **rule** of the CA. For a 2-state, 3-neighborhood CA, since f is a function of 3 variables, there can be 2^{2^3}(=256) possible next-state funtions. These 256 CA are generally referred to using a standard naming convention invented by Wolfram[41]. The rule of CA is a decimal number which gives the rule table in binary. For example, the following tables define the rules 90 and 150:

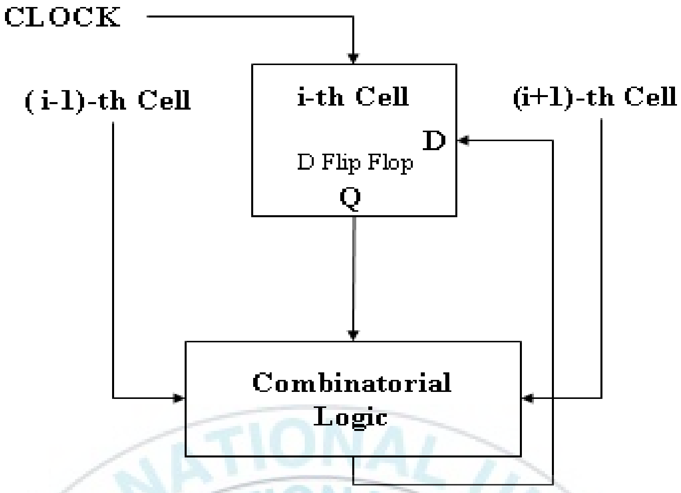

Figure 2: **A CA Cell**

Table 1. Rule Table

PS	111	110	101	100	011	010	001	000	
NS	0	1	0	1	1	0	1	0	rule 90
NS	1	0	0	1	0	1	1	0	rule 150

Note. PS and NS stand for Present State and Next State.

The top row gives all eight possible states of the three neighboring cells (the left neighborhood of the ith cell, the ith cell itself, and its right neighborhood) at the time instant t. The second and third rows give the corresponding states of the ith cell at time instant $t+1$ for a illustrative CA rules. According to rule 90, the value of a particular ith cell is the XOR of the values of its two neighborhoods on the previous time step t. On minimization, the rule tables for the rules 15, 51, 60, 85, 90, 102, 105, 150, 153, 165, 170, 195, 204, and 240 result in the following logic functions, where $\oplus$ denotes XOR

Table 2. Linear Rule

rule	Linear Rule(with XOR)
60	$q_i(t+1) = q_{i-1}(t) \oplus q_i(t)$
90	$q_i(t+1) = q_{i-1}(t) \oplus q_{i+1}(t)$
102	$q_i(t+1) = q_i(t) \oplus q_{i+1}(t)$
150	$q_i(t+1) = q_{i-1}(t) \oplus q_i(t) \oplus q_{i+1}(t)$
170	$q_i(t+1) = q_{i+1}(t)$
204	$q_i(t+1) = q_i(t)$
240	$q_i(t+1) = q_{i-1}(t)$

Table 3. Complemented Rule

rule	Complemented Rule (with XNOR)
195	$q_i(t+1) = \overline{q_{i-1}(t) \oplus q_i(t)}$
165	$q_i(t+1) = \overline{q_{i-1}(t) \oplus q_{i+1}(t)}$
153	$q_i(t+1) = \overline{q_i(t) \oplus q_{i+1}(t)}$
105	$q_i(t+1) = \overline{q_{i-1}(t) \oplus q_i(t) \oplus q_{i+1}(t)}$
85	$q_i(t+1) = \overline{q_{i+1}(t)}$
51	$q_i(t+1) = \overline{q_i(t)}$
15	$q_i(t+1) = \overline{q_{i-1}(t)}$

logic.

We introduce definitions which are extensively used in the subsequent chapters. These definitions are cited from ([1]).

Definition 2.1.1 If in a CA the next-state functions for each cell have XOR or XNOR logic only, then the CA is called an **additive CA**.

Definition 2.1.2 If in a CA the next-state function is only XOR, then it is called a **linear CA** and the corresponding rule is referred to as **linear rule**(Table 2). If in a additive CA the next-state function is not only XOR, then it is called a **complemented CA** and the corresponding rule involving the XNOR is called a **complemented rule**(Table 3).

According to the conditions, they are divided into 3 types: null boundary CA, periodic boundary CA, and intermediate boundary CA.

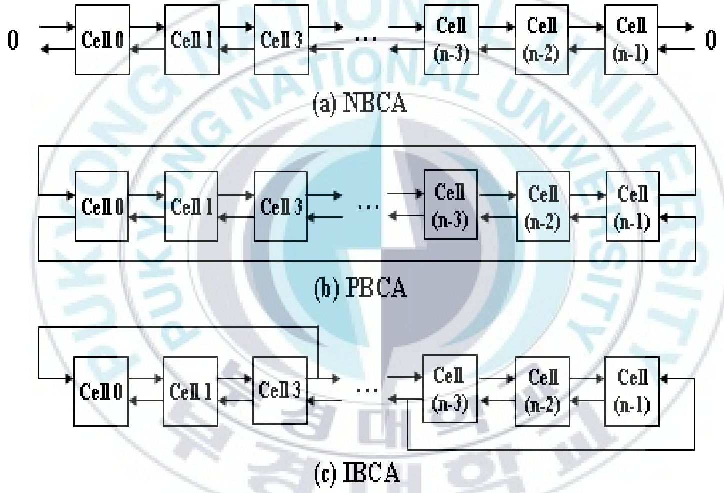

Figure 3: **NBCA, PBCA and IBCA**

Definition 2.1.3 ([42]) A CA is said to be a **Null Boundary CA**(NBCA) if the left neighborhood of the leftmost cell and right neighborhood of the rightmost cell are regarded to be 0. A CA is said to be a **Periodic Boundary CA**(PBCA) if the leftmost cell and the rightmost cell are regarded to be adjacent to each other, i.e., the left neighborhood of the leftmost cell becomes the rightmost cell, and the right neighborhood of rightmost cell becomes the leftmost cell. A CA is said to be a **Intermediate Boundary CA**(IBCA) if the left neighborhood of the leftmost cell is regarded to be the second right neighborhood, and right neighborhood of the rightmost cell is regarded to be the second left neighborhood(Figure 3).

Definition 2.1.4 If all the CA cells are configured with same rule, then the CA is said to be **uniform CA**, otherwise it is **hybrid CA**.

This thesis is restricted within the additive 1-D NBCA.

2.2 State-Transition Matrix

Since a linear CA employs XOR logic only as the next-state function for each cell, the next-state function of that can be represented as an $n \times n$ matrix referred to as the **state-transition matrix** over GF(2). The characterization of 1-D CA, using a matrix algebraic tools, has been reported in ([9]). An n-cell CA is characterized by an $n \times n$ state-transition matrix. The state-transtion matrix $T = (t_{ij})$ is constructed as:

$$(t_{ij}) = \begin{cases} 1, & \text{if the next state of the } i\text{th cell depends on} \\ & \text{the present state of the } j\text{th cell} \\ 0, & \text{otherwise} \end{cases}$$

For a 3-neighborhood CA, T is a tridiagonal matrix where the principal diagonal specifies the self-denpendency(viz., for the ith cell $T(i,i)$) if the next state of the ith cell depends on its present state. The other two diagonal specify the dependency of the corresponding cell on its left and right neighborhoods.

The **characteristic polynomial** $f(x)$ of a CA is defined by

$$f(x) = |T \oplus xI|$$

where x is an indeterminate, I is the $n \times n$ identity matrix and T is the CA state-transition matrix. Precisely, the polynimial of which T is a root is the characteristic polynimial of the CA.

If $f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$ is a given polynomial, then one can always define

$$f(T) = T^n + a_{n-1}T^{n-1} + a_{n-2}T^{n-2} + \cdots + a_1 T + a_0$$

for any $n \times n$ matrix T. There is an important interplay between polynomials and matrices. The vital role of the characteristic polynomial has already been observed, but there are other polynomials associated with a square matrix. One of these is the minimal polynomial. The Cayley-Hamilton theorem guarantees that for each $n \times n$ matrix T there is a polynomial (the characteristic polynomial) $f(x)$ of degree n such that $f(T) = 0$. A polynomial whose value is the **O** matrix at T is said to **annihilate** T. The unique monic polynomial $f(x)$ of minimum degree that annihilates T is called the **minimal polynomial** of T.

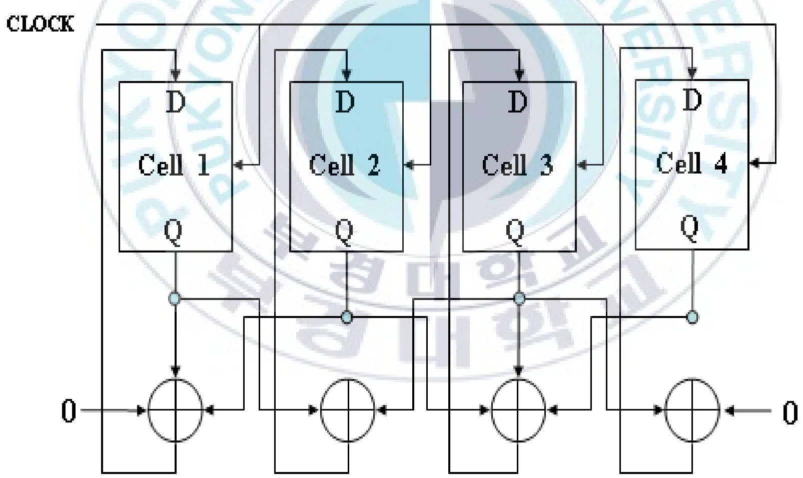

Figure 4: **4-cell CA with** $< 150, 90, 150, 90 >$

Example 2.2.1 The state-transition matrix of the CA configured with the rule vector $< 150, 90, 150, 90 >$ shown in Figure 4 is given by

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

and both the characteristic polynomial and the minimal polynomial of T is the same as $f(x) = x^4 + x + 1$.

If S_t represents the state at the time instant t, then the state of the next instant can be expressed by the state transition equation:

$$S_{t+1} = T \cdot S_t$$

and hence,

$$S_{t+2} = T \cdot S_{t+1} = T^2 \cdot S_t$$

Similarly, the states appearing after the mth time step is

$$S_{t+m} = T^m \cdot S_t$$

Since the XNOR logic is not linear, the additive CA with complemented rules cannot be expressed by the standard matrix notation. Those are formulated as follows.

Definition 2.2.2 An n-cell **complement vector** associated with an n-cell additive CA is n-cell binary vector in which a 1 in the ith position indicates that the rule at the ith cell is an complemented one.

Rule 195 represented as $\overline{q_{i-1}(t) \oplus q_i(t)}$ is the additive complement of rule 60 represented as $q_{i-1}(t) \oplus q_i(t)$. Let the XNOR function be represented as $\overline{T}$. Thus T represents the CA with XOR rules only and $\overline{T}$ with XNOR rules. In a uniform complemented CA the next state is obtained first by obtaining the XORed output and then complementing this state by XORing all the cells with logical 1's. This is equivalent to inverting the XORed output. Thus for a complemented CA:

$$S_{t+1} = \overline{T} \cdot S_t = F \oplus T \cdot S_t$$

Here, if n is the number of cells, complement vector F is an n-cell vector, responsible for inversion after XORing. F has nonzero entries in places of the cell positions where inversion is required.

Lemma 2.2.3([9]) Let $\overline{T}^p$ denote p times application of the complemented CA operator $\overline{T}$. Then

$$\overline{T}^p \cdot S_t = [I \oplus T \oplus T^2 \oplus \cdots \oplus T^{p-1}]F \oplus T^p \cdot S_t$$

where T is the state-transition matrix of the corresponding noncomplemented rule vector and F is a complement vector, S_t is the present states.

Exmaple 2.2.4 A 4-cell NBCA with rule vector $< 150, \overline{90}, \overline{150}, 90 >=< 150, 165, 105, 90 >$ shown in Figure 5 may be represented as follows:

$$S_{t+1} = \overline{T} \cdot S_t = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \oplus \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot S_t$$

where complement vector is $F = (0, 1, 1, 0)^t$.

For example, let the state at the time instant t be $S_t = (0, 0, 1, 1)^t$, then the next state of that is as follows:

$$S_{t+1} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \oplus \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

Figure 6 is the state-transition diagram of the CA in Example 2.2.4.

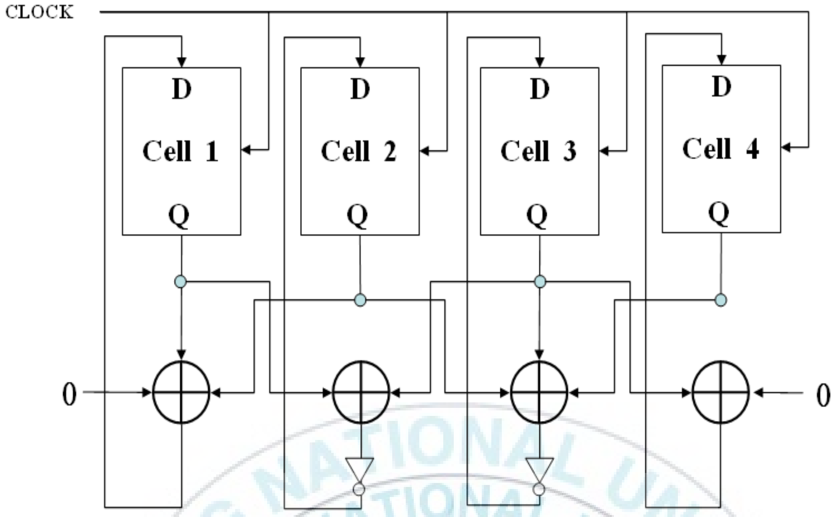

Figure 5: **Structure of the CA with** $< 150, 165, 105, 90 >$

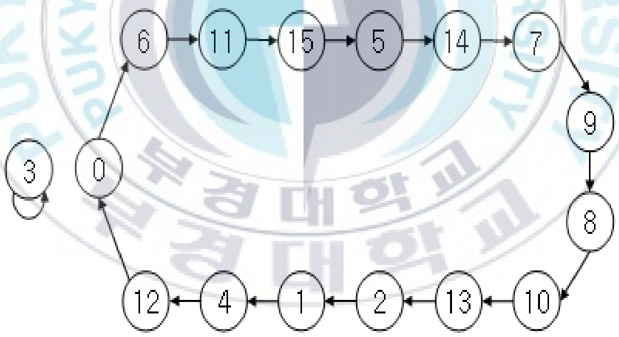

Figure 6: **State-transition diagram of the CA with** $< 150, 165, 105, 90 >$

2.3 Group CA

The state-transition diagrams of CA have been charaterized from its state-transtion matrix, characteristic polynomial and its minimal polynomial. The detailed characterizations of CA state transition behavior are reported in ([1],[10],[12]-[14],[16] etc.). Some fundamental results are presented below.

If all states in the state-transition diagram of a CA lie in cycles, it is called a **group CA**; otherwise it is a **nongroup CA**.

The analysis follows the basic framework of matrix algebraic tools introduced in ([1], [40]).

Since each of the states in the state-transtion diagram of a group CA has a unique immediate predecessor state, the state-transition matix T of a group CA is nonsingular, that is, $det(T) = |T| \neq 0$. In other words, there must exist some positive integer m such that

$$T^m = I$$

$$S_{t+m} = T^m \cdot S_t = S_t$$

A CA with such a property is referred to as a group CA.

A group CA has cycles whose length is m or factors of m with a nonzero starting state iff $det[T^m \oplus I] = 0$. If the order of the group CA characterized by T is a nonprime number, then the cycle lengths are equal to its factors only ([1]).

Group CA can be classified as **maximum**- and **nonmaximum**- length CA. The n-cell maximum-lengh CA(MLCA) which is a class of group CA having a cycle of length $2^n - 1$ with all non-zero states generates excellent psuedo-random sequence([43]). The characteristic polynomial of an n-cell CA is the n-degree primitive polynomial. A primitive polynomial $f(x)$ of degree n is an irreducible polynomial(that is, it does not have any factor), such that the minimum value of m for which $f(x)$ divides $x^m + 1$ is $2^n - 1$.

Example 2.3.2 Figure 7 shows the state-transition diagram of the CA $\mathbb{C}$ whose characteristic polynomial is $f(x) = x^4 + x + 1$ in Exmaple 2.2.1.

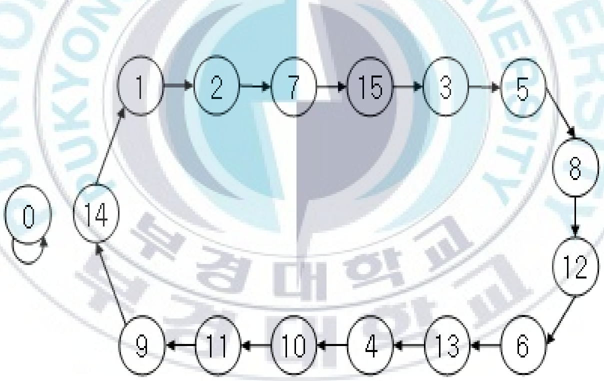

Figure 7: **State-transition diagram of the CA with** $< 150, 90, 150, 90 >$

Since the minimum value of m for which $f(x)$ divides $x^m + 1$ is $2^4 - 1$, $\mathbb{C}$ is MLCA having a cycle of length $2^4 - 1$ with all non-zero states and $f(x)$ is a primitive polynomial.

For a nonmaximum-length CA, the characteristic polynomial gets factored into invariant polynomials. the characteristic polynomial $f(x)$ of the T of such a CA can be represented as

$$f(x) = f_1(x)f_2(x)\cdots f_n(x)$$

Each of the invariant polynomials $f_i(x)$ forms a cyclic subspace. As a result, multiple elementary divisors of $f(x)$ lead to the generation multiple cycles. The entire state space V of a nonmaximum-length CA is the direct sum

$$V = I_1 \oplus I_2 \oplus \cdots \oplus I_n$$

where I_i is the cyclic subspace generated by the divisor $f_i(x)$([44]).

Example 2.3.3 Figure 8 shows the state-transition diagram of the CA with rule vector $< 150, 102, 90 >$ whose characteristic polynomial is $f(x) = x^3 + 1 = (x + 1)(x^2 + x + 1)$.

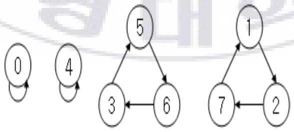

Figure 8: **3-cell CA with** $< 150, 102, 90 >$

The vector space S defined by T is decomposed into two sub-space I_1 and I_2 such that

$$S = I_1 \oplus I_2$$

Here I_1 is the invariant space corresponding to $x+1$ and I_2 is the invariant space corresponding to x^2+x+1. Since $I_1 = N(T \oplus I) = \{0,4\}$ and $I_2 = N(T^2 \oplus T \oplus I) = \{0,3,5,6\}$, $S = I_1 \oplus I_2 = \{0 \oplus 0, 0 \oplus 3, 0 \oplus 5, 0 \oplus 6, 4 \oplus 0, 4 \oplus 3, 4 \oplus 5, 4 \oplus 6\}$, where $N(A)$ is the null space of A.

$\mathbb{C}$ is a nonmaximum-length CA having cycles of length the divisors of $2^4 - 1$.

We may obtain the cycle structure of the state-transition diagram of any linear CA from the analysis of the characteristic polynomial of the T. However, this is not sufficient to characterize such CA. So we may need the minimal polynomial of T. In 1959, a linear machine has been characterized by Elspas([40]). However, the machines having same characteristic and minimal polynomials but different cycle structures could not be analyzed with the algorithm proposed in ([40]).

Chapter 3

Characterization of the Complemented CA derived from Linear Uniform Group CA

The VLSI era has informed in advance a new phase of the research of linear machines like the local neighborhood CA structures. The VLSI design community prefer to have simple, regular, modular, and cascadable structure with local interconnections. With the advancement of semiconductor technology, circuit delay due to interconnections on the silicon floor has become a major concern. Further, in the next-generation submicron technology, interconnections will behave more like a device on the silicon floor, thereby contributing a lion's share to the circuit delay. This situation invariably forces the designers to have local interconnections as far as possible, for reliable high-speed operations of the circuit. The simple, regular, modular, and cascadable structure of CA provides a solution in all these respects([1]). With the ever increasing growth of data communication, the need for security and privacy has become a necessity. Quality of randomness has been evaluated as per the criterion set by Knuth([45]). The advent of wireless communication and other handheld devices like presonal digital assistants and smart cards have made the implementation of cryptosystems a major issue. One important aspect of modern day ciphers is the scope for hardware sharing between the encryption and decryption algorithms. The CA can be programmed to perform both the operations without using any dedicated hardware.

The states of a nonmaximum-length group CA form multiple cycles. Das conjectured that if the order of the rule vector R of uniform group CA $\mathbb{C}$ is m, then the order generated by the rule vector$\overline{R}$ is m or $2m$. Mukhopadhyay ([13]) investigated the state spaces of the fundamental transformations of a group CA and proved new properties which relate the state spaces of the CA for the development of new encryption and key distribution protocols. And he asserted that an essential requirement is that the cycle length of a group CA has to be small, so that ciphering (or deciphering) is performed at the expense of few clock cycles. Moreover the length of the machines has to be equal so that the number of cycles required to encrypt or decrypt is predicted. So we need the analysis of group CA with special rules.

In this chapter, we analyze several complemented CA derived from a linear uniform group CA(LUGCA) with rule 60 or 102 according to the complement vector and investigate some properties of these CA. Also we show that Das's conjecture is true. And the order of the state transition operator of the complemented CA derived from a LUGCA with rule 60 or 102 is characterized explicitly. And we extend and generalize the results of Mukhopadhyay et al. ([13]). These properties will help the development of new encryption and key distribution.

3.1 Analysis of the Complemented CA derived from LUGCA

Theorem 3.1.1 ([40]) If the period of an irreducible polynomial $p(x)$ is k, then the period of $[p(x)]^j$ is kq^r, where $q^{r-1} < j \leq q^r$, q being the modulus.

Lemma 3.1.2 Let $\mathbb{C}$ be an n-cell linear uniform CA(LUCA) with rule 60 or 102. Then the minimal polynomial of the state-transition matrix T of $\mathbb{C}$ is $m(x) = (x+1)^n$.

Proof. Let $\mathbb{C}$ be an n-cell LUCA with rule 60. Then $(T \oplus I)^n = O$ and $(T \oplus I)^{n-1} = (a_{ij})$, where

$$a_{ij} = \begin{cases} 1, & \text{if } i = n,\ j = 1 \\ 0, & \text{otherwise} \end{cases}$$

Hence $m(x) = (x+1)^n$.

The proof for an n-cell LUCA with rule vector $R =< 102, 102, \cdots >$ is similar to the proof of the case of rule 60.

Let $\mathbb{C}$ be an n-cell LUCA with rule 60 or 102. Then the state-transition matrix T of $\mathbb{C}$ is nonsingular because $|T| = 0$. Therefore $\mathbb{C}$ is linear uniform group CA.

Lemma 3.1.3 ([46]) Let $\mathbb{C}$ be an n-cell LUGCA with rule 60 or 102 and state-transition matrix T. Then the order of T, $ord(T) = 2^a (a = 0, 1, 2, \cdots)$, where $2^{a-1} < n \leq 2^a$.

Lemma 3.1.4 Let $\mathbb{C}$ be an n-cell LUGCA with rule 60 or 102 and state-transition matrix T. Let $F = (1, \cdots, 1)^t$. Then $(T \oplus I)^{n-1}F \neq O$.

Proof. We only show that $(T \oplus I)^{n-1}F \neq O$. Let $R =< 60, 60, \cdots >$. Then $(T \oplus I)^{n-1} = (a_{ij})$, where

$$a_{ij} = \begin{cases} 1, & \text{if } i = n,\ j = 1 \\ 0, & \text{otherwise} \end{cases}$$

Thus $(T \oplus I)^{n-1}F = (0, 0, \cdots, 0, 1)^t$. Hence $(T \oplus I)^{n-1}F \neq O$.

The proof for an n-cell CA with rule 102 is similar to the proof of the case of rule 60.

Corollary 3.1.5 Let $\mathbb{C}$ be an n-cell LUGCA with rule 60 or 102 and state-transition matrix T. Let $F = (1, \cdots, 1)^t$. If $n = 2^k$, then

$$(I \oplus T)^{2^k-1}F = (I \oplus T \oplus \cdots \oplus T^{2^k-1})F \neq O$$

Lemma 3.1.6 Let $\mathbb{C}$ be a linear group CA with state-transition matrix T. Let $F \neq O$ and $ord(T) = m$. Then $ord(\overline{T}) = m$ or $2m$.

Proof. Since $ord(T) = m$, $T^m = I$ and thus

$$\begin{aligned} \overline{T}^{2m}X &= T^{2m}X \oplus (T^{2m-1} \oplus \cdots \oplus T^m \oplus T^{m-1} \oplus \cdots \oplus T \oplus I)F \\ &= T^{2m}X \oplus \{T^m(T^{m-1} \oplus \cdots \oplus T \oplus I) \oplus (T^{m-1} \oplus \cdots \oplus T \oplus I)\}F \\ &= T^{2m}X \oplus \{(T^{m-1} \oplus \cdots \oplus T \oplus I) \oplus (T^{m-1} \oplus \cdots \oplus T \oplus I)\}F \\ &= X \oplus O \\ &= X \end{aligned}$$

This means that $ord(\overline{T})$ is a divisor of $2m$. Let $ord(\overline{T}) = p$. Then

$$X = \overline{T}^p X = T^p X \oplus (T^{p-1} \oplus \cdots \oplus T \oplus I)F$$

for all X. Therefore $T^p X = X$ and $(T^{p-1} \oplus \cdots \oplus T \oplus I)F = O$ for all X. Since $ord(T) = m$ and $T^p X = X$ for all X, $m|p$. Hence $p = m$ or $p = 2m$. The proof for an n-cell CA with rule 102 is similar to the proof of the case of rule 60.

Let $\mathbb{C}$ be an n-cell LUGCA with rule 60 (resp. 102) and state-transition matrix T. Let $\mathbb{C}'$ be the complemented CA derived from $\mathbb{C}$ with the complement vector $F = (1, \cdots, 1)^t$. Then $\mathbb{C}'$ is an n-cell 195(resp. 153) UGCA with state-transition matrix $\overline{T}$.

The following theorem is an extension of Theorem 4 ([13]).

Theorme 3.1.7 Let $\mathbb{C}$ be an n-cell LUGCA with rule 60(resp. 102) and T the state-transition matrix of $\mathbb{C}$. Let $\mathbb{C}'$ be an n-cell 195(resp. 153) UGCA derived from $\mathbb{C}$ with state transition operator $\overline{T}$ and $ord(T) = m$. Then

$$ord(\overline{T}) = \begin{cases} 2m, & \text{if } n \text{ is a nonnegative integer power of 2,} \\ m, & \text{otherwise.} \end{cases}$$

Proof. Case 1. $n = 2^a (a \neq 0)$: By Lemma 3.1.3, $ord(T) = n = 2^a = m$. Since $m(x) = (1+x)^m$, $(T \oplus I)^m = (T \oplus I)^{2^a} = T^{2^a} \oplus I = O$ and $(T \oplus I)^{m-1} =$

$T^{m-1} \oplus T^{m-2} \oplus \cdots \oplus T \oplus I \neq O$. Therefore

$$\begin{aligned}\overline{T}^m X &= T^m X \oplus (T^{m-1} \oplus \cdots \oplus T \oplus I)F \\ &= X \oplus (T^{m-1} \oplus \cdots \oplus T \oplus I)F \\ &= X \oplus (T \oplus I)^{m-1} F \\ &\neq X\end{aligned}$$

by Corollary 3.1.5. Thus $ord(\overline{T}) = 2m$ by Lemma 3.1.6.

Case 2. $2^{k-1} < n < 2^k$: By Lemma 3.1.3, $ord(T) = 2^k = m$ and thus $n < m$. Therefore $(1+x)^n$ is a factor of $(1+x)^m$. Since $m(x) = (1+x)^n$,

$$(I \oplus T)^n = (I \oplus T)^{n+1} = \cdots = (I \oplus T)^m = O$$

Therefore

$$(I \oplus T)^{m-1} = T^{m-1} \oplus T^{m-2} \oplus \cdots \oplus T \oplus I = O$$

Hence

$$\begin{aligned}\overline{T}^m X &= T^m X \oplus (T^{m-1} \oplus \cdots \oplus T \oplus I)F \\ &= X \oplus (T^{m-1} \oplus \cdots \oplus T \oplus I)F \\ &= X\end{aligned}$$

Therefore $ord(\overline{T}) = m$.

Remark Theorem 3.1.7 shows that Das's conjecture([9]) is ture for a LUGCA with rule 60 or 102.

From Lemma 3.1.3 and Theorem 3.1.7, we obtain the following theorem.

Theorem 3.1.8 Let $\mathbb{C}$ be an n-cell LUGCA with rule 60(resp. 102) and T the state-transition matrix of $\mathbb{C}$. Let $\mathbb{C}'$ be an n-cell 195(resp. 153) UGCA derived from $\mathbb{C}$ with state transition operator $\overline{T}$. Then the state-transition diagram of $\mathbb{C}'$ consists of equal maximum cycles.

Proof. Case 1. $n = 2^a$: By Lemma 3.1.3 and Theorem 3.1.7, $ord(T) = 2^a$ and $ord(\overline{T}) = 2^{a+1}$. Suppose that X is a state lying on a cycle in $\mathbb{C}'$ whose length is $l = 2^p (p \leq a)$. Then

$$\overline{T}^{2^p} X = \overline{T}^{2^{p+1}} X = \cdots = \overline{T}^{2^a} X = \overline{T}^{2^{a+1}} X = X$$

Since $(T^{2^a-1} \oplus T^{2^a-2} \oplus \cdots \oplus T \oplus I)F \neq O$ by Corollary 3.5,

$$\overline{T}^{2^a} X = T^{2^a} X \oplus (T^{2^a-1} \oplus T^{2^a-2} \oplus \cdots \oplus T \oplus I)F \neq X$$

for all X. This is a contradiction. Hence the lengths of cycles in $\mathbb{C}'$ are the same as 2^{a+1}. Therefore all the lengths of cycles in $\mathbb{C}'$ are the same.

Case 2. $n \neq 2^a$: By Lemma 3.1.3 and Theorem 3.1.7, $ord(T) = 2^k$ and $ord(\overline{T}) = 2^k$, where $2^{k-1} < n < 2^k$. Since $m(x) = (x+1)^n$,

$$(I \oplus T)^n = (I \oplus T)^{n+1} = \cdots = (I \oplus T)^{2^k} = O$$

Suppose that X is a state lying on a cycle in $\mathbb{C}'$ whose length is $2^p (p < k)$. Then

$$\overline{T}^{2^p} X = \overline{T}^{2^{p+1}} X = \cdots = \overline{T}^{2^{k-1}} X = \overline{T}^{2^k} X = X$$

In case X is a state lying on a cycle in $\mathbb{C}$ whose length is less than 2^k, by Corollary 3.1.5,

$$\begin{aligned}
\overline{T}^{2^{k-1}}X &= T^{2^{k-1}}X \oplus (T^{2^{k-1}-1} \oplus \cdots \oplus T \oplus I)F \\
&= X \oplus (T \oplus I)^{2^{k-1}-1}F \\
&\neq X
\end{aligned}$$

This is a contradiction. In case X is a state lying on a cycle in $\mathbb{C}$ whose length is 2^k, let $X = (a_1, \cdots, a_n)^t$. Then

$$\begin{aligned}
\overline{T}^{2^{k-1}}X &= T^{2^{k-1}}X \oplus (T \oplus I)^{2^{k-1}-1}F \\
&= \begin{pmatrix} a_1 \\ \vdots \\ \frac{1+a_{2^{k-1}}}{1+a_1+a_{2^{k-1}+1}} \\ \vdots \end{pmatrix} \neq \begin{pmatrix} a_1 \\ \vdots \\ \frac{a_{2^{k-1}}}{1+a_1+a_{2^{k-1}+1}} \\ \vdots \end{pmatrix} = X
\end{aligned}$$

This is also a contradiction. Hence the lengths of cycles in $\mathbb{C}'$ are the same as 2^k. Therefore all the lengths of cycles in $\mathbb{C}'$ are the same. The proof for the case of the rule 153 is similar to the case of rule 195.

Corollary 3.1.9 If the uniform CA with rule 153 or 195 is a group CA, then its state-transition diagram consists of equal cycles whose cycle length is nonnegative integer power of 2.

Example 3.1.10 Let $\mathbb{C}$ be a 4-cell LUGCA with rule 102 and $F = (1, 1, 1, 1)^t$. Then we obtain the state-transtion diagrams of $\mathbb{C}$ and $\mathbb{C}'$ in Figure 9.

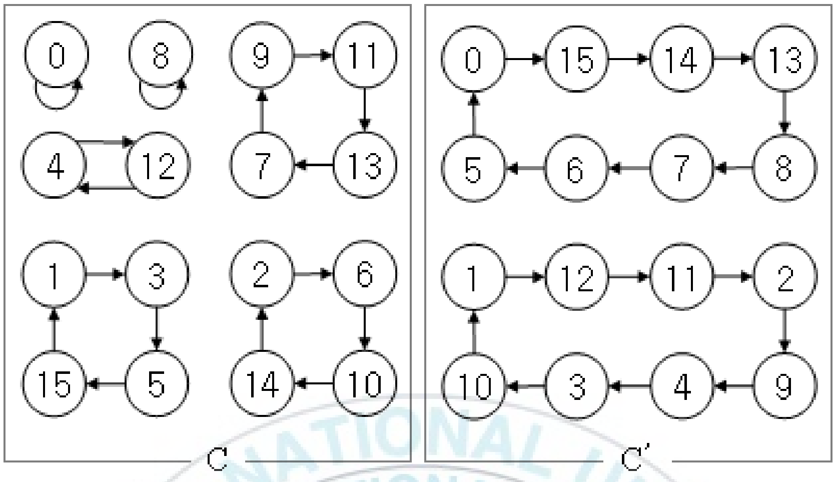

Figure 9: state-transition diagrams of 4-cell LUGCA with rule 102 and its complemented CA

The following lemma can be proved by mathematical induction.

Lemma 3.1.11 Let T (resp. S) be the state-transition matrix of an n-cell LUGCA with rule 60 (resp. 102), where $2^{k-1} < n \leq 2^k$. Let L (resp. U) be the $n \times n$ tridiagonal matrix consisting of 1's below (resp. above) the main diagonal, and 0's elsewhere. Then for each nonnegative integer a,

$$(*) \qquad T^{2^a} = I \oplus L^{2^a} \quad (resp.\ S^{2^a} = I \oplus U^{2^a})$$

where I is the $n \times n$ identity matrix.

Proof. First, $T = I \oplus L$. We will show $(*)$ by induction on a. For $a = 1$, $T^2 = (I \oplus L)^2 = I \oplus L^2$. Hence the statement is true for $a = 1$. Now assume that the statement is true for $a = k$. $T^{2^{k+1}} = T^{2^k}T^{2^k} = (I \oplus L^{2^k})(I \oplus L^{2^k}) =$

$I \oplus L^{2^{k+1}}$. Hence the statement is true for $a = k+1$. The proof for the case of S is similar to the proof for the case of T.

Lemma 3.1.12 Let $\mathbb{C}$ be an n-cell LUGCA with rule 60 (resp. 102), where $2^{k-1} < n \leq 2^k$. Let T (resp. S) be the state-transition matrix of $\mathbb{C}$. Then $T^{2^k} = S^{2^k} = I$ and $T^{2^{k-1}} = (t_{ij})$, where

$$t_{ij} = \begin{cases} 1, & \text{if } i = j \text{ or } i = j + 2^{k-1}, \\ 0, & \text{otherwise.} \end{cases}$$

and $S^{2^{k-1}} = (s_{ij})$, where

$$s_{ij} = \begin{cases} 1, & \text{if } j = i \text{ or } j = i + 2^{k-1}, \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Let L be the $n \times n$ tridiagonal matrix consisting of 1's below the main diagonal, and 0's elsewhere. Then $L^{2^a} = (b_{ij})$, where

$$b_{ij} = \begin{cases} 1, & \text{if } i = j + 2^a, \\ 0, & \text{otherwise.} \end{cases}$$

By Lemma 3.1.11, for each nonnegative integers a, $T^{2^a} = I \oplus L^{2^a} = (t_{ij})$, where

$$t_{ij} = \begin{cases} 1, & \text{if } i = j \text{ or } i = j + 2^a, \\ 0, & \text{otherwise.} \end{cases}$$

The proof for the case of S is similar to the proof for the case of T.

Theorem 3.1.13 Let $\mathbb{C}$ be an n-cell LUGCA with rule 60(resp. 102), where $2^{k-1} < n \leq 2^k$. Let T be the state-transition matrix of $\mathbb{C}$ and let $X = (1, a_2, \cdots, a_n)^t$ (resp. $X = (a_1, a_2, \cdots, a_{n-1}, 1)^t$. Then X lies on a cycle with maximum length in $\mathbb{C}$.

Proof. Since $ord(T) = 2^k$ by Lemma 3.1.2, $T^{2^k}X = X$. By Lemma 3.1.12,

$$T^{2^{k-1}}X = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 & 0 \\ & & & \ddots & & & & \\ 1 & 0 & 0 & \cdots & 1 & 0 & \cdots & 0 \\ & & & \vdots & & & & \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ a_2 \\ a_3 \\ \vdots \\ a_{2^{k-1}} \\ \underline{a_{2^{k-1}+1}} \\ \vdots \\ a_n \end{pmatrix} \neq \begin{pmatrix} 1 \\ a_2 \\ a_3 \\ \vdots \\ a_{2^{k-1}} \\ \underline{1 + a_{2^{k-1}+1}} \\ \vdots \end{pmatrix}$$

and thus $T^{2^{k-1}}X \neq X$. Hence X lies on a cycle with maximum length in $\mathbb{C}$. The proof for the case of the rule 102 is similar to the case of rule 60.

The following lemma can be easily proved.

Lemma 3.1.14 Let $\mathbb{C}$ be an n-cell LUGCA with rule 60 or 102. Let T be the state-transition matrix of $\mathbb{C}$. Let $X = (x_1, \cdots, x_n)^t$ be a state in $\mathbb{C}$. Then

$$(T \oplus I)^{m-1}X = \begin{cases} (0, 0, \cdots, \overset{m}{x_1}, x_2, \cdots, x_{n-m+1})^t, & \text{if } < 60, 60, \cdots >, \\ (x_m, \cdots, x_{n-1}, x_n, 0, \cdots, 0)^t, & \text{if } < 102, 102, \cdots >. \end{cases}$$

The following theorem and corollary give the condition for the order of the complemented CA derived from the n-cell LUGCA with rule 60 or 102 and state-transition matrix T is $2 \cdot ord(T)$ or $ord(T)$, where n is an integral power of 2.

Theorem 3.1.15 Let $\mathbb{C}$ be an n-cell LUGCA with rule 60(resp. 102), where $n = 2^k$. Let T be the state-transition matrix of $\mathbb{C}$. Let $\mathbb{C}'$ be the complemented CA derived from $\mathbb{C}$ with the complement vector $F(\neq 0)$. Then

$$ord(\overline{T}) = \begin{cases} 2\ ord(T), & \text{if } F = (1, a_2, \cdots, a_n)^t \text{ (resp. } F = (a_1, a_2, \cdots, a_{n-1}, 1)^t\text{)}, \\ ord(T), & \text{otherwise.} \end{cases}$$

Proof. Let $X = (x_1, \cdots, x_n)^t$ be a state in $\mathbb{C}'$. Then by Lemma 3.1.3,

$$\begin{aligned} \overline{T}^{2^{k+1}} X &= T^{2^{k+1}} X \oplus (T^{2^{k+1}-1} \oplus \cdots \oplus T \oplus I)F \\ &= X \oplus \{T^{2^k}(T^{2^k-1} \oplus \cdots \oplus T \oplus I) \oplus (T^{2^k-1} \oplus \cdots \oplus T \oplus I)\}F \\ &= X \end{aligned}$$

Therefore $ord(\overline{T})$ divides 2^{k+1}. Let $ord(\overline{T}) = p$. Since

$$X = \overline{T}^p X = T^p X \oplus (T^{p-1} \oplus \cdots \oplus T \oplus I)F$$

for all X, $T^p X = X$ and $(T^{p-1} \oplus \cdots \oplus T \oplus I)F = 0$. Therefore $ord(T) = 2^k$ divides p. Thus $p = 2^k$ or 2^{k+1}.

Case 1. Let $F = (1, a_2, \cdots, a_n)^t$. Then by Lemma 3.1.14

$$\begin{aligned} \overline{T}^{2^k} X &= T^{2^k} X \oplus (T \oplus I)^{2^k - 1} F \\ &= X \oplus \ (0, 0, \cdots, 1)^t \neq X \end{aligned}$$

Therefore $p = 2^{k+1}$.

Case II. Let $F = (0, a_2, \cdots, a_n)^t$. Then by Lemma 3.1.14

$$\overline{T}^{2^k} X = T^{2^k} X \oplus (T \oplus I)^{2^k - 1} F = X \oplus \ (0, 0, \cdots, 0)^t = X$$

Therefore $p = ord(\overline{T}) = 2^k$.

The proof for the case of the rule 102 is similar to the case of rule 60.

Theorem 3.1.16 Let $\mathbb{C}$ be an n-cell LUGCA with rule 60 or 102, where $2^{k-1} < n \leq 2^k$. Let T be the state-transition matrix of $\mathbb{C}$. Let $\mathbb{C}'$ be the complemented CA derived from $\mathbb{C}$ with the complement vector F. Then the lengths of all cycles in $\mathbb{C}'$ are equal in the following cases :

(1) $< 60, 60, \cdots >, \ F = (1, a_2, \cdots, a_n)^t$.

(2) $< 102, 102, \cdots >, \ F = (b_1, \cdots, b_{n-1}, 1)^t$.

Proof. First, we prove for the case $n = 2^k$.

(1) Let X be a state in $\mathbb{C}'$. Since $ord(\overline{T}) = 2^{k+1}, \overline{T}^{2^{k+1}} X = X$. Furthermore, by Lemma 3.1.14

$$\overline{T}^{2^k} X = T^{2^k} X \oplus (T \oplus I)^{2^k - 1} F \neq X$$

Thus X lies on a cycle whose length is 2^{k+1}. Hence the lengths of all cycles in $\mathbb{C}'$ are equal.

(2) We can prove the result by the similar method as the proof of (1).

Second, we prove for the case $2^k - 1 < n < 2^k$.

(1) Let X be a state in $\mathbb{C}'$. Since $ord(\overline{T}) = 2^k$ by Theorem 3.1.7, $\overline{T}^{2^k} X = X$. If X lies on a cycle in $\mathbb{C}$ whose cycle length is less than $ord(T) = 2^k$,

$$\begin{aligned} \overline{T}^{2^{k-1}} X &= T^{2^{k-1}} X \oplus (T \oplus I)^{2^{k-1}-1} F \\ &= X \oplus (T \oplus I)^{2^{k-1}-1} F \\ &\neq X \end{aligned}$$

by Lemma 3.1.14. If X lies on a maximum-length cycle in $\mathbb{C}$,

$$\begin{aligned} \overline{T}^{2^{k-1}} X &= T^{2^{k-1}} X \oplus (T \oplus I)^{2^{k-1}-1} F \\ &= (x_1, x_2, \cdots, x_{2^{k-1}}, x_{2^{k-1}+1} \oplus x_1, \cdots)^t + (0, 0, \cdots, 0, \overset{2^{k-1}}{1}, a_2, \cdots)^t \\ &= (x_1, x_2, \cdots, \overline{x_{2^{k-1}}}, a_2 \oplus x_1 \oplus x_{2^{k-1}+1}, \cdots)^t \\ &\neq X \end{aligned}$$

Therefore $T^{2^{k-1}} X \neq X$ and hence X lies on a maximum cycle in $\mathbb{C}'$.

(2) We can prove the result by the similar method as the proof of (1).

Table 4. n-cell LUGCA $\mathbb{C}$ with rule 60 or 102 and Complemented CA derived from $\mathbb{C}$

rule	60	102
characteristic polynomial	$(x+1)^n$	
minimal polynomial	$(x+1)^n$	
F (complement vector)	$(1, a_2, \cdots, a_n)$	$(b_1, \cdots, b_{n-1}, 1)$
$ord(T)$	$2^a(:= m)$, $(2^{k-1} < n \leq 2^k)$	
$ord(\overline{T})$	$\begin{cases} 2m, & n = 2^s \\ m, & \text{o/w} \end{cases}$ (equal length)	

The principal theorems in section 3.1 may be summarized as Table 4.

3.2 Relationship between Cycles of the Complemented CA

Mukhopadhyay et al.([13]) constructed two functions R_1 and R_2 and showed the relation between the state spaces of fundamental transformations. In this section we construct several functions which are different from R_1 and R_2 and analyze the properties of these functions.

Theorem 3.2.1 Let $\mathbb{C}$ be an n-cell uniform CA with rule 60(resp. 102). Let T be the state-transition matrix of $\mathbb{C}$. Let $\mathbb{C}'$ be an UGCA with rule 195(resp. 153) and state transition operator $\overline{T}$. Then the following hold :

(1) X and $X \oplus \overline{T}^2 X \oplus \overline{T}^3 X$ lie on different cycles.

(2) X and $X \oplus \overline{T}^4 X \oplus \overline{T}^5 X$ lie on different cycles.

(3) X and $X \oplus \overline{T} X \oplus \overline{T}^5 X$ lie on different cycles.

Proof. We only prove for the case of rule 102 and (1). Let $A = X \oplus \overline{T}^2 X \oplus \overline{T}^3 X$. Then

$$A = (T^3 \oplus T^2 \oplus I)X \oplus T^2 F = \begin{pmatrix} \vdots \\ x_{n-2} \oplus x_{n-1} \\ \overline{x_{n-1} \oplus x_n} \\ \overline{x_n} \end{pmatrix}$$

and

$$\overline{T}^a X = \begin{pmatrix} \vdots \\ x_{n-2} \oplus {}_aC_1 x_{n-1} \oplus {}_aC_2 x_n \oplus a \oplus {}_aC_2 \oplus {}_aC_3 \\ x_{n-1} \oplus {}_aC_1 x_n \oplus a \oplus {}_aC_2 \\ x_n \oplus a \end{pmatrix}$$

where $X = (x_1, x_2, \cdots, x_n)^t$. Suppose that there exists an integer a such that $\overline{T}^a X = A$.

Case 1. a is even:

Since $A = \begin{pmatrix} \vdots \\ \overline{x_n} \end{pmatrix}$ and $\overline{T}^a X = \begin{pmatrix} \vdots \\ x_n \end{pmatrix}$, $\overline{T}^a X \neq A$.

Case 1. a is odd :

(1) $a = 4n + 1$:

Since $A = \begin{pmatrix} \vdots \\ x_{n-2} \oplus x_{n-1} \\ \overline{x_{n-1} \oplus x_n} \\ \overline{x_n} \end{pmatrix}$ and $\overline{T}^a X = \begin{pmatrix} \vdots \\ \overline{x_{n-2} \oplus x_{n-1}} \\ \overline{x_{n-1} \oplus x_n} \\ \overline{x_n} \end{pmatrix}$, $\overline{T}^a X \neq A$.

(2) $a = 4n + 3$:

Since $A = \begin{pmatrix} \vdots \\ \overline{x_{n-1} \oplus x_n} \\ \overline{x_n} \end{pmatrix}$ and $\overline{T}^a X = \begin{pmatrix} \vdots \\ x_{n-1} \oplus x_n \\ \overline{x_n} \end{pmatrix}$, $\overline{T}^a X \neq A$.

This completes the proof. The proof for the case of 60 is similar to the case of 102.

[Construction of functions]

Define the functions R_i as follows :

$$R_1(X) = X \oplus \overline{T} X \oplus \overline{T}^2 X$$

$$R_2(X) = X \oplus \overline{T} X \oplus \overline{T}^3 X$$

$$R_3(X) = X \oplus \overline{T}^2 X \oplus \overline{T}^3 X$$

$$R_4(X) = X \oplus \overline{T}^4 X \oplus \overline{T}^5 X$$

$$R_5(X) = X \oplus \overline{T} X \oplus \overline{T}^5 X$$

The following lemmas can be easily proved.

Lemma 3.2.2 Let $\mathbb{C}$ be an n-cell LUGCA with rule 60(resp. 102). Let T be the state-transition matrix of $\mathbb{C}$. Let $\mathbb{C}'$ be an UGCA with rule 195(resp. 153) and state transition operator $\overline{T}$. Then $R_i(R_j(X)) = R_j(R_i(X))$, where $i, j = 1, 2, 3, 4, 5$.

Lemma 3.2.3 Let $\mathbb{C}$ be an n-cell LUGCA with rule 60(resp. 102). Let T be the state transition matrix of $\mathbb{C}$. Let $\mathbb{C}'$ be an UGCA with rule 195(resp. 153) and state transition operator $\overline{T}$. Then for each i $(1 \leq i \leq 5)$ $R_i(\overline{T}^a X) = \overline{T}^a(R_i(X))$, where a is any index.

Corollary 3.2.4 Let $\mathbb{C}$ be an n-cell LUGCA with rule 60(resp. 102). Let T be the state-transition matrix of $\mathbb{C}$. Let $\mathbb{C}'$ be an UGCA with rule 195(resp. 153) and state transition operator $\overline{T}$. Then the following hold :

For all integers i and j $(1 \leq i, j \leq 5)$,

$$\overline{T}^a(R_i R_j(\overline{T}^b(X))) = \overline{T}^b(R_j R_i(\overline{T}^a(X))),$$

where a and b are indices.

Lemma 3.2.5 Let $\mathbb{C}$ be an n-cell LUGCA with rule 60(resp. 102). Let T be the state-transition matrix of $\mathbb{C}$. Let $\mathbb{C}'$ be an UGCA with rule 195(resp. 153) and state transition operator $\overline{T}$. Then the following hold :

(1) $R_1(X \oplus Y) = R_1(X) \oplus R_1(Y) \oplus TF$.

(2) $R_2(X \oplus Y) = R_2(X) \oplus R_2(Y) \oplus (T^2 \oplus T)F$.

(3) $R_3(X \oplus Y) = R_3(X) \oplus R_3(Y) \oplus T^2F$.

(4) $R_4(X \oplus Y) = R_4(X) \oplus R_4(Y) \oplus T^4F$.

(5) $R_5(X \oplus Y) = R_5(X) \oplus R_5(Y) \oplus (T^4 \oplus T^3 \oplus T^2 \oplus T)F$.

Corollary 3.2.6 Let $\mathbb{C}$ be an n-cell LUGCA with rule 60(resp. 102). Let T be the state-transition matrix of $\mathbb{C}$. Let $\mathbb{C}'$ be the corresponding 195(resp. 153) UGCA with state transition operator $\overline{T}$. Then for all integers i and j $(1 \leq i, j \leq 5)$, X and $R_i(R_j(X))$ lie on different cycles, where $i \neq j$.

The following lemma can be proved by mathematical induction.

Lemma 3.2.7 Let $\mathbb{C}$ be an n-cell LUGCA with rule 60(resp. 102). Let T be the state-transition matrix of $\mathbb{C}$. Let $\mathbb{C}'$ be the corresponding 195(resp. 153) UGCA with state transition operator $\overline{T}$. Then for each nonnegative integer a the following hold :

(1) $R_1^{2^a}(X) = X \oplus \overline{T}^{2^a} X \oplus \overline{T}^{2^{a+1}} X$.

(2) $R_2^{2^a}(X) = X \oplus \overline{T}^{2^a} X \oplus \overline{T}^{3\cdot 2^a} X$.

(3) $R_3^{2^a}(X) = X \oplus \overline{T}^{2^{a+1}} X \oplus \overline{T}^{3\cdot 2^a} X$.

(4) $R_4^{2^a}(X) = X \oplus \overline{T}^{2^{a+2}} X \oplus \overline{T}^{5\cdot 2^a} X$.

(5) $R_5^{2^a}(X) = X \oplus \overline{T}^{2^a} X \oplus \overline{T}^{5\cdot 2^a} X$.

The following theorem can be proved by Lemma 3.2.7.

Theorem 3.2.8 Let $\mathbb{C}$ be an n-cell LUGCA with rule 60(resp. 102). Let T be the state-transition matrix of $\mathbb{C}$. Let $\mathbb{C}'$ be the corresponding 195(resp. 153) UGCA with state transition operator $\overline{T}$. Then for each nonnegative integer a the following holds:

For each integer i $(1 \leq i \leq 3)$,

$$\overline{T}^{i\cdot 2^a} R_i^{2^a}(X) = \{(T\oplus I)^{3\cdot 2^a}(T^i\oplus T\oplus I)^{2^a}\oplus I\}X\oplus(T\oplus I)^{3\cdot 2^a-1}(T^i\oplus T\oplus I)^{2^a}F$$

Proof. Case 1. $i=1$: We will show $\overline{T}^{2^a} R_1^{2^a}(X) = \{(T\oplus I)^{3\cdot 2^a}\oplus I\}X\oplus (T\oplus I)^{3\cdot 2^a-1}F$ by induction on a. For $a=0$,

$$\begin{aligned} & \overline{T}R_1(X) \\ = \ & \overline{T}(X\oplus\overline{T}X\oplus\overline{T}^2X) \\ = \ & \overline{T}X\oplus\overline{T}^2X\oplus\overline{T}^3X \\ = \ & (T^3\oplus T^2\oplus T)X\oplus(T^2\oplus I)F \\ = \ & \{(T\oplus I)^3\oplus I\}X\oplus(T\oplus I)^2F \end{aligned}$$

Hence the statement is true for $a=0$. Now assume that the statement is true for $a=k$.

$$\overline{T}^{2^{k+1}} R_1^{2^{k+1}}(X)$$

$$
\begin{aligned}
&= \overline{T}^{2^k} R_1^{2^k}(\overline{T}^{2^k} R_1^{2^k}(X)) \\
&= \overline{T}^{2^k} R_1^{2^k}(\{(T \oplus I)^{3\cdot 2^k} \oplus I\}X \oplus (T \oplus I)^{3\cdot 2^k - 1}F) \\
&= \{(T \oplus I)^{3\cdot 2^k} \oplus I\}(\{(T \oplus I)^{3\cdot 2^k} \oplus I\}X \oplus (T \oplus I)^{3\cdot 2^k - 1}F) \oplus (T \oplus I)^{3\cdot 2^k - 1}F \\
&= (T \oplus I)^{3\cdot 2^k}(T \oplus I)^{3\cdot 2^k}X \oplus X \oplus (T \oplus I)^{3\cdot 2^k}(T \oplus I)^{3\cdot 2^k - 1}F \\
&= \{(T \oplus I)^{3\cdot 2^{k+1}} \oplus I\}X \oplus (T \oplus I)^{3\cdot 2^{k+1} - 1}F
\end{aligned}
$$

Hence the statement is true for $a = k + 1$.

Case 2. $i = 2$: We will show $\overline{T}^{2^{a+1}} R_2^{2^a}(X) = \{(T \oplus I)^{3\cdot 2^a}(T^2 \oplus T \oplus I)^{2^a} \oplus I\}X \oplus (T \oplus I)^{3\cdot 2^a - 1}(T^2 \oplus T \oplus I)^{2^a}F$ by induction on a. For $a = 0$,

$$
\begin{aligned}
\overline{T}^2 R_2(X) &= \overline{T}^2(X \oplus \overline{T}X \oplus \overline{T}^3 X) \\
&= \overline{T}^2 X \oplus \overline{T}^3 X \oplus \overline{T}^5 X \\
&= (T^5 \oplus T^3 \oplus T^2)X \oplus (T^4 \oplus T^3 \oplus T \oplus I)F
\end{aligned}
$$

Since

$$
\begin{aligned}
T^5 \oplus T^3 \oplus T^2 &= T^3(T^2 \oplus I) \oplus (T^2 \oplus I) \oplus I \\
&= (T \oplus I)^2(T^3 \oplus I) \oplus I \\
&= (T \oplus I)^3(T^2 \oplus T \oplus I) \oplus I
\end{aligned}
$$

and

$$T^4 \oplus T^3 \oplus T \oplus I = T^3(T \oplus I) \oplus (T \oplus I) = (T^3 \oplus I)(T \oplus I) = (T \oplus I)^2(T^2 \oplus T \oplus I)$$

$\overline{T}^2 R_2(X) = \{(T \oplus I)^3(T^2 \oplus T \oplus I) \oplus I\}X \oplus (T \oplus I)^2(T^2 \oplus T \oplus I)F$. Hence the statement is true for $a = 0$. Now assume that the statement is true for $a = k$.

$$\begin{aligned}
& \overline{T}^{2^{k+2}} R_2^{2^{k+1}}(X) \\
= \;& \overline{T}^{2^{k+1}} R_2^{2^k}(\overline{T}^{2^{k+1}} R_2^{2^k}(X)) \\
= \;& \overline{T}^{2^{k+1}} R_2^{2^k}(\{(T \oplus I)^{3\cdot 2^k}(T^2 \oplus T \oplus I)^{2^k} \oplus I\}X \\
& \oplus (T \oplus I)^{3\cdot 2^k - 1}(T^2 \oplus T \oplus I)^{2^k} F) \\
= \;& \{(T \oplus I)^{3\cdot 2^k}(T^2 \oplus T \oplus I)^{2^k} \oplus I\}(\{(T \oplus I)^{3\cdot 2^k}(T^2 \oplus T \oplus I)^{2^k} \oplus I\}X \\
& \oplus (T \oplus I)^{3\cdot 2^k - 1}(T^2 \oplus T \oplus I)^{2^k} F) \oplus (T \oplus I)^{3\cdot 2^k - 1}(T^2 \oplus T \oplus I)^{2^k} F \\
= \;& (T \oplus I)^{3\cdot 2^k}(T^2 \oplus T \oplus I)^{2^k}(T \oplus I)^{3\cdot 2^k}(T^2 \oplus T \oplus I)^{2^k} X \oplus X \\
& \oplus \{(T \oplus I)^{3\cdot 2^k}(T^2 \oplus T \oplus I)^{2^k}\}\{(T \oplus I)^{3\cdot 2^k - 1}(T^2 \oplus T \oplus I)^{2^k}\}F \\
= \;& \{(T \oplus I)^{3\cdot 2^{k+1}}(T^2 \oplus T \oplus I)^{2^{k+1}} \oplus I\}X \\
& \oplus (T \oplus I)^{3\cdot 2^{k+1} - 1}(T^2 \oplus T \oplus I)^{2^{k+1}} F
\end{aligned}$$

Hence the statement is true for $a = k + 1$.

Case 3. $i = 3$: We will show $\overline{T}^{3\cdot 2^a} R_3^{2^a}(X) = \{(T \oplus I)^{3\cdot 2^a}(T^3 \oplus T \oplus I)^{2^a} \oplus I\}X \oplus (T \oplus I)^{3\cdot 2^a - 1}(T^3 \oplus T \oplus I)^{2^a} F$ by induction on a. For $a = 0$,

$$\begin{aligned}
\overline{T}^3 R_3(X) &= \overline{T}^3(X \oplus \overline{T}^2 X \oplus \overline{T}^3 X) \\
&= \overline{T}^3 X \oplus \overline{T}^5 X \oplus \overline{T}^6 X \\
&= (T^6 \oplus T^5 \oplus T^3)X \oplus (T^5 \oplus T^2 \oplus T \oplus I)F
\end{aligned}$$

Since

$$\begin{aligned}
& T^5 \oplus T^2 \oplus T \\
= \;& T^2(T^3 \oplus I) \oplus (T \oplus I) \oplus I \\
= \;& (T \oplus I)\{T^2(T^2 \oplus T \oplus I) \oplus I\} \oplus I \\
= \;& (T \oplus I)(T^4 \oplus T^3 \oplus T^2 \oplus I) \oplus I \\
= \;& (T \oplus I)\{T^3(T \oplus I) \oplus (T \oplus I)^2\} \oplus I \\
= \;& (T \oplus I)^2(T^3 \oplus T \oplus I) \oplus I
\end{aligned}$$

and

$$\begin{aligned}
T^6 \oplus T^5 \oplus T^3 &= T^5(T \oplus I) \oplus (T \oplus I)(T^2 \oplus T \oplus I) \oplus I \\
&= (T \oplus I)(T^5 \oplus T^2 \oplus T \oplus I) \oplus I \\
&= (T \oplus I)(T \oplus I)^2(T^3 \oplus T \oplus I) \oplus I \\
&= (T \oplus I)^3(T^3 \oplus T \oplus I) \oplus I
\end{aligned}$$

$\overline{T}^3 R_3(X) = \{(T \oplus I)^3(T^3 \oplus T \oplus I) \oplus I\}X \oplus (T \oplus I)^2(T^3 \oplus T \oplus I)F$. Hence the statement is true for $a = 0$. Now assume that the statement is true for $a = k$.

$$\begin{aligned}
& \overline{T}^{3\cdot 2^{k+1}} R_3^{2^{k+1}}(X) \\
= \;& \overline{T}^{3\cdot 2^k} R_3^{2^k}(\overline{T}^{3\cdot 2^k} R_3^{2^k}(X)) \\
= \;& \overline{T}^{3\cdot 2^k} R_3^{2^k}(\{(T \oplus I)^{3\cdot 2^k}(T^3 \oplus T \oplus I)^{2^k} \\
& \oplus I\}X \oplus (T \oplus I)^{3\cdot 2^k - 1}(T^3 \oplus T \oplus I)^{2^k} F)
\end{aligned}$$

$$
\begin{aligned}
&= \{(T\oplus I)^{3\cdot 2^k}(T^3\oplus T\oplus I)^{2^k}\oplus I\}[\{(T\oplus I)^{3\cdot 2^k}(T^3\oplus T\oplus I)^{2^k}\oplus I\}X \\
&\quad \oplus(T\oplus I)^{3\cdot 2^k-1}(T^3\oplus T\oplus I)^{2^k}F]\oplus(T\oplus I)^{3\cdot 2^k-1}(T^3\oplus T\oplus I)^{2^k}F \\
&= \{(T\oplus I)^{3\cdot 2^{k+1}}(T^3\oplus T\oplus I)^{2^{k+1}}\oplus I\}X \\
&\quad \oplus(T\oplus I)^{3\cdot 2^{k+1}-1}(T^3\oplus T\oplus I)^{2^{k+1}}F
\end{aligned}
$$

Hence the statement is true for $a = k+1$.

The proof for the case of 60 is similar to the case of 102.

Corollary 3.2.9 Let $\mathbb{C}$ be an n-cell LUGCA with rule 60(resp. 102), where $3\cdot 2^{a-1}\le n < 3\cdot 2^a$. Let T be the state-transition matrix of $\mathbb{C}$. Let $\mathbb{C}'$ be the corresponding 195(resp. 153) UGCA with state transition operator $\overline{T}$. Then the following hold :

For each integer i $(1\le i\le 3)$, X and $R_i^{2^a}(X)$ lie on the same cycle.

Corollary 3.2.10 Let $\mathbb{C}$ be an n-cell LUGCA with rule 60(resp. 102), where $3\cdot 2^{a-1}\le n < 3\cdot 2^a$. Let T be the state-transition matrix of $\mathbb{C}$. Let $\mathbb{C}'$ be the corresponding 195(resp. 153) UGCA with state transition operator $\overline{T}$. Then the following hold :

(1) $\overline{T}^{3\cdot 2^a}(R_1R_2)^{2^a}(X) = X$.

(2) $\overline{T}^{5\cdot 2^a}(R_2R_3)^{2^a}(X) = X$.

(3) $\overline{T}^{4\cdot 2^a}(R_3R_1)^{2^a}(X) = X$.

(4) $\overline{T}^{5\cdot 2^a}(R_1R_2R_3)^{2^a}(X) = X$.

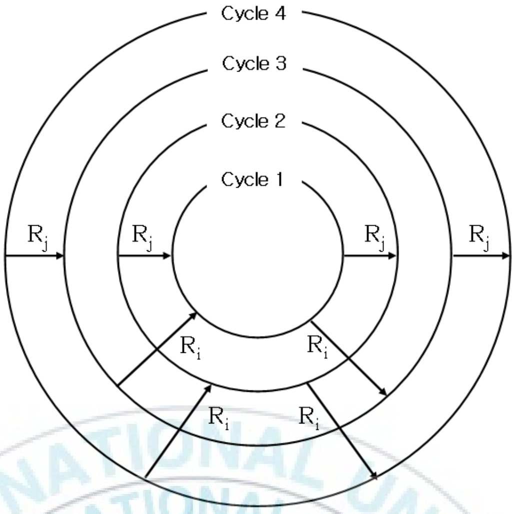

Figure 10: Inter-relationship between these cycles in the 5-cell UGCA with rule 153 or 195

Figure 10 shows the cycles of the state-transition diagram of the 5-cell UGCA with rule 153 or 195. The length of each cycle is 8. All states are divided in 4 cycles which are not loverlapping. Above theorems find out an inter-relationship between these cycles. And we find out a new set of functions. These can help elements to migrate from any position of the state space to another. Recently many researchers have identified the CA as the core of security algorithm. But to perform ciphering(or deciphering) at the expence of few clocks and predicide the number of cycles required to encrypt or decrypt, important requirements are that the length of cycles of the CA has to be small and equal. The specific classes of the complemented CA derived from LUGCA dealt with in this chapter perform an interesting key agreement property.

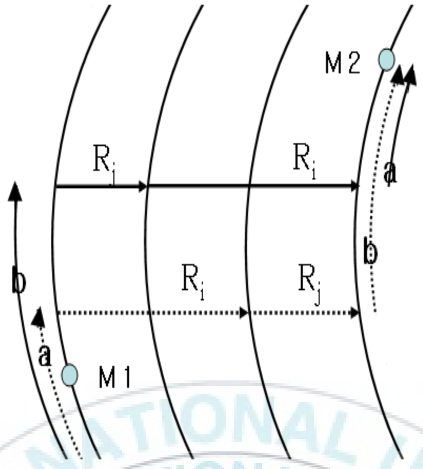

Figure 11: Key Agreement Property of the State Spaces

We will discuss a protocol that allows two parties to exchange a secret key over an insecure communications link.

System set up:

1) All participants share system parameters as a state vector M_1.

2) Each participant chooses a,b, and $R_i (1 \leq i, j \leq 5)$ which can help to migrate from any position of the state space to another. Participants keep (a, i), (b, j) secret.

System uses:

Let us now assume that Alice and Bob want to communicate with each other using a conventional cryptosystem, but that they have no secure channel to exchange a key. They can agree on the common secret key.

$$\overline{T}^b R_j R_i \overline{T}^a M_1 = M_2 = \overline{T}^a R_i R_j \overline{T}^b M_1$$

In Figure 11, M1 is an initial point of key agreement of two parties. After the initial key agreement both takes up different paths as shown by the dashed and the solid lines. From the above theorems, lemmas and corollarys, two paths converge again at M2 which is the second point of collision or key agreement. This property promises the development of an efficient key agreement protocol based on CA.

Chapter 4

Characterization of the Complemented CA derived from Linear Hybrid Group CA

4.1 Analysis of the Complemented CA derived LHGCA

In ([31]) , they represented an encryption system implemented on a structure of HACA(Hybrid Additive CA) used for securing the medical data sent over the internet. In this section, by using the results in chapter 3, we analyze a linear hybrid group CA(LHGCA) $\mathbb{C}$ with rules 60, 102 and 204 and the complemented CA $\mathbb{C}'$ derived from $\mathbb{C}$. And we give the conditions for the complement vectors which determine the state transition of the CA dividing the entire state space into smaller spaces of equal maximum cycle lengths.

Theorem 4.1.1 Let $\mathbb{C}$ be a linear hybrid n-cell CA with rule vector RV and state-transition matrix T, where RV is a combination of rules 60, 102 and 204. Then $\mathbb{C}$ is a LHGCA if and only if rule 60 is not followed immediately by rule 102.

Proof. Let $T(= T_n) =$

$$\begin{pmatrix} 1 & u_1 & 0 & 0 & \cdots & 0 \\ l_2 & 1 & u_2 & 0 & \cdots & 0 \\ 0 & l_3 & 1 & u_3 & \cdots & 0 \\ & & \vdots & & & \\ 0 & 0 & \cdots & l_{n-1} & 1 & u_{n-1} \\ 0 & 0 & 0 & \cdots & l_n & 1 \end{pmatrix}_{n\times n}.$$

Then $|T_n| = |T_{n-1}| = |T_{n-2}| = \cdots = |T_1| = 1$ because $l_i u_{i-1} \neq 1$ for $i \neq 1$. Therefore $\mathbb{C}$ is a group CA. Conversely, suppose that RV is of the form $RV =< \cdots, \overset{i}{102}, 60, \cdots >^t$ for some i with $1 \leq i \leq n-1$. Then the i-th row and $(i+1)$-th row of T are equal and thus $|T| = 0$. Therefore $\mathbb{C}$ is not a group CA.

Corollary 4.1.2 Let $\mathbb{C}$ be a hybrid n-cell CA with rule vector RV and state-transition matrix T, where RV is a combination of rules 60, 102 and 204. Then $\mathbb{C}$ is a nongroup CA if and only if rule 60 is followed immediately by rule 102 for some cell position.

Theorem 4.1.3 Let $\mathbb{C}$ be an n-cell LHGCA with rule vector RV and state-transition matrix T, where RV is a combination of rules 60, 102 and 204. Then the characteristic polynomial of T is $(x+1)^n$.

Proof. Let T be the same as Theorem 4.1.1. Then $l_i u_i \neq 1$. Since rule 60 is not followed immediately by rule 102, $l_i u_{i-1} = 0$ for $i = 2, 3, \cdots, n$. Hence

$$\begin{aligned} c(x) &= |T \oplus xI| = \det \begin{pmatrix} 1+x & u_1 & 0 & 0 & 0 & \cdots & 0 \\ l_2 & 1+x & u_2 & 0 & 0 & \cdots & 0 \\ 0 & l_3 & 1+x & u_3 & 0 & \cdots & 0 \\ & & & \vdots & & & \\ 0 & 0 & 0 & \cdots & l_{n-1} & 1+x & u_{n-1} \\ 0 & 0 & 0 & \cdots & 0 & l_n & 1+x \end{pmatrix} \\ &= (x+1)^n. \end{aligned}$$

By Theorem 4.1.1 $\mathbb{C}$ having the rule vector which is the only combination of the rule vectors $RV_i (i = 1, \cdots, 5)$ in Theorem 4.1.4 is a LHGCA. The following theorem characterizes the order and the minimal polynomial of the state transition matrix T of an n-cell LHGCA.

Theorem 4.1.4 Let $\mathbb{C}$ be an n-cell LHGCA and let $m(x)$ be the minimal polynomial of the state transition matrix T of $\mathbb{C}$. Then $m(x) = (x+1)^p$ in the following cases:

(1) $RV_1 = <\overset{a}{\overline{60, \cdots, 60}}, \overset{b}{\overline{102, \cdots, 102}}>, \ p = \max\{a, b\}$

(2) $RV_2 = <\overset{a}{\overline{60, \cdots, 60}}, 204, \overset{b}{\overline{60, \cdots, 60}}>, \ p = \max\{a, b+1\}$

(3) $RV_3 = <\overset{a}{\overline{60, \cdots, 60}}, 204, \overset{b}{\overline{102, \cdots, 102}}>, \ p = \max\{a, b\}$

(4) $RV_4 = <\overset{a}{\overline{102, \cdots, 102}}, 204, \overset{b}{\overline{60, \cdots, 60}}>, \ p = \max\{a+1, b+1\}$

(5) $RV_5 = <\overset{a}{\overline{102, \cdots, 102}}, 204, \overset{b}{\overline{102, \cdots, 102}}>, \ p = \max\{a+1, b\}$

Proof. We only prove for the case (4). Let $a+1 \geq b+1$. Partition $T \oplus I$ into 2×2 block matrices of the form

$$T \oplus I = \begin{pmatrix} T_1 & O \\ A & T_2 \end{pmatrix} = (a_{ij})$$

, where T_1 is a $(a+1) \times (a+1)$ matrix and

$$a_{ij} = \begin{cases} 1, & \text{if } (i = j-1, i < a+1) \ \text{ or } \ (i = j+1, \ i > a+1), \\ 0, & \text{otherwise} \end{cases}$$

Then

$$(T \oplus I)^q = \begin{pmatrix} T_1^q & O \\ T_2^{q-1}A & T_2^q \end{pmatrix}$$

Here $T_1^{a+1} = O,\ T_1^j \neq O\ (j < a+1)$ and $T_2^b = O$. Since $T_2^{q-1}A = (b_{ij})$, where

$$b_{ij} \ = \ \begin{cases} 1, & \text{if } i = q,\ j = a+1 \\ 0, & \text{otherwise} \end{cases}$$

for $1 \leq q \leq b,\ T_2^b A = O$. Therefore

$$(T \oplus I)^{a+1} = O, \qquad (T \oplus I)^j \neq O\ (j < a+1) \quad \cdots \qquad (4.1)$$

Let $a+1 < b+1$. Partition $T \oplus I$ into 2×2 block matrices of the form

$$T \oplus I = \begin{pmatrix} S_1 & B \\ O & S_2 \end{pmatrix} = (a_{ij})$$

, where S_1 is a $a \times a$ matrix and

$$a_{ij} \ = \ \begin{cases} 1, & \text{if } (j = i+1,\ j < a+2) \text{ or } (j = i-1,\ j > a), \\ 0, & \text{otherwise} \end{cases}$$

Then

$$(T \oplus I)^q = \begin{pmatrix} S_1^q & S_1^{q-1}B \\ O & S_2^q \end{pmatrix}$$

Here $S_1^a = O$ and $S_2^{b+1} = O$ but $S_2^j \neq O\ (j < b+1)$. Since $S_1^{q-1}B = (c_{ij})$ for $1 \leq q \leq a$, where

$$c_{ij} \ = \ \begin{cases} 1, & \text{if } i = a+1-q,\ j = 1 \\ 0, & \text{otherwise} \end{cases}$$

and $S_1^a B = O$,

$$(T \oplus I)^{b+1} = O, \qquad (T \oplus I)^j \neq O \ (j < b+1) \quad \cdots \quad (4.2)$$

By (4.1) and (4.2), $m(x) = (x+1)^p$.

Remark From Theorem 4.1.4 and Lemma in ([40]), we obtain $ord(T) = 2^r$, where $2^{r-1} < p \leq 2^r$.

Theorem 4.1.5 Let $\mathbb{C}$ be an n-cell LHGCA with rule vector $RV_i (i = 1, \cdots, 5)$ in Theorem 4.1.4 and state-transition matrix T. Let $\mathbb{C}'$ be the complemented group CA derived from $\mathbb{C}$ with complement vectors $F_i (i = 1, \cdots, 5)$ which are in below and state transition operator $\overline{T}$.

$$(1)\ RV_1 : \ F_1 \ = \ \begin{cases} (1, f_2, \cdots, f_n)^t, & \text{if } a \geq b \\ (f_1, \cdots, f_{n-1}, 1)^t, & \text{if } a < b \end{cases}$$

$$(2)\ RV_2 : \ F_2 \ = \ \begin{cases} (1, f_2, \cdots, f_n)^t, & \text{if } a \geq b+1 \\ (f_1, \cdots, f_a, 1, f_{a+2}, \cdots, f_n)^t, & \text{if } a < b+1 \end{cases}$$

$$(3)\ RV_3 : \ F_3 \ = \ \begin{cases} (1, f_2, \cdots, f_n)^t, & \text{if } a \geq b \\ (f_1, \cdots, f_{n-1}, 1)^t, & \text{if } a < b \end{cases}$$

$$(4)\ RV_4 : \ F_4 \ = \ \begin{cases} (f_1, \cdots, f_a, 1, f_{a+2}, \cdots, f_n)^t, & \text{if } a+1 \geq b+1 \\ (f_1, \cdots, f_a, 1, f_{a+2}, \cdots, f_n)^t, & \text{if } a+1 < b+1 \end{cases}$$

$$(5)\ RV_5 : \ F_5 \ = \ \begin{cases} (f_1, \cdots, f_a, 1, f_{a+2}, \cdots, f_n)^t, & \text{if } a+1 \geq b \\ (f_1, \cdots, f_{n-1}, 1)^t, & \text{if } a+1 < b \end{cases}$$

where $f_1, \cdots, f_n \in \{0, 1\}$.

Let the minimal polynomial $m(x)$ of T be $(x+1)^p$. If $ord(T) = 2^r$, then the following hold:

(a) All the lengths of cycles in $\mathbb{C}'$ are the same.

(b) $ord(\overline{T}) = \begin{cases} 2^r, & \text{if } 2^{r-1} < p < 2^r, \\ 2^{r+1}, & \text{if } p = 2^r \end{cases}$

Proof. We only prove for the case (2) with $a \geq b+1$. Let $X = (x_1, \cdots, x_n)^t$ be a state in $\mathbb{C}'$. Then

$$\begin{aligned} \overline{T}^{2^{r+1}} X &= T^{2^{r+1}} X \oplus (T^{2^{r+1}-1} \oplus \cdots \oplus T \oplus I)F \\ &= X \oplus \{T^{2^r}(T^{2^r-1} \oplus \cdots \oplus T \oplus I) \oplus (T^{2^r-1} \oplus \cdots \oplus T \oplus I)\}F = X. \end{aligned}$$

Therefore $ord(\overline{T})(:= l)$ divides 2^{r+1}. Since $X = \overline{T}^l X = T^l X \oplus (T^{l-1} \oplus \cdots \oplus T \oplus I)F$ for all X, $T^l X = X$ and $(T^{l-1} \oplus \cdots \oplus T \oplus I)F = 0$. Therefore $ord(T)$ divides l. Thus $l = 2^r$ or 2^{r+1}.

Case 1. Let $p = 2^r$. Then $(T \oplus I)^{2^r-1} = (a_{ij})$, where

$$a_{ij} = \begin{cases} 1, & \text{if } i = a,\ j = 1 \\ 0, & \text{otherwise} \end{cases}$$

Thus

$$\overline{T}^{2^r} X = T^{2^r} X \oplus (T \oplus I)^{2^r-1} F = X \oplus \ (0, \cdots, 0, \overset{a}{1}, 0, \cdots, 0)^t \neq X$$

for all X. Therefore $ord(\overline{T}) = 2^{r+1}$ and thus all the lengths of cycles in $\mathbb{C}'$ are the same.

Case 2. Let $2^{r-1} < p < 2^r$. Then $(T \oplus I)^{2^r - 1} = O$. Thus

$$\overline{T}^{2^r} X = T^{2^r} X \oplus (T \oplus I)^{2^r - 1} F = X$$

Therefore $ord(\overline{T}) = 2^r$. To show that all the lengths of cycles in $\mathbb{C}'$ are the same, suppose that $X = (x_1, \cdots, x_n)^t$ is a state lying on a cycle in $\mathbb{C}'$ whose length is 2^c $(c < r)$. Then

$$\overline{T}^{2^c} X = \overline{T}^{2^{c+1}} X = \cdots = \overline{T}^{2^{r-1}} X = \overline{T}^{2^r} X = X$$

and

$$(T \oplus I)^{2^{r-1}-1} F = (0, \cdots, 0, \overset{2^{r-1}}{\underline{1}}, \cdots)^t$$

First, let X be a state lying on a cycle in $\mathbb{C}$ whose cycle length is less than 2^r. Then

$$\begin{aligned} \overline{T}^{2^{r-1}} X &= T^{2^{r-1}} X \oplus (T^{2^{r-1}-1} \oplus \cdots \oplus T \oplus I) F \\ &= X \oplus (T \oplus I)^{2^{r-1}-1} F \neq X \end{aligned}$$

This is a contradiction.

Second, let X be a state lying on a cycle in $\mathbb{C}$ whose cycle length is 2^r. Partition T into 2×2 block matrices of the form

$$T = \begin{pmatrix} T_1 & O \\ O & T_2 \end{pmatrix}$$

, where T_1 and T_2 are the state transition matrices of uniform group CA with rule 60. Therefore by Lemmas 3.1.12 and 3.1.14

$$\begin{aligned}
\overline{T}^{2^{r-1}}X &= T^{2^{r-1}}X \oplus (T^{2^{r-1}-1} \oplus \cdots \oplus T \oplus I)F \\
&= T^{2^{r-1}}X \oplus (T \oplus I)^{2^{r-1}-1}F \\
&= \begin{pmatrix} {T_1}^{2^{r-1}} & O \\ O & {T_2}^{2^{r-1}} \end{pmatrix} X \oplus \begin{pmatrix} (T_1 \oplus I)^{2^{r-1}-1} & O \\ O & (T_2 \oplus I)^{2^{r-1}-1} \end{pmatrix} F \\
&= (\cdots, \overset{2^{r-1}}{\underline{x_{2^{r-1}}}}, \cdots)^t \oplus (\cdots, \overset{2^{r-1}}{\underline{1}}, \cdots)^t \neq X
\end{aligned}$$

This is a contradiction. Therefore all the lengths of cycles in $\mathbb{C}'$ are the same.

By the similar method we can prove for the case (2) with $a < b + 1$.

Let $\mathbb{C}$ be an n-cell LHGCA with rule vector $RV_i (i = 1, \cdots, 5)$ in Theorem 4.1.4 and state-transition matrix T. Let $\mathbb{C}'$ be the complemented CA derived from $\mathbb{C}$ with complement vector F_i in Theorem 4.1.5 and state transition operator $\overline{T}$. Let $m(x) = (x + 1)^p, (p = 2^r)$ and $ord(T) = 2^r$. Then there exists F such that $ord(\overline{T}) = 2^r$ (not 2^{r+1}). For example, let $\mathbb{C}$ be an n-cell LHGCA with rule vector $RV_2(a \geq b + 1), F = (0, f_2, \cdots, f_n)^t$ and $p = 2^r$. Then all the lengths of cycles in $\mathbb{C}'$ are the same and $ord(\overline{T}) = 2^r$ because $\overline{T}^{2^r}X = X \oplus O = X$.

The principal theorems in section 4.1 may be summarized as Table 5.

Table 5. n-cell LHGCA $\mathbb{C}$ with rule 60, 102, 204 and Complemented CA derived from $\mathbb{C}$

rule	characteristic polynomial	minimal polynomial $(x+1)^p$	F (complement vector)	$\mathrm{ord}(T)$	$\mathrm{ord}(\overline{T})$
RV_1	$(x+1)^n$	$p=\max\{a,b\}$	$\begin{cases}(1,f_2,\cdots f_n)^t, & a \ge b\\ (f_1,\cdots,f_{n-1},1)^t, & a < b\end{cases}$	$2^a(:=m)$, $(2^{k-1} < p \le 2^k)$	$\begin{cases}2m, & p=2^s\\ m, & o/w\end{cases}$ (equal length)
RV_2		$\max\{a,b+1\}$	$\begin{cases}(1,f_2,\cdots f_n)^t, & a \ge b+1\\ (f_1,\cdots,f_a,1,f_{a+2},\cdots,f_{n-1},1)^t, & a < b+1\end{cases}$		
RV_3		$\max\{a,b\}$	$\begin{cases}(1,f_2,\cdots f_n)^t, & a \ge b\\ (f_1,\cdots,f_{n-1},1)^t, & a < b\end{cases}$		
RV_4		$\max\{a+1,b+1\}$	$\begin{cases}(f_1,\cdots,f_a,1,f_{a+2},\cdots,f_{n-1},1)^t, & a+1 \ge b+1\\ (f_1,\cdots,f_a,1,f_{a+2},\cdots,f_{n-1},1)^t, & a+1 < b+1\end{cases}$		
RV_5		$\max\{a+1,b\}$	$\begin{cases}(f_1,\cdots,f_a,1,f_{a+2},\cdots,f_{n-1},1)^t, & a+1 \ge b\\ (1,f_2,\cdots f_n)^t, & a+1 < b\end{cases}$		

4.2 Relationship between Cycles of the Complemented CA

In this section, we show the relationship between cycles of complemented CA. Our results extend and generalize Mukhopadhyay's results([13]).

Theorem 4.2.1 Let $\mathbb{C}$ be an n-cell LHGCA with rule vector $RV_i(i = 1, \cdots, 5)$ in Theorem 4.1.4 and state-transition matrix T. Let $\mathbb{C}'$ be the complemented group CA derived from $\mathbb{C}$ with complement vector F_i which is in Theorem 4.1.5 and state transition operator $\overline{T}$. Then the following hold:

(1) X and $X \oplus \overline{T}X \oplus \overline{T}^2 X$ lie on different cycles.

(2) X and $X \oplus \overline{T}X \oplus \overline{T}^3 X$ lie on different cycles.

(3) X and $X \oplus \overline{T}^2 X \oplus \overline{T}^3 X$ lie on different cycles.

Proof. We only prove for the case (1) and $RV_4(a + 1 \geq b + 1)$.

Let T be the 2×2 block matrix of the form

$$T = \begin{pmatrix} T_1 & O \\ Q & T_2 \end{pmatrix}$$

, where T_1 is a $(a+1) \times (a+1)$ matrix. Then T_1 is the state-transition matrix of $(a+1)$-cell uniform CA with rule 102 and T_2 is the state-transition matrix of b-cell uniform CA with rule 60, and

$$Q = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ & \cdots & & \cdots & & \cdots & \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}_{b \times (a+1)}$$

Let $B = X \oplus \overline{T}X \oplus \overline{T}^2 X$ and $X = (x_1, x_2, \cdots, x_n)^t$. Then

$$B = (I \oplus T \oplus T^2)X \oplus TF = \begin{array}{cc} \left(\begin{array}{c} \vdots \\ \overline{x_a \oplus x_{a+1}} \\ \overline{x_{a+1}} \\ \overline{x_{a+1} \oplus x_{a+2}} \\ x_{a+1} \oplus x_{a+2} \oplus x_{a+3} \\ \vdots \end{array} \right) & \begin{array}{c} \\ \\ a+1 \\ \\ \\ \\ \end{array} \end{array}$$

and

$$\overline{T}^v X = \begin{array}{cc} \left(\begin{array}{c} \vdots \\ {}_vC_0 x_a \oplus {}_vC_1 x_{a+1} \oplus {}_vC_2 \\ {}_vC_0 x_{a+1} \oplus {}_vC_1 \\ {}_vC_1 x_{a+1} \oplus {}_vC_0 x_{a+2} \oplus {}_vC_2 \\ {}_vC_2 x_{a+1} \oplus {}_vC_1 x_{a+2} \oplus {}_vC_0 x_{a+3} \oplus {}_vC_3 \\ \vdots \end{array} \right) & \begin{array}{c} \\ \\ a+1 \\ \\ \\ \\ \end{array} \end{array}$$

for a positive integer v. Suppose that there exists an integer v such that $\overline{T}^v X = B$.

Case 1. v is even:

Since $B = (\cdots, \overset{a+1}{\overline{x_{a+1}}}, \cdots)^t$ and $\overline{T}^v X = (\cdots, \overset{a+1}{x_{a+1}}, \cdots)^t, \overline{T}^v X \neq B$.

Case 2. v is odd: (i) $v = 4m + 1$.

Since $B = (\cdots, \overset{a+2}{\overline{x_{a+1} \oplus x_{a+2}}}, \cdots)^t$ and $\overline{T}^v X = (\cdots, x_{a+1} \overset{a+2}{\oplus} x_{a+2}, \cdots)^t$, $\overline{T}^v X \neq B$.

(ii) $v = 4m + 3$.

Since

$$B = (\cdots, x_{a+1} \oplus \overset{a+3}{x_{a+2}} \oplus x_{a+3}, \cdots)^t$$

and

$$\overline{T}^v X = (\cdots, \overset{a+3}{\overline{x_{a+1} \oplus x_{a+2} \oplus x_{a+3}}}, \cdots)^t,$$

$$\overline{T}^v X \neq B.$$

This is a contradiction. By the similar method we can prove for the case (1) and $RV_4(a+1 < b+1)$. This completes the proof. Define the operators R_i as follows:

$$(1) R_1(X) = X \oplus \overline{T} X \oplus \overline{T}^2 X$$

$$(2) R_2(X) = X \oplus \overline{T} X \oplus \overline{T}^3 X$$

$$(3) R_3(X) = X \oplus \overline{T}^2 X \oplus \overline{T}^3 X$$

Since

$$\begin{aligned} & \overline{T}(X_1 \oplus X_2 \oplus \cdots \oplus X_{2n-1}) \\ = \ & T(X_1 \oplus X_2 \oplus \cdots \oplus X_{2n-1}) \oplus F \\ = \ & (TX_1 \oplus F) \oplus (TX_2 \oplus F) \oplus \cdots \oplus (TX_{2n-1} \oplus F) \\ = \ & \overline{T} X_1 \oplus \overline{T} X_2 \oplus \cdots \oplus \overline{T} X_{2n-1} \end{aligned}$$

, $\overline{T}$ acts as a linear operator on any sum of odd states. Also $\overline{T}^v(X_1 \oplus X_2 \oplus \cdots \oplus X_{2n-1}) = \overline{T}^v X_1 \oplus \overline{T}^v X_2 \oplus \cdots \oplus \overline{T}^v X_{2n-1}$, where v is a positive integer. The following lammas can be easily proved.

Lemma 4.2.2 Let $\mathbb{C}$ be an n-cell LHGCA with rule vector $RV_i(i = 1, \cdots, 5)$ in Theorem 4.1.4 and state-transition matrix T. Let $\mathbb{C}'$ be the complemented group CA derived from $\mathbb{C}$ with complement vector F_i which is in Theorem 4.1.5 and state transition operator $\overline{T}$.

Then the following hold:

$$\overline{T}^v(R_\alpha R_\beta(\overline{T}^u(X))) = \overline{T}^u(R_\beta R_\alpha(\overline{T}^v(X)))$$

Lemma 4.2.3 Let $\mathbb{C}$ be an n-cell LHGCA with rule vector $RV_i(i = 1, \cdots, 5)$ in Theorem 4.1.4 and state-transition matrix T. Let $\mathbb{C}'$ be the complemented group CA derived from $\mathbb{C}$ with complement vector F_i which is in Theorem 4.1.5 and state transition operator $\overline{T}$. Then for each nonnegative integer v,

$$\overline{T}^{\alpha\cdot 2^v} R_\alpha^{2^v}(X) = \{(T\oplus I)^{3\cdot 2^v}(T^\alpha\oplus T\oplus I)^{2^v}\oplus I\}X\oplus(T\oplus I)^{3\cdot 2^v-1}(T^\alpha\oplus T\oplus I)^{2^v}F$$

, where $1 \leq \alpha \leq 3$.

The following theorem can be proved by Lemmas 4.2.2 and 4.2.3.

Theorem 4.2.4 Let $\mathbb{C}$ be an n-cell LHGCA with rule vector $RV_i(i = 1, \cdots, 5)$ in Theorem 4.1.4 and state-transition matrix T. Let $\mathbb{C}'$ be the complemented group CA derived from $\mathbb{C}$ with complement vector F_i which is in Theorem 4.1.5 and state transition operator $\overline{T}$. Then the following hold:

(1) $\overline{T}^{\alpha\cdot 2^v} R_\alpha^{2^v}(X) = X$

(2) $\overline{T}^{(\alpha+\beta)\cdot 2^v}(R_\alpha R_\beta)^{2^v}(X) = X$ for $\alpha \neq \beta$

(3) $\overline{T}^{6\cdot 2^v}(R_1R_2R_3)^{2^v}(X) = X$

for $\alpha, \beta = 1, 2, 3$, where v is a nonnegative integer satisfying $3\cdot 2^{v-1} \leq p < 3\cdot 2^v$ and p is in Theorem 4.1.4.

Chapter 5

Phase Shifts of Sequences Generated by a 90/150 Maximum-Length CA

The linear CA with rules 60, 102 and 204 have nonmaximum-length cycles([1]). So In this chpater, we restrict 90/150 maximum-length CA. CA based pseudorandom generator has been studied in ([9],[49],[50],[51],[52]). Especially, the phase shift analysis of CA([4], [17], [18]), based on 90/150 matrices whose characterisitc polynomials are primitive, has been investigated by Bardell ([27]). He calculated the phase shifts between the output sequences generated by different stages of a maximum-length 90/150 CA by using discrete logarithms of a binary polynomial. Nandi and Chaudhuri ([32]) proposed a method for the study of phase shift analysis based on matrix algebra. They showed that every cell position of a 90/150 maximum-length CA(MLCA) generates the same pseudo-noise sequence corresponding to the characteristic polynomial of the CA with a phase shift.

Recently, Sarkar([29]) gave an algorithm to compute phase shifts. This was achieved by developing the proper algebraic framework for the study of CA sequences. Applications of CA sequences are in built-in self-test(BIST) structures and in the design of secure stream ciphers. In particular, the latter case is based on the fact that it is possible to choose a subset of the CA sequences such that the phase shift between any two seuqences of the subset is exponentially large in the length of the CA. This property helps us to avoid certain kinds of weakness of stream ciphers [53].

In this chapter, we study the sequences obtained from a 90/150 MLCA algebraically. And we apply these to phase shifting of sequences generated by a 90/150 MLCA. From these applications we give an improved method to compute phase shifts, which is different from those methods of Bardell's ([27]), Nandi and Chaudhuri's ([32]) , and Sarkar's ([29]).

5.1 Preliminaries

In this section, we investigate some properties of sequences generated by a 90/150 MLCA.

For example, if $T_6 =< 1, 0, 0, 0, 0, 0 >$ is the state-transition matrix for a given 6-cell 90/150 CA $\mathbb{C}$, then the characteristic polynomial is $f(x) = x^6 + x^5 + x^4 + x + 1$ which is primitive. Hence $\mathbb{C}$ is a 90/150 MLCA.

Tezuka and Fushimi ([28]) asserted that for a given primitive polynomial $f(x)$, there exist exactly two 90/150 MLCA whose characteristic polynomials are $f(x)$. If $T_n =< a_1, a_2, \cdots, a_n >$ is a state-transition matrix corresponding to $f(x)$, then the other is $T'_n =< a_n, a_{n-1}, \cdots, a_1 >$. For example, let $f(x) = x^6 + x^5 + x^4 + x + 1$. Then $T_6 =< 1, 0, 0, 0, 0, 0 >$ and $T'_6 =< 0, 0, 0, 0, 0, 1 >$ are state transition matrices corresponding to $f(x)$.

Lemma 5.1.1 ([48]) For any n-cell 90/150 CA whose state-transition matrix is T_n, the minimal polynomial for T_n is the same as the characteristic polynomial for T_n.

Theorem 5.1.2 Let T_n be the state-transition matrix for a given n-cell 90/150 MLCA and let v_0 be a nonzero vector of $\mathbb{F}_2^n$, where $\mathbb{F}_2^n = \{(b_1, b_2, \cdots, b_n)^T \mid b_i \in GF(2), 1 \leq i \leq n\}$. For $t \geq 1$, define $v_t = T_n v_{t-1}$. Then the sequence $V : v_0, v_1, v_2, \cdots$ has the maximal period $2^n - 1$.

Proof. Let $f(x)$ be the characteristic polynomial for T_n. For a given nonzero vector $v \in \mathbb{F}_2^n$, let $f_v(x)$ be the minimal polynomial for v. By Lemma

5.1 $f_v(x) = f(x)$ for all nonzero vectors $v \in \mathbb{F}_2^n$. If r is the period of V, then $T_n^r v_0 = v_0$. Therefore $f_{v_0}(x)$ divides $x^r - 1$. Since $f_{v_0}(x) = f(x)$ and $f(x)$ is primitive, $r = 2^n - 1$.

Definition 5.1.3 ([54], [55]) Let $f(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} + x^n$ be an n-degree primitive polynomial, where $c_0, c_1, \cdots, c_{n-1} \in GF(2)$. Then $f(x)$ generates a periodic sequence whose period is $2^n - 1$. This sequence is called a **pseudo-noise(PN) sequence**.

Theorem 5.1.2 says that if T_n is the state-transition matrix for a given n-cell 90/150 MLCA and if $v_t = (v_t^0, v_t^1, \cdots, v_t^{n-1})^t \in \mathbb{F}_2^n$, then $\{v_t^i\}(0 \le i \le n-1)$ is a PN sequence.

Theorem 5.1.4 ([30]) Let $f(x)$ be an n-degree primitive polynomial. Also let $\{s_t\} \in \Omega(f(x))$ and $s(x) = s_0 + s_1 x + \cdots + s_{r-1}x^{r-1}$, where $r = 2^n - 1$. If $\{u_t\}$ is the cyclic sequence such that $u(x) = s^*(x)$, then $\{u_t\} \in \Omega(f^*(x))$.

Example 5.1.5 Let $f(x) = x^4 + x + 1$. Then $s_{t+4} = s_t + s_{t+1}$. Therefore we obtain a sequence $\{s_t\} = 000100110101111000100110101111\cdots$. Since $f^*(x) = x^4 + x^3 + 1, u_{t+4} = u_t + u_{t+3}$. Hence we obtain a sequence $\{u_t\} = 011110101100100011110101100100\cdots$.

Let T be the following 90/150 tridiagonal matrix.

$$T = \begin{pmatrix} d_1 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & d_2 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & d_3 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & d_{n-1} & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & d_n \end{pmatrix}$$

(Hereafter we write T by $T =< d_1, d_2, \cdots, d_n >$, where $d_i \in \{0, 1\}$.)

Theorem 5.1.6 Let T_n be the state-transition matrix of an n-cell 90/150 MLCA. Then there exists $p(1 \le p \le 2^n - 2)$ such that $I_n \oplus T_n = T_n^p$.

Proof. Let $f(x)$ be the characteristic polynomial for T_n and let $f(\alpha) = 0$. Since $f(x)$ is primitive, $\{0, 1, \alpha, \cdots, \alpha^{2^n-2}\}$ is the finite field generated by α. Thus there exists $p(1 \le p \le 2^n - 2)$ such that $1 + \alpha = \alpha^p$. Since α is an eigenvector of T_n, $I_n \oplus T_n = T_n^p$.

Corollary 5.1.7 Let T_n be the state-transition matrix of an n-cell 90/150 MLCA. Then there exists $k(1 \le k \le 2^n - 2)$ such that $T_n^k \oplus T_n^{k+1} = I_n$.

Proof. By Theorem 5.1.6 there exists $p(1 \le p \le 2^n - 2)$ such that $I_n \oplus T_n = T_n^p$. Thus $T_n^{2^n-1-p}(I_n \oplus T_n) = T_n^{2^n-1} = I_n$. Let $k = 2^n - 1 - p$. Then $T_n^k(I_n \oplus T_n) = T_n^k \oplus T_n^{k+1} = I_n$.

Example 5.1.8 We consider a 6-cell 90/150 CA whose state-transition matrix T_6 is as the following :

$$T_6 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

The characteristic polynomial of T_6 is $f(x) = x^6 + x^5 + x^4 + x + 1$, which is primitive. We obtain $T_6^{24} \oplus T_6^{25} = I_6$.

The neighborhood dependence of rule 90 and rule 150 differ in only one position(self). Therefore, by allowing a single control line per cell, one can apply both rule 90 and rule 150 on the same cell at different time steps. Thereby, an n-cell CA structure can be used for implementing 2^n CA configurations. Realizing different CA configurations(cell updating rules) on the same structure can be achieved using a control logic to control the appropriate switches and a control program, stored in ROM, can be employed to activate the control. The 1(0) state of the ith bit of a ROM word closes(opens) the switch that controls the ith cell. Such a structure is referred as to as a programmable cellular automata([26]).

5.2 Analysis of Sequences generated by 90/150 MLCA

In this section, we study the sequences generated by a particular cell of a maximum-length 90/150 CA. Hereafter we will simply write T_n by T. Each cell position generates PN sequences ([32]). Unlike LFSRs, the phase shift is generally different between stages of a CA.

Theorem 5.2.1 Let T be the state-transition matrix for a given n-cell 90/150 MLCA. Then the ith row of T^h and T^m are always different, where $0 \leq i \leq n-1, 1 \leq h < m \leq 2^n - 2$.

Proof. We may assume that $w_0 = (0, 0, \cdots, 0, \overset{i}{1}, 0, \cdots, 0)$ is the initial configuration of T. Define $w_r = w_{r-1}T$, for $r \geq 1$. Suppose that the ith row of T^h and T^m are equal, where $0 \leq i \leq n-1, 1 \leq h < m \leq 2^n - 2$. Then $w_h = w_0 T^h = w_0 T^m = w_m$. Since $w_0, w_1, \cdots, w_{2^n-2}$ are all different, $w_h \neq w_m$. Hence the ith row of T^h and T^m are always different.

The following theorem shows that the phase shift is different between stages of a 90/150 MLCA.

Theorem 5.2.2 Let T be the state-transition matrix for a given n-cell 90/150 MLCA and let $w_0 \neq (0, 0, \cdots, 0)$ be the initial configuration of T. Then for any $1 \leq i < j \leq n-1$, there exists an integer h such that $q_j^{t+h} = q_i^t$ for all $t \geq 0$, where q_i^t denotes the state of the ith cell at time t.

Proof. Let $f(x)$ be the n-degree primitive characteristic polynomial of T. Then the $\{q_i^t\}$ and $\{q_j^t\}$ are nth order homogeneous linear recurring sequences. Also the periods of $\{q_i^t\}$ and $\{q_j^t\}$ are 2^n-1. Let $w_i = (q_0^i, \cdots, q_{n-1}^i), 0 \leq i \leq 2^n-2$. Then all $w_i's$ are all nonzero and different by Theorem 4.1. Since each cell position generates PN sequences, there exists an h such that $q_j^{t+h} = q_i^t$ for all $t \geq 0$.

Let T be the state-transition matrix for a given n-cell maximum-length 90/150 CA and let $w_0 = (1, 0, \cdots, 0)$ be the initial configuration of T. Then we obtain $(2^n-1) \times n$ matrix A consisting of n independent PN sequences generated by T as its columns. Let B^i be the $(2^n-1) \times (n-1)$ matrix obtained by deleting the ith column of A. Then the all-zeros $(n-1)$-tuple in B^i appears only once and every other nonzero $(n-1)$-tuple appears twice. In this case, the first row vector in B^0 is $(0, 0, \cdots, 0)$.

For example, let $T =< 0, 1, 1 >$. Then A and $B^i (i = 0, 1, 2)$ are given in Table 6.

Now we define the position of the all-zeros row vector in B^i as the row phase shift of B^0 with respect to B^i. In Table 6 the row phase shift of B^0 with respect to B^1 (resp. B^2) is 1 (resp. 5). That is, the row phase shifts of B^1 and B^2 with respect to B^0 are $-1 \equiv 6$ $(mod\ 7)$ and $-5 \equiv 2$ $(mod\ 7)$, respectively.

Table 6. Matrices A and B^i for $T = < 0, 1, 1 >$

	A	B^0	B^1	B^2
0	100	**00**	10	10
1	010	10	**00**	01
2	111	11	11	11
3	110	10	10	11
4	101	01	11	10
5	001	01	01	**00**
6	011	11	01	01

Theorem 5.2.3 Let T be the state-transition matrix of an n-cell 90/150 MLCA. Then there exists an integer $r_i (0 \leq i \leq n-1)$ such that

$$T^{r_i} w_0^t \oplus T^{r_i+1} w_0^t = (0, 0, \cdots, 0, \overset{i}{1}, 0, \cdots, 0)^t$$

Proof. We can find q_i such that $T^{q_i} w_0^t = (0, 0, \cdots, 0, \overset{i}{1}, 0, \cdots, 0)^t$. By Theorem 5.1.6 there exists p such that $(I_n \oplus T) = T^p$. Let $r_i \equiv q_i - p \ (mod\ 2^n - 1)$. This completes the proof.

We can find the position of the all-zeros $(n-1)$-tuple in B^i by the following corollary.

Corollary 5.2.4 Let T be the state-transition matrix of an n-cell 90/150 MLCA. Let r_i be an integer in Theorem 5.2.3. Then in B^i all-zeros tuple is the $(r_i + p)$th vector, where p is the integer in Theorem 5.1.6.

The following theorem gives a method to compute phase shifts.

Theorem 5.2.5 Let T be the state-transition matrix of an n-cell 90/150 MLCA $\mathbb{C}$. Let u_i be the phase shift(with respect to the 0th cell) of the ith cell in $\mathbb{C}, 0 \leq i \leq n-1$. Then $u_i \equiv -(r_i + p)\ (mod\ 2^n - 1)$, where r_i and p are in Theorem 5.2.3 and Theorem 5.1.6, respectively.

Proof. Let A be the $(2^n - 1) \times n$ matrix consisting of n independent PN sequences generated by T as its columns and let $(1, 0, \cdots, 0)$ be the initial configuration of T. For each $i(0 \leq i \leq n-1)$ let B^i be the $(2^n - 1) \times (n-1)$ matrix obtained by deleting the ith column of A. Let k_i be the row phase shift of B^0 with respect to B^i. Then $k_0 = 0$ and $-k_i\ (mod\ 2^n - 1)$ is the row phase shift of B^i with respect to B^0. Since T is symmetric, the phase shift of the ith cell with respect to the 0th cell is equal to the row phase shift of B^i with respect to B^0. By Corollary 5.2.4, $T^{r_i+p}(1, 0, \cdots, 0)^t = (0, 0, \cdots, 0, \overset{i}{1}, 0, \cdots, 0)^t$ and hence $k_i = r_i + p$. Since $\mathbb{C}$ is a maximum-length CA, T is invertible. Therefore $T^{-(r_i+p)}(0, 0, \cdots, 0, \overset{i}{1}, 0, \cdots, 0)^t = (1, 0, \cdots, 0)^t$ and hence $u_i \equiv -(r_i + p)\ (mod\ 2^n - 1)$.

Example 5.2.6 Let $T =< 1, 0, 0, 0, 0, 0 >$. Then the characteristic polynomial of T is $x^6 + x^5 + x^4 + x + 1$ and $I_6 \oplus T = T^{39}$. Since $T^0(1, 0, 0, 0, 0, 0)^t = (1, 0, 0, 0, 0, 0)^t, q_0 = 0$. Thus $r_0 = q_0 - p = -39 \equiv 24\ (mod\ 63)$. In fact, $T^{24}(1, 0, 0, 0, 0, 0)^t \oplus T^{25}(1, 0, 0, 0, 0, 0)^t = (1, 0, 0, 0, 0, 0)^t$. Since $T^{39}(1, 0, 0, 0, 0, 0)^t = (1, 0, 0, 0, 0, 0)^t, r_1 = q_1 - p \equiv 0\ (mod\ 63)$. Similarly $r_2 = 59, r_3 =$

$8, r_4 = 57$ and $r_5 = 56$. Since $u_i \equiv -(r_i + p)$ $(mod\ 63)$ by Theorem 5.2.5, the phase shifts are $u_0 = 0, u_1 = 24, u_2 = 28, u_3 = 16, u_4 = 30$ and $u_5 = 31$.

Let T be the state-transition matrix for a given n-cell maximum-length 90/150 CA and let $w_0 = (1, 0, \cdots, 0)$ be the initial configuration of T. Then we obtain a $(2^n - 1) \times n$ matrix A consisting of n independent PN sequences generated by T as its columns. The sum of some columns of A is also another PN sequence([59]). The number of PN sequences generated by n columns is equal to ${}_nC_1 + {}_nC_2 + \cdots + {}_nC_n = 2^n - 1$. Thus we can get a $(2^n - 1) \times (2^n - 1)$ matrix whose columns consist of all PN sequences generated by A. Such a matrix is referred to as matrix M.

For example, let $T =< 0, 1, 0, 1 >$. Then A and M are given in Table 7.

For two configurations v and w of T, we define the *row phase shift* h of v with respect to w such that $T^h v = w$. In Table 7 the row phase shift of v with respect to w is 12, where $w = (1, 1, 0, 0)$ and $v = (0, 0, 1, 1)$.

The relative phase shift of one column of M with respect to the other is specified in the following theorems. The PN sequence generated by some cell positions of the CA $\mathbb{C}$ is $\sum_{i=0}^{n-1} a_i q_i$ where a_i is the dependency of q_i.

For example, let $a_0 = a_1 = 1, a_2 = 0$ and $a_3 = 1$, then $\sum_{i=0}^{3} a_i q_i = q_0 \oplus q_1 \oplus q_3$. Therefore $q_0 \oplus q_1 \oplus q_3 = \{q_0^t \oplus q_1^t \oplus q_3^t\} = 1100101 \cdots$ is the 11th column of M.

Table 7. Matrices A and M for $T =< 0, 1, 0, 1 >$

	A	M
0	1000	100011100011101
1	0100	010010011011011
2	1110	111000101110001
3	1111	111100000011110
4	1100	110001111000110
5	1010	101010110101010
6	0001	000100101101111
7	0011	001101111011000
8	0110	011011001101100
9	1011	101110011000101
10	0010	001001010110111
11	0101	010110110110100
12	1101	110101010101001
13	1001	100111001110010
14	0111	011111100000011

Theorem 5.2.7 Let T be the state-transition matrix of an n-cell 90/150 MLCA and let $w = \sum_{i=0}^{n-1} a_i w_i$ and $v = \sum_{j=0}^{n-1} b_j w_j$, where w_i^t is the transpose of $w_i = (0, 0, \cdots, 0, \overset{i}{1}, 0, \cdots, 0)$ $(0 \leq i \leq n-1)$. Then there exists an integer r such that

$$T^r w^t \oplus T^{r+1} w^t = v^t$$

Proof. We can find β such that $T^\beta w^t = v^t$. By Theorem 5.1.6, there exists p such that $(I_n \oplus T) = T^p$. Let $r \equiv \beta - p \ (mod\ 2^n - 1)$. This completes the proof.

Theorem 5.2.7 says that $-\beta$ is the row phase shift of v with respect to w of A.

The following theorem gives a method to compute phase shifts.

Theorem 5.2.8 Let T be the state-transition matrix of an n-cell 90/150 MLCA $\mathbb{C}$. Let s and u be given two columns of M, where $s = \sum_{i=0}^{n-1} a_i q_i$ and $u = \sum_{j=0}^{n-1} b_j q_j$. If h is the phase shift of u with respect to s, then $h \equiv -(r+p) \ (mod\ 2^n - 1)$, where r and p are in Theorem 5.2.7 and Theorem 5.1.6, respectively.

Proof. Let A be the $(2^n - 1) \times n$ matrix consisting of n independent PN sequences generated by T as its columns and let $(1, 0, \cdots, 0)$ be the initial configuration of T. Let $w = \sum_{i=0}^{n-1} a_i w_i$ and $v = \sum_{j=0}^{n-1} b_j w_j$. Since T is symmetric, the phase shift of u with respect to s is equal to the row phase shift of v with respect to w. Therefore $h \equiv -(r+p)\ (mod\ 2^n - 1)$.

Example 5.2.9 Let $\mathbb{C}$ be the given CA with $T =< 0,1,0,1 >$ and $(1,0,0,0)$ the initial configuration of T. Then we obtain matrices A and M as Table 7. Since the characteristic polynomial of T is $x^4 + x + 1$, $p = 4$ in Theorem 5.1.6. Let $s = (1,1,0,0,0,1,0,0,1,1,0,1,0,1,1)^t$ and $u = (0,0,1,0,0,1,1,0,1,0,1,1,1,1,0)^t$ in M. If we put $w = (1,1,0,0)$ and $v = (0,0,1,1)$, then by Theorem 5.1.7 $r = 14$. Hence $h \equiv -(14{+}4) \equiv 12(mod\ 15)$. The phase shift of u (which is the sum of the 2nd cell position and the 3rd cell position of $\mathbb{C}$) with respect to s (which is the sum of the 0th cell and the 1st cell position of $\mathbb{C}$) is 12.

5.3 Algorithm to compute phase shifts

Now we give an algorithm to find the phase shifts in a given n-cell 90/150 MLCA. According to previous results, the following algorithm is introduced in Table 8.

The correctness of this algorithm follows from Theorem 5.2.5. There does not need the Shank's algorithm for the completion of this algorithm any more. The algorithm that we propose does not need any previous phase shifts. Whereas, it is required to compute all previous in Sarkar's method ([5]) which adopted the Shank's algorithm in order to get the phase shifts of the ith column with respect to the 0th cell. So, we can see that this is very practically useful for sufficiently large n.

Table 8. Algorithm FindPhaseShifts

```
Algorithm  FindPhaseShifts

Input : The state transition $n \times n$ matrix $T$,
initial vector $w = (1, 0, \cdots, 0)$.

Output : phaseshift[$n$].

Step 1 : mark$_{1 \times n}$ by 0; mark[0]=1;

         power=1; phaseshift[0]=0.

Step 2 : While (all mark $\neq$ 1) do step 3 to step 5.

Step 3 : $w^t = Tw^t$. /* Run the CA */

Step 4 : If ( $w$ contains single 1)

         then mark[position of 1]=1;

         phaseshift[position of 1] $\equiv -$power (mod $2^n - 1$).

Step 5 : power=power+1.
```

Table 9. Phase shifts with respect to 0th cell

Degree	CA rule	Phase shifts
4	0101	0, 14, 5, 9
8	01001011	0, 254, 147, 56, 131, 66, 126, 68
16	0001111001001000	0, 65534, 8108, 65532, 3385, 64168, 61463, 41934, 2370,54822, 47229, 1810, 63957, 6533, 63959, 63960
32	0000110001000111 0000110000000110	0, 4294967294, 3963262907, 4294967292, 2182065471, 3478064023, 2842396500, 3797410740, 2636154424, 1477132997, 2453647807, 3833928247, 4122644326, 2445882768, 3715941894, 3131603603, 3781145264, 724531189, 1964528637, 1178642835,1437488410, 2132417369, 2228497937, 2438002527, 3823282243,3142683718, 4037203264, 3657430022, 496625232, 3264387886, 25871502, 25871503

Phase shifts with respect to the 0th cell of the given CA up to degree 32 are in Table 9. And let s be the sequence combined the 0th column with the 1st column and u the sequence combined the $(n-2)$th column with the $(n-1)$th column of the matrix A obtained by the given CA rule and the initial vector $(1, 0, \cdots, 0)$. Phase shifts of the sequence u with respect to the sequence s are given in Table 10. Phase shifts in the table are obtained by the above algorithm.

Table 10. Phase shifts of the sequence u with respect to the sequence s

Degree	CA rule	Phase shift
3	110	4
4	0101	12
5	01111	8
6	000110	23
7	1011001	75
8	01001011	9
9	010011100	44
10	1111000011	994
11	01000011010	1426
12	100101010011	3882
13	0111001110110	7649
14	01000111001111	14568
15	100000011000001	9538
16	0001111001001000	63960
17	10011000110011001	77544
18	110001000000010011	241877
19	1101011101101001011	282318
20	01101011100001010110	314775
21	010010011001010010010	1676666
22	0100011010101101100010	1345981
23	01011010101100101011010	6095661
24	110100111100100111001011	199263
25	1010000011111011100000101	17370017
26	11001101111101111010110011	66236246
27	000110100110001011101011000	132625967
28	0101101110000001100111011010	195968798
29	01001000100101111100100010010	205911726
30	101000100111001101101010000101	404894385
31	1111101101100001100011011011111	2015461719
32	00001100010001110000110000000110	25871503

Chapter 6

Modelling Linear CA with the minimum stage corresponding to CCSG based on LFSR

CA have the characters of simplicity of basic components, locality of CA interactions, massive parallelism of information processing, and exhibit complex global properties. These ensure that CA have higher speed and more potential applications than LFSR. The locality of signal path of CA contributes more higher speed than LFSR. So in the form of VLSI implementation, CA have more speed advantages than LFSR ([2]).

Pseudorandom sequences were produced by generators which accompany several LFSRs joined by nonlinear functions or irregular clocking techniques. The theory for CA based pseudorandom number generator is well developed ([1]) and n-stage linear CA can be designed to generate sequences with desirable properties: maximum period $2^n - 1$, uniform distribution of n-tuples and balanced distribution of 1 and 0 ([56],[57]).

Pseudorandom sequence generators intend to be used in a stream cipher. Especially, the Shrinking Generator(SG) proposed by Coppersmith et al. ([58]) is a popular form of pseudorandom sequence generators that employ the irregular clocking. It has one or more LFSRs whose clocking is controlled by the output sequence of one. Such a sequence is called a *clock-controlled sequence* ([59]). The SG generally uses two sources of pseudorandom sequences to create the third source of pseudorandom sequence, having better cryptographic quality(long period, high linear complexity, good statistical properties, etc.) than the original sources.

Clock-controlled LFSRs have become important building blocks for keystream generators in stream cipher applications, because they are known to produce sequences of long period and high linear complexity ([33], [34]).

In ([35]), they showed that CCSGs can be described in terms of linear CA configurations by using mirror image and the Cattell and Muzio synthesis algorithm ([36]). Since the CA obtained by the Sabater et al.'s method has the maximum stage, the method has a waste of space. Also the sequence obtained by CA is not secure because the rule of this CA is symmetrical.

In this chapter, we propose a new method of modelling linear CA with the minimum stage corresponding to CCSGs based on LFSR using the Cho et al.'s synthesis algorithm to overcome these weak points ([38]).

6.1 Preliminaries

6.1.1 Synthesis of CA

A polynomial is said to be a *CA-polynomial* if it is the characteristic polynomial of some CA [36]. All irreducible polynomials are CA-polynomials([36], [38]).

In ([36]), authors proposed a method for the synthesis of one-dimensional 90/150 Linear Hybrid Group Cellular Automata(LHGCA) for irreducible CA-polynomial.

In ([38]), Cho et al. proposed a new method for the synthesis of one-dimensional 90/150 LHGCA for any CA-polynomial. In this case CA-polynomial need not irreducible. This algorithm is efficient and suitable for all practical applications. Table 11 shows an algorithm for finding the 90/150 CA for the given CA-polynomial. In this paper we propose a new method of modelling linear CA with the minimum stage corresponding to CCSGs based on LFSR using this algorithm.

6.1.2 Clock-Controlled Shrinking Generator

Two LFSRs are used, both clocked regularly. If the output of the first LFSR is 1, the output of the second LFSR becomes the output of the generator. If the output of the first LFSR is 0, however, the output of the second is discarded. Figure 12 shows the structure of a SG. This mechanism suffers from timing attacks on the second generator, since the speed of the output is variable in a manner that depends on the second generator's state.

Table 11. Cho et al.'s Synthesis Algorithm

```
Algorithm   Cho et al.'s Synthesis Algorithm
Input : CA-polynomial $f(x)$
Output : 90/150 group/nongroup CA
Step 1 : Make the matrix $B$ which is the $n \times n$ matrix
     obtained by reducing the $n$ polynomials
     $x^{i-1} + x^{2i-1} + x^{2i}$ (mod $f(x)$) $(i = 1, 2, \cdots, n)$.
Step 2 : Solve the equation $Bv = (0, \cdots, 0, 1)^T$.
Step 3 : Construct a Krylov matrix $H = K(C^T, v)$ by the seed vector $v$
    which is a solution of the equation in Step 2.
Step 4 : Compute the LU factorization $H = LU$.
Step 5 : Compute CA for $f(x)$ by the matrix $U$.
```

This can be alleviated by buffering the output. CCSGs are a class of clock-controlled sequence generators [61]. They have applications to cryptography, error correcting codes and digital signature. A CCSG consists of two LFSRs **A**(control register) and **B**(generating register). The **A** is clocked normally, but the **B** is clocked by one plus the integer value represented in selected w fixed stages of the **A**. The output bits of the system are produced by shrinking the output of **B** under the control of **A** as the following. At any time t the output of **B** is taken if the current output of **A** is 1, otherwise it is discarded. Suppose as the following Table 12.

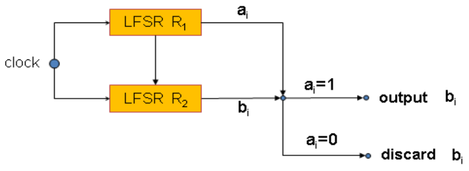

Figure 12: **The structure of a SG**

Table 12. LFSRs **A** and **B**

LFSR	stage	characteristic polynomial	initial state
A	m	$R(x)$	A_0
B	n	$S(x)$	B_0

F is a function that acts on the state of **A** at a given time t to determine the number of times which **B** is clocked such that

$$F(A_t) = 1 + 2^0 A_{i_0}(t) + 2^1 A_{i_1}(t) + \cdots + 2^{w-1} A_{i_{w-1}}(t)$$

for $w < m$, and distinct integers $i_0, i_1, \cdots, i_{w-1} \in \{0, 1, \cdots, m-1\}$, A_t is the state at the time instant t. If no stages are selected (i.e. $w = 0$), define $F(A_t) = 1$.

In this way, the output sequence of a CCSG is obtained from a double decimation. First, the sequence $\{b_i\}$ of **B** is decimated by $F(A_t)$ giving rise to the sequence $\{b'_i\}$. Next, if the output of **A** is 1, b'_i becomes the output of the generator, otherwise b'_i is discarded.

Example 6.1.1 Let **A** be the 4-stage LFSR with the characteristic polynomial $R(x) = x^4 + x + 1$ and the initial state $(0, 0, 0, 1)$. The sequence $\{a_i\}$ generated by **A** is

$$\{a_i\} = \{0,0,0,1,0,0,1,1,0,1,0,1,1,1,1,0,0,0,1,0,0,1,1,0,1,0,1,1,1,1,\cdots\}$$

with period $2^4 - 1 = 15$. And let **B** be the 5-stage LFSR with the characteristic polynomial $S(x) = x^5 + x^2 + 1$ and the initial state $(0, 0, 0, 0, 1)$. The sequence $\{b_i\}$ generated by **B** is

$$\{b_i\} = \{0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, \\ 0, 0, 0, 0, 1, \cdots\}$$

with period $2^5 - 1 = 31$. If $w = 1$, then

$$F(A_t) = 1 + 2^0 A_{i_0}(t)$$

Thus $\{X_{t_i}\}$ is produced by $F(A_t)$ as the following:

$$\{X_{t_i}\} = \{1, 1, 1, 2, 1, 1, 2, 2, 1, 2, 1, 2, 2, 2, 2, 1, 1, 1, 2, \cdots\}$$

In [25], they defined the cumulative function G_A of **A** to be

$$G_A(X_{t_i}) = 2^{m-1}(2^w + 1) - 1$$

Then $G_A(X_{t_i}) = 2^{4-1}(2^1 + 1) - 1 = 23$. That is, $1+1+1+2+1+1+2+2+1+2+1+2+2+2+2 = 23$. In brief, after clocking **A** $2^4 - 1 (= 15)$ times, **B** is clocked 23 times.

According to the following,

$$\begin{cases} b'_0 := b_0 \\ b'_{i+1} := b_j, \quad j = \sum_{k=0}^{i} X_{t_i} \end{cases}$$

the underlined bits $\underline{0}$ or $\underline{1}$ of $\{b_i\}$ are outputted in order to produce the sequence $\{b'_i\}$.

$\{b_i\}$	$\underline{0}, \underline{0}, \underline{0}, \underline{0}, 1, \underline{0}, \underline{0}, \underline{1}, 0, \underline{1}, 1, \underline{0}, \underline{0}, 1, \underline{1}, \underline{1}, 1, \underline{1}, \cdots$
$\{X_{t_i}\}$	$1, 1, 1, 2, 1, 1, 2, 2, 1, 2, 1, 2, 2, 2, 2, 1, 1, 1, 2, \cdots$
$\{b'_i\}$	$0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, \cdots$

Then the output sequence $\{z_i\}$ of the CCSG is given by shrinking $\{b'_i\}$ with $\{a_i\}$

$\{a_i\}$	$0, 0, 0, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 0, 0, 1, \cdots$
$\{b'_i\}$	$0, 0, 0, \underline{0}, 0, 0, \underline{1}, \underline{1}, 0, \underline{0}, 1, \underline{1}, \underline{1}, \underline{0}, \underline{1}, 0, 1, 1, \underline{1}, 1, 0, \underline{1}, \cdots$
$\{z_i\}$	$0, 1, 1, 0, 1, 1, 0, 1, 1, 1, 0, 1, 1, 1, 1, 1, 0, 1, \cdots$

The underlined bits $\underline{0}$ or $\underline{1}$ of b'_i are outputted.

6.2 90/150 CA-based CCSG

In this section, we analyze the period of sequences generated by CCSG based on LFSR.

Definition 6.2.1 Let $\{a'_i\}$ be the sequence obtained by concatenations of $\{C_i\}$'s.

$$C_0 := 1$$

$$C_i := \begin{cases} 1, & X_{t_i} = 1, \\ (\overbrace{0, \cdots, 0, 1}^{k}), & X_{t_i} = k, \ (k \geq 2). \end{cases}$$

Example 6.2.2 $\{b'_i\}$ in Example 6.1.1 can be obtained by shrinking $\{b_i\}$ with $\{a'_i\}$. That is, $\{X_{t_i}\}$ in Example 6.1.1 can be represented by $\{a'_i\}$.

$$\{a'_i\} = \{1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, \cdots\}$$

If a'_i is 1, b_i becomes the output of the generator, otherwise the output of b_i is discarded. This is just b'_i. The decimated sequence $\{b'_i\}$ is given by

$\{a'_i\}$	$1, 1, 1, 1, 0, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, \cdots$
$\{b_i\}$	$\underline{0}, \underline{0}, \underline{0}, \underline{0}, 1, \underline{0}, \underline{0}, \underline{1}, 0, \underline{1}, 1, \underline{0}, \underline{0}, 1, \underline{1}, \underline{1}, 1, \underline{1}, 0, \underline{0}, 0, \underline{1}, 1, \underline{0}, \cdots$
$\{b'_i\}$	$0, 0, 0, 0, 0, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, \cdots$

Theorem 6.2.3 Let **A** (resp. **B**) be an m (resp. n)-stage LFSR whose characteristic polynomial is primitive. And let $\{a'_i\}$ be the sequence obtained by concatenations of $\{C_i\}$'s in Definition 4.1. The period of $\{a'_i\}$ is $2^{m-1}(2^w + 1) - 1$ for a given w.

Proof. Because $G_A(X_{t_i}) = 2^{m-1}(2^w + 1) - 1$ for a given w, the period of $\{a'_i\}$ is $2^{m-1}(2^w + 1) - 1$ by Definition 4.1.

Theorem 6.2.4 Let **A** (resp. **B**) be an m (resp. n)-stage LFSR whose characteristic polynomial is primitive. And let $\{b'_i\}$ be a sequence given by shrinking $\{b_i\}$ with $\{a'_i\}$. The period of $\{b'_i\}$ is

$$\frac{(2^m - 1)lcm(G_A(X_{t_i}), 2^n - 1)}{G_A(X_{t_i})}$$

Proof. The period of the output sequence $\{b_i\}$ of **B** is $2^n - 1$. $\{a'_i\}$ repeats $G_A(X_{t_i})$ period sequences $\frac{lcm(G_A(X_{t_i}),2^n-1)}{G_A(X_{t_i})}$ times and $(2^m - 1)$ 1's occurs in a full period of $\{a'_i\}$. Thus the period of $\{b'_i\}$ is

$$\frac{(2^m - 1)lcm(G_A(X_{t_i}), 2^n - 1)}{G_A(X_{t_i})}$$

Theorem 6.2.5 Let **A** (resp. **B**) be an m (resp. n)-stage LFSR whose characteristic polynomial is primitive. And let $\{z_i\}$ be a sequence given by shrinking $\{b'_i\}$ with $\{a_i\}$. The period of $\{z_i\}$ is

$$\frac{2^{m-1}lcm(G_A(X_{t_i}), 2^n - 1)}{G_A(X_{t_i})}$$

Proof. The period of the output sequence $\{b'_i\}$ is $(2^m-1)\,\frac{lcm(G_A(X_{t_i}),2^n-1)}{G_A(X_{t_i})}(:= h)$. $\{a_i\}$ repeats $\frac{lcm(G_A(X_{t_i}),2^n-1)}{G_A(X_{t_i})}$ period sequences $\frac{lcm(2^m-1,h)}{2^m-1}$ times and (2^{m-1}) 1's occurs in a full period of $\{a_i\}$. Thus the period of $\{z_i\}$ is

$$\begin{aligned} & \frac{2^{m-1}\ lcm(2^m-1, \frac{lcm(G_A(X_{t_i}), 2^n-1)}{G_A(X_{t_i})})}{2^m-1} \\ = \quad & 2^{m-1} lcm(G_A(X_{t_i}), 2^n-1)/G_A(X_{t_i}) \end{aligned}$$

Remark If 2^n-1 and $G_A(X_{t_i})$ are relatively prime, $lcm(G_A(X_{t_i}), 2^n-1)/G_A(X_{t_i}) = 2^n-1$. Therefore in this case, the period of the output sequence by CCSG is $2^{m-1}(2^n-1)$. Thus the characteristic polynomial of such output sequence is of the form $F(x) = (n \text{ stage primitive polynomial})^N$, $2^{m-2} < N \leq 2^{m-1}$.

In [35], they proposed the algorithm that converts a given CCSG into a CA-based linear model using mirror image and the Cattell and Muzio synthesis algorithm. Therefore $N = 2^{m-1}$ is the maximum stage. Also this CA-based linear model is symmetrical and has a waste of space.

6.3 Modelling Linear CA with the minimum stage

In this section, we propose a method that converts a given CCSG into a CA-based linear model by using Cho et al.'s Synthesis Algorithm [38].

According to the previous results, the following algorithm that converts a given CCSG into a CA-based linear model is introduced in Table 13.

The following example shows modelling of linear CA with the minimum stage corresponding to CCSG based on LFSR using this algorithm.

Example 6.3.1 Let **A** be the 4-stage LFSR with a primitive polynomial of degree 4, and **B** be the 5-stage LFSR with a primitive polynomial of degree 5. Let $w = 1$. Then CCSG with **A** and **B** has the characteristic polynomial $F(x) = (5 - \text{stage primitive polynomial})^{(2^{4-2}-1)} = (x^5+x^2+1)^3$. By the proposed algorithm, we can compute a CA with $T_{15} =< 0,0,0,1,0,1,0,1,1,1,0,1,1,0,1 >$. If the algorithm in [35] is used, they must compute a CA with $T_{20} =< 1,1,1,1,1,1,1,1,1,1,\ 0,0,1,1,1,1,1,1,1,1\ >$ corresponding to $F(x) = (x^5 + x^2 + 1)^4$.

Table 13. Algorithm for modelling 90/150 CA

```
Algorithm   ModellingOf90/150CA
Input : A CCSG characterized by:
        The stages $m$ of LFSR($\mathbf{A}$) and $n$ of LFSR($\mathbf{B}$), $w$
          ($2^n - 1$ and $G_A(X_{t_i}) = 2^{m-1}(2^w + 1) - 1$ are relatively prime.)
Output : Linear CA with the minimum stage corresponding
        to CCSG based on LFSR
Step 1 : Compute the characteristic polynomial $F(x)$ for the given CCSG,
    where $F(x) = (n \text{ stage primitive polynomial})^N$, $N = 2^{m-2} + 1$.
Step 2 : Compute CA by Algorithm "Cho et al.'s Synthesis Algorithm".
```

Chapter 7

Analysis of the structure and the characteristic polynomial of $GF(2^p)$ group CA

CA has been used as modeling and computing paradigm for a long time. And 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 CA based model becomes very complex and difficult to track analytically. Also such models fail to recognize the presence of inherent hierarchical nature of a physical system.

To overcome these problems Sikdar et al. [37] and Cho et al. [39] studied $GF(2^p)$ CA.

In this chapter, by using the results in ([36], [38], [40],) we analyze the transition rule, the characteristic polynomial and the cycle structure of $GF(2^p)$ CA.

7.1 $GF(2^p)$ CA preliminaries

A $GF(2^p)$ CA can be viewed as an extension of $GF(2)$ CA. It consists of an array of cells, spartially 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

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

where ϕ denotes the local transition function of the ith cell and w_{i-1}, w_i and $w_{i+1} \in GF(2^p)$ specify the weights of interconnections as in Figure 13.

The transition rule for a three neighborhood $GF(2^p)$ CA cell is represented by a vector of length 3, $< w_{i-1}, w_i, w_{i+1} >$. 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 dependency on itself and its right neighborhood respectively. If the same transition rule vector is applied to all the cells of a $GF(2^p)$ CA, the CA is called an **uniform** $GF(2^p)$ CA, otherwise it is called a **hybrid** $GF(2^p)$ CA.

An n cell $GF(2^p)$ CA can be characterized by an $n \times n$ state transition matrix $T = (t_{ij})$ as follows:

$$t_{ij} = \begin{cases} w_{ij}, & \text{if the next state of the } i\text{th cell depends on the present} \\ & \text{state of the } j\text{th cell by a weight } w_{ij} \in GF(2^p), \\ 0, & \text{otherwise.} \end{cases}$$

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

$$T = \begin{pmatrix} 0 & \alpha^2 & 0 \\ \alpha^2 & \alpha & \alpha^2 \\ 0 & \alpha^2 & 1 \end{pmatrix}$$

where α is a generator of $GF(2^2) = \{0, 1, \alpha, \alpha^2\}$. α is a solution of the generator polynomial $g(x) = x^2 + x + 1$ and the generating matrix M is as the following form:

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

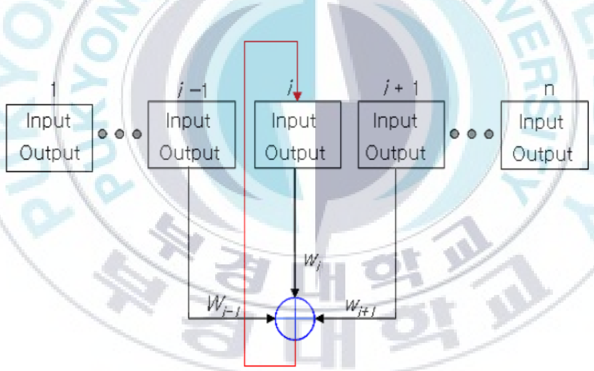

Figure 13: **A $GF(2^p)$ CA Structure**

The next state X' of the present state X of an n-cell $GF(2^p)$ CA with state transition matrix T is given by $X' = TX$. Here T is an $n \times n$ matrix and X and X' are $n \times 1$ vectors.

For the vectors X and X' we need a vector representation of each α^i. Each of the vectors X and X' consists of a string of elements $\alpha^i \in GF(2^p)$.

Table 14. Multiplication and addition over $GF(2^2)$

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	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

Therefore we need a binary representation of each of these α^i. The last column vector of M^i is used as the vector representation of α^i.

The addition and multiplication operations follow the additive and multiplicative rules of the underlying $GF(2^2)$ as noted in Table 14.

In the above example M^i $(i = 2, 3)$ and α^i $(i = 1, 2, 3)$ are as the following form:

$$M^2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad M^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\alpha =< 10 >= 2, \alpha^2 =< 11 >= 3, \alpha^3 =< 01 >= 1$$

The *characteristic polynomial* $\Delta(x)$ of the state transition matrix T of a $GF(2^p)$ CA is $\Delta(x) = |T + xI|$. In the above example the characteristic polynomial of T is $\Delta(x) = x^3 + 2x^2 + 3x + 3$. This polynomial is a primitive polynomial on $GF(2^2)$ and thus its period is 63.

Let $\mathbb{C}$ be a $GF(2^p)$ CA whose state transition matrix is T. If $\det(T) \neq 0$, then $\mathbb{C}$ is called a **group** $GF(2^p)$ CA, otherwise it is called a **nongroup** $GF(2^p)$ CA.

7.2 The cycle structure of $GF(2^p)$ CA

In this section we analyze the cycle structure of $GF(2^p)$ CA.

Let $T_{R,n}$ denote the matrix of a $GF(2^p)$ CA with n cells and with uniform rule R. The rule vector R is of the form $<\alpha_l, \alpha_s, \alpha_r>$ where $\alpha_l, \alpha_s, \alpha_r \in GF(2^p)$. The state transition matrix of such null boundary $GF(2^p)$ CA is as the following form:

$$T_{R,n} = \begin{pmatrix} \alpha_s & \alpha_r & 0 & 0 & 0 & \cdots & 0 & 0 \\ \alpha_l & \alpha_s & \alpha_r & 0 & 0 & \cdots & 0 & 0 \\ 0 & \alpha_l & \alpha_s & \alpha_r & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & \alpha_l & \alpha_s \end{pmatrix}$$

Theorem 7.2.1 Let $\mathbb{C}$ be an n-cell uniform $GF(2^p)$ CA with transition rule $<\alpha_l, \alpha_s, \alpha_r>$, where $\alpha_s \neq 0$ and $\alpha_l\alpha_r = 0$. Then $\mathbb{C}$ is a group CA.

Proof. For the case $\alpha_l = \alpha_r = 0$, the state transition matrix T of $\mathbb{C}$ becomes a diagonal matrix. Since $\alpha_s \neq 0$, $\det(T) = \alpha_s^n \neq 0$. Therefore $\mathbb{C}$ is a group $GF(2^p)$ CA. For the case $\alpha_l = 0$ (resp. $\alpha_r = 0$), the state transition matrix T of $\mathbb{C}$ becomes an upper diagonal(resp. lower diagonal) matrix. Since $\alpha_s \neq 0$, $\det(T) = \alpha_s^n \neq 0$. Therefore $\mathbb{C}$ is a group $GF(2^p)$ CA.

Theorem 7.2.2 Let $\mathbb{C}$ be an n-cell uniform $GF(2^p)$ CA with transition rule $<\alpha_l, \alpha_s, \alpha_r>$, where $\alpha_l \neq 0, \alpha_s \neq 0, \alpha_r \neq 0$, $\alpha_s^2 = \alpha_l\alpha_r$ and $n(mod\ 3) \neq 2$ (resp. $n(mod\ 3) = 2$). Then $\mathbb{C}$ is a group(resp. nongroup) $GF(2^p)$ CA.

Proof. Let $T_{R,n}$ be the state transition matrix of $\mathbb{C}$. Then the determinant $|T_{R,n}|$ of $T_{R,n}$ satisfies the following:

$$|T_{R,n}| = \alpha_s |T_{R,n-1}| + \alpha_l \alpha_r |T_{R,n-2}|$$

For the case $n = 1$, $|T_{R,1}| = \alpha_s \neq 0$. For the case $n = 2$, $|T_{R,2}| = \alpha_s^2 + \alpha_l \alpha_r = 0$. For the case $n = 3$, $|T_{R,3}| = \alpha_s |T_{R,2}| + \alpha_l \alpha_r |T_{R,1}| = \alpha_l \alpha_s \alpha_r \neq 0$. Suppose that $|T_{R,m}| \neq 0$ for $m = 3p$ or $m = 3p + 1$, and $|T_{R,m}| = 0$ for $m = 3p + 2$. Then

(i) $|T_{R,3(p+1)}| = |T_{R,3p+3}| = \alpha_s |T_{R,3p+2}| + \alpha_l \alpha_r |T_{R,3p+1}| = \alpha_l \alpha_r |T_{R,3p+1}| \neq 0$

(ii) $|T_{R,3(p+1)+1}| = |T_{R,3p+4}| = \alpha_s |T_{R,3p+3}| + \alpha_l \alpha_r |T_{R,3p+2}| = \alpha_s |T_{R,3p+3}| \neq 0$

(iii)

$$\begin{aligned} |T_{R,3(p+1)+2}| &= |T_{R,3p+5}| = \alpha_s |T_{R,3p+4}| + \alpha_l \alpha_r |T_{R,3p+3}| \\ &= (\alpha_s^2 + \alpha_l \alpha_r) |T_{R,3p+3}| = 0 \end{aligned}$$

Hence $\mathbb{C}$ is a group $GF(2^p)$ CA for $n(mod\ 3) \neq 2$ and $\mathbb{C}$ is a nongroup $GF(2^p)$ CA for $n(mod\ 3) = 2$.

Theorem 7.2.3 Let $\mathbb{C}$ be an n-cell uniform $GF(2^p)$ CA with transition rule $< \alpha_l, \alpha_s, \alpha_r >$, where $\alpha_s = 0, \alpha_l \neq 0$ and $\alpha_r \neq 0$. Then $\mathbb{C}$ is a group(resp. nongroup) $\mathbb{C}\mathbb{A}$ for even(resp. odd) n.

Proof. (i) $n = 2m + 1$: Since $|T_{R,1}| = \alpha_s = 0$,

$$|T_{R,2m+1}| = \alpha_l \alpha_r |T_{R,2m-1}| = (\alpha_l \alpha_r)^2 |T_{R,2m-3}| = \cdots = (\alpha_l \alpha_r)^m |T_{R,1}| = 0$$

(ii) $n = 2m$: Since $|T_{R,2}| = \alpha_l \alpha_r \neq 0$,

$$|T_{R,2m+1}| = \alpha_l \alpha_r |T_{R,2m-1}| = (\alpha_l \alpha_r)^2 |T_{R,2m-3}| = \cdots = (\alpha_l \alpha_r)^m |T_{R,1}| = 0$$

By (i) and (ii) we obtain the following:

$$|T_{R,n}| = \begin{cases} (\alpha\alpha)^{\frac{n}{2}}, & n\text{:even} \\ 0, & n\text{:odd} \end{cases}$$

Theorem 7.2.4 Let $\mathbb{C}$ be an n-cell hybrid $GF(2^p)$ CA with rule vector R_i, where $i = 1, 2$. Let $R_i (i = 1, 2)$ be of the following form.

$$R_1 = \begin{cases} < \alpha_l, 0, \alpha_r >, \textit{ the cell number is odd} \\ < \alpha_l, \alpha_s, \alpha_r >, \textit{ the cell number is even} \end{cases}$$

$$R_2 = \begin{cases} < \alpha_l, \alpha_s, \alpha_r >, \textit{ the cell number is odd} \\ < \alpha_l, 0, \alpha_r >, \textit{ the cell number is even} \end{cases}$$

Then the following hold:

$$|T_{R_1,n}| = \begin{cases} (\alpha_l\alpha_r)^{\frac{n}{2}}, & n\text{: even} \\ 0, & n\text{:odd} \end{cases}$$

$$|T_{R_2,n}| = \begin{cases} (\alpha_l\alpha_r)^{\frac{n}{2}}, & n\text{: even} \\ \alpha_s(\alpha_l\alpha_r)^{\frac{n-1}{2}}, & n(\text{mod } 4)\text{=1} \\ 0, & \text{otherwise} \end{cases}$$

Proof. Let $T_{R_i,(k,n)} (i = 1, 2)$ be the submatrix obtained from $T_{R_i,n}$ by deleting from the 1st row to the $(k-1)$th row and from the 1st column to the $(k-1)$th column.

(i) $n = 2m$: $|T_{R_i,n}| = 0 \cdot |T_{R_i,(2,n)}| + \alpha_l\alpha_r|T_{R_i,(3,n)}| = \alpha_l\alpha_r|T_{R_i,(3,n)}|$. Therefore we obtain $|T_{R_i,n}| = (\alpha_l\alpha_r)^m$.

(ii) $n = 2m + 1$:

For the rule vector R_1, $|T_{R_1,2m+1}| = \alpha_l\alpha_r|T_{R_1,2m-1}| = (\alpha_l\alpha_r)^2|T_{R_1,2m-3}| = \cdots = (\alpha_l\alpha_r)^m|T_{R_1,1}| = (\alpha_l\alpha_r)^m \cdot 0 = 0$.

For the rule vector R_2, since

$$\begin{aligned}
|T_{R_2,n}| &= \alpha_s|T_{R_2,(2,n)}| + \alpha_l\alpha_r|T_{R_2,(3,n)}| \\
&= \alpha_s(0 + \alpha_l\alpha_r|T_{R_2,(3,n)}|) + \alpha_l\alpha_r(\alpha_s|T_{R_2,(3,n)}| + \alpha_l\alpha_r|T_{R_2,(4,n)}|) \\
&= (\alpha_l\alpha_r)^2|T_{R_2,(4,n)}|
\end{aligned}$$

we obtain

$$|T_{R_2,n}| = \begin{cases} (\alpha_l\alpha_r)^{2m}\alpha_s, & n{=}4m{+}1 \\ (\alpha_l\alpha_r)^{2m}|T_{R_2,(4m+1,4m+3)}| = 0, & n{=}4m{+}3 \end{cases}$$

This completes the proof.

Denote the minimal polynomial by $m(x)$. Let $m(x) = x^d\phi(x)$. If $d > 0$, then $\mathbb{C}$ is a nongroup $GF(2^p)$ CA and if $d = 0$, then $\mathbb{C}$ is a group $GF(2^p)$ CA. d determines the depth of the tree of the state-transition diagram of $\mathbb{C}$. Also $\phi(x)$ determines the cycle structure of the state-transition diagram of $\mathbb{C}$. We can write $\phi(x)$ as the following:

$$\phi(x) = [f_1(x)]^{r_1}[f_2(x)]^{r_2}\cdots[f_h(x)]^{r_h}$$

where $f_i(x)$ is an irreducible polynomial for all $i = 1, 2, \cdots, h$.

Elspas [40] analyzed the cycle structure of $GF(2)$ CA. By using the results of Elspas [40] we can extend these results over $GF(2^p)$ CA.

(i) $\phi(x) = [f(x)]^r$ ($f(x)$ is an irreducible polynomial.)

Let the period of $f(x)$ be k. Then the cycle structure is $[1(1), \mu_1(k)]$, where $\mu_1 = \frac{2^{np}-1}{k}$.

(ii) $\phi(x) = [f(x)]^r$ ($f(x)$ is irreducible polynomial.)

Let the period of $f(x)$ be k and $2^{r_1-1} < r \leq 2^{r_1}$. Then in the state-transition diagram there exist cycles whose lengths are $1, k, 2k, 2^2k, \cdots, 2^{r_1}k$. Also the cycle structures are $[1(1), \mu_1(k), \mu_2(2k), \mu_3(2^2k), \cdots, \mu_{r_1+1}(2^{r_1}k)]$. In $\mu_i(k_i)$, μ_i is the number of cycles whose period is k_i.

Let $U_i = \{x | [f(T)]^i x = 0\}$ and $x \in U_2 - U_1$. Then $[f(T)]^2 x = 0$ and $f(T)x \neq 0$. This vector x belongs to the cycle with the period $[f(x)]^2$. Thus $\mu_i = \frac{n(U_{i-1}-U_{i-2})}{2^{i-1}k}$. Here $n(A)$ is the number of elements of A.

Example 7.2.5 Let $\mathbb{C}$ be a 6-cell $GF(2^2)$ CA with the minimal polynomial $(x^2+2x+2)^3$. Since x^2+2x+2 is a primitive polynomial over $GF(2^2)$, the period of x^2+2x+2 is $2^{2 \cdot 2}-1 = 15$. Also since $2 < 3 \leq 2^2$, the lengths of all existing cycles are $1, 15, 2 \times 15, 2^2 \times 15$, i.e., $1, 15, 30, 60$. The number of cycle containing the vector 0 is 1, the number of cycles of length 15 is $\frac{(2^2)^2-1}{15} = 1$ and the number of cycles of length 30 is $\frac{(2^2)^4-(2^2)^2}{30} = 8$. Finally, the number of cycles of length 60 is $\frac{(2^2)^6-(2^2)^4}{60} = 64$.

(iii) $\phi(x) = f(x)g(x)$ ($f(x)$ and $g(x)$ are irreducible polynomials.)

Let the degree of $f(x)$ (resp. $g(x)$) be d_1 (resp. d_2) and the period of $f(x)$ (resp. $g(x)$) be k_1 (resp. k_2). Then the cycle generated by $f(x)$ (resp. $g(x)$) is $[1(1), \mu_1(k_1)]$ (resp. $[1(1), \mu_2(k_2)]$). Thus the cycle structure is

$$[1(1), \mu_1(k_1)][1(1), \mu_2(k_2)] = [1(1), \mu_1(k_1), \mu_2(k_2), \mu(k)]$$

where $\mu = \mu_1\mu_2 \gcd(k_1, k_2)$ and $k = lcm(k_1, k_2)$.

Example 7.2.6 Let $\mathbb{C}$ be a 7-cell $GF(2^2)$ CA with the minimal polynomial $m(x) = (x+3)(x^2+x+2)^3$. Then the cycle structure is

$$[1(1), 1(3)][1(1), 1(15), 8(30), 64(60)] = [1(1), 1(3), 4(15), 32(30), 256(60)]$$

7.3 The characteristic polynomial of $GF(2^p)$ CA

In the state transition matrix T of $GF(2^p)$ CA $\mathbb{C}$ let the weight of the right state and the weight of the left state be the same. Then this $GF(2^p)$ CA is the natural extension of 90/150 $GF(2)$ CA. Therefore the T is as the following:

$$T = \begin{pmatrix} d_1 & i & 0 & \cdots & 0 & 0 \\ i & d_2 & i & \cdots & 0 & 0 \\ 0 & i & d_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & i & d_n \end{pmatrix}$$

where $i \in \{0, 1, 2, \cdots, 2^p - 1\}$ is the weight.

Remark We denote the state transition matrix T by $T =< d_1, d_2, \cdots, d_n >_i$, where $d_j \in GF(2^p)$.

The following theorem can be proved by mathematical induction.

Theorem 7.3.1 Let $\mathbb{C}$ be an n-cell $GF(2^p)$ CA with the state transition matrix $T =< d_1, d_2, \cdots, d_n >_i$ and with the characteristic polynomial Δ_n. Then we obtain the following equation.

$$\begin{aligned} \Delta_{-1} &= 0 \\ \Delta_0 &= 1 \\ \Delta_k &= (x + d_k)\Delta_{k-1} + i^2\Delta_{k-2} \qquad (7.1) \end{aligned}$$

where Δ_k is the characteristic polynomial of $< d_1, d_2, \cdots, d_k >_i$,$k = 1, 2, \cdots, n$.

Theorem 7.3.1 provides an efficient algorithm to compute the characteristic polynomial of a $GF(2^p)$ CA. Initially, Δ_{-1} and Δ_0 are set to zero and one, respectively. Equation (7.1) is applied to obtain Δ_1. It is then reapplied to Δ_0 and Δ_1 to calculate Δ_2. Continuing, the polynomials $\Delta_3, \Delta_4, \cdots, \Delta_n$ are computed. Since Δ_n is the characteristic polynomial of T, the calculation of the characteristic polynomial is completed.

The following is an example of the calculation of the characteristic polynomial of the $GF(2^p)$ CA with the rule vector $< 0, 1, 2, 1 >_2$.

Example 7.3.2 Let $\mathbb{C}$ be a $GF(2^2)$ CA with the rule vector $< 0, 1, 2, 1 >_2$.

$$
\begin{aligned}
\Delta_{-1} &= 0 \\
\Delta_0 &= 1 \\
\Delta_1 &= (x + d_1)\Delta_0 + 2^2\Delta_{-1} \\
&= (x + 0) \cdot 1 + 2^2 \cdot 0 \\
&= x \\
\Delta_2 &= (x + d_2)\Delta_1 + 2^2\Delta_0 \qquad (7.2) \\
&= (x + 1) \cdot x + 2^2 \cdot 1 \\
&= x^2 + x + 3 \\
\Delta_3 &= (x + d_3)\Delta_2 + 2^2\Delta_1 \\
&= (x + 2) \cdot (x^2 + x + 3) + 2^2 \cdot x \\
&= x^3 + 3x^2 + 2x + 1 \\
\Delta_4 &= (x + d_4)\Delta_3 + 3^2\Delta_2
\end{aligned}
$$

$$\begin{aligned} &= (x+1)\cdot(x^3+3x^2+2x+1)+2^2\cdot(x^2+x+3) \\ &= x^4+2x^3+2x^2+3 \end{aligned}$$

This recurrence relation forms the basis for the synthesis of $GF(2^p)$ CA. Initially, we show how recurrence (7.1) satisfies the division algorithm for polynomials. Then we demonstrate that the repeated application of the recurrence relation is a reverse GCD computation.

We now show that repeated application of the division algorithm reverses the computation of the characteristic polynomial of a $GF(2^p)$ CA. Suppose that Δ_n and Δ_{n-1} are known. By the division algorithm, $x+d_n$ and Δ_{n-2} are uniquely determined and easily calculated. If the division algorithm is then applied to Δ_{n-1} and Δ_{n-2}, it will calculate $x+d_{n-1}$ and Δ_{n-3}. We may continue this process until we have computed $x+d_1$ and $\Delta_{-1}=0$.

Example 7.3.3 Let $\mathbb{C}$ be a 4-cell $GF(2^2)$ CA with $\Delta_4 = x^4+2x^3+2x^2+3$ and $\Delta_3 = x^3+3x^2+2x+1$.

dividend	*divisor*	*quotient*	*remainder*	$GF(2^2)$ *CA byte*	
Δ_4	Δ_3	$x+1$	$2^2(x^2+x+3)$	1	
Δ_3	x^2+x+3	$x+2$	2^2x	2	(7.3)
x^2+x+3	x	$x+1$	$2^2\cdot 1$	1	
x	1	$x+0$	$2^2\cdot 0$	0	

From the calculation, we see that the divisor column is the same as the dividend column shifted up one position and the remainder column is a shift of the i^2 times with the divisor column. Comparing (7.2) to (7.3), we see that the sequence of polynomial in (7.3) is the reverse of the sequence of intermediate polynomials in the characteristic polynomial calculation. Furthermore, (7.3) yields the sequence of quotients

$$[x+0, x+1, x+2, x+1]$$

By taking the constant terms of these quotients and reversing, we obtain the rule vector $< 0, 1, 2, 1 >_2$.

In Example 7.3.3 let $\Delta_3 = x^3 + 3$. Then we obtain the rule vector $< 3, 1, 2, 2 >_3$. Also let $\Delta_3 = x^3$. Then we obtain the rule vector $< 0, 0, 0, 2 >_3$.

If $\mathbb{C}$ is an n-cell $GF(2)$ 90/150 CA with the primitive polynomial as the characteristic polynomial, then there exist two Δ_{n-1}. But the Δ_{n-1} are several in the Example 7.3.3.

By Theorem 7.3.1 we can obtain a $GF(2^p)$ CA with Δ_n and Δ_{n-1}. But the method for finding Δ_{n-1} does not exist until now.

Theorem 7.3.4 Let $\mathbb{C}$ be an n-cell $GF(2^p)$ CA with the state transition matrix $T =< d_1, d_2, \cdots, d_n >_i$. And let $p(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ be the primitive polynomial which is the characteristic polynomial of T. For the nonsingular upper tridiagonal matrix U and for the companion matrix C of $p(x)$, let U and C be as the following:

$$U = (u_{ij}) = \begin{cases} u_i, \ i = j \\ a_i, \ i = j-1 \\ 0, \ i > j \\ x_{ij} \in GF(2^p), \ otherwise \end{cases} \qquad C = (s_{ij}) = \begin{cases} 1, \ i = j+1 \ (j < n) \\ c_{i-1}, \ j = n \\ 0, \ otherwise \end{cases}$$

where c_i is the coefficient of $p(x)$. Then we obtain the following equation.

$$\begin{cases} d_1 = u_1^{-1}a_1 \\ d_k = u_{k-1}^{-1}a_{k-1} + u_k^{-1}a_k \ (1 < k < n) \\ d_n = u_{n-1}^{-1}a_{n-1} + c_{n-1} \end{cases} \tag{7.4}$$

Proof. Since the characteristic polynomials and the minimal polynomials of T and C are the same, T and C are similar. So $TU = UC$. Then we obtain the following:

$$\begin{cases} a_1 = u_1 d_1 \\ a_k = ia_{k-1} + u_k d_k \ (1 < k < n) \\ c_{n-1}u_n = ia_{n-1} + u_n d_n \\ u_{i+1} = iu_i \end{cases} \tag{7.5}$$

Since $i = u_{k-1}^{-1}u_k$, we obtain the following required result

$$\begin{cases} d_1 = u^{-1}a_1 \\ d_k = u_{k-1}^{-1}a_{k-1} + u_k^{-1}a_k \ (1 < k < n) \\ d_n = u_{n-1}^{-1}a_{n-1} + c_{n-1} \end{cases} \tag{7.6}$$

Example 7.3.5 Let $T =< 0, 3, 1 >_2$. Since the characteristic polynomial of T is $x^3 + 2x^2 + 3x + 3$,

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

Since $i = 2$, we obtain U as the following:

$$U = \begin{pmatrix} u_1 & a_1 & * \\ 0 & 2u_1 & a_2 \\ 0 & 0 & 3u_1 \end{pmatrix}$$

Solving $TU = UC$, we obtain U as the following:

$$U = \begin{pmatrix} u_1 & 0 & * \\ 0 & 2u_1 & u_1 \\ 0 & 0 & 3u_1 \end{pmatrix} = u_1 \begin{pmatrix} 1 & 0 & * \\ 0 & 2 & 1 \\ 0 & 0 & 3 \end{pmatrix},\ u_1(\neq 0) \in GF(2^2)$$

The possible U is the following:

$$U_1 = \begin{pmatrix} 1 & 0 & * \\ 0 & 2 & 1 \\ 0 & 0 & 3 \end{pmatrix},\ U_2 = \begin{pmatrix} 2 & 0 & * \\ 0 & 3 & 2 \\ 0 & 0 & 1 \end{pmatrix},\ U_3 \begin{pmatrix} 3 & 0 & * \\ 0 & 1 & 3 \\ 0 & 0 & 2 \end{pmatrix}$$

By the equation (7.6) we obtain d_1, d_2, d_3 as the following: $d_1 = 1 \cdot 0 = 0,\ d_2 = 0 + 2^{-1} \cdot 1 = 3,\ d_3 = 3 + 1 = 1$

Chapter 8

Conclusion

We provided a comprehensive survey on CA and analyzed several complemented CA derived from a LUGCA with rule 60 or 102 according to the complement vector and investigated some properties of these CA and showed that Das's conjecture is true. Also the order of the state transition operator of the complemented CA derived from a LUGCA with rule 60 or 102 is characterized explicitly. we analyzed a LHGCA $\mathbb{C}$ with rules 60, 102 and 204 and the complemented CA $\mathbb{C}'$ derived from $\mathbb{C}$. And we gave the conditions for the complement vectors which determine the state transition of the CA dividing the entire state space into smaller spaces of equal maximum cycle lengths. And we investigated the sequences obtained from a 90/150 MLCA algebraically. And we applyed these to phase shifting of sequences generated by a 90/150 MLCA. From these applications we gave an improved method to compute phase shifts, which is different from those methods of Bardell's ([27]), Nandi and Chaudhuri's ([32]) and Sarkar's ([29]). Also we proposed a new method of modelling linear CA with the minimum stage corresponding to CCSGs based on LFSR. Finally, by using the results in ([36], [40]) we analyzed the transition rule, the characteristic polynomial and the cycle structure of $GF(2^p)$ CA.

References

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

[2] Z. Chauanwu and L. Libin, *VLSI characteristic of cellular automata as LFSR*, Communications and Information Technology, 2005. ISCIT 2005, IEEE International Symposium. Vol. 2, 2005, pp. 1031-1034.

[3] J. Von Neumann, *The Theory of Self-reproducing Automata*, A.W. Burks ed. (Univ. of Illinois Press, Urbana and London), 1966.

[4] S. Wolfram, *Statistical Mechanics of Cellular Automata*, Rev. Mod. Phys., Vol. 55, 1983, pp. 601-644.

[5] J. Thatcher, *Universality in von Neumann Cellular Model*, Tech. Rep. 0310530-T, ORA, University of Michigan, 1964.

[6] C.h. Lee, *Synthesis of a Cellular Universal Machine Using 29-state Model of von Neumann*, in The University of Machigan Engineering Summer Conferences, 1964.

[7] E.F. Codd, *Cellular Automata*, Academic Press Inc., 1968.

[8] F.C. Hennie, *Iterative Arrays of Logical Circuits*, Academic, Nework, London, 1961.

[9] 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.

[10] A.K. Das and P.P. Chaudhuri, *Efficient Characterization of Cellular Automata*, Proc. IEE(Part E), Vol. 137, No. 1990, pp. 81-87.

[11] 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.

[12] S. Nandi , B.K. Kar and P.P. Chaudhuri, *Theory and Applications of Cellular Automata in Cryptography*, IEEE Trans. Computers, Vol. 43, 1994, pp. 1346-1357.

[13] D. Mukhopadhyay and D.R. Chowdhury, *Characterization of a Class of Complemented Group Cellular Automata*, Lecture Notes in Computer Science, Vol. 3305, 2004, pp. 775-784.

[14] S. Chakraborty, D.R. Chowdhury, P.P. Chaudhuri, *Theory and Application of Nongroup Cellular Automata for Synthesis of Easily Testable Finite State Machines*, IEEE Trans. Computers, Vol. 45, No. 7, 1996, pp. 769-781.

[15] 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.

[16] 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, Vol. 3305, 2004, pp. 31-39.

[17] S.J. Cho , U.S. Choi and H.D. Kim, *Analysis of Complemented CA derived from a Linear TPMACA*, Computers and Mathematics with Applications, Vol. 45, 2003, pp. 689-698.

[18] 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, Vol. 36, 2002, pp. 979-986.

[19] S.J. Cho, Y.H. Hwang, U.S. Choi, H.D. Kim and Y.S. Pyo, *Characterizatioin of a class of the Complemented CA derived from Linear Uniform CA*, submitted.

[20] S. Sen, C. Shaw, D.R. Chowdhury, N. Ganguly and P.P. Chaudhuri, *Cellular Automata based Cryptosystem*, ICICS 2002, Lecture Notes in Computer Science, Vol. 2513, 2002, pp. 303-314.

[21] M. Mukherjee, N. Ganguly and P.P. Chaudhuri, *Cellular Automata base Authentication*, ACRI 2002, Lecture Notes in Computer Science, Vol. 2493, 2002,pp. 259-269.

[22] J.C Jeon, K.W. Kim and K.Y. Yoo, *Non-group Cellular Automata Based One Time Password Authentication Scheme in Wireless Networks*, MADNES 2005, Lecture Notes in Computer Science, Vol. 4074, 2006, pp. 110-116.

[23] M. Seredynski, P. Bouvry, *Block Encryption Using Reversible Cellular Automata*, ACRI 2004, Lecture Notes in Computer Science, Vol. 3305, 2004, pp. 785-792.

[24] J.C. Jeon and K.Y. Yoo, *Authentication Based on Singular Cellular Automata*, ACRI 2006, Lecture Notes in Computer Science, Vol. 4173, 2006, pp. 605-610.

[25] A. Martin del Rey, *Message Authentication Protocol Based on Cellular Automata*, EvoWorkshops 2007, Lecture Notes in Computer Science, Vol. 4448, 2007, pp. 52-60.

[26] M. Mihaljevic, Y. Zheng and H. Imai, *A cellular automaton based fast one-way hash function suitable for hardware implementation*, PKC' 98, Lecture Notes in Computer Science, Vol. 1431, 1998, pp. 217-233.

[27] P.H. Bardell, *Analysis of Cellular Automata used as Pseudorandom Pattern Generators*, Proc. IEEE int. Test. Conf., 1990, pp. 762-767.

[28] S. Tezuka and M. Fushimi, *A Method of Designing Cellular Automata as Pseudorandom Number Generators for Built-In Self-Test for VLSI*, Comtermporary Mathematica, Vol. 168, 1994, pp. 363-367.

[29] P. Sarkar, *Computing Shifts in 90/150 Cellular Automata Sequences*, Finite Fields Their Appl., Vol. 42, 2003, pp. 340-352.

[30] S.J. Cho, *Analysis of Pseudo-Noise Sequences Generated by Cellular Automata*, Submitted.

[31] A. Petre, I. Silviu and S. Emil,*Block Encryption Using Hybrid Additive Cellular Automata Hybrid Intelligent Systems*, HIS 2007. 7th International Conference, 2007, pp. 132 - 137.

[32] S. Nandi and P.P. Chaudhuri, *Additive Cellular Automata as an on-chip test pattern generator*, IEEE, 1993, pp. 166-171.

[33] J.D. Golic, *Toward fast correlation attacks on irregularly clocked shift registers*, Advances in Cryptology - EUROCRYPT'95, Lecture Notes in Computer Science, Vol. 921, 1995, pp. 248-262.

[34] D. Gollmann and W.G. Chambers, *Clock controlled shift registers: a review*, IEEE J. Sel. Ar. Commun., Vol. 7(4), 1989, pp. 525-533.

[35] A.F. Sabater and D.G. Martinez, *Modelling nonlinear sequence genterators in terms of linear cellular automata*, Applied Mathematical Modelling, Vol. 31, 2007, pp. 226-235.

[36] K. M. Cattell and Jon C. Muzio, *Synthesis of One-Dimensional Linear Hybrid Cellular Automata*, IEEE Trans. Comput-Aided Des. Integr. Circuits Syst., Vol 15(3), 1996, pp. 325-335.

[37] 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, pp. 403-408.

[38] 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, Vol. 26(9), 2007, pp. 1720 - 1724.

[39] S.J. Cho, U.S. Choi, Y.H. Hwang, H.D. Kim and H.H. Choi, *Behavior of Single Attractor Cellular Automata over Galois Field* $GF(2^p$, Lecture Notes in Computer Science, Vol. 4173, 2006, pp. 232-237.

[40] B. Elspas, *The Theory of autonomous linear sequential networks*, TRE Trans. on Circuits, CT-6(1), 1959, pp. 45-60.

[41] S. Wolfram, *Cryptography with cellular automata*, Proc. Crypto'85, Lect. Notes Comput. Sci.Springer Verlag, Vol. 218, 1986, pp. 429-432.

[42] J.C. Jeon and K.Y. Yoo, *Design of Montgomery Multiplication Architecture based on Programmable Cellular Automata*, Computational intelligence 20, 2004, pp. 495-502.

[43] P.D. Hortencius, R.D. McLeod, W. Pries, D.M. Miller, and H.C. Card. *Cellular automata based pseudorandom number generators for built-in self test*, IEEE Transaction on CAD, 8(8), 1989, pp. 842-849.

[44] F.R. Gantmacher, *The Theory of Matrices*, Chelsea Publishing Company New York, 1959.

[45] D.E. Knuth, *The Art of Computer Programming - Seminumerical Algorithms*, Addison-Wesley, 1981.

[46] W. Pries, A. Thanailakis and H.C. Card, *Group Properties of Cellular Automata and VLSI Applications*, IEEE Trans. Computers, Vol. C-35, 1986, pp. 1013-1024.

[47] C.L. Chen, *Exhautive Test Pattern Generation Using Cyclic Codes*, IEEE Trans. Comput., Vol. C-37, 1988, pp. 225-228.

[48] 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.

[49] Ph. Tsalides, *Cellular Automata based Built-In Self-Test Structures for VLSI Systems*, Elect. Lett., Vol. 26, no.17, 1990, pp. 1350-1352.

[50] Ph. Tsalides, T.A. York, and A. Thanailakis, *Pseudo-random Number Generator for VLSI Systems based on Linear Cellular Automata*, IEE Proc. E. Comput. Digit. Tech., Vol. 138, no. 4, 1991, pp. 241-249.

[51] P.D. Hortensius et al., *Cellular Automata Based Pseudo-random Number Generators for Built-In Self-Test*, IEEE Trans. Computer-Aided Design, Vol. 8, 1989, pp. 842-859.

[52] D.R. Chowdhury, P.P. Chaudhuri, *Parallel Memory Testing : a BIST Approach*, in Proc. 3rd Intl. Workshop on VLSI Design. Bangalore, India, 1989, pp.373-377.

[53] P. Sarkar, *The filter-combiner model for memoryless synchronous stream ciphers*, in Proceedings of Crypto 2002, Lecture Notes in Computer Science, Springer, Berlin 2442, 2002, pp. 533-548.

[54] S.W. Golomb, *Shift Register Sequeces*, Holden Day, 1967.

[55] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, 1997.

[56] A.J. Menezes, P.C. van Oorschot and S.A. Vanstone, *Handbook of Applied Cryptography,* CRC Press, 1997.

[57] P.H. Bardell, W.H. McAnney and J. Savir, *Built-In Test for VLSI: Pseudorandom Techniques*, A Wiley-Interscience Publication, 1987.

[58] D. Coppersmith, H. Krawczyk and Y. Mansour, *The shrinking generator*, Lecture Notes in Computer Science, Vol. 773, 1994, pp. 22-39.

[59] G. Gong, *Theory and applications of q-ary interleaved sequences*, IEEE Transaction on Information Theory, Vol. 41(2), 1995, pp. 400-411.

[60] H. Umeo, T. Yanagihara and M. Kanazawa, *State-Efficient Firing Squad Synchronization Protocols for Communication-Restricted Cellular Automata*, Lecture Notes in Computer Science, Vol. 4173, 2006, pp. 169-181.

[61] A. Kanso, *Clock-controlled shrinking generators*, Lecture Notes in Computer Science, Vol. 2727, 2003, pp. 443-451.

[62] S.J. Cho, U.S. Choi, Y.H. Hwang, H.D. Kim, H.H. Choi, *Behavior of Single Attractor Cellular Automata over Galois Field $GF(2^p)$*, Lecture Notes in Computer Science, Vol. 4173, 2007. pp. 232-237.

감사의 글

대학원 6년과정은 공부가 내가 좋아하고 내가 가진 능력 중에서 가장 잘 할 수 있는 일임을 깨닫는 소중한 시간이었습니다.

부족한 제자를 긴장과 여유로 진정한 학문의 기쁨을 알게 해주신 조성진 지도 교수님께 감사드립니다. 바쁘신 와중에도 논문을 심사해 주신 이경현 교수님, 권기룡 교수님, 신상욱 교수님, 신원 교수님과 대학원 진학을 결심했을 때 셀룰라 오토마타라는 연구실을 소개해 주신 박용범 교수님께 감사드립니다. 대학원 생활 내내 학문과 인생에 자문을 아끼지 않으셨던 최언숙 선배님과 대학원 동기, 선후배님께도 감사드립니다.

연구에 큰 도움을 주시고 기다려지는 세미나 시간을 만들어주신 세미나 팀(조성진 교수님, 김한두 교수님, 표용수 교수님, 최언숙 선배, 허성훈 선배, 권민정 선생님, 진경언니, 봉수)께 감사드립니다.

학사 졸업 직전, 계속 공부하고 싶다던 딸에게 두 말없이 지지해 주시고 6년 동안 끊임없는 관심과 믿음으로 지켜봐주신 어머니와 아버지께 감사드립니다. 며느리 졸업한다고 기뻐해 주시고 빠쁜 저를 이해해 주시고 묵묵히 도움을 주신 아버님께 감사드립니다.

언제나 나를 안팎에서 트레이닝 해주는 든든한 남편 임동찬과 변변하게 같이 놀아주지 못한 사랑하는 아들 민규에게 감사의 마음을 전합니다.

저의 졸업을 고대했던 서울의 윤경 언니, 형부, 그리고 힘이 되는 칭찬을 아끼지 않았던 동생 재용이에게 감사의 마음을 전합니다.

저를 대신하여 민규를 챙겨주셨던 어린이집 원장선생님과 나의 사소한 고민을 같이 해준 친구 주현이에게 감사합니다.