교 육 학 석 사 학 위 논 문

90/150 셀룰라 오토마타에 의해 생성된 최대 길이를 갖는 수열에 관한 연구

지 도 교 수 조 [illegible]

이 논문을 [illegible] 교육학석사 학위논문으로 제출함

2004 년 8 월

부경대학교 교육대학원

수 학 교 육 전 공

고 정 희

고정희의 교육학석사 학위논문을 인준함

2004년 6월 18일

주 심 이학박사 표 용 수 

위 원 이학박사 박 진 한 

위 원 이학박사 조 성 진 

< 목 차 >

Abstract 1

1. 서론 2

2. 셀룰라 오토마타 3

2.1. 셀룰라 오토마타의 정의 3

2.2. 1차원 CA rule 3

2.3. 특성행렬과 특성다항식 8

2.4. group CA 9

3. 원시다항식과 최대주기수열 14

4. 90/150 CA에 의해 생성된 PN 수열 25

4.1. 90/150 CA의 특성행렬의 분석 25

4.2. 90/150 CA에 의해 생성된 PN 수열의 분석 30

참 고 문 헌 44

그림 목차

그림 2.1 : rule 150의 선형 셀 구조 4
그림 2.2> 1차원 CA의 경계조건 7
그림 2.3> 최대길이를 갖는 group CA 11
그림 2.4> 최대길이를 갖지 않는 group CA 12
그림 2.5> nongroup CA 13
그림 4.1> 행렬 C_1 와 C_2 의 각 행백터들의 상태 변화 41

표 목차

표 2.1> CA의 기호 3
표 2.2> rule 90와 rule 150의 상태배열 5
표 2.3> additive CA rules 6
표 4.1> 행렬 B 의 범위와 변위 33
표 4.2> 행렬 C 의 범위, 변위과 행렬 P 35

A study on maximum-length sequences generated by 90/150 Cellular Automata

Jung Hee Ko

Graduate School of Education,

Pukyoung National University

Abstract

Cellular automata are mathematical idealizations of physical systems in which space and time are discrete, and each cell can assume the value either 0 or 1. Each cell is essentially comprised of a memory element and a combinatorial logic that generates the next-state of the cell from the present-state of its neighboring cells(left, right and self).

In view of its applications in the fields of simulation, data encryption, logic circuit testing, and such, high-quality pseudorandom pattern generators are widely used. For a complex circuit with large number of inputs, pseudoexhaustive testing has been found to be suitable where each of the outputs depends only on a subset of inputs. This obviously results in a much smaller test set size compared to the exhaustive test set size of 2^n for an n-input circuit under test.

A group cellular automata has a nonsingular characteristic matrix. Further, group cellular automata can be divided inte two classes-maximum-length and nonmaximum-length. All $(2^n - 1)$ nonzero states of a linear n-cell maximum-length group cellular automata form a single cycle Such a group cellular automata has been projected as a generator of pseudorandom patterns of high quality.

This paper present properties of a characteristic matrix of a maximum-length 90/150 cellular automata and pseudo-noise sequences generated by this cellular automata.

1.서론

셀룰라 오토마타(Cellular Automata, CA)는 동력학계를 해석하는 한 방법으로 시간과 공간을 이산적으로 다루고, 각각의 셀의 값을 0 또는 1로 가정한다. 이러한 이산적인 공간을 셀룰라 공간(cellular space)의 기본 단위인 각 셀이 취할 수 있는 상태를 유한하게 처리하며, 각 셀들의 상태가 국소적인 상호작용에 의해서 동시에 갱신되는 시스템이다.

이러한 CA는 시뮬레이션, 데이터 암호, 논리회로 테스트 등과 같은 고품질의 랜덤 패턴 생성분야에서 수요가 있다. 많은 수의 입력값을 가지는 복잡한 회로에서 몇 개의 부분적인 입력값에만 의존하는 출력값의 위치를 찾는데 적합한 방법들이 연구되어져 왔다. 이는 그것의 다양한 단계(즉, 셀의 위치)로부터의 출력 비트수열의 성질에 기인하다. 본 논문에서 소개될 group CA는 최대 길이를 갖는 것과 그렇지 않은 것으로 나뉜다. 이 중 최대 길이를 가지는 n 셀 CA의 정칙인 특성행렬은 0을 제외한 $2^n - 1$ 개의 최대주기수열을 생성한다.

본 논문에서는 이러한 최대주기수열을 생성하는 생성기로써의 90/150 최대 길이를 가지는 CA의 특성행렬과 이러한 90/150 CA에 의해서 생성된 PN 수열(pseudo-noise sequence)을 분석한다.

본 논문의 구성은 다음과 같다. 2장에서는 셀룰라 오토마타(Cellular Automata, 이하 CA)에 관하여 알아보고, 3장에서는 원시다항식과 최대주기수열에 대해 살펴본다. 4장에서는 90/150 CA에 의해 생성된 PN 수열에 대해 분석하고, 5장에서는 결론을 맺는다.

2. 셀룰라 오토마타

2.1. 셀룰라 오토마타의 정의

셀룰라 오토마타(Cellular Automata, 이하 CA)는 Von Neumann[13]과 Wolfram에 의해 스스로 조직화하고 재생산할 수 있는 모델로 소개되었으며, 이후 Das[6,7,8] 등에 의해서 행렬 대수학으로 분석이 이루어졌다. 최근에는 Chaudhuri, Chowdhury[2], Nandi[9], Cho[3,4,5] 등 여러 학자들에 의해 연구되고 있다.

CA란 동역학계를 해석하는 한 방법으로 공간과 시간을 이산적으로 다루고, 이산적인 공간을 셀룰라 공간(cellular space)의 기본 단위인 각 셀이 취할 수 있는 상태를 유한하게 처리하며, 각 셀들의 상태가 국소적인 상호작용에 의해서 동시에 생신되는 시스템이다.

2.2. 1차원 CA rule

가장 간단한 구조를 가지는 1차원 CA에서는 모든 셀들이 선형으로 배열되어 있고 국소적 상호 작용이 세 개의 셀, 즉 자기 자신과 인접한 두 셀에 의해 이루어지는 3 이웃(3 neighbourhood) CA이다.

CA를 설명하기 위해서는 다음 기호들이 사용된다.

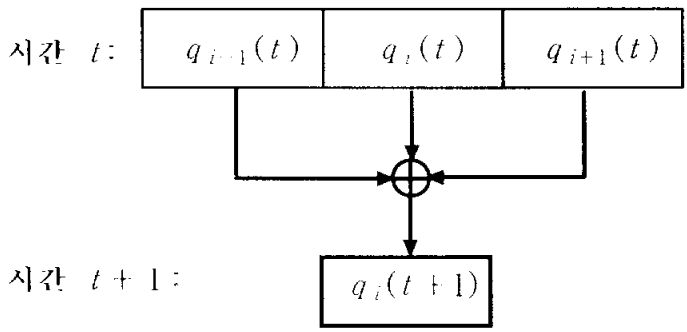
i	일차원으로 배열되어 있는 각 셀들의 위치
t	시간단계
$q_i(t)$	시간 t에서 i번째 셀의 상태

<표 2.1> CA의 기호

3 이웃 CA의 상태전이함수(state transition function)는 다음과 같다.

$$q_i(t+1) = f[q_{i-1}(t), q_i(t), q_{i+1}(t)] \qquad (2.1)$$

여기서 3 이웃 상태전이함수에서 f 는 입력논리를 가지는 국소 전이함수이다. f 는 3개의 변수를 가지는 Boolean 함수이며 따라서 $2^{2^3}(=256)$ 개의 상태전이함수로 되어있고, 이것을 CA rule이라 한다. 예를 들어 rule 90은 왼쪽 셀과 오른쪽 셀에 영향을 받고, rule 150은 왼쪽과 자기 자신, 오른쪽 셀에 영향을 받아 다음상태가 만들어진다. <그림 2.1>은 rule 150 선형 셀 구조이다.



<그림 2.1> rule 150의 선형 셀 구조

3 이웃 CA에서 rule 90와 rule 150의 다음 상태배열의 예를 살펴보면 다음과 같다.

$(q_{i-1}(t), q_i(t), q_{i+1}(t))$	(1,1,1)	(1,1,0)	(1,0,1)	(1,0,0)	(0,1,1)	(0,1,0)	(0,0,1)	(0,0,0)	rule
$q_i(t+1)$	0	1	0	1	1	0	1	0	90
$q_i(t+1)$	1	0	0	1	0	1	1	0	150

<표 2.2> rule 90와 rule 150의 상태배열

이 기서, rule 90와 rule 150의 $q_i(t+1)$의 상태를 차례로 나타내면 각각 01011010, 10010110 이 되고, 이를 십진수로 나타내면 90와 150이 된다.

위의 rule 90 rule 150에 대한 결합논리는 다음식으로 표현될 수 있다. 여기서 $\oplus$는 XOR논리를 나타낸다.

$$\text{rule 90} : \; q_i(t+1) = q_{i-1}(t) \oplus q_{i+1}(t)$$

$$\text{rule 150} : \; q_i(t+1) = q_{i-1}(t) \oplus q_i(t) \oplus q_{i+1}(t)$$

1차원 CA는 셀들에 적용되는 rule의 논리의 종류에 따라 linear CA, additive CA, nonadditive CA로 분류된다. 모든 셀들의 rule이 XOR논리로만 이루어진 CA를 linear CA, XOR과 XNOR의 조합으로 이루어진 CA를 additive CA, AND OR논리로 이루어진 CA를 nonadditive CA라 한다. 다음은 additive CA rule이다.

Linear rule		Complemented rule	
rule	$q_i(t+1)$	rule	$q_i(t+1)$
60	$q_{i-1}(t) \oplus q_i(t)$	195	$q_{i-1}(t) \oplus \overline{q_i(t)}$
90	$q_{i-1}(t) \oplus q_{i+1}(t)$	165	$q_{i-1}(t) \oplus \overline{q_{i+1}(t)}$
102	$q_i(t) \oplus q_{i-1}(t)$	153	$\overline{q_i(t)} \oplus \overline{q_{i-1}(t)}$
150	$q_{i-1}(t) \oplus q_i(t) \oplus q_{i+1}(t)$	105	$q_{i-1}(t) \oplus q_i(t) \oplus \overline{q_{i+1}(t)}$
170	$q_{i+1}(t)$	85	$\overline{q_{i+1}(t)}$
204	$q_i(t)$	51	$\overline{q_i(t)}$
240	$q_{i-1}(t)$	15	$\overline{q_{i-1}(t)}$

<표2.3> additive CA rules

모든 셀에 같은 rule이 적용되었느냐 아부에 따라 uniform CA, hybrid CA로 분류된다.

· uniform CA : 모든 CA의 셀들이 같은 rule이 적용되는 CA

· hybrid CA : 같은 rule이 적용되지 않는 CA

셀들이 rule에 의해 변화되는 상태에 따라 group CA, nongroup CA로 분류된다.

· group CA : 모든 셀들의 상태가 몇 개의 싸이클을 이루며 반복되는 CA

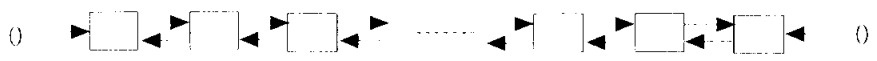
· nongroup CA : 싸이클을 이루지 않는 셀들이 존재하는 CA

CA에서 가장 왼쪽과 가장 오른쪽 셀은 자기 자신과 하나의 이웃만을 가지므로 이들의 나머지 다른 하나의 이웃을 설정해 주는 일은 매우 중요하며 이들 이웃을 설정해 주는 것을 CA의 경계조건이라 한다. 일반적으로 CA의 경계조

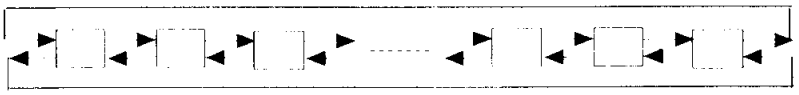
건에 따라 다음 세 가지로 분류한다.

- NBCA(Null Boundary CA) : 가장 왼쪽과 가장 오른쪽의 셀들이 0 상태에 연결되어 있는 경우
- PBCA(Periodic Boundary CA) : 양 끝의 셀들이 연결되어 있는 경우
- IBCA(Intermediate Boundary CA) : 가장 왼쪽(오른쪽)셀의 다음 상태가 그 자신과 그것의 오른쪽(왼쪽) 두 개의 이웃의 상태에 의존하는 경우

<그림 2.2>은 CA의 경계조건을 나타낸 것이다.



(1)1차원 NBCA



(2) 1차원 PBCA

(3) 1차원 IBCA

<그림 2.2> 1차원 CA의 경계조건

2.3. 특성행렬과 특성다항식

n 개의 셀을 가지는 1차원 CA에서 현재 상태를 다음 상태로 전이시키는 작용소를 n 차 정방행렬로 나타낼 수 있는데 이것을 CA의 특성행렬(characteristic matrix)이라 한다.

특성행렬 T에서 i번째 행은 i번째 셀에 적용되는 rule이며 그 셀의 다음 상태가 현재 상태에 의존하면 1, 그렇지 않으면 0으로 쓴다.

$f_t(x)$ 가 t시점에서 CA의 상태를 나타내면 시간 $t+1$에서의 상태는 다음과 같다.

$$f_{t+1}(x) = T \cdot f_t(x) \tag{2.2}$$

<예 2.3.1> 4 셀의 1차원 NBCA의 rule이 <150, 90, 150, 90 >이라면 특성행렬은 다음과 같다.

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

그리고 이 CA의 현재 상태가 $f_t(x) = [1\ 0\ 0\ 0]'$ 이면 다음상태는 다음과 같다.

$$f_{t+1}(x) = T \cdot f_t(x) = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

CA의 천이행렬이 T일 때, T의 특성다항식(characteristic polynomial) $\Delta(x)$는 다음과 같다. 여기서 I는 n차 단위행렬이다.

$$\Delta(x) = |T + xI| \tag{2.3}$$

<예 2.3.2> 위의 예 2.3.1에서 사용한 T에 대한 특성다항식은 다음과 같다.

$$\Delta(x) = |T + xI| = \begin{vmatrix} x+1 & 1 & 0 & 0 \\ 1 & x & 1 & 0 \\ 0 & 1 & x+1 & 1 \\ 0 & 0 & 1 & x \end{vmatrix}$$

$$= (x+1)\begin{vmatrix} x & 1 & 0 \\ 1 & x+1 & 1 \\ 0 & 1 & x \end{vmatrix} + 1\begin{vmatrix} 1 & 0 & 0 \\ 1 & x+1 & 1 \\ 0 & 1 & x \end{vmatrix}$$

$$= x^4 + x + 1$$

2.4. group CA

$f_t(x)$가 시간 t일 때 셀의 상태를 나타낸다면 다음 순간에서의 상태는 상태천이 방정식에 의해서 다음과 같이 나타내어질 수 있다.

$$f_{t+1}(x) = T \cdot f_t(x)$$

$$f_{t+2}(x) = T \cdot f_{t+1}(x)$$

$$= T^2 \cdot f_t(x)$$

같은 방법으로 m번째 다음상태는

$$f_{t+m}(x) = T^m \cdot f_t(x) \tag{2.4}$$

와 같이 나타낼 수 있다.

특성행렬 T를 가지는 CA가 cyclic group을 이룬다면 다음을 만족하는 자연수 m이 존재한다.

$$f_{t+m}(x) = T^m \cdot f_t(x) = f_t(x)\ , \tag{2.5}$$

즉,

$$T^m = I \tag{2.6}$$

(I : 단위행렬)

이런 성질을 가지는 CA를 특별히 group CA라 한다.

<정리 2.4.1> T가 CA의 특성행렬일 때, 이 CA가 group CA이기 위한 필요충분조건은 $|T| = 1$ 이다.

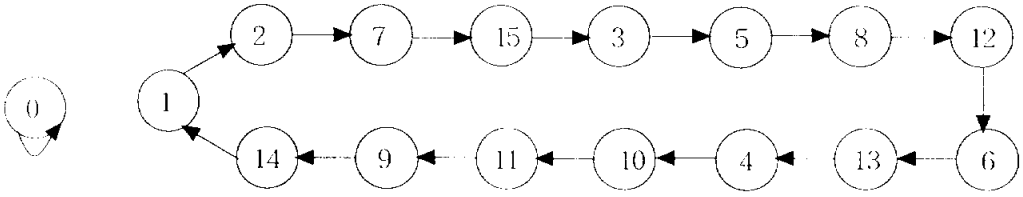
증명> ($\Rightarrow$) n셀 CA가 group CA이면 CA의 상태전이 그래프는 사이클을 이루어야 하므로 CA의 임의의 한 상태 y에 대하여 $Tx = y$인 x가 유일해야 한다. 따라서 T는 정칙이다. 즉 $|T| = 1$ 이다.

(⇐) n 셀 CA가 nongroup CA이면 상태 0에 대한 식전자가 2개 이상 존재한다. 즉, $Tx = 0$을 만족하는 x가 2개 이상 존재하므로 dim N(T) ≥1이다. 따라서 rank(T) < n이고 따라서 T는 정칙이 아니다. 즉, $|T|$ =0이다. □

group CA에서는 $|T| = 1$ 이므로 이에 대응하는 특성행렬 T는 역행렬이 존재한다. 따라서, 임의의 상태에 대하여 이전 상태를 알 수 있다. group CA는 최대길이를 갖는 CA와 최대길이를 갖지 않는 CA로 구별할 수 있다.

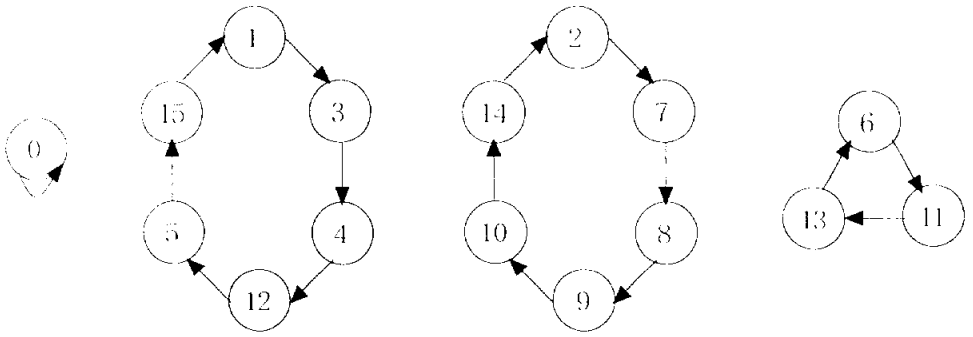
n 개의 셀로 이루어진 CA에서 모든 셀의 상태가 0인 경우를 제외한 $2^n - 1$ 개의 상태가 하나의 사이클 안에 있을 때 최대길이를 가진다고 한다.

<그림 2.3>은 rule <90, 150, 90, 150>인 4개의 cell로 구성된 최대길이를 갖는 NBCA의 상태 전이 그래프이다.



<그림 2.3> 최대길이를 갖는 group CA

<그림 2.4>은 최대길이를 갖지 않는 선형 CA로써 rule <102, 102, 102, 150>을 갖는 PBCA의 상태 전이 그래프이다.



<그림 2.4> 최대길이를 갖지 않는 group CA

<그림 2.4>에서 알 수 있듯이 0을 제외한 다른 상태들이 몇 개의 서로 다른 싸이클로 분리되어 있다. 이 싸이클 길이의 최소공배수가 해당 CA의 주기가 된다. 즉, rule이 <102, 102, 102, 150>인 PBCA는 0을 제외한 각 싸이클의 길이가 3과 6이다. 따라서 이 CA의 주기는 6이 된다.

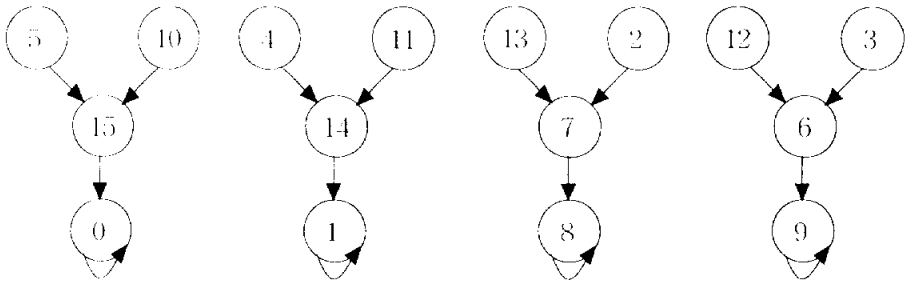
CA의 특성행렬 T의 행렬식이 0이면, 즉 $|T| = 0$이면, 해당 CA는 nongroup CA이다. nongroup CA는 특성행렬에 대한 역행렬이 존재하지 않으므로 임의의 상태에 대하여 이전 상태를 명확하게 알 수 없다.

rule <102, 102, 60, 60>을 갖는 NBCA의 특성행렬은 다음과 같다.

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

이 CA는 $|T| = 0$이므로 nongroup CA이다.

<그림 2.5>은 이 CA의 상태 천이 그래프이다.



<그림 2.5> nongroup CA

3. 원시다항식과 최대주기수열

이 장에서는 F_2 상에서의 선형점화수열의 특성다항식이 원시다항식인 최대주기수열 즉, PN 수열(pseudo noise sequence)에 대해 서술한다.

<정의 3.1.> F_2 상에서, 수열 $\{s_t\}$ 이 다음 동차 선형 점화 관계식을 만족한다고 하자.

$$s_{t+n} = c_0 s_t + c_1 s_{t+1} + \cdots + c_{n-1} s_{t+n-1}$$

$$(t = 0, 1, 2, \cdots), (c_0, c_1, \cdots, c_{n-1} \in F_2)$$

그러면 $f(x)$ 는 $\{s_t\}$ 의 특성다항식이라 한다.

$\Omega(f(x))$가 $f(x)$를 특성다항식으로 가지는 모든 수열 $\{s_t\}$ 의 집합이라 하면 다음과 같다.

$$\Omega(f(x)) = \left\{ \{s_t\} \mid s_{t+n} = \sum_{i=0}^{n-1} c_i s_{t+i}, t = 0, 1, 2, \cdots \right\}$$

F_2 에서 임의의 수열 $s_0, s_1, \cdots$ 가 주어지면, 그것과 생성함수 $G(x)$ 의 관계식은 다음과 같다.

$$G(x) = s_0 + s_1 x + s_2 x^2 + \cdots + s_n x^n + \cdots = \sum_{i=0}^{\infty} s_i x^i$$

<보조정리 3.2> $\{s_t\} \in \Omega(f(x))$라 하고, $f^*(x)$를 $f(x)$의 상반다항식, 그리고 $\{s_t\}$의 생성함수 $G(x) = s_0 + s_1 x + s_2 x^2 + \cdots + s_n x^n + \cdots = \sum_{i=0}^{\infty} s_i x^i$ 라 하면, 다음을 만족한다.

$$G(x) = \frac{g(x)}{f^*(x)}$$

여기서

$$g(x) = -\sum_{j=0}^{k-1} \sum_{i=0}^{j} c_{i+k-j} s_j x^j$$

$$c_k = -1$$

이다.

다음 정리는 PN 수열에 대한 연구에 매우 중요한 정리이다.

<정리 3.3> $f(x)$가 n차 원시다항식이라고 하고, $\{s_t\} \in \Omega(f(x))$이고, $s(x) = s_0 + s_1 x + \cdots + s_{r-1} x^{r-1}$, $r = 2^r - 1$라 하자. $\{u_t\}$를 다음을 만족하는 주기 수열이라 하자.

$$u(x) := u_0 + u_1 x + \cdots + u_{r-1} x^{r-1} = s^*(x)$$

이면 $\{u_t\} \in \Omega(f^*(x))$ 이다.

증명 : $G(x) = \sum_{t=0}^{\infty} s_t x^t$ 을 $\{s_t\}$ 의 생성함수라 하자. 그러면 다음을 만족한다.

$$G(x) = \frac{g(x)}{f^*(x)} = \frac{s(x)}{1-x^r}$$

$f^*(x)s(x) = g(x)(1-x^r)$, $f(x)s^*(x) = g^*(x)(x^r-1)$ 이므로 다음이 만족한다.

$$\frac{g(x)}{f^*(x)} = \frac{s^*(x)}{1-x^r}$$

$F(x)$ 을 $\{u_t\}$ 의 생성함수라 하자. 그러면 다음을 만족한다.

$$F(x) = \frac{u(x)}{1-x^r} = \frac{s^*(x)}{1-x^r} = \frac{g^*(x)}{f(x)}$$

따라서, $\{u_t\} \in \Omega(f^*(x))$ 이다.

<예제 3.4> $f(x) = x^4 + x + 1$ 이라 하면, $s_{t+4} = s_t + s_{t+1}$ 이다. 따라서 다음 수열을 얻을 수 있다.

$$\{s_t\} = 0001001101011110001001101011111\cdots$$

$f^*(x) = x^4 + x^3 + 1$ 이기 때문에 $u_{t+4} = u_t + u_{t+3}$ 이다. 따라서 다음 순환을 얻을 수 있다.

$$\{u_t\} \quad 011110101100100011110101100100\cdots$$

이 경우에

$$g(x) = x^3$$

$$g^*(x) = x$$

$$\begin{aligned} s(x) &= x^3 + x^6 + x^7 + x^9 + x^{11} + x^{12} + x^{13} + x^{14} \\ &= x^3(x+1)(x^2+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1) \end{aligned}$$

$$\begin{aligned} u(x)(=s^*(x)) &= x + x^2 + x^3 + x^4 + x^6 + x^8 + x^9 + x^{12} \\ &= x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+x^2+x+1) \end{aligned}$$

이므로 다음이 만족한다.

$$G(x) = \frac{g(x)}{f^*(x)} = \frac{s(x)}{1-x^r}$$

$$F(x) = \frac{u(x)}{1-x^r} = \frac{s^*(x)}{1-x^r} = \frac{g^*(x)}{f(x)}$$

<정리 3.5> 체 F_2 위의 n 차의 다항식

$$f(x) = -c_0 - c_1 x - \ldots - c_{n-1}x^{n-1} + x^n$$

가 기약다항식이고 $f(0) \neq 0$ 일 때, α를 체 F_{q^n}에서의 $f(x)$의 근이라고 하면 다음이 성립한다.

(1) $\mathrm{ord}(f(x))$는 곱셈군 $F_{q^n}^*$에서의 α의 위수와 일치한다.

(2) $\mathrm{ord}(f(x)) \mid q^n - 1$

증명> 이제 α를 체 F_{q^n}에서의 $f(x)$의 근이라고 하면, $f(x)$는 F_q 위의 기약다항식인 동시에 그 최고차 항의 계수가 1이므로 $f(x)$는 F_q 위에서의 α의 최소다항식이다. 따라서 양의 정수 e에 대하여

$$\alpha^e = 1 \quad \Leftrightarrow \quad \alpha^e - 1 = 0 \quad \Leftrightarrow \quad f(x) \mid x^e - 1$$

이므로 α의 위수에 대한 정의와 $\mathrm{ord}(f(x))$의 위수에 대한 정의에 의하여, $\mathrm{ord}(f(x))$는 곱셈군 $F_{q^n}^*$에서의 α의 위수와 일치한다. 한편, 곱셈군 $F_{q^n}^*$는 위수 $q^n - 1$인 순환군이므로 α의 위수는 $q^n - 1$의 약수이다. 따라서 $\mathrm{ord}(f(x))$는 $q^n - 1$의 약수이다.

<정리 3.6> 체 F_q 위의 n차의 다항식 $p(x)$가 $p(0) \neq 0$인 기약다항식일 때, $p(x)$가 체 F_q 위의 n차의 원시다항식이기 위한 필요충분조건은 $\mathrm{ord}(p(x)) = q^n - 1$인 것이다.

증명> $\alpha \in F_{q^n}$를 $p(x)$의 한 근이라고 할 때, $p(x)$가 F_q 위의 n차의 원시다항식이기 위한 필요충분조건은 $\alpha \in F_{q^n}^*$의 위수가 $q^n - 1$이다. 따

라서 성립한다.

<정리 3.7> 체 F_q 위의 n 차 다항식

$$f(x) = -c_0 - c_1 x - \cdots - c_{n-1} x^{n-1} + x^n$$

에서 $c_0 \neq 0$ 일 때, 수열 $\{s_t\} \in \Omega(f(x))$ 에 대하여 다음이 성립한다.

(1) $\{s_t\}$ 는 순환수열이고 그 주기는 $\mathrm{ord}(f(x))$ 의 약수이다.

(2) $\{s_t\}$ 의 초기 상태벡터가 $(s_0, s_1, \ldots, s_{n-1}) = (0, 0, \ldots, 0, 1)$ 이면, 이 수열의 주기는 $f(x)$ 의 위수 $\mathrm{ord}(f(x))$ 와 같다.

증명> 다항식 $f(x)$ 의 동반행렬을 A 라고 하면, $\det A = (-1)^{n+1} c_0 \neq 0$ 이므로 A 는 정칙행렬이다.

(1) $\{s_t\}$ 는 순환수열이고 또 그 주기를 r 라고 하면 r 는 행렬 A 의 위수의 약수이다. 한편, A 의 위수는 $\mathrm{ord}(f(x))$ 와 같으므로, r 는 $\mathrm{ord}(f(x))$ 의 약수이다

(2) 수열 $\{s_t\}$ 의 초기 상태벡터가 $(s_0, s_1, \cdots, s_{n-1}) = (0, 0, \cdots, 0, 1)$ 일 때, 수열 $\{s_t\}$ 의 주기를 r 라고 하자. 이 때,

$$s_{t+r} = s_t \qquad (t = 0, 1, 2, \cdots)$$

이므로

$$[\, s_{t+r}\ s_{t+r+1}\ \cdots\ s_{t+r+n-1}\,] = [\, s_t\ s_{t+1}\ \cdots\ s_{t+n-1}\,] \qquad (t = 0, 1, 2, \cdots)$$

이고 이로부터 다음 식과를 얻는다.

$$[\, s_t\ s_{t+1}\ \cdots\ s_{t+n-1}\,]\, A^r = [\, s_t\ s_{t+1}\ \cdots\ s_{t+n-1}\,] \qquad (t = 0, 1, 2, \cdots)$$

$$(*) \qquad [\, s_t\ s_{t+1}\ \cdots\ s_{t+n-1}\,](A^r - I) = [\, 0\ 0\ \cdots 0\,] \qquad (t = 0, 1, 2, \cdots)$$

그런데, 가정에 의하여

$$\begin{aligned}
(s_0, s_1, \ldots, s_{n-1}) &= (0, 0, \ldots, 0, 1),\\
(s_1, s_2, \ldots, s_n) &= (0, 0, \ldots, 1, *),\\
&\vdots\\
(s_{n-1}, s_n, \cdots, s_{2n-1}) &= (1, *, \cdots, *, *)
\end{aligned}$$

이므로 (*)에 의하여

$$A^r - I = O \quad \text{즉} \quad A^r = I$$

이므로 A의 위수는 r의 약수이다. 그런데, (1)의 증명에 의하여 r는 A의 위수의 약수이고 A의 위수는 $\mathrm{ord}\,(f(x))$와 같으므로 $r = \mathrm{ord}\,(f(x))$이다.

<정리 3.8> 체 F_q 위의 n차의 위시다항식

$$f(x) = -c_0 - c_1 x - \cdots - c_{n-1} x^{n-1} + x^n$$

에 대하여, $\alpha \in F_{q^n}$ 를 $f(\alpha) = 0$ 인 원시원소라고 하면, 각 t $(t = 0, 1, 2, \cdots)$에 대하여, α^t 는 다음과 같은 꼴로 나타내어진다.

$$\alpha^t = s_{0,t}\alpha^{n-1} + s_{1,t}\alpha^{n-2} + \cdots + s_{n-2,t}\alpha + s_{n-1,t} = \sum_{j=0}^{n-1} s_{j,t}\alpha^{n-1-j}$$

$$(s_{0,t}, s_{1,t}, \cdots, s_{n-1,t} \in F_q)$$

이 때, n 개의 수열 $\{s_{0,t}\}, \{s_{1,t}\}, \cdots, \{s_{n-1,t}\}$ 는 $f(x)$ 를 고유다항식으로 가지는 주기 $q^n - 1$ 의 최대주기수열 또는 PN 수열 (pseudo noise sequence)이다.

증명> 가정에 의하여 $f(\alpha) = 0$ 이므로

$$\alpha^n = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1} = \sum_{i=0}^{n-1} c_i\alpha^i$$

이고 또 가정에 의하여 다음 등식이 성립한다.

$$\sum_{j=0}^{n-1} s_{j,t+n}\alpha^{n-1-j} = \alpha^{t+n} = \alpha^n\alpha^t = \left(\sum_{i=0}^{n-1} c_i\alpha^i\right)\alpha^t$$

$$= \sum_{i=0}^{n-1} c_i\alpha^{t+i} = \sum_{i=0}^{n-1} c_i\left(\sum_{j=0}^{n-1} s_{j,t+i}\alpha^{n-1-j}\right)$$

$$= \sum_{j=0}^{n-1}\left(\sum_{i=0}^{n-1} c_i s_{j,t+i}\right)\alpha^{n-1-j} \qquad (t = 0, 1, 2, \cdots)$$

원소 $1, \alpha, \cdots, \alpha^{n-1}$는 체 F_q 위에서 일차독립이므로 위의 등식에 의하여

$$s_{j,t+n} = \sum_{i=0}^{n-1} c_i s_{j,t+i} \qquad (0 \le j \le n-1,\ t = 0, 1, 2, \cdots)$$

이고 따라서 각 j $(0 \le j \le n-1)$에 대하여 수열 $\{s_{j,t}\}$의 고유다항식은 $f(x)$이다. 또 $s_{0,n-1} = s_{1,n-2} = \cdots = s_{n-2,1} = s_{n-1,0} = 1$이므로 이들 수열은 영수열이 아니다. 그러므로 각 $\{s_{j,t}\}$는 주기 q^{n-1}인 최대주기수열이다.

<예제 3.9> 다항식 $g(x) = 1 + x^2 + x^5$는 체 F_2 위에서의 5차의 원시다항식이다. 이제 $\alpha \in F_{2^5}$를 $f(\alpha) = 0$인 원시원소라고 하면 다음이 성립한다.

$$\alpha^5 + \alpha^2 + 1 = 0,\ \alpha^5 = \alpha^2 + 1$$

$$F_{2^5} - \{0\} = \langle \alpha \rangle = \{1, \alpha, \alpha^2, \cdots, \alpha^{30}\},\ \alpha^{31} = 1$$

$$\alpha^0 = 0\alpha^4 + 0\alpha^3 + 0\alpha^2 + 0\alpha + 1 \qquad 0\ 0\ 0\ 0\ 1$$

$$\alpha^1 = 0\alpha^4 + 0\alpha^3 + 0\alpha^2 + 1\alpha + 0 \qquad 0\ 0\ 0\ 1\ 0$$

$$\alpha^2 = 0\alpha^4 + 0\alpha^3 + 1\alpha^2 + 0\alpha + 0 \qquad 0\ 0\ 1\ 0\ 0$$

$$\alpha^3 = 0\alpha^4 + 1\alpha^3 + 0\alpha^2 + 0\alpha + 0 \qquad 0\ 1\ 0\ 0\ 0$$

$$\alpha^4 = 1\alpha^4 + 0\alpha^3 + 0\alpha^2 + 0\alpha + 0 \qquad 1\ 0\ 0\ 0\ 0$$

$$\alpha^5 = 0\alpha^4 + 0\alpha^3 + 1\alpha^2 + 0\alpha + 1 \qquad 0\ 0\ 1\ 0\ 1$$

$\alpha^{6} = 0\alpha^{4} + 1\alpha^{3} + 0\alpha^{2} + 1\alpha + 0$ 0 1 0 1 0

$\alpha^{7} = 1\alpha^{4} + 0\alpha^{3} + 1\alpha^{2} + 0\alpha + 0$ 1 0 1 0 0

$\alpha^{8} = 0\alpha^{4} + 1\alpha^{3} + 1\alpha^{2} + 0\alpha + 1$ 0 1 1 0 1

$\alpha^{9} = 1\alpha^{4} + 1\alpha^{3} + 0\alpha^{2} + 1\alpha + 0$ 1 1 0 1 0

$\alpha^{10} = 1\alpha^{4} + 0\alpha^{3} + 0\alpha^{2} + 0\alpha + 1$ 1 0 0 0 1

$\alpha^{11} = 0\alpha^{4} + 0\alpha^{3} + 1\alpha^{2} + 1\alpha + 1$ 0 0 1 1 1

$\alpha^{12} = 0\alpha^{4} + 1\alpha^{3} + 1\alpha^{2} + 1\alpha + 0$ 0 1 1 1 0

$\alpha^{13} = 1\alpha^{4} + 1\alpha^{3} + 1\alpha^{2} + 0\alpha + 0$ 1 1 1 0 0

$\alpha^{14} = 1\alpha^{4} + 1\alpha^{3} + 1\alpha^{2} + 0\alpha + 1$ 1 1 1 0 1

$\alpha^{15} = 1\alpha^{4} + 1\alpha^{3} + 1\alpha^{2} + 1\alpha + 1$ 1 1 1 1 1

$\alpha^{16} = 1\alpha^{4} + 1\alpha^{3} + 0\alpha^{2} + 1\alpha + 1$ 1 1 0 1 1

$\alpha^{17} = 1\alpha^{4} + 0\alpha^{3} + 0\alpha^{2} + 1\alpha + 1$ 1 0 0 1 1

$\alpha^{18} = 0\alpha^{4} + 0\alpha^{3} + 0\alpha^{2} + 1\alpha + 1$ 0 0 0 1 1

$\alpha^{19} = 0\alpha^{4} + 0\alpha^{3} + 1\alpha^{2} + 1\alpha + 0$ 0 0 1 1 0

$\alpha^{20} = 0\alpha^{4} + 1\alpha^{3} + 1\alpha^{2} + 0\alpha + 0$ 0 1 1 0 0

$\alpha^{21} = 1\alpha^{4} + 1\alpha^{3} + 0\alpha^{2} + 0\alpha + 0$ 1 1 0 0 0

$\alpha^{22} = 1\alpha^{4} + 0\alpha^{3} + 1\alpha^{2} + 0\alpha + 1$ 1 0 1 0 1

$\alpha^{23} = 0\alpha^{4} + 1\alpha^{3} + 1\alpha^{2} + 1\alpha + 1$ 0 1 1 1 1

$\alpha^{24} = 1\alpha^{4} + 1\alpha^{3} + 1\alpha^{2} + 1\alpha + 0$ 1 1 1 1 0

$\alpha^{25} = 1\alpha^{4} + 1\alpha^{3} + 0\alpha^{2} + 0\alpha + 1$ 1 1 0 0 1

$\alpha^{26} = 1\alpha^{4} + 0\alpha^{3} + 1\alpha^{2} + 1\alpha + 1$ 1 0 1 1 1

$\alpha^{27} = 0\alpha^{4} + 1\alpha^{3} + 0\alpha^{2} + 1\alpha + 1$ 0 1 0 1 1

$$\alpha^{28} = 1\alpha^4 + 0\alpha^3 + 1\alpha^2 + 1\alpha + 0 \qquad 1\ 0\ 1\ 1\ 0$$

$$\alpha^{29} = 0\alpha^4 + 1\alpha^3 + 0\alpha^2 + 0\alpha + 1 \qquad 0\ 1\ 0\ 0\ 1$$

$$\alpha^{30} = 1\alpha^4 + 0\alpha^3 + 0\alpha^2 + 1\alpha + 0 \qquad 1\ 0\ 0\ 1\ 0$$

따라서 다음 수열은 체 F_2 위의 원시다항식 $f(x)$ 를 고유다항식으로 가지는 주기 31인 최대주기수열이다.

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 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 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 1 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 …

1 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 …

4. 90/150 CA에 의해 생성된 PN 수열

이 장에서는 CA의 패턴 생성 능력에 관하여 서술한다. 시뮬레이션, 데이터 암호, 논리회로 테스트 등과 같은 고품질의 랜덤 패턴 생성분야에서 CA의 수요가 있다.

입·출력 많은 수의 입력값을 가지는 복잡한 회로에서 몇 개의 부분적인 입력값에만 의존하는 출력값의 위치를 찾는데 적합한 방법들이 연구되어왔다. 1장에서 언급되었던 group CA는 역행원이 존재하는 상태전이 행렬을 가진다. 또한 group CA는 최대 길이를 가지는 것과 그렇지 않은 것으로 나뉜다. 여기서 최대 길이를 가지는 n 셀 CA는 0을 제외한 2^n-1 개의 모든 상태가 한 개의 사이클을 이룬다. 이러한 group CA는 고품질의 랜덤 패턴 생성기로 연구되어 왔다. 그리고 부호공간(code space)을 이런 사이클 부분공간으로 나누는 CA에 의해 생성된다. 부호 공간의 성질들은 원시다항식에 의해 만들어 지는 PN(pseudo noise) 수열들을 열로 구성한 행렬들의 성질과 유사하다. 이런 행렬들의 분석이 이 절에서 다루어질 주요 내용들이다.

4.1. 90/150 CA의 특성행렬의 분석

n 차 원시다항식에 의해 생성되는 PN 수열의 길이는 2^n-1 이다. 이 절에서는 특성다항식이 원시다항식인 90/150 NBCA에 대해 다룬다. 이러한 n 셀 CA의 특성행렬은 다음과 같다.

$$T = \begin{vmatrix} a_1 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & a_2 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & a_3 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & 1 & a_n \end{vmatrix} \tag{4.1}$$

여기서 $a_1, a_2, \cdots, a_n \in \{0, 1\}$ 이다.

n 차 90/150 CA의 특성행렬을 T_n 이라 두고 $T_n = \langle a_1, a_2, \cdots, a_n \rangle$ 라 쓰자. 그러면 다음이 성립한다.

$$|T_n| = a_1|T_{n-1}| + |T_{n-2}| \tag{4.2}$$

<정리 4.1.1> $T_n = \langle a_1, a_2, \cdots, a_n \rangle$, $T'_n = \langle a_n, a_{n-1}, \cdots, a_1 \rangle$ 라 두면 $|T_n| = |T'_n|$이다.

증명> 행렬식값의 성질에 의해 명백하다. □

<정리 4.1.2> 90/150 CA의 특성행렬 T_n에서 $a_1 = a_3 = \cdots = a_{2m-1} = 0$, $a_2 = a_4 = \cdots = a_{2m} = 1$ 이고, $n(=2m)$이 짝수라면 $|T_n| = 1$ 이다.

증명> (4.2)에서 $a_1 = 0$ 이므로 다음이 성립한다.

$$|T_n| = |T_{n-2}|$$

$|T_2| = 1$ 이므로 귀납법에 의하여 $|T_n| = 1$ 성립한다. □

<따름정리 4.1.3> 90/150 CA의 특성행렬에서 $a_1 = a_3 = \cdots = a_{2m-1} = 1$, $a_2 = a_4 = \cdots = a_{2m} = 0$ 이고, $n(=2m)$ 이 짝수이면 $|T_n| = 1$ 이다.

증명> 정리 4.1.1과 정리 4.1.2에 의하여 명백하다. □

<따름정리 4.1.4> 90/150 CA의 특성행렬에서 $a_1 = a_3 = \cdots = a_{2m-1} = 1$, $a_2 = a_4 = \cdots = a_{2m-2} = 0$, $a_n = 1$ 이고, $n = 1 \bmod 4$ 이면 $|T_n| = 1$ 이다.

증명> $n-1$ 이 짝수이기 때문에 따름정리 4.1.3에 의하여 다음과 같은 식이 성립한다.

$$|T_n| = |T_{n-1}| + |T_{n-2}| = 1 + |T_{n-2}|$$

$|T_3| = |T_1| = 1$ 이고 $|T_5| = 1$ 이므로 귀납법에 의해 $|T_n| = 1$ 성립한다. □

<정리 4.1.5> 90/150 CA의 특성다항식 $f(x)$ 에 대하여 서로 다른 2개의 특성행렬이 존재한다. [ ]

<예제 4.1.6> 주어진 90/150 CA의 특성다항식이 $f(x) = x^5 + x^2 + 1$ 이면 이에 대응하는 90/150 CA의 특성행렬은 $T_5 = \langle 1, 1, 1, 1, 0 \rangle$ 와 $T'_5 = \langle 0, 1, 1, 1, 1 \rangle$ 두 개다.

<보조정리 4.1.7> 90/150 CA의 특성행렬에 대해 T의 특성다항식은 T의 최소다항식과 같다. □

<정리 4.1.8> T_n을 특성다항식이 원시다항식인 90/150 CA, v_0를 F_2^n에서 $\mathbf{0}$이 아닌 초기벡터라 두자. 그러면 $t \geq 1$에 대하여 다음이라 정의하자.

$$v_t = T_n \cdot v_{t-1}$$

그러면 수열 $V: v_0, v_1, v_2, \cdots$는 최대주기 $2^n - 1$을 가진다.

증명> 주어진 $\mathbf{0}$가 아닌 초기벡터 $v_0 \in F_2^n$에 대하여 v에 대한 최소다항식을 $f_v(x)$라 두자. 보조정리 4.1.7에 의해서 $\mathbf{0}$가 아닌 벡터 $v \in F_2^n$에 대하여 $f_v(x) = f(x)$이다. 수열 V의 주기가 r이라면

$$T_n^r \cdot v_0 = v_0$$

이다. 따라서 $f_v(x)$는 $x^r - 1$을 나눈다. $f_v(x) = f(x)$이고 $f(x)$는

원시다항식이기 때문에 $r = 2^n - 1$ 이다. □

정리 4.1.8로부터 $\{v_0, v_1, \cdots, v_{2^n-2}\}$과 $F_2^n \setminus \{0\}$가 같음을 알 수 있다.

<따름정리 4.1.9> 특성다항식이 원시다항식인 90/150 CA의 특성행렬을 T_n이라 하고 $w_0 = (w_{0_0}, w_{0_1}, \cdots, w_{0_{n-1}})$, $w_{0_0}, w_{0_1}, \cdots, w_{0_{n-1}} \in F_2$ 중 0가 아닌 벡터라 하자. $r \geq 1$에 대하여 $w_r = w_{r-1} \cdot T_n$이라 정의하자. 그러면 $\{w_0, w_1, \cdots, w_{2^n-2}\}$는 최대 주기 $2^n - 1$을 가진다. ||

따름정리 4.1.9로부터 $w_0, w_1, \cdots, w_{2^n-2}$는 T_n의 열벡터의 결합임을 알 수 있다.

<정리 4.1.10> 특성다항식이 원시다항식인 90/150 CA의 특성행렬을 T_n이라 하면 T_n^h와 T_n^m $(0 \leq i \leq n-1,\ 1 \leq h < m \leq 2^n - 1)$의 각각의 i 행벡터는 다르다.

증명> T_n의 상태변화에서 초기벡터를 i번째 성분만 1이고 나머지 성분은 0인 $w = (0, 0, \cdots, 0, 1, 0, \cdots, 0)$이라 하고 T_n^h와 T_n^m의 각각의 i 행벡터가 같다고 가정하면 다음이 성립한다.

$$w_h = w_0 T_n^h = w_0 T_n^m = w_m$$

따름정리 4.1.9에 의하여 $w_0, w_1, \cdots, w_{2^n-2}$가 모두 다른 값이기 때문

에 $w_h \neq w_m$ 이다. 이것은 모순이다. 그러므로 T_n^h 와 T_n^m 의 각각의 i 행들은 다르다. □

<정리 4.1.11> 특성다항식이 원시다항식인 90/150 CA의 특성행렬을 T_n 이라 하고 $S^0 \neq (0, 0, \cdots, 0)$ 을 초기 벡터라 하자. 그러면 $1 \leq i < j \leq n$ 에 대하여 다음을 만족하는 정수 h 가 존재한다.

$$S_i^{t+h} = S_j^t \quad (t \geq 0)$$

<증명> T_n 의 특성다항식 $f(x)$ 가 n 차 원시다항식이라 하면 수열 $\{S_i^t\}, \{S_j^t\}$ 은 n 차 동형 선형 점화 수열이다. 또한 $\{S_i^t\}, \{S_j^t\}$ 의 주기는 $2^n - 1$ 이다. $W = (S_i^0, \cdots, S_i^{n-1})$ 라 두면 $(S_j^k, S_j^{k+1}, \cdots, S_j^{k+n-1})$, $k = 0, \cdots, 2^n - 2$ 는 정리 4.1.10에 의하여 모두 다른 0 가 아닌 수열이 되므로 $W = (S_j^r, \cdots, S_j^{r+n-1})$ 인 r 이 존재한다. 따라서 $t \geq 0$ 에 대하여 $S_j^{t+h} = S_i^t$ 이다. □

4.2. 90/150 CA에 의해 생성된 PN 수열의 분석

다음은 PN 수열을 얻는 가지는 행렬을 기초로 하여 얻은 몇 가지 이론적인 결과들이다. 전이규칙이 <150, 90, 150, 90>인 특성다항식 $f(x) = x^4 + x + 1$ 은 원시다항식이다. 그림 4.1(a)는 초기값을 <0 0 0 1> 로 하여 전이규칙 <150, 90, 150, 90>에 대응하는 특성행렬 T에 의해 생성되는 벡터들을 나열한 것을 행렬 A로 둔 것이다. 이

행렬의 모든 원소은 특성다항식 $f(x) = x^4 + x + 1$을 사용하여 만들 수 있는 PN 수열을 원소로 가진다. 또한 이 행렬에서 다음과 같은 몇 가지 사실들을 얻을 수 있다.

$$A = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \qquad B = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix} \begin{matrix} \leftarrow B_0 \\ \leftarrow B_1 \\ \leftarrow B_2 \\ \leftarrow B_3 \\ \leftarrow B_4 \\ \leftarrow B_5 \\ \leftarrow B_6 \\ \leftarrow B_7 \\ \leftarrow B_8 \\ \leftarrow B_9 \\ \leftarrow B_{10} \\ \leftarrow B_{11} \\ \leftarrow B_{12} \\ \leftarrow B_{13} \\ \leftarrow B_{14} \end{matrix}$$

<행렬 A의 성질>

성질1) A의 모든 열들은 서로 동일하며 단지 각 셀의 위치가 일정 량만큼 이동(shift)된 것이다.

성질2) n개의 성분으로 이루어진 벡터에서 나타날 수 있는 0이 아닌 가능한 $2^n - 1$개의 모든 벡터들은 A의 행에서 나타난다.

성질3) 모든 원소이 독립이기 때문에 $rank(A) = n$이다.

성질4) A의 임 중 한 개를 삭제하면 $(2^n - 1) \times (m - 1)$ 행렬이 되며 모두 0인 벡터가 정확히 한 번 나타나고 0이 아닌 $(m - 1)$개의 성분으로 이루어진 벡터가 두 번씩 나타난다.

A에서 한 열을 삭제하여 얻은 행렬을 B라 하고 일반성을 잃지 않

고 모두 0인 벡터를 첫 번째 행으로 하여 나열하면 $(m-1)$개의 성분으로 이루어진 벡터에서 나올 수 있는 벡터들이 한 번씩 다 나오기 위해서는 행의 길이 s가 $2^{m-1} \le s \le 2^m - 1$이어야 한다.

<정의 4.2.1> 행렬 B에서 $(m-1)$개의 성분으로 이루어진 행벡터 B_r $(0 \le r \le 2^{n-2})$의 범위(range)는 B_r에서 출발하여 **0** 벡터를 포함하여 모든 벡터들이 최소한 다 한번씩은 나올 때까지의 최소 길이이다.

<정의 4.2.2> 행렬 B에서 행벡터 B_r의 변위(offset) r은 **0** 벡터에서부터 B_r까지의 거리이다.

<정의 4.2.3> 행렬 B의 모든 행벡터들의 범위 중에서 가장 작은 범위를 최소 범위(minimum range)라고 한다.

<정의 4.2.4> 행렬 B의 최소 범위인 행벡터의 시초 중 가장 작은 시초를 최소 변위(minimum offset)이라 한다.

<예제 4.2.5> 행렬 B에서 행벡터 B_r의 범위와 변위는 다음과 같다

행렬 B	십진수표현	범위	변위
0 0 0	0	12	0
0 0 1	1	15	1
0 1 1	3	14	2
1 1 1	7	13	3
0 0 1	1	12	4
0 1 0	2	12	5
1 0 0	4	11	6
1 1 0	6	10	7
0 1 1	3	9	8
1 1 0	6	9	9
0 1 0	2	13	10
1 0 1	5	12	11
1 0 1	5	11	12
1 0 0	4	14	13
1 1 1	7	13	14

<표 4.1> 행렬 B의 범위와 변위

여기서 최소 범위는 9이고 최소 변위는 8이다.

앞서 살펴본 바와 같이 행렬 B는 $m-1$개의 독립적인 열들로 구성되었고, 각각의 열들은 m차 원시다항식에 의해 얻어지는 PN 수열이

다. 또한 행렬 B는 행렬 A의 한 열을 제거함으로써 얻을 수 있으므로 만들 수 있는 행렬 B의 개수는 m개이다.

<보조정리 4.2.6> 행렬 A에서 얻어지는 모든 행렬 B들의 최소 범위와 최소 변위는 서로 같다.

증명> $rank(B) = m-1$이므로 기본 열 조작에 의해 다음과 같이 행렬 B를 변형할 수 있다.

$$C = \begin{vmatrix} \mathbf{0} \\ I_{m-1} \\ Q \end{vmatrix}$$

여기서 $\mathbf{0}$는 영벡터, I_{m-1}은 $m-1$차 단위행렬이고 Q는 영행렬이 아닌 $(2^m - m - 1) \times (m-1)$행렬이다. PN 수열들끼리의 합도 PN 수열이므로 행렬 C의 원소도 m차 원시다항식에 의해 생성된 PN 수열임을 알 수 있다. 행렬 C의 구조의 장점에 의하여 행렬 C는 유일한 행렬이다. 따라서 특별한 m차 원시다항식에 대응하는 행렬 B는 기본 열 조작에 의하여 하나의 표준 행렬로 변형될 수 있다. 다음을 만족하는 역행렬이 존재하는 행렬 P를 구성할 수 있다.

$$B \cdot P = C$$

즉, 행렬 B의 모든 행벡터들은 행렬 C의 행벡터들로 유일하게 재배열될 수 있다. [ ]

<예제 4.2.7> 다음은 4차 원시다항식 $f(x) = x^4 + x + 1$에 대한 행렬 C와 행렬 B를 표준 행렬 C로 변형시킨 행렬 P이다.

행렬 C	변위	범위	행렬 P
0 0 0	0	12	
1 0 0	1	15	
0 1 0	2	14	
0 0 1	3	13	
1 0 0	4	12	
1 1 0	5	12	
0 1 1	6	11	0 1 1
1 0 1	7	10	1 1 0
0 1 0	8	9	1 0 0
1 0 1	9	9	
1 1 0	10	13	
1 1 1	11	12	
1 1 1	12	11	
0 1 1	13	14	
0 0 1	14	13	

<표 4.2> 행렬 C의 범위, 변위과 행렬 P

보조정리 4.2.6의 증명에 의해 특별한 m차 원시다항식의 행렬 B에서 최소 범위와 최소 변위는 각각 같다.

<정리 4.2.8> T가 특성다항식 $f(x)$이 n차 원시다항식인 90/150 NBCA의 특성행렬이면 다음을 만족하는 $p(1 \le p \le 2^n - 2)$가 존재한다.

$$I_n \oplus T = T^p$$

증명> $f(\alpha) = 0$라면, α에 의해 생성된 유한체는 $F_2^n = \{0, 1, \alpha, \cdots \alpha^{2^n-2}\}$이다. 따라서 $1 + \alpha = \alpha^p$을 만족하는 $p(1 \le p \le 2^n - 2)$는 존재한다. 그러므로 $I_n \oplus T = T^p$이다. □

<따름정리 4.2.9> T가 특성다항식 $f(x)$이 n차 원시다항식인 90/150 NBCA의 특성행렬이면 다음을 만족하는 $k(1 \le k \le 2^n - 2)$가 존재한다.

$$T^k \oplus T^{k+1} = I_n$$

증명> 정리 4.2.8에 의해서 $T^{2^n-1-p}(I_n \oplus T) = T^{2^n-1} = I_n$이다. 여기서 $k = 2^n - 1 - p$라 두면 $T^k(I_n \oplus T) = T^k \oplus T^{k+1} = I_n$이다. □

<따름정리 4.2.10> T가 특성다항식 $f(x)$이 n차 원시다항식인 90/150 NBCA의 특성행렬이라 하자. $a \oplus b = (0, 0, \cdots, 0, 1)^t$를 만족하는 상태가 0이 아닌 두 벡터에 대해 다음을 만족하는 $k(1 \le k \le 2^n - 2)$가 존재한다.

$$T^k(0,0,\cdots,0,1)^t = a$$
$$T^{k+1}(0,0,\cdots,0,1)^t = b$$

증명> 따름정리 4.2.9에 의해 명백하다. □

<예제 4.2.11> 6 셀 group CA $\mathbb{C}$의 특성행렬을 T가 다음과 같으면 특성다항식은 $f(x) = x^6 + x^5 + x^4 + x + 1$ 이고, $f(x)$ 은 원시다항식이다.

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

여기서 $T^{24} \oplus T^{25} = I_6$ 이다.

<보조정리 4.2.12> 6 셀 90/150 NBCA의 특성다항식 $f(x)$가 6 차 원시다항식인 특성행렬을 T라 두고, $f^*(x)$는 $f(x)$의 상반다항식이고 이에 대응하는 특성행렬을 T'라 두자. 그러면 $T^k \oplus T^{k+1} = I_n$인 k $(1 \le k \le 2^n - 1)$에 대하여 k'를 다음과 같이 두면 $k' = 2^n - k - 2$ 이다.

$$T'^{k'} \oplus T^{k+1} = I_n$$

증명> 따름정리 4.2.9에 의하여 $T^k \oplus T^{k+1} = I_n$ 을 만족하는 k $(1 \le k \le 2^n - 1)$ 가 존재한다. 그러면 다음을 만족한다.

$$(T'^{-1})^k \oplus (T'^{-1})^{k+1} = (T'^{-1})^{k+1} \oplus (T'^{-1})^k = I_n$$

$T'^{2^n-1} = I_n$ 이기 때문에, 다음이 성립한다.

$$(T'^{-1})^{k+1} = T'^{-(k+1)} = T'^{2^n-1-(k+1)}$$

따라서, $k' = 2^n - k - 2$ 이다. □

<예제 4.2.13> 예제 4.2.11에서 T에 대응하는 T'은 다음과 같다.

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

T'의 특성다항식 $f^*(x) = x^6 + x^5 + x^2 + x + 1$ 이고, 이는 예제 4.2.11에서 $f(x)$의 상반다항식이다. 이기서 $T'^{38} \oplus T'^{39} = I_6$ 이다. 즉, $38 = 2^6 - 24 - 2$ 임을 알 수 있다.

<따름정리 4.2.14> 원시다항식의 최소 범위와 그것의 상반다항식의 최소 범위는 서로 같다.

증명> 특성다항식 $f(x)$는 n차 원시다항식이고, 이것의 상반다항식을 $f^*(x)$라 두자. $f(x)$의 표준 행렬 C_1, $f^*(x)$의 표준 행렬을 C_2라 하자. 따름정리 4.2.9에 C_1과 C_2에서 각각 인이어 같은 두 행벡터가 있다. C_1의 행벡터를 십진 표현하여 연이어 같은 두 행벡터를 시작으로 재배열하고, C_2는 행벡터를 십진 표현하여 연이어 같은 두 행벡터를 시작으로 역으로 재배열하면, 보조정리 4.2.10에 의하여 시작 벡터를 찾을 수 있다. 여기서 다음을 만족하는 치환 σ를 구할 수 있다.

$$C_1\sigma = C_2$$

따라서 $f(x)$와 $f^*(x)$의 최소 범위는 서로 같다. □

<예제 4.2.15> 예제 4.2.7의 특성다항식 $f(x)$과 그것의 상반다항식 $f^*(x)$을 가지는 행렬 C_1와 C_2의 행벡터들을 십진 표현하여 나열하면 다음과 같다.

$$C_1 = 042146352567731$$

$$C_2 = 042115767253463$$

보조정리 4.2.10에 의하여 C_1에서 벡터 $\langle 111 \rangle$, 십진 표현 7이 연이어 같은 두 벡터가 나타나고, C_2에서는 벡터 $\langle 001 \rangle$, 십진 표현 1이 연이어 같은 두 벡터가 나타난다. 따름정리 4.2.14의 증명에서처럼 이를 재배열하면 다음과 같다.

$$C_1 = 7731042146352 56$$

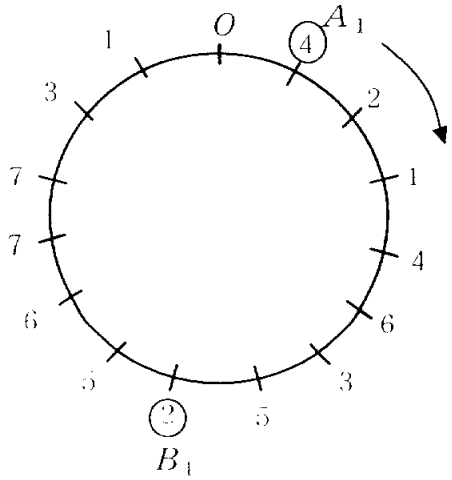
$$C_2 = 1124036435276 75$$

여기서 치환 σ는 다음과 같다.

$$\sigma = \begin{pmatrix} 7 & 1 & 4 & 3 & 2 & 6 & 5 \\ 1 & 4 & 3 & 2 & 6 & 5 & 7 \end{pmatrix}$$

따라서 행렬 C_1와 C_2의 최소 범위는 같다. □

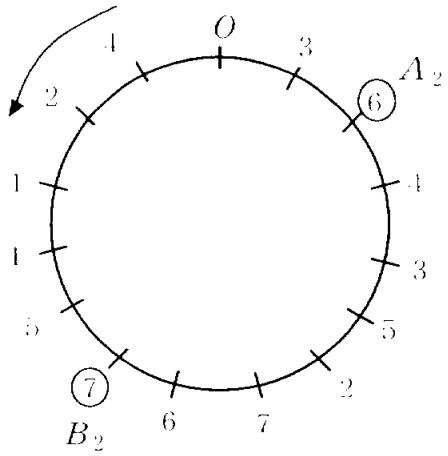
다음 그림은 예제 4.2.15의 행렬 C_1와 C_2의 각 행벡터들의 상태 변화를 십진 표현으로 나타낸 것을 **0** 벡터를 기준으로 나타낸 것이다.



$d = |\overrightarrow{B_1A_1}| = 9$

$O_1 = |OB_1| = 8$

C_1



$d = |\overrightarrow{A_2B_2}| = 9$

$O_2 = |OA_2| = 13$

C_2

<그림 4.1> 행렬 C_1와 C_2의 각 행벡터들의 상태 변화

다음 정리는 따름정리 4.2.17에서 필요한 조건을 보여준다.

<정리 4.2.16> O_1과 O_2를 각각 n차 원시다항식과 그것의 상반다항식의 최소 변위이라 하고, d를 이것들의 최소 범위라 하자. $|OA_1| = a$, $|A_2O| = b$, $|B_1O| = y$라 두면 다음 식이 성립한다.

$$O_1 + O_2 = 2(2^n - 1) - b - y$$

증명 $|OB_2| = z$라 두면 다음이 성립한다.

$$a + (d-1) + y = b + (d-1) + z = 2^n - 1$$

$$O_1 = a + (d-1)$$

$$O_2 = (d-1) + z$$

이러므로 다음을 만족한다.

$$\begin{aligned} 2(2^n - 1) &= a + b + y + z + 2(d-1) \\ &= (a + d - 1) + (d - 1 + z) + b + y \\ &= O_1 + O_2 + b + y \end{aligned}$$

따라서, $O_1 + O_2 = 2(2^n - 1) - b - y$ 이다.

<따름정리 4.2.17> O_1 과 O_2 를 각각 n 차 원시다항식과 그것의 상반다항식의 최소 변위이라 하고, d 를 이것들의 최소 범위라 하자. $|OA_1|\,(=a) \neq |A_2O|\,(=b)$, $|B_1O| = y$ 라 두면 다음과 같다.

$$O_1 + O_2 \neq (2^n - 1) + |A_1B_1|$$

증명 : $|OB_2| = z$ 라 두자. $O_1 + O_2 = (2^n - 1) + |A_1B_1|$ 라 가정하자. 이러면 다음식에 의해 모순임을 알 수 있다.

$$2^n - 1 = x + b + y \neq a + x + y\,(\because 2^n - 1)$$

□

<따름정리 4.2.18> O_1과 O_2를 각각 n차 원시다항식과 그것의 상반다항식의 최소 변위이라 하고, d를 이것들의 최소 범위라 하자. $|OA_1| = |A_2O|$라 두면 다음이 성립한다.

$$O_2 = 2(2^n - 1) - (O_1 + d) + 1$$

증명> 정리 4.2.16에 의해 성립한다.

참 고 문 헌

[1] P.H. Bardell, *Analysis of Cellular Automata Used As Pseudorandom Pattern Generators*, Proc. IEEE int. Test. Conf., pp. 762 767, 1990.

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

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

[4] S.J. Cho, U.S. Choi and H.D. Kim, *Behavior of Complemented CA which the Complement Vector is Acyclic in a Linear TPMACA*, Mathematical and Computer Modelling, Vol. 36, 2002, pp. 979 986.

[5] S.J. Cho, U.S. Choi and H.D. Kim, *Linear Nongroup One Dimensional Cellular Automata Characterization on GF(2)*, J. Korea Multimedia Soc., Vol. 4, No. 1, 2001, pp. 91 95.

[6] A.K. Das, Additive Cellular Automata: Theory and Application as a Built In Self Test Structure, Ph.D thesis, I.I.T., Kharagpur, India, 1990.

[7] A.K. Das and P.P. Chaudhuri, *Efficient Characterization of Cellular Automata*, Proc. IEE(part E), Vol. 137, No. 1, 1990, pp. 81 87.

[8] A.K. Das and P.P. Chaudhuri, *Vector Space Theoretic Analysis of Additive Cellular Automata and its Application for Pseudo Exhaustive Test Pattern Generation*, IEEE Trans.

Computers, Vol. 42, 1993, pp. 340 352.

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

[10] P. Sarkar, *Computing shifts in 90/150 cellular automata sequences*, Finite Fields Their Appl., Vol. 42, pp. 340 352, 2003.

[11] C.E. Shannon, *A Mathematical Theory of Communication*, Bell System Technical Journal, Vol. 27, 1948, pp. 379 423, 623 656.

[12] S. Tezuka and M. Fushimi, *A method of designing cellular automata as pseudorandom number generators for built in self test for VLSI*, Comtemporary Mathmatica, Vol. 168, pp. 363 367, 1994.

[13] J. Von Neumann, Theory of Self Reproducing Automata, University of Illinois Press, Urbana, 1966.

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