



저작자표시-비영리-변경금지 2.0 대한민국

이용자는 아래의 조건을 따르는 경우에 한하여 자유롭게

- 이 저작물을 복제, 배포, 전송, 전시, 공연 및 방송할 수 있습니다.

다음과 같은 조건을 따라야 합니다:



저작자표시, 귀하는 원저작자를 표시하여야 합니다.



비영리, 귀하는 이 저작물을 영리 목적으로 이용할 수 없습니다.



변경금지, 귀하는 이 저작물을 개작, 변형 또는 가공할 수 없습니다.

- 귀하는, 이 저작물의 재이용이나 배포의 경우, 이 저작물에 적용된 이용허락조건을 명확하게 나타내어야 합니다.
- 저작권자로부터 별도의 허가를 받으면 이러한 조건들은 적용되지 않습니다.

저작권법에 따른 이용자의 권리는 위의 내용에 의하여 영향을 받지 않습니다.

이것은 [이용허락규약\(Legal Code\)](#)을 이해하기 쉽게 요약한 것입니다.

[Disclaimer](#)

이학박사 학위논문

GF(2^p)위에서의 SACA와 HCA의
특성에 관한 연구



부 경 대 학 교 대 학 원

응 용 수 학 과

최 향 희

이학박사 학위논문

$GF(2^p)$ 위에서의 SACA와 HCA의
특성에 관한 연구

지도교수 조 성 진

이 논문을 이학박사 학위논문으로 제출함.

2008년 2월

부 경 대 학 교 대 학 원

응 용 수 학 과

최 향 희

최향희의 이학박사 학위논문을 인준함.

2008년 2월 26일

주 심 이학박사 김 도 상 ㉠

위 원 이학박사 김 한 두 ㉠

위 원 이학박사 표 용 수 ㉠

위 원 이학박사 박 진 한 ㉠

위 원 이학박사 조 성 진 ㉠

목 차

그림 목차	v
표 목차	vi
Abstract	vii
1. 서론	1
2. 셀룰라 오토마타	3
2.1 CA의 정의 및 분류	3
2.2 CA의 전이행렬과 특성다항식	8
2.3 Group CA	13
2.4 Nongroup CA	19
3. 유한체 위에서의 인수분해	23
3.1 유한체	23
3.2 $GF(2^p)$ 위에서의 연산	27
3.3 확장체에서의 다항식의 인수분해	34
4. $GF(2^p)$ SACA의 특성분석	55
4.1 $GF(2^p)$ SACA	55
4.2 여원 $GF(2^p)$ SACA	60

4.3 $GF(2^p)$ SACA 트리구성	64
5. $GF(2^p)$ HCA의 특성분석	65
5.1 $GF(2^p)$ HCA의 전이규칙 및 성질	65
5.2 $GF(2^p)$ HCA의 특성다항식	76
6. 결론	81
참고 문헌	82



그 립 목 차

<그림 2.1> 3-이웃 선형 CA의 셀 구조	7
<그림 2.2> 서로 다른 경계 조건을 가지는 CA	8
<그림 2.3> 최대 길이를 갖는 Group CA	10
<그림 2.4> 최대 길이를 갖지 않는 Group CA	11
<그림 2.5> Nongroup CA	11
<그림 3.1> $GF(2^n)$ HCA의 구조	27
<그림 4.1> 3셀 $GF(2^2)$ SACA의 상태전이 그래프	57
<그림 4.2> 3셀 여원 $GF(2^2)$ SACA의 상태전이 그래프	63
<그림 5.1> 3셀 $GF(2^2)$ HCA의 상태전이 그래프	73
<그림 5.2> 3셀 $GF(2^2)$ HCA의 상태전이 그래프	74
<그림 5.3> 3셀 $GF(2^2)$ HCA의 상태전이 그래프	75

표 목차

<표 2.1> 선형 규칙	5
<표 2.2> 여원 규칙	6
<표 2.3> GF(2)위에서 10차까지의 원시다항식이 아닌 기약다항식	16
<표 2.4> GF(2)위에서 40차까지의 원시다항식	18
<표 3.1> $f(x) = x^4 + x^3 + 1$ 를 이용한 유한체 구성	25
<표 3.2> GF(2^2)위에서 곱셈과 덧셈	29
<표 3.3> GF(2^3)위에서 곱셈과 덧셈	31
<표 3.4> GF(2^4)위에서 곱셈과 덧셈	32
<표 3.5> GF(2^2)위에서 기약다항식들의 주기	33
<표 4.1> 선형 SACA와 여원 SACA의 상태배열 관계	61

Characterizations of Single Attractor Cellular Automata and Hierarchical Cellular Automata on $\text{GF}(2^p)$

Hyang-Hee Choi

*Department of Applied Mathematics, Graduate School
Pukyong National University*

Abstract

Cellular Automata(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 becomes to difficult to track analytically. A new cellular structure called $\text{GF}(2^p)$ CA is analytically characterized in this thesis. Each cell of the $\text{GF}(2^p)$ CA is capable of storing a value from the set $\{0, 1, \dots, 2^p - 1\}$. Though $\text{GF}(2^p)$ CA can only handle data with bit units $\text{GF}(2^p)$ HCA can handle data with units more than bit units.

In this thesis we analyze the state-transition of nongroup CA with a single attractor over $\text{GF}(2^p)$ and give the method for the construction of the state-transition diagram of a linear SACA over $\text{GF}(2^p)$ by using the concept of basic path. And we propose the state-transition diagram of the nonlinear complemented SACA by using the state-transition diagram of a linear SACA. Also we analyze transition rules, characteristic polynomials and cyclic structures of HCA over $\text{GF}(2^p)$.

1. 서론

셀룰라 오토마타(Cellular Automata, 이하 CA)는 Von Neumann[26]에 의해서 스스로 조직화하고 재생산할 수 있는 모델로 처음 소개되었다. 이후 Wolfram[35]은 각 셀이 0과 1, 두 상태를 가지고 다음 상태가 자기 자신과 인접한 두 이웃에 의해 갱신되는 3-이웃(3-neighbourhood) CA를 제안하였다. 특히 CA 가운데 다음 상태를 결정하는 함수가 선형적인 CA는 LFSR(Linear Feedback Shift Register)의 대안으로 제안되고, 이로 인해 테스트 패턴 생성[13], 압축치 분석[18] 등 많은 분야에 응용되었다. 1990년에 이르러 Das 등은 행렬대수학을 이용하여 선형 CA의 상태전이 행동분석을 하였다[15 ~ 18]. CA는 Wolfram[35]에 의하여 처음으로 암호학에 도입되었고, Chaudhuri, Nandi 등이 많은 분야에 CA를 폭넓게 활용하였다[11, 23 ~ 25, 28]. 그리고 Muzio와 Cattell 등에 의해서 LFSR에 대응하는 CA에 대한 연구가 이루어졌으며, 최소비용으로 최대길이를 갖는 CA를 찾는 연구가 수행되었다[15 ~ 17].

CA는 간단하고 규칙적이며 작은 단위로 확장 연결할 수 있는 구조이기 때문에 하드웨어 구현에 적합하다. GF(2)위에서의 CA에 대한 분석은 많은 연구가 이루어졌으며, 이러한 CA는 폭넓게 응용되었다[12, 21, 27, 29, 32 ~ 34]. 특히 Cho 등은 GF(2)위에서 TPMACA(Two Predecessor Multiple Attractor Cellular Automata)의 상태전이그래프를 기본경로를 이용하여 구성하는 알고리즘을 제안하였다[5 ~ 7].

GF(2)위에서의 CA는 셀이 한 개의 비트로 이루어져 있으므로 데이터 처리가 비트 단위로 이루어진다. 그러나 GF(2^n)위에서의 CA는 여러 개의 비트가 한 개의 셀을 이룬다. 따라서 바이트 단위 이상의 단위로 데이터 처리가 가능하다. CA는 컴퓨팅 패러다임과 많은 물리계를 모델링하는데 사용되어 왔다

[1, 3, 4, 14]. 그런데 시스템 모델을 연구함에 있어서 물리계의 복잡성이 증가함에 따라 CA를 이용한 모델은 매우 복잡하고 분석적으로 추적하기가 어렵게 되었다. 또한 그러한 모델들은 물리계의 내재적 계층적 성질을 인식할 수 없다는 문제점이 있다. 이러한 문제점을 해결하기 위하여 계층적 셀룰라 오토마타 (Hierarchical Cellular Automata, 이하 HCA)에 관한 연구를 하기 시작했다 [9, 10, 12]. Sikdar 등은 테스트 패턴 생성을 위하여 계층적 구조를 갖는 $GF(2^p)$ 위에서의 group CA를 사용하였으며 VLSI 회로의 고장을 진단하기 위하여 $GF(2^p)$ MACA를 이용하였다[18, 19, 30, 31].

본 논문의 구성은 2장에서는 CA의 정의와 여러 기준에 따른 CA의 분류를 소개하고 CA의 상태를 변화시키는 상태전이함수인 전이규칙에 대해 서술한다. 특히 선형 CA의 전이함수는 선형변환이므로, 이 선형변환을 표준행렬로 표현한 전이행렬과 전이행렬에 대한 특성다항식을 소개한다. 또한 group CA의 성질을 바탕으로 CA의 최소다항식과 사이클 구조를 소개하고 선형 nongroup CA의 성질을 서술한다.

3장에서는 유한체의 특성에 대해 알아보고 $GF(2^p)$ HCA의 구조와 확장체에서의 다항식의 인수분해 등을 살펴본다. 먼저 $GF(q)$ 위에서의 임의의 다항식을 인수분해하는 Berlekamp의 알고리즘을 소개하고 $GF(2^p)$ HCA의 인수분해로 확장한다.

4장에서는 $GF(2^p)$ 위에서 선형 SACA(Single Attractor Cellular Automata)를 특성화하고 상태전이 그래프를 효과적으로 구성하는 알고리즘을 제안한다. 또한 선형 SACA에 대응하는 여원 SACA의 상태전이 그래프를 구성하는 알고리즘을 제안한다.

5장에서는 HCA의 전이규칙, 특성다항식과 사이클 구조를 분석하고 6장에서 결론을 맺는다.

2. 셀룰라 오토마타

2.1 CA의 정의 및 분류

2.1.1 CA의 정의와 규칙

CA란 동역학계를 해석하는 한 방법으로 공간과 시간을 이산적으로 다루는 시스템이며 셀룰라 공간의 기본 단위는 하나의 셀이다. 이 시스템에서 셀의 다음 상태는 어떤 규칙에 따라 정해진다. 즉, 각 셀들은 자기 자신과 이웃 셀의 함수값에 의해 다음 상태가 결정되어 동시에 갱신된다. CA는 간단하고 규칙적이며 작은 단위로 확장 연결할 수 있는 구조이기 때문에 VLSI 하드웨어 구현에 알맞다.

가장 간단한 구조를 가지는 1차원 CA(One-Dimensional CA, 이하 1-D CA)에서는 모든 셀들이 선형으로 배열되어 있고 1-D CA중에서 국소적 상호작용이 세 개의 셀, 즉 자신과 인접한 두 셀에 의해 이루어지는 CA를 3-이웃(3-neighbourhood) CA라 한다. 본 논문에서 다루는 CA는 3-이웃 CA에 국한시킨다. 다음은 CA에 사용되는 기호이다.

- i : 일차원으로 배열되어 있는 각 셀들의 위치
- t : 시간 단계
- $q_i(t)$: 시간 t 에서 i 번째 셀의 상태
- $q_i(t+1)$: 시간 $t+1$ 에서 i 번째 셀의 상태

세 개의 이웃을 가지는 CA에 대한 다음상태 전이함수(transition function)는 다음과 같이 나타낸다.

$$q_i^{t+1} = f(q_{i-1}^t, q_i^t, q_{i+1}^t) \quad (2.1)$$

여기서 f 는 결합논리를 가지는 국소 전이함수이다. f 는 3개의 변수를 가지는 Boolean 함수이므로 2^3 , 즉 256개의 다음 상태 전이함수들이 있으며 이것을 CA의 규칙(rule)이라고 한다. CA의 셀들의 상태를 0과 1의 두 가지 값으로 다루고 주어진 CA의 다음상태 전이함수를 아래와 같이 표현한다.

이웃상태	111	110	101	100	011	010	001	000	규칙
다음상태	0	0	1	1	1	1	0	0	60
다음상태	1	0	0	1	0	1	1	0	150

여기서 첫 행은 시간 t 에서 인접한 세 개의 셀들의 가능한 8가지 상태의 배열이고 다음 행들은 시간 $t+1$ 에서 i 번째 셀의 갱신된 상태이다. 이진법의 수 $111100_{(2)}$ 를 십진법의 수로 변환하면 $1 \times 2^5 + 1 \times 2^4 + 1 \times 2^3 + 1 \times 2^2 = 60$ 이므로 규칙 60이라 하고 같은 방법으로 이진법의 수 $10010110_{(2)}$ 를 십진법의 수로 변환하면 150이므로 규칙 150이라 한다. 위의 규칙에 대한 결합논리는 다음 식으로 표현할 수 있고 $\oplus$ 는 XOR논리를 나타낸다.

$$\text{규칙 60} : q_i(t+1) = q_{i-1}(t) \oplus q_i(t) \quad (2.2)$$

$$\text{규칙 150} : q_i(t+1) = q_{i-1}(t) \oplus q_i(t) \oplus q_{i+1}(t) \quad (2.3)$$

2.1.2 CA의 분류

(1) 셀의 배열상태에 따른 분류

- ① 1차원 CA : 셀이 선형으로 배열되어 있는 CA
- ② 2차원 CA : 셀이 평면으로 배열되어 있는 CA
- ③ 3차원 CA : 셀이 공간으로 배열되어 있는 CA

(2) 적용되는 rule에 따른 분류

① 가산 CA (Additive CA)

가. 선형 CA (Linear CA) : 모든 셀의 규칙이 XOR 논리로만 이루어진 CA

나. 여원 CA (Complemented CA) : 셀의 규칙이 XNOR과 XOR 논리로 이루어진 CA

② 비가산 CA(Nonadditive CA) : 셀들의 규칙이 AND-OR 논리로 이루어진 CA

선형규칙	전이함수
규칙 60	$q_i(t+1) = q_{i-1}(t) \oplus q_i(t)$
규칙 90	$q_i(t+1) = q_{i-1}(t) \oplus q_{i+1}(t)$
규칙 102	$q_i(t+1) = q_i(t) \oplus q_{i+1}(t)$
규칙 150	$q_i(t+1) = q_{i-1}(t) \oplus q_i(t) \oplus q_{i+1}(t)$
규칙 170	$q_i(t+1) = q_{i+1}(t)$
규칙 204	$q_i(t+1) = q_i(t)$
규칙 240	$q_i(t+1) = q_{i-1}(t)$

<표 2.1> 선형규칙

여원규칙	전이함수
규칙 195	$q_i(t+1) = \overline{q_{i-1}(t) \oplus q_i(t)}$
규칙 165	$q_i(t+1) = \overline{q_{i-1}(t) \oplus q_{i+1}(t)}$
규칙 153	$q_i(t+1) = \overline{q_i(t) \oplus q_{i+1}(t)}$
규칙 105	$q_i(t+1) = \overline{q_{i-1}(t) \oplus q_i(t) \oplus q_{i+1}(t)}$
규칙 85	$q_i(t+1) = \overline{q_{i+1}(t)}$
규칙 51	$q_i(t+1) = \overline{q_i(t)}$
규칙 15	$q_i(t+1) = \overline{q_{i-1}(t)}$

<표 2.2> 여원규칙

(3) 모두 같은 규칙이 적용되는 규칙의 개수에 따른 분류

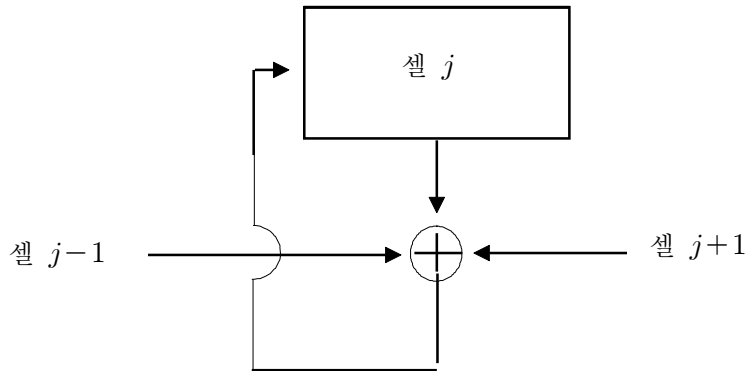
- ① Uniform CA : 모든 CA의 셀들에 같은 규칙이 적용된 CA
- ② Hybrid CA : 2가지 이상의 서로 다른 규칙이 적용된 CA

(4) 상태전이그래프의 형태에 따른 분류

- ① Group CA : 모든 셀들의 상태가 몇 개의 사이클을 이루며 반복되는 CA
- ② Nongroup CA : Group CA가 아닌 CA

Group CA는 모든 셀들의 상태가 몇 개의 사이클을 이루며 반복되는 CA로 임의의 한 상태에 대한 이전 상태가 유일하다. 이와 달리 Nongroup CA는 상태전이그래프가 트리 구조를 이루고 있으며 상태전이 함수에 의해 얻어질 수 있는 상태인 도달 가능한 상태와 상태전이 함수에 의해 나타날 수 없는 도달 불가능한 상태로 나누어진다. Nongroup CA는 임의의 한 상태에 대한 이전 상태가 존재하지 않거나 2개 이상이다.

그림 2.1은 3-이웃 선형 CA의 셀의 구조이다.

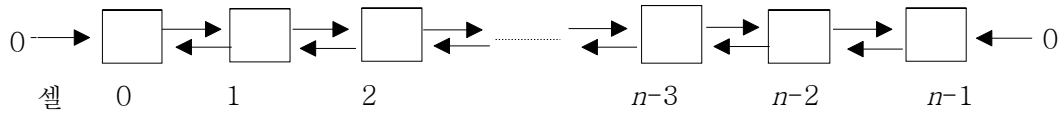


<그림 2.1> 3-이웃 선형 CA의 셀 구조

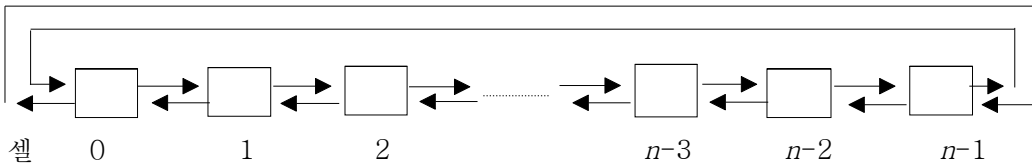
2.1.3 CA의 경계조건

CA에서 가장 왼쪽과 오른쪽의 셀은 2개의 이웃만을 가지므로 세 번째 이웃의 상태를 결정해 주어야 한다. 이것을 CA의 경계조건이라 하고 일반적으로 다음 세 가지의 경계조건이 있다. 제일 왼쪽과 오른쪽의 셀들이 0상태에 연결되어 있는 NBCA(Null Boundary CA), 양끝의 셀들이 서로 연결되어 있는 PBCA(Periodic Boundary CA), 가장 왼쪽(오른쪽) 셀의 다음 상태가 그 자신과 그것의 오른쪽(왼쪽) 이웃, 두 번째 오른쪽(왼쪽) 이웃 셀의 상태에 의존하는 IBCA(Intermediate Boundary CA)이다. 그림 2.2는 각각의 경계조건에 따라 분류된 CA의 연결 상태를 나타낸 것이다. 본 논문에서는 NBCA만 다룬다.

(1) NBCA



(2) PBCA



(3) IBCA



<그림 2.2> 서로 다른 경계조건을 가지는 CA

2.2 CA의 전이행렬과 특성다항식

2.2.1 CA의 전이행렬

n 개의 셀을 가지는 선형 1-D CA에서는 현재 상태를 다음 상태로 전이시키는 전이함수를 $n \times n$ 행렬로 나타낼 수 있으며, 이것을 전이행렬(transition matrix)이라 한다. 전이행렬 T 에서 i 번째 행은 i 번째 셀에 적용되는 규칙이며 그 셀의 다음 상태가 현재 상태에 의존하면 1, 그렇지 않으면 0으로 쓴다. 3-이웃 CA의

전이행렬은 정방행렬의 주 대각선과 그 윗 대각선과 아래 대각선을 제외한 나머지가 0인 삼중대각행렬(tridiagonal matrix)이다. 예를 들어 네 개의 셀을 가진 NBCA의 규칙이 $\langle 60, 150, 102, 90 \rangle$ 이면 전이행렬은 다음과 같다.

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (2.4)$$

S_t 가 시간 t 에서 CA의 상태를 나타내면 시간 $t+1$ 에서 CA의 상태는 다음 식으로 표현된다.

$$S_{t+1} = TS_t \quad (2.5)$$

만약 CA의 현재 상태가 $S_t = [1010]^t$ 이면 다음 상태 S_{t+1} 은 아래와 같다.

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

또한 시간 $t+2$ 에서 CA의 상태는 다음과 같다.

$$S_{t+2} = TS_{t+1} = T(TS_t) = T^2 S_t \quad (2.6)$$

p 단계 후의 CA의 상태는 다음과 같다.

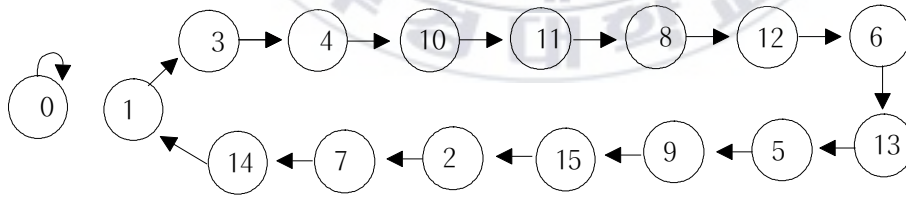
$$S_{t+p} = T^p S_t \quad (2.7)$$

CA의 전이행렬 T 가 정칙행렬 즉 $\det(T)=1$ 이면 이 CA는 group CA이다. Group CA는 모든 상태들이 일정한 사이클을 이루며 T 에 의해 상태가 반복되는 것으로 임의의 상태에 대하여 유일한 이전 상태를 가진다. 따라서 전이행렬의 역행렬을 구하여 현재 상태에 적용하면 이전 상태를 명확하게 얻을 수 있다. 즉,

$$S_{t-1} = T^{-1} S_t \quad (2.8)$$

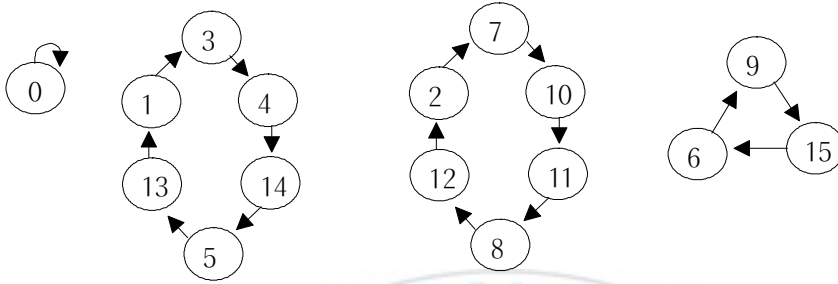
이다. Group CA는 최대 길이를 갖는 CA와 최대 길이를 갖지 않는 CA로 구별할 수 있다. n 개의 셀로 이루어진 CA에서 상태가 0인 경우를 제외한 $2^n - 1$ 개의 상태가 하나의 주기 안에 있을 때 최대 길이를 가진다고 하고 이 CA를 최대길이 CA(Maximal length CA 이하 MLCA)라 한다.

그림 2.3은 규칙이 $\langle 150, 90, 150, 150 \rangle$ 인 4개의 셀로 구성된 최대길이를 가지는 선형 CA이다.



<그림 2.3> 최대 길이를 갖는 Group CA

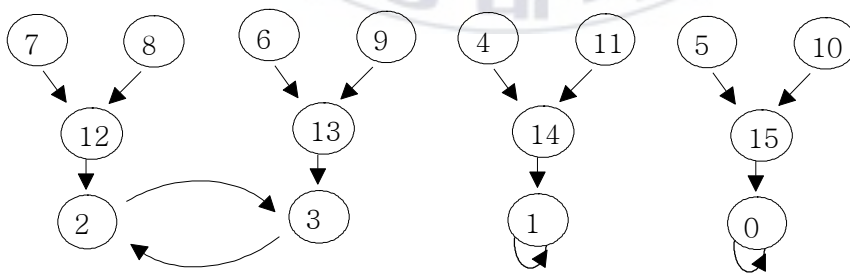
그림 2.4는 최대길이를 갖지 않는 선형 CA로 규칙 $\langle 150, 150, 150, 150 \rangle$ 을 갖는 uniform CA이다. 그림에서 알 수 있듯이 0을 제외한 다른 상태들이 몇 개의 서로 다른 사이클로 분리되어 있다. 각 사이클 길이의 최소공배수 6이 CA의 주기가 된다.



<그림 2.4> 최대 길이를 갖지 않는 Group CA
cCaCACACA CA gGroup CA

그림 2.5는 규칙이 $\langle 102, 60, 60, 150 \rangle$ 인 Nongroup CA의 상태전이 그래프이다.

이 CA의 전이행렬은 $T = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ 이고 상태전이 그래프는 트리 구조를 이룬다.



<그림 2.5> Nongroup CA

2.2.2 CA의 특성다항식

<정의 2.1> 특성다항식(characteristic polynomial) : 주어진 CA의 상태 전이행렬 T 에 대하여 특성다항식은 $GF(2)$ 위에서 $(T + xI)$ 의 행렬식 값이다.
즉

$$C(x) = |T + xI| \quad (2.9)$$

여기서 I 는 n 차 단위행렬이다.

<정의 2.2> 최소다항식 (minimal polynomial) : 특성다항식의 인수 중 T 를 근으로 갖는 차수가 가장 낮은 다항식을 최소다항식이라 한다.

예를 들어, 행렬 (2.4)에 대한 특성다항식을 구하면 다음과 같다.

$$|T + xI| = \begin{vmatrix} 1+x & 0 & 0 & 0 \\ 1 & 1+x & 1 & 0 \\ 0 & 0 & 1+x & 1 \\ 0 & 0 & 1 & x \end{vmatrix} = (x+1)^2(x^2+x+1) \quad (2.10)$$

그림 2.3의 전이행렬은 다음과 같고 특성다항식은 $x^4 + x^3 + 1$ 이다.

$$T = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \quad (2.11)$$

2.3 Group CA

Group CA는 LFSR의 대안으로 제안되면서 테스트 패턴 생성, 의사 난수열 생성, 오류정정부호의 설계 등에 응용되면서 활발하게 연구되어 왔다 [5, 7, 18, 19]. Group CA에서 자주 사용되는 용어들을 정의하고 group CA의 성질을 살펴본다.

2.3.1 선형 group CA

Group CA는 모든 셀들의 상태가 몇 개의 사이클을 이루며 반복되는 CA로 임의의 한 상태에 대하여 유일한 이전 상태를 가진다. 따라서 전이행렬의 역행렬을 구하여 현재 상태에 적용하면 이전 상태를 명확하게 얻을 수 있다.

<정리 2.1[11]> T 가 CA의 전이행렬일 때, 이 CA가 group CA이기 위한 필요충분조건은 $|T| = 1$ 이다.

<정리 2.2[7]> Group CA가 0이 아닌 상태로 시작하면서 길이가 p 또는 p 의 인수인 사이클을 갖기 위한 필요충분조건은 $|T^p \oplus I| = 0$ 이다.

2.3.2 CA의 최소다항식과 사이클 구조

Group CA는 최대길이를 갖는 CA (MLCA)와 그렇지 않은 CA로 분류할 수 있다. n 셀 최대길이를 가지는 CA는 0이 아닌 모든 상태가 한 개의 사이클을 이루며 이 사이클의 길이는 $2^n - 1$ 이다.

<정의 2.3[16]> n 차 기약다항식 (irreducible polynomial) : 다항식의 차수가 n 이고 인수분해 되지 않는 다항식을 n 차 기약다항식이라 한다.

$f(0) \neq 0$ 인 n 차 기약다항식 $f(x)$ 는 $x^{2^n-1} - 1$ 을 나눈다. 그러나 $f(x)$ 가 기약다항식이 아닌 경우는 일반적으로 $x^{2^n-1} - 1$ 을 나누지 않는다. CA가 최대길이를 갖는지 여부는 그 CA의 최소다항식이 원시다항식인지 아닌지와 관계가 있다.

<정의 2.4[16]> 원시다항식 (primitive polynomial) : $p(0) \neq 0$ 인 n 차 다항식 $p(x)$ 가 기약다항식이고 $p(x)$ 가 $x^m - 1$ 을 나누는 최소의 m 이 $2^n - 1$ 일 때 $p(x)$ 를 원시다항식이라 한다.

<정리 2.3[16]> n 셀 MLCA의 최소다항식은 n 차 원시다항식이다.

<정리 2.4[16]> $2^n - 1$ 이 소수인 n 차 기약다항식은 원시다항식이다.



표 2.3는 GF(2)위에서 10 차까지의 원시다항식이 아닌 기약다항식을 나타낸 표이다.

차수	기약다항식(주기)
4	$x^4 + x^3 + x^2 + x + 1(5)$
6	$x^6 + x^3 + 1(9)$, $x^6 + x^4 + x^2 + x + 1(21)$, $x^6 + x^5 + x^4 + x^2 + 1(21)$
8	$x^8 + x^5 + x^4 + x^3 + 1(17)$, $x^8 + x^7 + x^6 + x^4 + x^2 + x + 1(17)$ $x^8 + x^4 + x^3 + x + 1(51)$, $x^8 + x^7 + x^4 + x^3 + x^2 + x + 1(51)$ $x^8 + x^7 + x^5 + x^4 + 1(51)$, $x^8 + x^7 + x^6 + x^5 + x^4 + x + 1(51)$ $x^8 + x^5 + x^4 + x^3 + x^2 + x + 1(85)$ $x^8 + x^6 + x^5 + x^4 + x^2 + x + 1(85)$ $x^8 + x^6 + x^5 + x^4 + x^3 + x + 1(85)$, $x^8 + x^7 + x^3 + x + 1(85)$ $x^8 + x^7 + x^5 + x + 1(85)$, $x^8 + x^7 + x^5 + x^4 + x^3 + x^2 + 1(85)$ $x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + 1(85)$ $x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + 1(85)$
9	$x^9 + x + 1(73)$, $x^9 + x^4 + x^2 + x + 1(73)$, $x^9 + x^6 + x^3 + x + 1(73)$ $x^9 + x^6 + x^5 + x^2 + 1(73)$, $x^9 + x^7 + x^4 + x^3 + 1(73)$, $x^9 + x^8 + 1(73)$ $x^9 + x^8 + x^6 + x^3 + 1(73)$, $x^9 + x^8 + x^7 + x^5 + 1(73)$
10	$x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1(11)$ $x^{10} + x^7 + x^5 + x^3 + 1(33)$, $x^{10} + x^9 + x^5 + x + 1(33)$ $x^{10} + x^5 + x^4 + x^2 + 1(93)$, $x^{10} + x^8 + x^3 + x + 1(93)$ $x^{10} + x^8 + x^6 + x^5 + 1(93)$, $x^{10} + x^9 + x^7 + x^2 + 1(93)$ $x^{10} + x^9 + x^7 + x^5 + x^2 + x + 1(93)$

차수	기약다항식(주기)
10	$x^{10} + x^9 + x^8 + x^5 + x^3 + x + 1(93), x^{10} + x^3 + x^2 + x + 1(341)$ $x^{10} + x^4 + x^3 + x^2 + 1(341), x^{10} + x^6 + x^2 + x + 1(341)$ $x^{10} + x^6 + x^4 + x + 1(341), x^{10} + x^6 + x^5 + x + 1(341)$ $x^{10} + x^7 + x^6 + x^5 + x^3 + x^2 + 1(341)$ $x^{10} + x^8 + x^4 + x^3 + x^2 + x + 1(341), x^{10} + x^7 + x^4 + x^3 + 1(341)$ $x^{10} + x^7 + x^5 + x^3 + x^2 + x + 1(341), x^{10} + x^7 + x^6 + x^3 + 1(341)$ $x^{10} + x^8 + x^6 + x^5 + x^2 + x + 1(341)$ $x^{10} + x^8 + x^7 + x^4 + x^3 + x + 1(341)$ $x^{10} + x^8 + x^7 + x^5 + x^3 + x + 1(341)$ $x^{10} + x^8 + x^7 + x^5 + x^4 + x^3 + 1(341), x^{10} + x^8 + x^7 + x^6 + 1(341)$ $x^{10} + x^9 + x^5 + x^4 + 1(341), x^{10} + x^9 + x^6 + x^4 + 1(341)$ $x^{10} + x^9 + x^7 + x^5 + x^3 + x^2 + 1(341)$ $x^{10} + x^9 + x^7 + x^5 + x^4 + x^3 + x^2 + x + 1(341)$ $x^{10} + x^9 + x^7 + x^6 + x^3 + x^2 + 1(341)$ $x^{10} + x^9 + x^7 + x^6 + x^5 + x^4 + x^2 + x + 1(341)$ $x^{10} + x^9 + x^8 + x^3 + x^2 + x + 1(341)$ $x^{10} + x^9 + x^8 + x^4 + 1(341), x^{10} + x^9 + x^8 + x^5 + x^4 + x^2 + 1(341)$ $x^{10} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + x + 1(341)$ $x^{10} + x^9 + x^8 + x^7 + 1(341), x^{10} + x^9 + x^8 + x^7 + x^2 + x + 1(341)$ $x^{10} + x^9 + x^8 + x^7 + x^5 + x^3 + 1(341)$ $x^{10} + x^9 + x^8 + x^7 + x^6 + x^2 + 1(341)$ $x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^3 + x + 1(341)$

<표 2.3> GF(2)위에서 10차까지의 원시다항식이 아닌 기약다항식

표 2.4는 GF(2)위에서 40차까지의 원시다항식을 나타낸 표이다.

차수	원시다항식
2	$x^2 + x + 1$
3	$x^3 + x + 1$
4	$x^4 + x + 1$
5	$x^5 + x^2 + 1, x^5 + x^3 + x + 1$
6	$x^6 + x + 1, x^6 + x^5 + x^4 + x + 1$
7	$x^7 + x + 1, x^7 + x^4 + x^3 + x^2 + 1, x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$
8	$x^8 + x^7 + x^2 + x + 1, x^8 + x^7 + x^6 + x^5 + x^4 + x^2 + 1$
9	$x^9 + x^4 + 1, x^9 + x^6 + x^5 + x^3 + 1, x^9 + x^8 + x^7 + x^6 + x^3 + x^2 + 1$
10	$x^{10} + x^3 + 1, x^{10} + x^8 + x^3 + x^2 + 1, x^{10} + x^7 + x^6 + x^5 + x^2 + x + 1$
11	$x^{11} + x^2 + 1, x^{11} + x^{10} + x^8 + x + 1, x^{11} + x^9 + x^7 + x^5 + x^2 + x + 1$
12	$x^{12} + x^{10} + x^2 + x + 1, x^{12} + x^{10} + x^9 + x^8 + x^6 + x^2 + 1$
13	$x^{13} + x^8 + x^5 + x^3 + 1, x^{13} + x^{12} + x^{10} + x^5 + x^2 + x + 1$
14	$x^{14} + x^{12} + x^{11} + x + 1, x^{14} + x^{11} + x^5 + x^4 + x^3 + x + 1$
15	$x^{15} + x + 1, x^{15} + x^{12} + x^4 + x^3 + 1, x^{15} + x^{13} + x^8 + x^7 + x^6 + x^5 + 1$
16	$x^{16} + x^{15} + x^{12} + x^{10} + 1, x^{16} + x^{14} + x^{13} + x^{12} + x^9 + x^2 + 1$
17	$x^{17} + x^3 + 1, x^{17} + x^{16} + x^{12} + x^4 + 1, x^{17} + x^{13} + x^8 + x^6 + x^5 + x^2 + 1$
18	$x^{18} + x^7 + 1, x^{18} + x^{16} + x^{11} + x^4 + 1, x^{18} + x^{10} + x^8 + x^7 + x^4 + x + 1$
19	$x^{19} + x^{10} + x^9 + x^3 + 1, x^{19} + x^{18} + x^{16} + x^{13} + x^{12} + x^6 + 1$
20	$x^{20} + x^3 + 1, x^{20} + x^{13} + x^7 + x^2 + 1, x^{20} + x^{18} + x^{16} + x^{14} + x^{10} + x + 1$
21	$x^{21} + x^2 + 1, x^{21} + x^9 + x^4 + x^3 + 1, x^{21} + x^{19} + x^{18} + x^{14} + x^8 + x^6 + 1$
22	$x^{22} + x + 1, x^{22} + x^{12} + x^7 + x^3 + 1, x^{22} + x^{21} + x^{14} + x^9 + x^4 + x^2 + 1$
23	$x^{23} + x^5 + 1, x^{23} + x^{15} + x^8 + x^4 + 1, x^{23} + x^{17} + x^{13} + x^{12} + x^{11} + x^5 + 1$

차수	원시다항식
24	$x^{24} + x^{11} + x^5 + x^2 + 1, x^{24} + x^{23} + x^{16} + x^7 + x^6 + x^3 + 1$
25	$x^{25} + x^3 + 1, x^{25} + x^{13} + x^{12} + x^7 + 1$ $x^{25} + x^{23} + x^{15} + x^{13} + x^{10} + x^7 + 1$
26	$x^{26} + x^{23} + x^{15} + x^{13} + 1, x^{26} + x^{24} + x^{17} + x^{15} + x^6 + x + 1$
27	$x^{27} + x^{23} + x^{22} + x^{17} + 1, x^{27} + x^{19} + x^{18} + x^{17} + x^{11} + x^6 + 1$
28	$x^{28} + x^3 + 1, x^{28} + x^{24} + x^8 + x^5 + 1$ $x^{28} + x^{27} + x^{24} + x^{21} + x^{11} + x^5 + 1$
29	$x^{29} + x^2 + 1, x^{29} + x^{16} + x^6 + x^2 + 1$ $x^{29} + x^{22} + x^{16} + x^{15} + x^{11} + x^3 + 1$
30	$x^{30} + x^{27} + x^{10} + x^9 + 1, x^{30} + x^{29} + x^{28} + x^{24} + x^{12} + x^{11} + 1$
31	$x^{31} + x^3 + 1, x^{31} + x^{25} + x^{23} + x^8 + 1$ $x^{31} + x^{16} + x^{14} + x^{10} + x^8 + x + 1$
32	$x^{32} + x^{16} + x^7 + x^2 + 1, x^{32} + x^{30} + x^{17} + x^{12} + x^3 + x + 1$
33	$x^{33} + x^{13} + 1, x^{33} + x^{26} + x^{16} + x^{11} + 1$ $x^{33} + x^{32} + x^{19} + x^{17} + x^8 + x + 1$
34	$x^{34} + x^{17} + x^{12} + x^8 + 1, x^{34} + x^{31} + x^{20} + x^{14} + x^7 + x^4 + 1$
35	$x^{35} + x^2 + 1, x^{35} + x^{27} + x^{17} + x^9 + 1$ $x^{35} + x^{32} + x^{31} + x^{23} + x^{21} + x^2 + 1$
36	$x^{36} + x^{11} + 1, x^{36} + x^{33} + x^{12} + x^7 + 1$ $x^{36} + x^{28} + x^{26} + x^{25} + x^{17} + x^6 + 1$
37	$x^{37} + x^{22} + x^{14} + x^2 + 1, x^{37} + x^{33} + x^{31} + x^{30} + x^{21} + x^3 + 1$
38	$x^{38} + x^{27} + x^6 + x^5 + 1, x^{38} + x^{36} + x^{20} + x^{11} + x^9 + x^6 + 1$
39	$x^{39} + x^4 + 1, x^{39} + x^{35} + x^{23} + x^{16} + 1$ $x^{39} + x^{38} + x^{36} + x^{15} + x^{13} + x^2 + 1$
40	$x^{40} + x^{29} + x^{27} + x^{23} + 1, x^{40} + x^{36} + x^{28} + x^{18} + x^7 + x^6 + 1$

<표 2.4> GF(2)위에서 40차까지의 원시다항식

2.4 Nongroup CA

Nongroup CA가 이미지 압축, 해쉬 함수, 부울 방정식의 해법, 암호 알고리즘 등에 응용이 되면서 최근 연구가 활발히 이루어지고 있다[11, 35]. Nongroup CA의 정의와 자주 사용되는 용어들을 정의하고 nongroup CA의 성질에 대하여 살펴본다.

2.4.1 선형 Nongroup CA

선형 nongroup CA는 다음 상태를 결정짓는 상태전이 함수가 XOR 논리로만 이루어진 CA로 group CA가 아닌 CA이다. 즉, 사용되는 규칙이 60, 90, 102, 150, 170, 204, 240이고 상태전이그래프가 트리 구조를 가지는 CA이고 $|T| = 0$ 으로 역행렬이 존재하지 않는다. 그러므로 임의의 상태에 대한 이전 상태 수는 0이거나 2 이상이다. 어떤 상태의 이전 상태수가 0이란 의미는 이전 상태가 존재하지 않는다는 것으로 주어진 상태는 도달 불가능한 상태이다. 이와 달리 이전 상태수가 2 이상이란 의미는 주어진 상태가 도달 가능한 상태이며, 2개 이상의 이전 상태가 존재한다는 것을 말한다. 이처럼 nongroup CA는 상태전이 함수가 일대일 대응 함수가 아니다. 그러므로 주어진 상태에 대하여 이전 상태를 구하는 것이 불가능하다. 선형 nongroup CA에서 자주 사용되는 용어들을 정의하고 nongroup CA의 성질을 살펴본다.

<정의 2.5> (1) 선형 Nongroup CA : Nongroup CA 중 다음 상태를 결정하는 상태전이 함수가 XOR 논리만으로 이루어진 CA를 말한다.

(2) 순환상태(cyclic state) : Nongroup CA의 상태전이그래프의 사이클 안에

존재하고 일정한 시간 단계 후 그 상태가 반복되는 상태로, 상태 y 가 순환상태이면 $T^k y = y$ 를 만족하는 k 가 존재한다. 여기서 k 의 최소값이 상태 y 가 놓이는 사이클의 길이이다.

(3) **attractor** : 순환상태들 중 사이클의 길이가 1인 상태를 attractor라 한다. 어떤 상태 x 가 attractor이면 전이행렬 T 에 대하여 $Tx = x$ 를 만족한다.

(4) **MACA(Multiple-Attractor CA)** : Nongroup CA의 모든 순환상태들이 attractor인 CA를 MACA라 부른다. 특히 직전자 수가 2인 MACA를 **TPMACA(Two Predecessor Multiple-Attractor CA)**라 부른다. Attractor의 수가 1인 MACA를 **SACA(Single-Attractor CA)**라 부르며 특히 직전자의 수가 2인 SACA를 **TPSACA(Two Predecessor Single-Attractor CA)**라 부른다.

(5) α -트리 : 순환상태 α 를 root로 하는 트리이다.

(6) **깊이(depth)** : Nongroup CA의 상태전이그래프에서 임의의 도달 불가능한 상태에서 가장 가까운 순환상태로 전이되는데 걸리는 최소 상태 전이 수를 깊이라 부른다.

(7) **level** : 어떤 상태 x 가 α -트리의 level l ($l \leq$ 깊이)에 있다는 것은 상태 x 가 정확히 l 번 상태 전이 후 상태 α 가 되는 위치에 있다는 것이다. 즉 $T^l x = \alpha$ 가 되는 p 값 중 최소값이 l 이다.

(8) **주기** : 상태전이그래프에서 나타나는 사이클 길이의 최소공배수로 임의의 순환상태 y 에 대하여 $T^c y = y$ 인 최소의 c 가 주기가 된다.

그림 2.5에서 순환상태는 0, 1, 2, 3이다. 특히 상태 0과 1은 사이클의 길이가 1이므로 attractor이다. 상태 2, 3은 사이클의 길이가 2인 사이클에 존재한다. 그러므로 이 CA의 주기는 1과 2의 최소공배수인 2이다. 각 트리의 깊이는 2이다. 2-트리는 상태 2를 root로 하는 트리이므로 상태 7, 8, 12, 2가 2-트리에 속한다. 각 트리의 level 1의 상태는 12, 13, 14, 15이고 level 2에 있는 상태들은 4, 5, 6, 7, 8, 9, 10, 11이다. 다음은 4셀 TPMACA의 예이다.

<예 2.1> 4개의 셀로 이루어진 CA가 규칙 $\langle 60, 102, 60, 102 \rangle$ 을 가질 때, 전이행렬은

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad (2.12)$$

이고, 특성다항식은 $x^2(1+x)^2$ 이며 최소다항식은 $x^2(1+x)$ 이다. 주어진 T의 계수(rank)는 3이다. 각 트리의 깊이는 2이고, attractor는 0, 1, 8, 9이다. 상태 0, 2, 4, 6은 0-트리에 속하고, 상태 1, 3, 5, 7은 1-트리에 속한다.

2.4.2 선형 Nongroup CA의 성질

선형 nongroup CA에서 0-트리와 다른 순환상태를 root로 하는 트리는 매우 밀접한 관계를 가지고 있으며 다음의 정리들은 선형 nongroup CA의 기본적인 성질이다.

<정리 2.5[7]> 선형 nongroup CA에서 상태 0은 attractor이다.

<보조정리 2.6[7]> 선형 nongroup CA의 전이행렬 T 의 영공간 (null space)의 차원이 d 이면 상태 0의 직전자의 수는 2^d 이다.

<정리 2.7[7]> 선형 nongroup CA에서 도달 가능한 상태의 직전자의 수는 상태 0의 직전자의 수와 같다.

<정리 2.8[7]> 선형 nongroup CA의 상태전이그래프에서 0-트리의 깊이를 d 라 하고 주어진 전이행렬 T 의 영공간의 차원이 r 이면 0-트리의 상태의 수는 2^{rd} 이다.

선형 nongroup CA의 전이행렬의 최소다항식은 $m(x) = x^d \phi(x)$ 로 표현된다. 여기서 d 는 CA의 깊이가 되고 $\phi(x)$ 가 $x^c + 1$ 를 나누는 c 중 최소의 c 가 주기가 된다. 그림 2.5의 선형 nongroup CA의 최소다항식은 $x^4 + x^2 = x^2(x^2 + 1)$ 이다. 그러므로 깊이는 2이고 $\phi(x) = x^2 + 1$ 이다. 또한 이 CA의 주기는 2이다.

3. 유한체에서의 인수분해

3.1 유한체

<정의 3.1> 군(Group) : 집합 G 위에 정의된 이항연산 $\cdot$ 에 대하여 다음 세 조건을 만족하면, $(G, \cdot)$ 를 군이라 한다.

(1) 임의의 원소 $a, b, c \in G$ 에 대하여

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \text{가 성립한다.}$$

(2) 임의의 원소 $a \in G$ 에 대하여

$$a \cdot e = e \cdot a \text{를 만족하는 } e \in G \text{가 존재한다.}$$

(3) 각 원소 $a \in G$ 에 대하여

$$a \cdot a^{-1} = a^{-1} \cdot a = e \text{를 만족하는 } a^{-1} \in G \text{가 존재한다.}$$

<정의 3.2> 유한체(Finite field) : 유한집합 $F (\neq \emptyset)$ 위에 정의된 두 연산 $+$ 와 $\cdot$ 에 대하여 다음 조건들을 만족하면, $(F, +, \cdot)$ 를 유한체라고 한다.

(1) $(F, +)$ 는 항등원 0을 가지는 가환군이다.

(2) $(F - \{0\}, \cdot)$ 는 가환군이다.

(3) 임의의 $a, b, c \in F$ 에 대하여

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ (분배법칙)이 성립한다.}$$

임의의 소수 p 와 양의 정수 m 에 대하여 $q = p^m$ 이라고 할 때, q 개의 원소로 이루어진 유한체가 존재한다. 이것을 $GF(q)$ 로 나타내고 이 체를 q 개의 원소를 가진 유한체라고 한다.

$GF(q^m) = \{0, 1, \dots, q^m - 1\}$ 은 $GF(q) = \{0, 1, \dots, q - 1\}$ 의 확대체이다.

<정의 3.3> 표수(characteristic) : 체 F 의 단위원 1에 대하여 다음과 같은 양의 정수 n 이 존재하는 경우에 이와 같은 양의 정수 중에서 가장 작은 n 을 체 F 의 표수라고 한다.

$$n \cdot 1 = 1 + 1 + \dots + 1 = 0 \quad (1 \text{ 이 } n \text{ 개})$$

<정의 3.4> 주기(Order) : $f(0) \neq 0$ 인 다항식 $f(x)$ 에 대하여 다음과 같이 $\min \{a : f(x) \mid x^a - 1\} = m$ 을 만족할 때, m 을 $f(x)$ 의 주기라 하고, 기호로 $\text{ord}(f(x)) = m$ 이라 쓴다.

<정리 3.1[20]> 유한체의 표수 q 는 소수이다.

<정리 3.2[20]> $a (\neq 0)$ 가 유한체 $GF(q)$ 의 원소이면, $a^{q-1} = 1$ 이다.

<예 3.1> $f(x) = x^3 + x + 1$ 이면 $f(x)$ 는 기약다항식이고 $\alpha^3 = \alpha + 1$ 이다.
 $GF(2^3) = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$ 에서 $\alpha^4 = \alpha(\alpha + 1) = \alpha^2 + \alpha$ 이고
 $\alpha^5 = \alpha^2 + \alpha + 1$, $\alpha^6 = \alpha^2 + 1$ 이다. 따라서 $\alpha^7 = \alpha^3 + \alpha = 1$ 이다.

<정리 3.3> $a (\neq 0)$ 가 유한체 $GF(q)$ 의 원소이고, $\text{ord}(a) = n$ 이면 n 은 $q - 1$ 의 약수이다.

(증명) $F^* = F - \{0\}$ 는 원소의 수가 $q - 1$ 개인 곱셈군이고, $\{1, \alpha, \dots, \alpha^{n-1}\}$ 은

n 개의 원소를 갖는 부분군이다. 따라서 라그랑지 정리에 의하여 n 은 $q - 1$ 의 약수이다.

<예 3.2> $q = 2, n = 4$ 인 경우, $f(x) = x^4 + x + 1$ 를 이용하여 2^4 개의 원소를 갖는 유한체 $GF(2^4)$ 를 구성할 수 있다. $x \bmod (x^4 + x + 1)$ 에 대응하는 체의 원소를 $\alpha = (0, 0, 1, 0)$ 로 나타내면, 다음의 표를 얻을 수 있다.

i	α^i	$ord(\alpha^i)$	α^i 의 최소다항식
0	0001	1	$x + 1$
1	0010	15	$x^4 + x + 1$
2	0100	15	$x^4 + x + 1$
3	1000	5	$x^4 + x^3 + x^2 + x + 1$
4	0011	15	$x^4 + x + 1$
5	0110	3	$x^2 + x + 1$
6	1100	5	$x^4 + x^3 + x^2 + x + 1$
7	1011	15	$x^4 + x^3 + 1$
8	0101	15	$x^4 + x + 1$
9	1010	5	$x^4 + x^3 + x^2 + x + 1$
10	0111	3	$x^2 + x + 1$
11	1110	15	$x^4 + x^3 + 1$
12	1111	5	$x^4 + x^3 + x^2 + x + 1$
13	1101	15	$x^4 + x^3 + 1$
14	1001	15	$x^4 + x^3 + 1$

<표 3.1> $f(x) = x^4 + x^3 + 1$ 를 이용한 유한체 구성

위의 표에서 최소다항식을 구하는 방법은 다음과 같다. 예를 들어 α^3 의 최소다항식을 구해보자. $GF(2^4)$ 는 $GF(2)$ 위에서 4차원 벡터공간이므로, 5개 벡터 $\alpha^3, (\alpha^3)^2, (\alpha^3)^3, (\alpha^3)^4, (\alpha^3)^5 = 1$ 는 일차종속이다. $\alpha^3 = \beta$ 라 놓으면 $\beta, \beta^2, \beta^3, \beta^4, 1$ 은 일차종속이다. 그리고 $1 = 0001, \beta = 1000, \beta^2 = 1100, \beta^3 = 1010, \beta^4 = 1111$ 이므로, 이들 5개 벡터의 일차종속 관계는 $\beta^4 = a \cdot \beta^3 + b \cdot \beta^2 + c \cdot \beta + d \cdot 1$ 을 만족하는 $(a, b, c, d) \neq (0, 0, 0, 0)$ 을 구하면 된다.

$$\begin{aligned}(1, 1, 1, 1) &= a(1, 0, 1, 0) + b(1, 1, 0, 0) + c(1, 0, 0, 0) + d(0, 0, 0, 1) \\ &= (a + b + c, b, a, d)\end{aligned}$$

로부터 $a = b = c = d = 1$ 을 얻는다. 따라서 $\beta^4 = \beta^3 + \beta^2 + \beta + 1$ 이므로 $\beta^4 + \beta^3 + \beta^2 + \beta + 1 = 0$ 이고 $\beta = \alpha^3$ 의 최소다항식은 $x^4 + x^3 + x^2 + x + 1$ 이다.

위의 표 3.1에서 4차의 원시다항식은 8개이며 종류는 2가지이다. 원시다항식이 되는 α^i 는 $i = 1, 2, 4, 7, 8, 11, 13, 14$ 이다. 이 수들은 모두 15와 서로소인 수들이다. 따라서 서로 다른 n 차 원시다항식의 개수는 다음과 같다.

$$\frac{\phi(2^4 - 1)}{4} = \frac{8}{4} = 2 \quad (3.1)$$

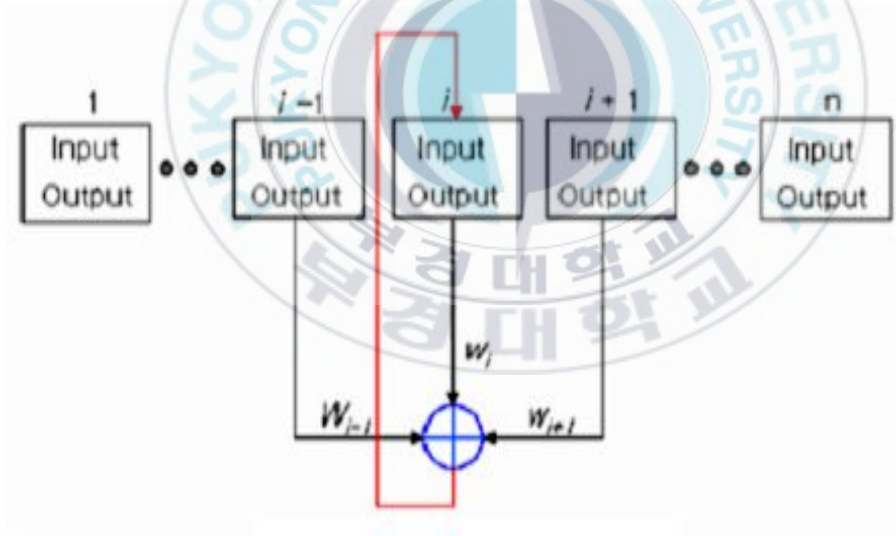
이 때, ϕ 는 오일러의 ϕ 함수이며, $\phi(n)$ 은 정수 $0, 1, 2, \dots, n-1$ 중에서 n 과 서로소인 전체 개수를 나타낸다.

3.2 GF(2^p) 위에서의 연산

다음은 이 논문의 전개에 필요한 몇 가지 용어들을 정의한다.

<정의 3.5> 선형 GF(2^p) HCA : 셀의 각 상태에 GF(2^p)의 원소인 가중치를 곱한 후 XOR하여 다음 상태로 갱신되는 CA를 선형 GF(2^p) HCA라 한다.

GF(2) CA는 한 개의 셀이 가질 수 있는 상태는 0, 1로 2개이다. 반면 GF(2^p) HCA는 p 개의 기억소자가 한 개의 셀을 이루기 때문에 하나의 셀이 가질 수 있는 상태는 2^p 개로 $\{0, 1, 2, \dots, 2^p - 1\}$ 의 원소이다. GF(2^p)는 GF(2)의 확대체로 2^p 개의 원소로 이루어지고, 구조는 다음과 같다.



<그림 3.1> GF(2^p) HCA의 구조

<정의 3.6> 생성다항식(generator polynomial) : $GF(2^p)$ 를 생성하는 다항식을 생성다항식(generator polynomial)이라 한다.

<정의 3.7> 생성행렬(generator matrix) : 생성다항식을 특성다항식으로 갖는 삼중대각행렬 M 을 생성행렬이라 한다.

주어진 i 번째 셀의 다음 상태는 자신과 이웃하는 두 개의 셀의 상태에 따라 결정되는데 $GF(2^p)$ HCA의 다음 상태를 결정하는 상태전이함수는 다음과 같다.

$$q_i(t+1) = \phi(w_{i-1}q_{i-1}(t), w_iq_i(t), w_{i+1}q_{i+1}(t)) \quad (3.2)$$

여기서 $q_i(t)$ 는 시간 t 에서 i 번째 셀의 상태를 나타내며 $w_i \in GF(2^p)$ 는 가중치를 나타낸다. 선형 $GF(2^p)$ HCA의 상태전이행렬은 다음과 같은 삼중대각행렬로 이루어진다. 이 때 w_{ij} 는 j 번째 셀의 현재상태가 i 번째 셀의 다음상태에 영향을 주는 정도를 나타내는 가중치이며 $GF(2^p)$ 의 원소이다.

$$T = \begin{pmatrix} w_{11} & w_{12} & 0 & \dots & 0 \\ w_{21} & w_{22} & w_{23} & \dots & 0 \\ 0 & w_{32} & w_{33} & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & w_{nn} \end{pmatrix} \quad (3.3)$$

<예 3.3> 3셀 $GF(2^2)$ HCA의 전이행렬이 다음과 같다고 하자.

$$T = \begin{pmatrix} 1 & \alpha & 0 \\ \alpha & \alpha^2 & \alpha \\ 0 & \alpha & \alpha \end{pmatrix} \quad (3.4)$$

여기서 α 는 $GF(2^2)$ 를 생성하는 생성자이다. 따라서 $GF(2^2)$ 의 원소는 $0, 1, \alpha, \alpha^2$ 이다. 또한 α 는 생성다항식 $g(x) = x^2 + x + 1$ 의 해가 되고 생성행렬 M 은 다음과 같다.

$$M = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \quad (3.5)$$

유한체 위에서 곱셈과 덧셈을 대응시키기 위해 α^i 와 M^i 의 마지막 열벡터를 대응시킨다. 위의 예에서 생성행렬 M^i 와 α^i 는 다음과 같다.

$$M^2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad M^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad (3.6)$$

$\alpha = \langle 10 \rangle = 2$, $\alpha^2 = \langle 11 \rangle = 3$, $\alpha^3 = 1 = \langle 01 \rangle = 1$, $0 = \langle 00 \rangle = 0$ 이다.

따라서 $GF(2^2)$ 위에서 덧셈과 곱셈은 표 3.2와 같다.

$\times$	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

<표 3.2> $GF(2^2)$ 위에서 곱셈과 덧셈

$GF(2^2)$ 위에서 기약다항식들의 주기는 <표 3.5>와 같다. $GF(q)$ 에서 기약

다항식의 개수는 n 이 다항식의 차수일 때 $N_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{\frac{n}{d}}$ 이다.

<정의 3.8> 뫼비우스 함수(Möbius function) : 정수 n 의 소인수분해가 $n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$ 일 때, 함수 $\mu : \mathbb{N} \rightarrow \{-1, 0, 1\}$ 를 뫼비우스 함수라고 한다.

$$\mu(n) = \begin{cases} 1 & , n = 1 \\ (-1)^m & , e_1 = e_2 = \cdots = e_m = 1 \\ 0 & , \text{기타} \end{cases} \quad (3.7)$$

예를 들어, $GF(2^2)$ 위에서 4차의 원시다항식의 개수는 $\frac{\phi(4^4 - 1)}{4} = 32$ 이고

기약다항식의 개수는 $\frac{1}{4} (\mu(1)(2^2)^4 + \mu(2)(2^2)^2 + \mu(4)(2^2)^1) = 60$ 이다.

또한 모든 n 차 기약다항식은 $x^{2^n-1} - 1$ 을 나눈다.

<예 3.4> $M = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$ 이면 $g(x) = x^3 + x + 1$ 이다.

$$\alpha \rightarrow \langle 011 \rangle = 3 \qquad \alpha^2 \rightarrow \langle 100 \rangle = 4$$

$$\alpha^3 \rightarrow \langle 010 \rangle = 2 \qquad \alpha^4 \rightarrow \langle 111 \rangle = 7$$

$$\alpha^5 \rightarrow \langle 110 \rangle = 6 \qquad \alpha^6 \rightarrow \langle 101 \rangle = 5$$

$$\alpha^7 \rightarrow \langle 001 \rangle = 1$$

GF(2³)과 GF(2⁴)위에서 곱셈과 덧셈표는 다음과 같이 만들 수 있다.

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	5	7	6	4	3	1
3	0	3	7	4	2	1	5	6
4	0	4	6	2	7	3	1	5
5	0	5	4	1	3	6	7	2
6	0	6	3	5	1	7	2	4
7	0	7	1	6	5	2	4	3

<표 3.3> GF(2³)위에서 곱셈과 덧셈

<예 3.5> $M = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix}$ 이면 $g(x) = x^4 + x + 1$ 이다.

$$\alpha \rightarrow \langle 0011 \rangle = 3$$

$$\alpha^2 \rightarrow \langle 0110 \rangle = 6$$

$$\alpha^3 \rightarrow \langle 1011 \rangle = 11$$

$$\alpha^4 \rightarrow \langle 0010 \rangle = 2$$

$$\alpha^5 \rightarrow \langle 0101 \rangle = 5$$

$$\alpha^6 \rightarrow \langle 1101 \rangle = 13$$

$$\alpha^7 \rightarrow \langle 1001 \rangle = 9$$

$$\alpha^8 \rightarrow \langle 0111 \rangle = 7$$

$$\alpha^9 \rightarrow \langle 1000 \rangle = 8$$

$$\alpha^{10} \rightarrow \langle 0100 \rangle = 4$$

$$\alpha^{11} \rightarrow \langle 1110 \rangle = 14$$

$$\alpha^{12} \rightarrow \langle 1111 \rangle = 15$$

$$\alpha^{13} \rightarrow \langle 1100 \rangle = 12$$

$$\alpha^{14} \rightarrow \langle 1010 \rangle = 10$$

$$\alpha^{15} \rightarrow \langle 0001 \rangle = 1$$

+	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	1	0	3	2	5	4	7	6	9	8	11	10	13	12	15	14
2	2	3	0	1	6	7	4	5	10	11	8	9	14	15	12	13
3	3	2	1	0	7	6	5	4	11	10	9	8	15	14	13	12
4	4	5	6	7	0	1	2	3	12	13	14	15	8	9	10	11
5	5	4	7	6	1	0	3	2	13	12	15	14	9	8	11	10
6	6	7	4	5	2	3	0	1	14	15	12	13	10	11	8	9
7	7	6	5	4	3	2	1	0	15	14	13	12	11	10	9	8
8	8	9	10	11	12	13	14	15	0	1	2	3	4	5	6	7
9	9	8	11	10	13	12	15	14	1	0	3	2	5	4	7	6
10	10	11	8	9	14	15	12	13	2	3	0	1	6	7	4	5
11	11	10	9	8	15	14	13	12	3	2	1	0	7	6	5	4
12	12	13	14	15	8	9	10	11	4	5	6	7	0	1	2	3
13	13	12	15	14	9	8	11	10	5	4	7	6	1	0	3	2
14	14	15	12	13	10	11	8	9	6	7	4	5	2	3	0	1
15	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

×	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	0	2	7	5	10	8	13	15	12	14	11	9	6	4	1	3
3	0	3	5	6	14	13	11	8	4	7	1	2	10	9	15	12
4	0	4	10	14	5	1	15	11	2	6	8	12	7	3	13	9
5	0	5	8	13	1	4	9	12	10	15	2	7	11	14	3	6
6	0	6	13	11	15	9	2	4	14	8	3	5	1	7	12	10
7	0	7	15	8	11	12	4	3	6	1	9	14	13	10	2	5
8	0	8	12	4	2	10	14	6	11	3	7	15	9	1	5	13
9	0	9	14	7	6	15	8	1	3	10	13	4	5	12	11	2
10	0	10	11	1	8	2	3	9	7	13	12	6	15	5	4	14
11	0	11	9	2	12	7	5	14	15	4	6	13	3	8	10	1
12	0	12	6	10	7	11	1	13	9	5	15	3	14	2	8	4
13	0	13	4	9	3	14	7	10	1	12	5	8	2	15	6	11
14	0	14	1	15	13	3	12	2	5	11	4	10	8	6	9	7
15	0	15	3	12	9	6	10	5	13	2	14	1	4	11	7	8

<표 3.4> GF(2⁴)위에서 곱셈과 덧셈

차수	주기 (개수)	기약다항식
1	1(2)	$x, x + 1$
	3(2)	$x + 2, x + 3$
2	5(2)	$x^2 + 2x + 1, x^2 + 3x + 1$
	15(4)	$x^2 + x + 2, x^2 + x + 3, x^2 + 2x + 2, x^2 + 3x + 3$
3	7(2)	$x^3 + x + 1, x^3 + x^2 + 1$
	9(2)	$x^3 + 2, x^3 + 3$
	21(4)	$x^3 + 2x + 1, x^3 + 2x^2 + 1, x^3 + 3x + 1, x^3 + 3x^2 + 1$
	63(12)	$x^3 + x^2 + x + 2, x^3 + 3x^2 + 3x + 3, x^3 + x^2 + 3x + 2, x^3 + 2x^2 + 3x + 3$
		$x^3 + x^2 + 2x + 3, x^3 + 3x^2 + 2x + 2, x^3 + x^2 + x + 3, x^3 + 2x^2 + 2x + 2$ $x^3 + 2x^2 + 3x + 2, x^3 + 2x^2 + x + 3, x^3 + 3x^2 + x + 2, x^3 + 3x^2 + 2x + 3$
4	17(4)	$x^4 + 2x^3 + x^2 + 2x + 1, x^4 + 3x^3 + x^2 + 3x + 1, x^4 + x^3 + 2x^2 + x + 1$ $x^4 + x^3 + 3x^2 + x + 1$
	51(8)	$x^4 + x^3 + 2x^2 + 2x + 3, x^4 + x^3 + 3x^2 + 3x + 2, x^4 + 2x^3 + x^2 + x + 2$ $x^4 + 2x^3 + 2x^2 + x + 2, x^4 + 2x^3 + 2x^2 + 3x + 3, x^4 + 3x^3 + x^2 + x + 3$ $x^4 + 3x^3 + 3x^2 + x + 3, x^4 + 3x^3 + 3x^2 + 2x + 2$
		$x^4 + x^2 + 2x + 1, x^4 + x^2 + 3x + 1, x^4 + 3x^2 + 2x + 1, x^4 + 3x^2 + 3x + 3$ $x^4 + x^3 + 2x + 1, x^4 + x^3 + 3x + 1, x^4 + x^3 + x^2 + 2, x^4 + 2x^3 + x + 1$ $x^4 + 2x^3 + x^2 + 1, x^4 + 2x^3 + 2x^2 + 3x + 1, x^4 + 2x^3 + 3x^2 + 1$ $x^4 + 2x^3 + 3x^2 + 3x + 1, x^4 + 3x^3 + x + 1, x^4 + x^2 + 3x + 1$ $x^4 + 3x^3 + 2x^2 + 2x + 1, x^4 + 3x^3 + 3x^2 + 2x + 1$
	85(16)	$x^4 + x^2 + 2x + 3, x^4 + x^2 + 3x + 2, x^4 + 2x^2 + 2x + 2, x^4 + 2x^2 + 2x + 3$ $x^4 + 2x^2 + 3x + 3, x^4 + 3x^2 + 2x + 2, x^4 + 3x^2 + 3x + 2, x^4 + 3x^3 + 3x + 3$ $x^4 + x^3 + x + 2, x^4 + x^3 + x + 3, x^4 + x^3 + x^2 + 2, x^4 + x^3 + x^2 + 3$ $x^4 + x^3 + x^2 + 2x + 2, x^4 + x^3 + x^2 + 3x + 3, x^4 + x^3 + 2x^2 + 3$ $x^4 + x^3 + 2x^2 + 2x + 2, x^4 + x^3 + 3x^2 + 2, x^4 + x^3 + 3x^2 + 3x + 3$ $x^4 + 2x^3 + x + 3, x^4 + 2x^3 + 2x + 2, x^4 + 2x^3 + 3x + 2, x^4 + 2x^3 + x^2 + 2x + 3$ $x^4 + 2x^3 + 2x^2 + 3, x^4 + 2x^3 + 3x^2 + 3, x^4 + 2x^3 + 3x^2 + 2x + 3$ $x^4 + 3x^3 + x + 2, x^4 + 3x^3 + 2x + 3, x^4 + 3x^3 + 3x + 3, x^4 + 3x^3 + x^2 + 3x + 2$ $x^4 + 3x^3 + 2x^2 + 2, x^4 + 3x^3 + 2x^2 + 3x + 2, x^4 + 3x^3 + 3x^2 + 2$

<표 3.5> GF(2²) 위에서 기약다항식들의 주기

3.3 확장체 위에서의 다항식의 인수분해

3.3.1 GF(2)에서의 인수분해

$f(x) = \sum_{i=0}^n a_i x^i$ 는 GF(2)위의 제곱 항이 없는 n 차 모닉다항식이라 하고, $f(x)$ 는 r 개의 서로 다른 기약다항식 $f_1(x), f_2(x), \dots, f_r(x)$ 의 곱이라 가정하자. 즉 $f(x) = f_1(x) \cdots f_r(x)$. 각 i ($1 \leq i \leq r$)에 대하여 $d_i = \deg(f_i(x))$ 라 하고 $p^{e_i} \mid d_i$ 라 하자. 그리고 $e = \max\{e_i \mid 1 \leq i \leq r\}$ 라 하자.

<예 3.6> 이진다항식 $f(x) = x^7 + x^5 + x^4 + x^2 + x + 1$

$$\begin{aligned} &= (x+1)(x^6 + x^5 + x^3 + x^2 + 1) \\ &= f_1(x)f_2(x) \end{aligned}$$

일 때 $d_1 = 1$, $d_2 = 6$, $e_1 = 0$, $e_2 = 1$ 이고 $e = 1$ 이다.

다항식을 인수분해하는 문제는 일반적으로 매우 어렵지만 소수 p 를 범으로 하는 다항식의 인수분해 문제는 조금 쉬워진다. 범 2에 관하여 차수 n 인 임의의 다항식을 인수분해하는 문제가 n 비트 정수를 인수분해하는 알려진 어떤 방법보다도 훨씬 쉽다. 다항식의 인수분해는 임의의 다항식을 인수분해하는 Berlekamp[2]의 구성적 알고리즘을 이용하면 된다.

3.3.2 GF(2)위에서의 Berlekamp의 다항식 인수분해 알고리즘

$f(x) = \sum_{i=0}^m a_i x^i$ 가 GF(q)위의 m 차 모닉다항식일 때, $g(x) = \gcd(f(x), f'(x))$ 를 계산한다. $g(x)$ 의 차수가 양수이면 $g(x) \mid f(x)$ 이므로 $g(x)$ 와 $f(x)/g(x)$ 에 이 알고리즘을 적용할 수 있다. 만일 $g(x) = 1$ 이면 $f(x)$ 는 중근을 갖지 않으므로 $f(x)$ 는 r 개의 서로 다른 기약다항식 $f_1(x), \dots, f_r(x)$ 의 곱으로 인수분해된다. 그러므로 서로 다른 기약다항식만을 인수로 갖는 다항식을 인수분해하는 문제만 생각하면 된다. 따라서 지금부터 $f(x)$ 는 서로 다른 기약 다항식만을 인수로 갖는 다항식이라 가정한다.

<정의 3.9> $m \times m$ 행렬 $Q = (Q_{i,j})$ 를 다음과 같이 정의한다.

$x^{iq} \bmod f(x) = Q_{i+1,1} + Q_{i+1,2}x + \dots + Q_{i+1,m}x^{m-1}$ 일 때, Q 의 i 행이 $(Q_{i+1,1}, Q_{i+1,2}, \dots, Q_{i+1,m})$ 인 행렬이다.

<예 3.7> 다항식 $f(x) = x^8 + x^7 + x^3 + x + 1$ 에 대해 8차 행렬 $Q = (Q_{i,j})_{8 \times 8}$ 를 구성하기 위하여 다음이 필요하다.

$$\begin{aligned} x^{2(1-1)} &= x^0 = 1 \\ x^{2(2-1)} &= x^2 \\ x^{2(3-1)} &= x^4 \\ x^{2(4-1)} &= x^6 \\ x^{2(5-1)} &= x^8 = 1 + x + x^3 + x^7 \\ x^{2(6-1)} &= x^{10} = 1 + x^4 + x^5 \\ x^{2(7-1)} &= x^{12} = x^2 + x^6 + x^7 \\ x^{2(8-1)} &= x^{14} = x + x^2 \end{aligned}$$

그러므로

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

<보조정리 3.4> GF(q)위의 $m-1$ 차 다항식 $g(x) = \sum_{i=0}^{m-1} g_i x^i$ 에 대하여

$$g(x)^q - g(x) \equiv 0 \pmod{f(x)} \Leftrightarrow (g_0, g_1, \dots, g_{m-1})(Q - I) = 0 \quad (3.8)$$

여기서 I 는 m 차 단위행렬이다.

(증명) 모든 $\beta \in \text{GF}(q)$ 에 대하여 $q\beta = 0$ 이므로

$$\begin{aligned} g(x)^q &= g(x^q) \\ &= \sum_{i=0}^{m-1} g_i x^{iq} \\ &= \sum_{i=0}^{m-1} g_i \left(\sum_{k=0}^{m-1} Q_{i+1, k+1} x^k \right) \pmod{f(x)} \\ &= \sum_{k=0}^{m-1} \left(\sum_{i=0}^{m-1} g_i Q_{i+1, k+1} \right) x^k \end{aligned}$$

여기서 $\sum_{i=0}^{m-1} g_i Q_{i+1, k+1}$ 은 행렬곱 $(g_0, g_1, \dots, g_{m-1})Q$ 의 $k+1$ 번째 성분

이다. 또한 g_i 는 행렬곱 $(g_0, g_1, \dots, g_{m-1})I$ 의 $k+1$ 번째 성분이다.
그러므로

$$\begin{aligned} g(x)^q - g(x) &= \sum_{k=0}^{m-1} \left(\left(\sum_{i=0}^{m-1} g_i Q_{i+1, k+1} \right) - g_k \right) x^k = 0 \\ \Leftrightarrow \text{모든 } k (0 \leq k \leq m-1) \text{에 대하여 } \left(\sum_{i=0}^{m-1} g_i Q_{i+1, k+1} \right) - g_k &= 0 \\ \Leftrightarrow (g_0, g_1, \dots, g_{m-1})(Q - I) &= 0 \end{aligned}$$

<정리 3.5> $f(x) = \sum_{i=0}^m a_i x^i$ 가 $GF(q)$ 위의 m 차 모닉다항식일 때,

$$f(x) = \prod_{s \in GF(q)} \gcd(f(x), g(x) - s) \quad (3.9)$$

이다. 이 때 $g(x) = \sum_{i=0}^{m-1} g_i x^i$ 는 $(g_0, g_1, \dots, g_{m-1})(Q - I) = 0$ 이다.

(증명) 보조정리 3.4에 의하여 $f(x) \mid (g(x)^q - g(x))$ 가 성립한다. 임의의 y 에 대하여 모든 $s \in F$ 가 $y^q - y = 0$ 의 근이므로 다음과 같은 식이 성립한다.

$$y^q - y = \prod_{s \in GF(q)} (y - s) \text{이다. 따라서 } g(x)^q - g(x) = \prod_{s \in GF(q)} (g(x) - s) \text{이다.}$$

$$f(x) \mid \prod_{s \in GF(q)} (g(x) - s) \text{이므로 } f(x) = \gcd(f(x), \prod_{s \in GF(q)} (g(x) - s)) \text{이다.}$$

$$f(x) = \gcd(f(x), \prod_{s \in GF(q)} (g(x) - s)) \mid \prod_{s \in GF(q)} \gcd(f(x), g(x) - s) \text{이다.}$$

한편 $\gcd(f(x), g(x) - s) \mid f(x)$ 이고 $GF(q)$ 의 서로 다른 원소 s, t 에 대하여 $g(x) - s, g(x) - t$ 는 서로소이다. 그러므로 $\gcd(f(x), g(x) - s)$ 와 $\gcd(f(x), g(x) - t)$ 는 서로소이므로 $\prod_{s \in GF(q)} \gcd(f(x), g(x) - s \mid f(x))$ 이다.

또한 $f(x)$ 가 모닉다항식이므로 $f(x) = \prod_{s \in GF(q)} \gcd(f(x), g(x) - s)$ 이다. $\square$

<정리 3.6> 중국인의 나머지 정리

영이 아닌 $GF(q)$ 위의 다항식 $u_1(x), \dots, u_r(x)$ 가 쌍마다 서로소라고 하자.

임의의 다항식 $p_1(x), \dots, p_r(x)$ 에 대해 연립일차합동식

$$\begin{aligned} v(x) &\equiv p_1(x) \pmod{u_1(x)} \\ &\vdots \\ v(x) &\equiv p_r(x) \pmod{u_r(x)} \end{aligned}$$

은 법 $u(x) \equiv u_1(x) \cdots u_r(x)$ 에 관하여 단 한 개의 해 $v(x)$ 를 가진다.

(증명) (유일성) $v(x)$ 와 $h(x)$ 가 연립일차합동식의 해라 가정하자.

$$\text{즉 } v(x) \equiv p_i(x) \pmod{u_i(x)} \quad (1 \leq i \leq r)$$

$$h(x) \equiv p_i(x) \pmod{u_i(x)} \quad (1 \leq i \leq r)$$

그러면 $v(x) - h(x) \equiv 0 \pmod{u_i(x)} \quad (1 \leq i \leq r)$ 이다. $u_1(x), \dots, u_r(x)$ 가 쌍마다 서로소이므로 $v(x) - h(x) \equiv 0 \pmod{u_1(x) \cdots u_r(x)}$ 이다. 따라서

$$v(x) \equiv h(x) \bmod u(x) = u_1(x) \cdots u_i(x).$$

(존재성) 각 $i = 1, \dots, r$ 에 대하여 $\hat{u}_i(x) = \frac{u(x)}{u_i(x)}$ 라 하자. $\hat{u}_i(x)$ 와 $u_i(x)$ 가 서로소이므로 $a_i(x)\hat{u}_i(x) + b_i(x)u_i(x) = 1$ 인 다항식 $a_i(x), b_i(x)$ 가 존재한다. 특히 $a_i(x)\hat{u}_i(x) \equiv 1 \bmod (u_i(x))$ 이므로 $a_i(x)$ 는 법 $u_i(x)$ 에 관한 $\hat{u}_i(x)$ 의 곱셈에 관한 역원이다. $v(x) = a_1(x)\hat{u}_1(x)p_1(x) + \cdots + a_r(x)\hat{u}_r(x)p_r(x)$ 라 하면 $j \neq i$ 일 때 $u_i(x) \mid \hat{u}_j(x)$ 이므로 $v(x) = a_i(x)\hat{u}_i(x)p_i(x) \equiv p_i(x) \bmod u_i(x)$ 이다. 따라서 $v(x)$ 가 주어진 연립일차함동식의 해이다. $\square$

<보조정리 3.7> $f(x)$ 의 서로 다른 기약 인수의 개수는 다음과 같다.

$$\dim \{(g_0, g_1, \dots, g_{m-1}) \mid (g_0, g_1, \dots, g_{m-1})(Q-I) = 0\} \quad (3.10)$$

즉 $Q-I$ 의 영 공간 $\{(g_0, g_1, \dots, g_{m-1}) \mid (g_0, g_1, \dots, g_{m-1})(Q-I) = 0\}$ 의 차원이 $f(x)$ 의 서로 다른 기약 인수의 개수이다.

(증명) $f(x)$ 가 r 개의 서로 다른 기약다항식 $f_1(x), \dots, f_r(x)$ 의 곱 $f(x) = f_1(x) \cdots f_r(x)$ 으로 인수분해된다고 하자. 보조정리 3.4에 의하여

$$(g_0, g_1, \dots, g_{m-1}) \in N(Q-I) \Leftrightarrow f(x) \mid (g(x)^q - g(x)) = \prod_{\alpha_i \in F} (g(x) - \alpha_i)$$

$f_i(x)$ 에 대하여 $f_i(x) \mid (g(x) - a_{j_i})$ 인 a_{j_i} 가 존재한다.

$$\Leftrightarrow \exists (a_{j_1}, \dots, a_{j_r}) \in GF(q)^r; g(x) \equiv a_{j_1} \bmod f_1(x)$$

$$\vdots$$

$$g(x) \equiv a_{j_r} \bmod f_r(x)$$

한편 임의의 원소 $a_1, \dots, a_n \in GF(q)$ 에 대하여 중국인의 나머지 정리로부터 연립일차합동식의 유일한 해 $g(x) \bmod f(x)$ 가 존재한다.

$$g(x) \equiv a_1 \bmod f_1(x)$$

$$\vdots$$

$$g(x) \equiv a_r \bmod f_r(x)$$

각 a_i 에 대하여 q 개 원소가 가능하므로 q^r 가지 방법으로 $a_1, \dots, a_r$ 을 선택할 수 있다. 그러므로 $g(x)^q - g(x) \equiv 0 \bmod f(x)$ 인 q^r 개의 원소 $g(x)$ 가 $GF(q)[x]$ 안에 있다. 그러므로 $Q-I$ 의 영공간에는 q^r 개 원소가 있다. 그러므로 $GF(q)$ 위의 $Q-I$ 의 영공간의 차원은 r 이다. 즉 $f(x)$ 의 서로 다른 기약인수의 개수이다. $\square$

$$\text{<예 3.8> } N(Q-I) = \{ (g_0, 0, 0, 0, 0, 0, 0, 0) \mid g_0 \in \{0, 1\} \}$$

$$= \{ (0, 0, 0, 0, 0, 0, 0, 0), (1, 0, 0, 0, 0, 0, 0, 0) \} \text{라 하면}$$

$N(Q-I)$ 는 1차원 공간이다. 그러므로 $f(x)$ 는 한 개의 기약인수를 갖는다. 그러므로 $f(x)$ 가 기약이거나 $f(x)$ 가 이진 1차 기약다항식의 8제곱이거나 $f(x)$ 가 이진 2차 기약다항식의 네제곱이거나 $f(x)$ 가 이진 4차 기약다항식의 제곱이다. 그러나 0과 1이 $f(x)$ 의 근이 아니므로 $f(x)$ 는 1차 인수를 갖지 않는다. 2차 기약다항식은 x^2+x+1 뿐이고, 이 다항식은 $f(x)$ 의 약수가 아니다.

3차 기약다항식은 $x^3 + x + 1, x^3 + x^2 + 1$ 뿐이고, 이 두 다항식은 $f(x)$ 의 약수가 아니다. 4차 기약다항식은 $x^4 + x^3 + 1, x^4 + x^3 + x^2 + x + 1, x^4 + x + 1$ 뿐이고 이 세 다항식은 $f(x)$ 의 약수가 아니다. 그러므로 $f(x)$ 가 기약다항식임을 알 수 있다.

<예 3.9> 이진다항식 $f(x) = x^7 + x^5 + x^4 + x^2 + x + 1$ 에 대하여 7차 행렬 $Q = (Q_{ij})_{7 \times 7}$ 를 구성하기 위하여 $x^0, x^2, x^4, \dots, x^{12}$ 를 구하면 다음과 같다.

$$x^0 = 1$$

$$x^2$$

$$x^4$$

$$x^6$$

$$x^8 = x + x^2 + x^3 + x^5 + x^6$$

$$x^{10} = x^3 + x^4 + x^5 + x^7 + x^8 = 1 + x^5 + x^6$$

$$x^{12} = x^2 + x^7 + x^8 = 1 + x^2 + x^3 + x^4 + x^6$$

그러므로 $Q - I = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 \end{pmatrix}$

$$(g_0, g_1, \dots, g_6) \in N(Q - I) \text{ 이라면}$$

$$\begin{aligned}
g_5 + g_6 &= 0 \\
g_1 + g_4 &= 0 \\
g_1 + g_2 + g_4 + g_6 &= 0 \\
g_3 + g_4 + g_6 &= 0 \\
g_2 + g_4 + g_6 &= 0 \\
g_4 &= 0 \\
g_3 + g_4 + g_5 &= 0
\end{aligned}$$

이 방정식들로부터 $0 = g_4 = g_1$, $g_2 = g_3 = g_5 = g_6$ 를 얻는다. 그러므로 $g(x) = x^6 + x^5 + x^3 + x^2 + g_0$ 이다.

<예 3.10> $g_0 = 1$ 인 $g(x) = x^6 + x^5 + x^3 + x^2 + 1$ 와 $f(x)$ 의 최대공약수를 구해보자.

$$g(x) = x^6 + x^5 + x^3 + x^2 + 1$$

$$f(x) = x^7 + x^5 + x^4 + x^2 + x + 1 = (x+1)(x^6 + x^5 + x^3 + x^2 + 1)$$

이므로 $\gcd(f(x), g(x)) = x^6 + x^5 + x^3 + x^2 + 1$ 이다.

$$\begin{aligned}
N(Q-I) &= \{(g_0, 0, g_2, g_2, 0, g_2, g_2) \mid g_0, g_2 \in \{0, 1\}\} \\
&= \{(0, 0, 0, 0, 0, 0, 0), (0, 0, 1, 1, 0, 1, 1), \\
&\quad (1, 0, 0, 0, 0, 0, 0), (1, 0, 1, 1, 0, 1, 1)\}
\end{aligned}$$

은 2차원 공간이다. 그래서 $f(x)$ 는 두 개의 서로 다른 기약인수를 갖는다. 그러므로 $h(x) = x^6 + x^5 + x^3 + x^2 + 1$ 이 기약이거나 $h(x)$ 가 이진 3차 기약다항식의 제곱이거나 $h(x)$ 가 이진 2차 기약다항식의 세 제곱이다.

$$\begin{aligned}
(x^2 + x + 1)^3 &= x^6 + x^2(x+1)(x^2 + x + 1) + (x+1)^3 \\
&= x^6 + (x^3 + x^2)(x^2 + x + 1) + x^3 + x(x+1) + 1 \\
&= x^6 + x^5 + x^4 + x^3 + x^4 + x^3 + x^2 + x^3 + x^2 + x + 1 \\
&= x^6 + x^5 + x^3 + x + 1 \neq h(x)
\end{aligned}$$

$(x^3 + x + 1)^2 = x^6 + x^2 + 1 \neq h(x)$, $(x^3 + x^2 + 1)^2 = x^6 + x^4 + 1 \neq h(x)$
 이므로 $h(x)$ 는 기약다항식이다. 따라서 $f(x)$ 는 두 기약다항식 $x + 1$, $x^6 + x^5 + x^3 + x^2 + 1$ 의 곱이다.

3.3.3 $\text{GF}(2^p)$ 위에서의 다항식 인수분해

$u(x)$ 는 계수가 집합 $\text{GF}(2^p) = \{0, 1, 2, \dots, 2^p - 1\}$ 의 원소인 n 차 모닉 다항식이라 하자. $u(x)$ 를 r 개의 서로 다른 기약 모닉다항식 $p_1(x), \dots, p_r(x)$ 에 대해 $u(x) = p_1(x)^{e_1} p_2(x)^{e_2} \cdots p_r(x)^{e_r}$ ($p_i(x) \in \text{GF}(2^p)[x]$)로 인수분해 하는 것이 목표이다. 첫 단계로, 지수들 $e_1, e_2, \dots, e_r$ 중 1보다 큰 것이 어느 것인가를 결정한다.

$u(x) = u_n(x)^n + \cdots + u_0 = v(x)^2 w(x)$ 인 경우 $\text{GF}(2^p)$ 에서

$$\begin{aligned}
u'(x) &= n u_n(x)^{n-1} + \cdots + u_1 \\
&= v(x)^2 w'(x) + 2v(x)v'(x)w(x) \\
&= v(x)^2 w'(x)
\end{aligned}$$

는 $v(x)$ 의 배수가 된다는 것을 알 수 있다. 즉 $u(x)$ 가 $v(x)$ 의 제곱을 인수로 갖는다면, $u(x)$ 와 $u'(x)$ 는 $v(x)$ 를 인수로 갖는다. 다시 말해, $u(x)$ 가 제곱인수를 갖는다면, $u(x)$ 와 $u'(x)$ 는 서로소가 아니다. 그러므로 $d(x) = \gcd(u(x), u'(x))$ 를 계산한다. $d(x)$ 에 따라 다음과 같은 세 가지로 나눌 수 있다.

(1) 만일 $d(x) = 1$ 이면 $u(x)$ 는 중근을 갖지 않으므로 $u(x)$ 는 r 개의 서로 다른 기약다항식 $u_1(x), \dots, u_r(x)$ 의 곱 $u(x) = u_1(x) \cdots u_r(x)$ 으로 인수 분해된다.

<예 3.11> $\text{GF}(2^4)$ 위에서

$$u(x) = x^4 + 7x^3 + x^2 + 11x + 2, \quad u'(x) = 4x^3 + 8x^2 + 2x + 11,$$

$$x^4 + 7x^3 + x^2 + 11x + 2 = (5x + 14)(4x^3 + 8x^2 + 2x + 11) + 12x^2 + 13x + 8$$

$$4x^3 + 8x^2 + 2x + 11 = (15x + 11)(12x^2 + 13x + 8) + 7x + 14$$

$12x^2 + 13x + 8 = (5x + 5)(7x + 4) + 9$ 이므로 $\gcd(u(x), u'(x)) = 1$ 이 고 따라서 $u(x)$ 와 $u'(x)$ 는 서로소이다.

(2) $d(x) \neq 1$ 이고 $d(x) \neq u(x)$ 이면, $d(x)$ 는 $u(x)$ 의 자명하지 않은 인수이다.

$d(x)$ 의 인수들과 $\frac{u(x)}{d(x)}$ 의 인수들에 이 알고리즘을 적용하여 $u(x)$ 의 인수들을 빠르게 구할 수 있다.

(3) $d(x) = u(x)$ 이면 $u'(x) = 0$ 이다. 이 경우는 $u(x)$ 의 항 x^k 들 중에서, k 가 2^p 의 배수인 경우만 x^k 의 계수가 0이 아니고, 2^p 의 배수가 아닌 경우는 0일 때이다.

<예 3.12> $GF(2^4)$ 위에서 계수가 $\{0, 1, 2, \dots, 2^4 - 1\}$ 의 원소인 다항식

$$u(x) = u_2 x^{2 \cdot 2^4} + u_1 x^{2^4} + u_0, \text{ 여기서 } u_i \in \{0, 1, 2, \dots, 2^4 - 1\} - \{0\} \text{ 일 때,}$$

$$u'(x) = 32u_2 x^{31} + 16u_1 x^{15} = 0 \text{ 이다.}$$

$$\begin{aligned} u(x) &= u_2 x^{32} + u_1 x^{16} + u_0 \\ &= u_2^{16} x^{32} + u_1^{16} x^{16} + u_0^{16} \\ &= u_2 (x^2)^{16} + u_1^{16} x^{16} + u_0^{16} \\ &= (u_2 x^2)^{16} + (u_1 x)^{16} + u_0^{16} \\ &= (u_2 x^2 + u_1 x + u_0)^{16} \\ &= v(x)^{2^4} \end{aligned}$$

여기서 $v(x) = u_2 x^2 + u_1 x + u_0$ 이다.

<예 3.13> $GF(2^p)$ 위에서 계수가 $\{0, 1, 2, \dots, 2^p - 1\}$ 의 원소인 다항식

$$u(x) = u_k x^{2^p \cdot k} + u_{k-1} x^{2^p \cdot (k-1)} + \dots + u_1 x^{2^p} + u_0 \text{ 인 경우}$$

$$\begin{aligned} u(x) &= u_k x^{2^p \cdot k} + u_{k-1} x^{2^p \cdot (k-1)} + \dots + u_1 x^{2^p} + u_0 \\ &= u_k (x^{2^p})^k + u_{k-1} (x^{2^p})^{k-1} + \dots + u_1 x^{2^p} + u_0 \\ &= u_k^{2^p} (x^{2^p})^k + u_{k-1}^{2^p} (x^{2^p})^{k-1} + \dots + u_1^{2^p} x^{2^p} + u_0^{2^p} \\ &= (u_k x^k)^{2^p} + (u_{k-1} x^{k-1})^{2^p} + \dots + (u_1 x)^{2^p} + u_0^{2^p} \\ &= (u_k x^k + u_{k-1} x^{k-1} + \dots + u_1 x + u_0)^{2^p} \\ &= v(x)^{2^p} \end{aligned}$$

여기서 $v(x) = v_u x^k + u_{k-1} x^{k-1} + \cdots + u_1 x + u_0$. 이 경우 $v(x)$ 를 기약 인수들로 인수분해한 다음, 각 기약 인수를 2^p 배하면 $u(x)$ 의 인수분해를 얻는다.

$$\text{GF}(2) \text{에서 } u(x) = x^4 + x^2 + 1 = (x^2 + x + 1)^2 = v(x)^2$$

$$u(x) = x^8 + x^4 + 1 = (x^2 + x + 1)^{2^2} = v(x)^{2^2} \text{ 이다.}$$

그러므로 서로 다른 기약다항식만을 인수로 갖는 다항식을 인수분해하는 문제만 생각한다. 따라서 $u(x)$ 는 서로 다른 기약다항식만을 인수로 갖는 다항식이라 가정한다. n 차 다항식 $u(x)$ 는 r 개의 서로 다른 기약다항식 $u_1(x), \cdots, u_r(x)$ 의 곱 $u(x) = u_1(x) \cdots u_r(x) = \prod_{i=1}^r u_i(x)$ 이라 가정한다.

그리고 $Q = (Q_{ij})_{n \times n}$ 는 i 행이 $x^{2^p(i-1)} \bmod u(x)$ 인 $\text{GF}(2^p)$ 위의 n 차 행렬이라 하자.

<정의 3.10> 각 $i = 0, \cdots, n-1$ 에 대하여

$$x^{i \cdot 2^p} \bmod u(x) = Q_{i+1,1} + Q_{i+1,2}x + \cdots + Q_{i+1,n}x^{n-1} \quad (3.11)$$

이 $i+1$ 행인 행렬을 $Q = (Q_{ij})$ 라 정의한다.

<예 3.14> $\text{GF}(2^4)$ 위에서 $u(x) = x^8 + x^6 + 10x^4 + 10x^3 + 8x^2 + 2x + 8$ 를 인수분해해 보자. $u(x) = x^8 + x^6 + 10x^4 + 10x^3 + 8x^2 + 2x + 8$ 는 제곱인수를 갖지 않는다.

8×8 행렬 Q 를 구성하기 위하여 $x^{q(i-1)}$ ($i = 1, 2, \dots, 8, q = 2^4$) 을 구한다.

$$x^0 = 1$$

$$x^{2^4},$$

$$x^{2^4 \cdot 2},$$

$$x^{2^4 \cdot 3},$$

$$x^{2^4 \cdot 4},$$

$$x^{2^4 \cdot 5},$$

$$x^{2^4 \cdot 6},$$

$$x^{2^4 \cdot 7},$$

$$x^8 = x^6 + 10x^4 + 10x^3 + 8x^2 + 2x + 8$$

$$x^9 = x^7 + 10x^5 + 10x^4 + 8x^3 + 2x^2 + 8x$$

$$x^{10} = 11x^6 + 10x^5 + 2x^4 + 8x^3 + 2x + 8$$

$$x^{11} = 11x^7 + 10x^6 + 22x^5 + 8x^4 + 2x^2 + 8x$$

$$x^{12} = 10x^7 + 9x^6 + 8x^5 + 6x^4 + 4x^3 + 7x^2 + 9x + 15$$

$$x^{13} = 9x^7 + 2x^6 + 6x^5 + 8x^4 + 11x^3 + 14x^2 + 4x + 7$$

$$x^{14} = 2x^7 + 15x^6 + 8x^5 + 6x^4 + 3x^3 + 7x^2 + 9x + 3$$

$$x^{15} = 15x^7 + 10x^6 + 6x^5 + 8x^4 + 12x^3 + 5x^2 + 4x + 12$$

$$x^{16} = 10x^7 + 9x^6 + 8x^5 + 2x^4 + 11x^3 + 9x^2 + 15x + 13$$

$$x^{32} = (x^{16})^2 = (10x^7 + 9x^6 + 8x^5 + 2x^4 + 11x^3 + 9x^2 + 15x + 13)$$

$$= 10x^7 + 14x^6 + 8x^5 + 8x^4 + 4x^3 + 10x^2 + 14x + 2$$

$$Q = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 13 & 15 & 9 & 11 & 2 & 8 & 9 & 10 \\ 2 & 14 & 10 & 4 & 8 & 8 & 14 & 10 \\ 9 & 9 & 5 & 9 & 14 & 1 & 5 & 5 \\ 15 & 15 & 10 & 5 & 10 & 12 & 13 & 11 \\ 7 & 2 & 2 & 3 & 7 & 2 & 15 & 13 \\ 6 & 12 & 9 & 14 & 11 & 10 & 7 & 2 \\ 0 & 3 & 6 & 13 & 5 & 10 & 8 & 3 \end{pmatrix} \begin{pmatrix} x^{2^4 \times 0} \\ x^{2^4 \times 1} \\ x^{2^4 \times 2} \\ x^{2^4 \times 3} \\ x^{2^4 \times 4} \\ x^{2^4 \times 5} \\ x^{2^4 \times 6} \\ x^{2^4 \times 7} \end{pmatrix}$$

<보조정리 3.8> GF(2^p) 위의 n-1차 이하인 다항식 $g(x) = \sum_{i=0}^{n-1} g_i x^i$ 에

대하여 I가 n차 단위행렬일 때, 다음 식이 성립한다.

$$g(x)^{2^p} - g(x) \equiv 0 \pmod{u(x)} \Leftrightarrow (g_0, g_1, \dots, g_{n-1})(Q-I) = 0 \quad (3.12)$$

(증명) 모든 $\beta \in \text{GF}(2^p)$ 에 대하여 $2^p \beta = 0$ 이므로

$$\begin{aligned} g(x)^{2^p} &= g(x^{2^p}) \\ &= \sum_{i=0}^{n-1} g_i x^{i 2^p} \\ &= \sum_{i=0}^{n-1} g_i \left(\sum_{k=0}^{n-1} Q_{i+1, k+1} x^k \right) \pmod{u(x)} \\ &= \sum_{k=0}^{n-1} \left(\sum_{i=0}^{n-1} g_i Q_{i+1, k+1} \right) x^k \end{aligned}$$

여기서 $\sum_{i=0}^{n-1} g_i Q_{i+1, k+1}$ 은 행렬곱 $(g_0, g_1, \dots, g_{m-1})Q$ 의 k+1번째 성분이다.

또한 g_i 는 행렬곱 $(g_0, g_1, \dots, g_{m-1})I$ 의 $k+1$ 번째 성분이다.

$$g(x)^{2^p} - g(x) = \sum_{k=0}^{n-1} ((\sum_{i=0}^{n-1} g_i Q_{i+1, k+1}) - g_k) x^k = 0$$

$$\Leftrightarrow \text{모든 } k(0 \leq k \leq n-1) \text{에 대하여 } (\sum_{i=0}^{n-1} g_i Q_{i+1, k+1}) - g_k = 0$$

$$\Leftrightarrow (g_0, g_1, \dots, g_{n-1})(Q-I) = 0 \quad \square$$

<보조정리 3.9> $u(x) = \sum_{i=0}^n a_i x^i$ 가 $GF(2^p)$ 위의 n 차 모닉다항식일 때,

$$u(x) = \prod_{s \in GF(2^p)} [\gcd(u(x), g(x) - s)] \quad (3.13)$$

$$g(x) = \sum_{i=0}^{n-1} g_i x^i \text{는 } (g_0, g_1, \dots, g_{n-1})(Q-I) = 0 \text{을 만족하는 다항식이다.}$$

(증명) 보조정리 3.8에 의하여 $u(x) \mid (g(x)^{2^p} - g(x))$ 가 성립한다. 임의의 y 에 대하여 모든 $s \in F$ 가 $y^{2^p} - y = 0$ 의 근이므로 $y^{2^p} - y = \prod_{s \in GF(2^p)} (y - s)$ 이다.

따라서 $g(x)^{2^p} - g(x) = \prod_{s \in GF(2^p)} (g(x) - s)$ 이다. $u(x) \mid \prod_{s \in GF(2^p)} (g(x) - s)$ 이므로

$$u(x) = \gcd(u(x), \prod_{s \in GF(2^p)} (g(x) - s)) \text{이다.}$$

$$\text{또한 } u(x) = \gcd(u(x), \prod_{s \in GF(2^p)} (g(x) - s)) \mid \prod_{s \in GF(2^p)} \gcd(u(x), g(x) - s) \text{이다.}$$

한편 $\gcd(u(x), g(x) - s) \mid u(x)$ 이고 $GF(2^p)$ 의 서로 다른 원소 s, t 에

대하여 $g(x)-s, g(x)-t$ 는 서로소이다. 그러므로 $\gcd(u(x), g(x)-s)$ 와 $\gcd(u(x), g(x)-t)$ 는 서로소이므로 $\prod_{s \in GF(2^p)} \gcd(u(x), g(x)-s) \mid u(x)$ 이다.

$u(x)$ 가 모닉다항식이므로 $u(x) = \prod_{s \in GF(2^p)} \gcd(u(x), g(x)-s)$ 이다. $\square$

<정리 3.10> $u(x)$ 의 서로 다른 기약 인수들의 개수는 다음과 같다.

$$\dim \{(g_0, g_1, \dots, g_{m-1}) \mid (g_0, g_1, \dots, g_{m-1})(Q-I) = 0\} \quad (3.14)$$

이다. 즉 $Q-I$ 의 영공간 $\{(g_0, g_1, \dots, g_{m-1}) \mid (g_0, g_1, \dots, g_{m-1})(Q-I) = 0\}$ 의 차원이 $u(x)$ 의 서로 다른 기약인수의 개수이다.

(증명) $u(x)$ 가 r 개의 서로 다른 기약다항식 $u_1(x), \dots, u_r(x)$ 의 곱으로 다음과 같이 $u(x) = u_1(x) \dots u_r(x)$ 으로 인수분해 된다고 하자.

$$(g_0, g_1, \dots, g_{m-1}) \in N(Q-I)$$

$$\Leftrightarrow u(x) \mid (g(x)^q - g(x)) = \prod_{a_i \in GF(2^p)} (g(x) - a_i)$$

$$\Leftrightarrow i = 1, 2, \dots, r \text{인 모든 } u_i(x) \text{에 대해}$$

$$u_i(x) \mid (g(x) - a_{j_i}) \text{인 } a_{j_i} \in GF(2^p) \text{가 존재한다.}$$

$$\Leftrightarrow \text{즉 } (a_{j_1}, \dots, a_{j_r}) \in GF(2^p)^r \text{가 존재한다.}$$

$$g(x) \equiv a_{j_1} \bmod u_1(x)$$

$$\vdots$$

$$g(x) \equiv a_{j_r} \bmod u_r(x)$$

한편 임의의 원소 $a_1, \dots, a_n \in \text{GF}(2^p)$ 에 대하여 중국인의 나머지 정리로부터 연립일차합동식의 유일한 해 $g(x) \bmod u(x)$ 가 존재한다.

$$g(x) \equiv a_1 \bmod u_1(x)$$

$$\vdots$$

$$g(x) \equiv a_r \bmod u_r(x)$$

각 a_i 에 대하여 2^p 개 원소가 가능하므로 $(2^p)^r$ 가지 방법으로 $a_1, \dots, a_r$ 을 선택할 수 있다. 그러므로 $g(x)^{2^p} - g(x) = 0 \bmod u(x)$ 인 $(2^p)^r$ 개 원소 $g(x)$ 가 $\text{GF}(2^p)[x]$ 안에 있다. 그러므로 $Q-I$ 의 영공간에는 $(2^p)^r$ 개 원소가 있다. 그러므로 $\text{GF}(2^p)$ 위의 $Q-I$ 의 영공간의 차원은 r 이다. 즉 $u(x)$ 의 서로 다른 기약 인수의 개수이다. $\square$

단계 1 : $d(x)$ 를 계산한다.

$d(x) \neq 1$ 이면 $u(x)$ 를 제곱항이 없는 형태로 만든다.

단계 2 : 식 3.8에서 정의한 행렬 Q 를 구성한다.

단계 3 : $Q-I$ 의 영공간을 구한다.

영공간으로부터 각 $j(1 \leq j \leq r)$ 에 대하여 $v^{[j]}(Q-I) = (0, \dots, 0)$ 인 r 개의 일차독립인 벡터 $v^{[1]}, \dots, v^{[r]}$ 을 구한다. $v^{[1]}$ 은 자명한 해인 $(1, 0, \dots, 0)$ 으로 둔다. 이 때 $Q-I$ 의 영공간의 차원은 $u(x)$ 의 기약인수의 개수이다.

단계 4 : 각 $s(0 \leq s < 2^p - 1)$ 에 대하여 $\gcd(u(x), v^{[2]}(x) - s)$ 을 계산한다.

여기서 $v^{[2]}(x)$ 는 $v^{[2]}$ 에 의해 표현된 다항식이다.

$\gcd(u(x), v^{[2]}(x) - s)$ 는 $u(x)$ 의 자명하지 않은 인수이다.

$v^{[2]}(x)$ 는 0이 아니고, $v^{[2]}(x) - s$ 의 차수는 $u(x)$ 의 차수보다 작고, $v(x)$ 가 $v(x)^q \equiv v(x) \pmod{u(x)}$, $\deg v(x) < \deg u(x)$ 를 만족할 때마다

$u(x) = \prod_{0 \leq s < 2^p - 1} \gcd(v(x) - s, u(x))$ 이 성립하기 때문이다.

$v^{[2]}(x)$ 를 이용하여 $u(x)$ 를 r 개의 인수로 분해하지 못했다면

$v^{[k]}(x) (k = 3, 4, \dots)$ 에 대하여, r 개의 인수를 찾을 때까지

$\gcd(v^{[k]}(x) - s, w(x))$ 을 계산하여 구할 수 있다. 여기서 $w(x)$ 는 $u(x)$ 의 이미 밝혀진 인수로 나눈 다항식이다.

<예 3.15>

$$Q = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 13 & 15 & 9 & 11 & 2 & 8 & 9 & 10 \\ 2 & 14 & 10 & 4 & 8 & 8 & 14 & 10 \\ 9 & 9 & 5 & 9 & 14 & 1 & 5 & 5 \\ 15 & 15 & 10 & 5 & 10 & 12 & 13 & 11 \\ 7 & 2 & 2 & 3 & 7 & 2 & 15 & 13 \\ 6 & 12 & 9 & 14 & 11 & 10 & 7 & 2 \\ 0 & 3 & 6 & 13 & 5 & 10 & 8 & 3 \end{pmatrix}$$

$$Q - I = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 13 & 14 & 9 & 11 & 2 & 8 & 9 & 10 \\ 2 & 14 & 11 & 4 & 8 & 8 & 14 & 10 \\ 9 & 9 & 5 & 8 & 14 & 1 & 5 & 5 \\ 15 & 15 & 10 & 5 & 11 & 12 & 13 & 11 \\ 7 & 2 & 2 & 3 & 7 & 3 & 15 & 13 \\ 6 & 12 & 9 & 14 & 11 & 10 & 6 & 2 \\ 0 & 3 & 6 & 13 & 5 & 10 & 8 & 2 \end{pmatrix}$$

$Q - I$ 의 영공간의 일차독립인 벡터는 $(1, 0, 0, 0, 0, 0, 0, 0)$, $(0, 14, 11, 1, 7, 15, 1, 1)$, $(0, 9, 11, 1, 9, 11, 0, 1)$ 이다. 그러므로 $u(x)$ 는 3개의 기약인수를 갖는다.

$$v^{[1]} = (1, 0, 0, 0, 0, 0, 0, 0)$$

$$v^{[2]} = (0, 14, 11, 1, 7, 15, 1, 0)$$

$$v^{[3]} = (0, 9, 11, 1, 9, 11, 0, 1)$$

$\gcd(u(x), v^{[2]}(x) - s) \ (0 \leq s \leq 2^4 - 1)$ 를 계산하면 다음과 같다.

$$v^{[2]}(x) - 4 = (0, 0, 0, 0, 7, 15, 1, 0)$$

$$v^{[3]}(x) - 2 = (0, 0, 0, 0, 0, 0, 1, 12)$$

$$v^{[3]}(x) - 7 = (0, 0, 0, 0, 1, 14, 12, 4)$$

그러므로 주어진 다항식의 인수분해는 다음과 같다.

$$x^4 + 2x^3 + 2x^2 + 7x + 3$$

$$x + 12$$

$$x^3 + 14x^2 + 12x + 4$$

$$x^8 + x^6 + 10x^4 + 10x^3 + 8x^2 + 2x + 8$$

$$= (x^4 + 2x^3 + 2x^2 + 7x + 3)(x + 12)(x^3 + 14x^2 + 12x + 4)$$

3.3.4 시간복잡도

$GF(2^p)$ 에서 인수분해의 시간복잡도는 $O(n^3 + m rn^2)$ 이다. 여기서 $m = 2^p$, n 은 다항식의 차수이다. 전형적으로 r 은 $\ln n$ 이다. 단계 1에서 $O(n^2)$, 단계 2에서 $O(mn^2)$, 영 공간 알고리즘에서 일반적으로 $O(n^3)$, $\gcd(f(x), g(x))$ 를 계산하는 유클리드 알고리즘에서 $O(\deg(f)\deg(g))$, 단계 4에서 기껏해야 $O(mrn^2)$ 이다. 그러므로 전체 시간복잡도는 $O(n^3 + m rn^2)$ 이다.

4. $GF(2^p)$ SACA의 특성분석

4.1 $GF(2^p)$ SACA

<정의 4.1> 선형 n 셀 $GF(2^p)$ SACA : 선형 n 셀 $GF(2^p)$ SACA $\mathbb{C}$ 는 상태 0만 유일한 attractor로 $\mathbb{C}$ 의 상태전이 그래프는 깊이가 n 인 한 개의 트리 구조로 구성된다.

선형 n 셀 $GF(2^p)$ SACA $\mathbb{C}$ 의 모든 상태의 개수는 2^{np} 이고, 임의의 도달 가능한 상태의 직전자의 수는 2^p 이다. 다음 정리는 $\mathbb{C}$ 의 전이행렬 T 의 중요한 성질이다.

<정리 4.1> 선형 n 셀 $GF(2^p)$ SACA $\mathbb{C}$ 의 전이행렬을 T 라 하면 다음이 성립한다.

- (1) $rank(T) = n - 1$
- (2) $rank(T + I) = n$
- (3) T 의 특성다항식과 최소다항식은 x^n 이다.

(증명) (1) 상태 0의 직전자의 집합은 $\{x \mid Tx = 0\}$ 이다. $\mathbb{C}$ 의 상태전이 그래프에서 상태 0의 직전자의 수는 $|\{x \mid Tx = 0\}| = 2^p$ 이어야 하므로 행렬 방정식 $Tx = 0$ 에서 자유변수는 1개이다. 따라서 $\dim N(T) = 1$ 이므로 $rank(T) = n - 1$ 이다.

(2) $\mathbb{C}$ 의 상태전이그래프에서 $\{x \mid Tx = x\} = \{x \mid (T + I)x = 0\} = \{0\}$ 이다. 또한 $\dim N(T + I) = 0$ 이므로 $rank(T + I) = n$ 이다.

(3) $\mathbb{C}$ 의 상태전이 그래프의 깊이는 n 이므로 모든 상태 y 에 대하여 $T^n y = 0$ 이어야 한다. 따라서 $T^n = 0$ 을 만족해야 하므로 T 의 최소다항식은 $m(x) = x^n$ 이다. 그런데 T 의 특성다항식은 n 차 다항식이다. 그러므로 T 의 특성다항식과 최소다항식은 모두 x^n 이다.

<예 4.1> 전이행렬이 $T = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 3 \end{pmatrix}$ 인 선형 3셀 GF(2^2) CA에 대하여 다음

이 성립한다.

(1) $\text{rank}(T) = 2$

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

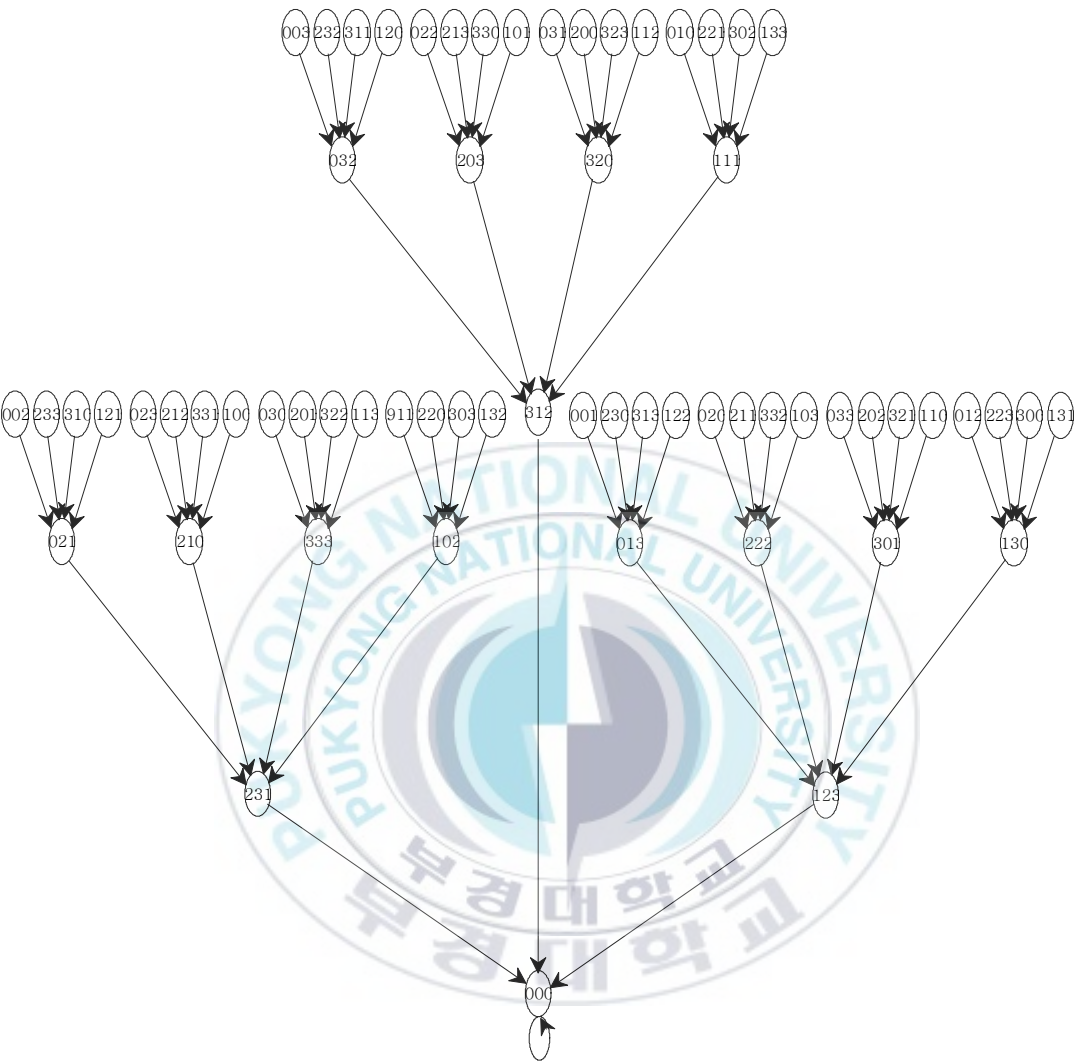
(2) $\text{rank}(T+I) = 3$

$$T+I = \begin{pmatrix} 3 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 2 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 2 & 0 \\ 0 & 2 & 1 \\ 0 & 1 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 3 \\ 0 & 1 & 2 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix}$$

(3) T 의 특성다항식 $C(x) = x^3$ 과 최소다항식은 같다.

$$C(x) = \begin{vmatrix} 2+x & 1 & 0 \\ 1 & x+1 & 1 \\ 0 & 1 & 3+x \end{vmatrix} = x^3$$

그림 4.1은 예 4.1의 전이행렬에 대응하는 $GF(2^2)$ 선형 SACA의 상태전이 그래프이다.



<그림 4.1> 3셀 $GF(2^2)$ SACA의 상태전이 그래프

<정리 4.2> 선형 $GF(2^p)$ SACA $\mathbb{C}$ 에서 임의의 도달 가능한 상태의 서로 다른 두 직전자의 합은 상태 0의 0이 아닌 직전자 중의 하나이다.

(증명) 도달 가능한 상태 x 의 서로 다른 직전자 y 와 z 에 대하여 $Ty = Tz = x$ 이다. $T(y+z) = 0$ 이므로 $y+z$ 는 0의 직전자이다. $y \neq z$ 이므로 $y+z \neq 0$ 이다. 따라서 $y+z$ 는 0이 아닌 0의 직전자 중의 하나이다.

그림 4.1에서 상태 $\langle 11 \rangle$ 의 직전자 중 $\langle 30 \rangle$ 과 $\langle 12 \rangle$ 의 합은 상태 0의 직전자 중 $\langle 22 \rangle$ 과 같다. $\mathbb{C}$ 의 한 임의의 도달 가능한 상태에서 가장 가까운 순환상태 k 로 가는 상태변화를 k -트리의 경로라 한다. 그림 4.1에서 $002 \rightarrow 021 \rightarrow 231 \rightarrow 000$ 은 0-트리의 경로 중 하나이다.

<정리 4.3> 선형 $GF(2^p)$ SACA $\mathbb{C}$ 에서 하나의 0-트리의 경로를 알 때 이를 기본경로로 하여 0-트리의 나머지 부분을 기본경로에 놓인 상태들의 합으로 구성할 수 있다.

(증명) 상태 x 가 $\mathbb{C}$ 의 상태전이 그래프에서 한 도달 불가능한 상태라 하고 x 로부터 T 를 연속하여 적용하여 0-트리의 한 기본경로 $x \rightarrow Tx \rightarrow \dots \rightarrow T^{n-l-1}x (= 0)$ 를 얻을 수 있다. $S_{l,0} = T^{n-l-1}x$ 라 하자. $\mathbb{C}$ 의 상태전이 그래프에서 레벨 l 의 k 번째 상태 $S_{l,k}$ ($k=0, 1, 2, \dots, n-l$)를 다음과 같이 두자.

$$S_{l,k} = (b_l + 1)S_{l,0} + \sum_{i=1}^{l-1} b_i S_{i,0} \quad (4.1)$$

여기서 b_i 는 k 를 2^p 진법으로 표현했을 때 각 자리의 수이다. 즉,

$k = b_l b_{l-1} \cdots b_{1_{(2^p)}} \ (0 \leq k \leq (2^p)^{l-1} (2^p) - 1)$ 이다. 그러면 레벨 1부터 레벨 n 까지 상태 수는 다음과 같다.

$$\sum_{l=1}^n (2^p)^{l-1} (2^p - 1) = (2^p)^n - 1 \quad (4.2)$$

Attractor를 포함한 $\mathbb{C}$ 의 상태전이 그래프의 모든 상태 수는 $(2^p)^n - 1 + 1 = 2^m$ 이다. 또한 다음이 성립한다.

$$\begin{aligned} TS_{l,k} &= T((b_l + 1)S_{l,0} + \sum_{i=1}^{l-1} b_i S_{i,0}) \\ &= (b_l + 1)TS_{l,0} + \sum_{i=1}^{l-1} b_i TS_{i,0} \\ &= (b_l + 1)S_{l-1,0} + b_{l-1}S_{l-2,0} + \cdots + b_2S_{l,0} + b_1S_{0,0} \end{aligned} \quad (4.3)$$

식 (4.3)에서 $S_{0,0} = 0$ 이고 상태전이 그래프에서 레벨이 하나 낮아질 때마다 상태의 수는 2^p 개씩 작아지므로 $k' = \left\lfloor \frac{k}{2^p} \right\rfloor$ 라 두면 $k = b_l b_{l-1} \cdots b_{1_{(2^p)}}$, $k' = b_l b_{l-1} \cdots b_{2_{(2^p)}} = b'_{l-1} \cdots b'_{1_{(2^p)}}$ 이 된다. 따라서 식 (4.3)은 다음과 같다.

$$TS_{l,k} = (b'_{l-1} + 1)S_{l-1,0} + \sum_{i=1}^{l-2} b'_i S_{i,0} = S_{l-1,k'} \quad (4.4)$$

그림 4.1의 $002 \rightarrow 021 \rightarrow 231 \rightarrow 000$ 를 0-트리의 기본경로라 하면 $S_{3,9} = \langle 201 \rangle$ 은 $1 \langle 002 \rangle + 2 \langle 021 \rangle + 1 \langle 231 \rangle = \langle 201 \rangle$ 을 만족한다.

4.2 여원 GF(2^p) SACA

<정의 4.2> 여원벡터 : 각 셀에 적용되는 상태전이 규칙이 XOR 논리와 XNOR 논리의 조합으로 이루어지는 여원 CA의 다음 상태를 나타내는 함수는 $y = \overline{T}x = Tx + F$ 이다. 여기서 F 를 여원벡터라 한다.

예 4.1의 전이행렬 T 가 다음과 같은 3-셀 GF(2²) HCA를 생각해보자.

$$T = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 3 \end{pmatrix} \quad (4.5)$$

이때, 여원벡터를 $F = [123]^t$ 라 하면 주어진 3-셀 GF(2²) HCA의 구조는 다음과 같다. 현재 상태가 $x = [222]^t$ 일 때, 다음 상태 y 는 $y = Tx + F$ 에 의해 구한다. GF(2²)위에서의 곱셈과 덧셈표를 이용하여 y 를 구하면 다음과 같다.

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

현재 상태 x 에서 k 단계 후의 다음 상태는 다음과 같다.

$$\overline{T^k}x = T^kx + (T^{k-1} + \dots + T + I)F \quad (4.6)$$

GF(2^p)위의 선형 n 셀 SACA $\mathbb{C}$ 에서 여원벡터 F 가 $\mathbb{C}$ 의 상태전이 그래프에서 레벨 l 에 있는 상태라 하면 $\mathbb{C}$ 에 대응하는 여원 CA 역시 SACA $\mathbb{C}'$ 가

된다. 여원벡터의 위치가 SACA의 상태전이 그래프에서 레벨 l 에 있을 때, 여원 SACA $\mathbb{C}'$ 의 상태전이 그래프는 표 4.1과 같은 규칙으로 재배열된다.

GF(2^p)위에서 선형 SACA	GF(2^p)위에서 여원 SACA
레벨 l 보다 상위 레벨에 있는 상태	레벨이 변하지 않는다
레벨 l 보다 하위 레벨에 있는 상태	레벨 l 에 재배열된다
상태 F (여원벡터)	레벨 $l-1$ 에 놓인다
레벨 l 에 있는 상태	레벨 l 이하에 놓인다

<표 4.1> 선형 SACA와 여원 SACA의 상태배열 관계

<정리 4.4> $\mathbb{C}$ 에서 하나의 0-트리의 경로를 알고 주어진 여원벡터에 의해 $\mathbb{C}$ 로부터 유도되는 $\mathbb{C}'$ 의 기본경로를 알면 이 두 경로에 의해 $\mathbb{C}'$ 의 상태전이 그래프를 구성할 수 있다.

(증명) $S_{n,0} \rightarrow S_{n-1,0} \rightarrow \dots \rightarrow S_{0,0}(=0)$ 을 $\mathbb{C}$ 의 기본경로라 하고 $\mathbb{C}'$ 의 기본경로를 $\overline{S_{n,0}} \rightarrow \overline{S_{n-1,0}} \rightarrow \dots \rightarrow \overline{S_{0,0}}$ 라 하자. $\mathbb{C}'$ 의 상태전이 그래프에서 레벨 l 의 k 번째 상태 $\overline{S_{l,k}}$ ($k=1, 2, \dots, n-1$)를 다음과 같이 정의하자.

$$\overline{S_{l,k}} = \overline{S_{l-1,0}} + (b_l + 1)S_{l,0} + \sum_{i=1}^{l-1} b_i S_{i,0} \quad (4.7)$$

b_i 는 k 를 2^p 진법으로 표현했을 때 각 자리의 수이다. 즉 $k = b_l b_{l-1} \dots b_{1(2^p)}$ ($0 \leq k \leq (2^p)^{l-1}(2^p) - 1$)이다. 그러면 레벨 1부터 레벨 n 까지 상태 수는 다음과 같다.

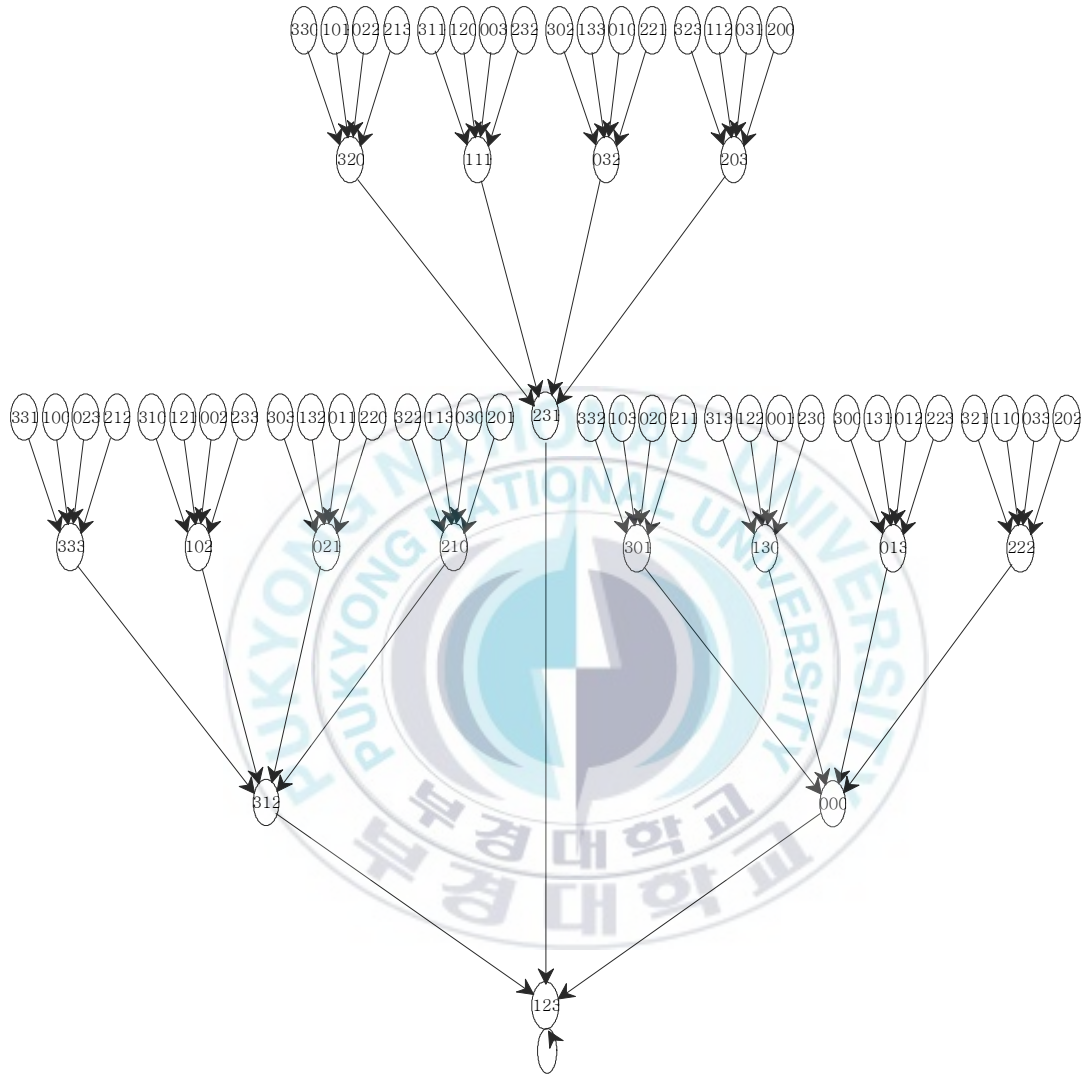
$$\sum_{l=1}^n (2^p)^{l-1} (2^p - 1) = (2^p)^n - 1 \quad (4.8)$$

Attractor를 포함한 $\mathbb{C}'$ 의 상태전이 그래프의 모든 상태 수는 $(2^p)^n - 1 + 1 = 2^{pn}$ 이다. 또한 다음이 성립한다.

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

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

그림 4.2은 예 4.1의 전이행렬에 대응하는 여원 $GF(2^2)$ SACA의 상태전이 그래프이다.



<그림 4.2> 3셀 여원 $GF(2^2)$ SACA의 상태전이 그래프

4.3 GF(2^p) SACA 트리구성

정리 4.3 과 정리 4.4 에 의하여 다음과 같은 GF(2^p) 위에서 SACA 상태전이 그래프 트리구성 알고리즘을 제안한다.

Step 1. 전이행렬 T 에 대하여 $T^n x = 0$ 이고 $T^{n-1}x \neq 0$ 인 0-트리의 도달 불가능상태 x 를 찾는다.

Step 2. x 를 시작으로 하는 0-트리의 기본경로를 찾는다.

$$x(S_{n,0}) \rightarrow Tx(S_{n-1,0}) \rightarrow \cdots \rightarrow 0$$

Step 3. $S_{l,k} = (b_l + 1)S_{l,0} + \sum_{i=1}^{l-1} b_i S_{i,0}$ 에 의하여 0-트리를 구성한다.

Step 4. 여원 SACA의 기본경로를 구한다. 여원벡터 F 가 도달 불가능한 상태면 $0(\bar{S}_{n,0}) \rightarrow \bar{T}0(\bar{S}_{n-1,0}) \rightarrow \cdots \rightarrow \bar{T}^n 0$ 가 여원 SACA의 기본경로가 되고 여원벡터 F 가 0이 아닌 도달가능한 상태면 Step 1에서 구한 선형 SACA의 도달 불가능한 상태 x 에 대해

$$x(\bar{S}_{n,0}) \rightarrow \bar{T}x(\bar{S}_{n-1,0}) \rightarrow \cdots \rightarrow \bar{T}^n x$$

여원 SACA의 기본경로가 된다.

Step 5. $\bar{S}_{l,k} = \bar{S}_{l-1,0} + (b_l + 1)S_{l,0} + \sum_{i=1}^{l-1} b_i S_{i,0}$ 에 의하여 $\mathbb{C}'$ 의 트리를 구성한다.

5. $GF(2^p)$ HCA의 특성분석

5.1 $GF(2^p)$ HCA의 전이규칙 및 성질

$GF(2^2)$ 위에서 다항식 $x^3 + x^2 + 2x + 3$ 은 원시다항식으로 주기가 63이다. 이와 같이 $GF(2^p)$ HCA는 $GF(2)$ CA와 비교하여 같은 차수의 원시다항식에 대하여 훨씬 주기가 길어지므로 아주 유용하다. 또한 차수가 같은 다항식에 대하여 원시다항식도 더 많이 존재하기 때문에 다양하게 응용할 수도 있다. 예를 들어 $GF(2)$ 위에서 3차 다항식은 $x^3 + x + 1$, $x^3 + x^2 + 1$ 로 2개 존재하지만 $GF(2^2)$ 위에서의 원시다항식은 모두 12개로 다음과 같다.

$$\begin{aligned} & x^3 + x^2 + x + 2, \quad x^3 + 3x^2 + 3x + 3, \quad x^3 + x^2 + 3x + 2, \quad x^3 + 2x^2 + 3x + 3 \\ & x^3 + x^2 + 2x + 3, \quad x^3 + 3x^2 + 2x + 2, \quad x^3 + x^2 + x + 3, \quad x^3 + 2x^2 + 2x + 2 \\ & x^3 + 2x^2 + 3x + 2, \quad x^3 + 2x^2 + x + 3, \quad x^3 + 3x^2 + x + 2, \quad x^3 + 3x^2 + 2x + 3 \end{aligned}$$

$GF(2^p)$ 위에서 n 차 원시다항식의 개수는 $\frac{\phi(2^{np} - 1)}{n}$ 이다. 예를 들어 $p = 2$, $n = 3$ 인

경우 원시다항식의 개수는 $\frac{\phi(2^{3 \cdot 2} - 1)}{3} = \frac{\phi(63)}{3} = 12$ 이다.

다음은 $GF(2^p)$ HCA의 특성다항식 및 전이규칙에 대한 성질들을 분석하고 그룹 $GF(2^p)$ HCA의 사이클 구조를 분석한다.

5.1.1 $GF(2^p)$ HCA의 전이규칙

$GF(2)$ 위에서 uniform CA를 $GF(2^p)$ 확장한 uniform HCA는 각 셀에 대하여 왼쪽 이웃에 대한 가중치가 모두 같고 오른쪽 이웃에 대한 가중치가 모두 같다. 즉 각 셀의 3-이웃에 대한 가중치를 $\langle \alpha_l, \alpha_s, \alpha_r \rangle$ 라 하면 식 (3.2)의 상태전이 행렬은 다음과 같다.

$$T = \begin{pmatrix} \alpha_s & \alpha_r & 0 & \cdots & 0 \\ \alpha_l & \alpha_s & \alpha_r & \cdots & 0 \\ 0 & \alpha_l & \alpha_s & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \alpha_s \end{pmatrix} \quad (5.1)$$

여기서 α_l 은 셀의 왼쪽이웃에 대한 가중치를 나타내고 α_s 는 자기 자신에 대한 가중치, α_r 은 오른쪽 이웃에 대한 가중치를 나타낸다. 이러한 uniform HCA는 적용하는 전이규칙에 따라 그룹 HCA 또는 비그룹 HCA가 되기도 한다. 그룹 HCA는 상태전이행렬의 행렬식이 0이 아니고 임의의 상태에 따른 이전 상태가 유일하다. 그러나 비그룹 HCA는 상태전이행렬의 행렬식이 0이고, 임의의 상태에 대한 이전 상태가 유일하지 않고 상태전이그래프는 트리모양이 된다.

<정리 5.1> 전이규칙이 다음과 같은 n 셀 uniform HCA는 다음을 만족한다. 여기서 일반적인 α_i 는 0이 아니다.

- (1) $\langle \alpha_l, \alpha_s, \alpha_r \rangle$ 가 $\langle 0, \alpha_s, 0 \rangle$, $\langle 0, \alpha_s, \alpha_r \rangle$ 또는 $\langle \alpha_l, \alpha_s, 0 \rangle$ 인 모든 크기의 HCA는 그룹이다.

(2) $\alpha_s^2 = \alpha_l \alpha_r$ 을 만족하는 셀의 크기 n 에 대하여 $n \bmod 3 \neq 2$ 인 HCA는 그룹 HCA이고 $n \bmod 3 = 2$ 인 HCA는 비그룹 HCA이다.

(3) $\langle \alpha_l, \alpha_s, \alpha_r \rangle$ 가 $\langle \alpha_l, 0, \alpha_r \rangle$ 이고 셀의 수가 짝수인 HCA는 그룹 HCA이다.

(증명) (1) $\langle \alpha_l, \alpha_s, \alpha_r \rangle$ 가 $\langle 0, \alpha_s, 0 \rangle$ 인 경우의 상태전이행렬은 대각성분이 α_s 이고 나머지 성분은 0인 대각행렬이고 $\langle 0, \alpha_s, \alpha_r \rangle$ 인 경우의 상태전이행렬은 상삼각행렬이며 $\langle \alpha_l, \alpha_s, 0 \rangle$ 인 경우는 하삼각행렬로 상태전이행렬의 행렬식은 모두 α_s^n 이다. 그러므로 주어진 uniform HCA는 그룹 HCA이다.

(2) 주어진 규칙을 갖는 n 셀 uniform HCA의 상태전이행렬을 $T_{R,n}$ 이라 하자.

$T_{R,n}$ 의 행렬식에 대하여 다음과 같은 점화식이 성립한다.

$$|T_{R,n}| = \alpha_s |T_{R,n-1}| + \alpha_l \alpha_r |T_{R,n-2}| \quad (5.2)$$

여기서 $T_{R,n-1}$ 은 상태전이행렬 $T_{R,n}$ 에서 n 행과 n 열을 제거한 부분행렬이다. 이를 이용하여 주어진 정리를 수학적 귀납법으로 증명할 수 있다.

$n = 1$ 일 때 $|T_{R,1}| = \alpha_s \neq 0$ 이다.

$n = 2$ 일 때 $|T_{R,2}| = \begin{vmatrix} \alpha_s & \alpha_r \\ \alpha_l & \alpha_s \end{vmatrix} = \alpha_s^2 + \alpha_l \alpha_r$ 이고 가정에 의해 0이다.

$n = 3$ 일 때 $|T_{R,3}| = \begin{vmatrix} \alpha_s & \alpha_r & 0 \\ \alpha_l & \alpha_s & \alpha_r \\ 0 & \alpha_l & \alpha_s \end{vmatrix} = \alpha_s |T_{R,2}| + \alpha_l \alpha_r |T_{R,1}| = \alpha_l \alpha_s \alpha_r$

$m = 3p$ 또는 $m = 3p + 1$ 에 대하여 $|T_{R,m}| \neq 0$ 이고 $m = 3p + 2$ 에 대하여

$|T_{R,m}| = 0$ 이라 할 때, $|T_{R,m+1}|$ 에 대하여

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

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

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

그러므로 $n \bmod 3 \neq 2$ 인 HCA는 그룹 HCA이고 $n \bmod 3 = 2$ 인 HCA는 비그룹 HCA이다.

(3) i) $n = 2m + 1$ 인 경우, $|T_{R,1}| = \alpha_s = 0$ 이므로 다음이 성립한다.

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

ii) $n = 2m$ 인 경우, $|T_{R,2}| = \begin{vmatrix} 0 & \alpha_r \\ \alpha_l & 0 \end{vmatrix} = \alpha_l \alpha_r (\neq 0)$ 이므로 다음이 성립한다.

$$\begin{aligned}
|T_{R,2m}| &= \alpha_l \alpha_r |T_{R,2m-2}| = (\alpha_l \alpha_r)^2 |T_{R,2m-4}| = \dots \\
&= (\alpha_l \alpha_r)^{m-1} |T_{R,2}| = (\alpha_l \alpha_r)^m |T_{R,1}| \neq 0
\end{aligned}$$

그러므로 $|T_{R,n}|$ 은 다음과 같다.

$$|T_{R,n}| = \begin{cases} (\alpha_l \alpha_r)^{\frac{n}{2}}, & n \text{ 은 짝수} \\ 0, & n \text{ 은 홀수} \end{cases}$$

□

주어진 $GF(2^p)$ HCA의 각 셀에 적용되는 전이규칙이 2가지 이상인 CA를 hybrid HCA라 한다. 다음 정리는 특정한 전이규칙이 교대로 사용되는 hybrid HCA에 대한 특성이다.

<정리 5.2> n 셀 $GF(2^p)$ HCA의 각 셀에 적용되는 전이규칙 R_1, R_2 가 다음과 같다고 하자.

$$R_1 = \begin{cases} \langle \alpha_l, 0, \alpha_r \rangle, \\ \langle \alpha_l, \alpha_s, \alpha_r \rangle \end{cases}$$

$$R_2 = \begin{cases} \langle \alpha_l, \alpha_s, \alpha_r \rangle, \\ \langle \alpha_l, 0, \alpha_r \rangle \end{cases}$$

그러면 다음이 성립한다.

$$|T_{R_1, n}| = \begin{cases} (\alpha_l \alpha_r)^{\frac{n}{2}}, & n \text{ 짝수} \\ \alpha_s (\alpha_l \alpha_r)^{\frac{n-1}{2}}, & n \bmod 4 = 1 \\ 0, & \text{기타} \end{cases}$$

(증명) $T_{R, (k, n)}$ 을 $T_{R, n}$ 에서 1행부터 $k-1$ 행까지, 1열부터 $k-1$ 열까지 제거한 부분행렬이라 하자. 예를 들어 $T_{R, (2, n)}$ 은 $T_{R, n}$ 에서 1행과 1열을 제거한 부분행렬이다.

i) $n = 2m$ 인 경우 전이규칙 R_1, R_2 에 대하여

$$|T_{R, n}| = 0 \cdot |T_{R, (2, n)}| + \alpha_l \alpha_r |T_{R, (3, n)}| = \alpha_l \alpha_r |T_{R, (3, n)}| \text{ 이다.}$$

이를 반복 적용하면 $|T_{R, n}| = (\alpha_l \alpha_r)^m$ 이다.

또한 R_2 에 대하여 다음이 성립한다.

$$|T_{R_1, n}| = \alpha_l \alpha_r |T_{R, n-2}| \text{ 이므로 반복하여 적용하면 } |T_{R_1, n}| = (\alpha_l \alpha_r)^m$$

ii) $n = 2m + 1$ 일 때, 전이규칙 R_1 에 대하여 다음이 성립한다.

$$\begin{aligned} |T_{R_1, 2m+1}| &= \alpha_l \alpha_r |T_{R_1, 2m-1}| = (\alpha_l \alpha_r)^2 |T_{R_1, 2m-3}| = \cdots \\ &= (\alpha_l \alpha_r)^m |T_{R_1, 1}| = (\alpha_l \alpha_r)^m \cdot 0 = 0 \end{aligned}$$

iii) 전이규칙 R_2 에 대하여

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

이므로 $n = 4m + 3$ 인 경우는

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

이다. 그러므로 셀의 수가 짝수이고, 전이규칙 R_1 또는 R_2 를 갖는 hybrid HCA는 그룹이고, 셀의 수가 $n = 4m + 1$ 이고 전이규칙 R_2 를 갖는 hybrid HCA는 그룹 HCA이다. $\square$

5.1.2 그룹 HCA의 사이클 구조

선형 n 셀 $\text{GF}(2^p)$ HCA가 그룹 HCA인지 비그룹 HCA인지를 알 수 있는 방법은 상태전이행렬의 정칙여부에 따라 결정된다. 그러나 이 HCA의 상태전이행동을 구체적으로 알기에는 부족하다. 이 절에서는 HCA의 구체적인 상태전이행동을 분석하기 위해서 상태전이행렬의 특성다항식을 이용한다. 그룹 HCA의 상태전이는 임의의 상태에 대한 이전 상태가 유일하게 결정되지만, 비그룹

HCA는 그렇지 못하다. HCA의 특성다항식의 인수 $f(x)$ 중 $f(T)=0$ 을 만족하는 최소차수의 다항식을 $GF(2^p)$ HCA의 **최소다항식** ($m(x)$)이라 한다. $m(x)=x^d\phi(x)$ 일 때, $d>0$ 이면 HCA는 비그룹 HCA이고, $d=0$ 이면 HCA는 그룹 HCA이다. d 는 상태전이그래프에서 트리의 깊이를 결정하며 임의의 도달 불가능한 상태에서 가장 가까운 상태에 도달하는데 걸리는 시간이다. $\phi(x)$ 는 HCA의 사이클 구조를 결정한다[19].

$\phi(x)$ 는 다음과 같은 형태를 이룬다.

$$\phi(x) = [f_1(x)]^{r_1} [f_2(x)]^{r_2} \cdots [f_h(x)]^{r_k} \quad (5.3)$$

Elspas[19]는 $GF(2)$ 위에서의 사이클 구조를 분석하였는데 이러한 결과는 $GF(2^p)$ 에서도 자연스럽게 확장가능하다. $GF(2^p)$ HCA의 사이클 구조를 분석하기 위하여 다음과 같은 경우로 간단히 하여 분석한다.

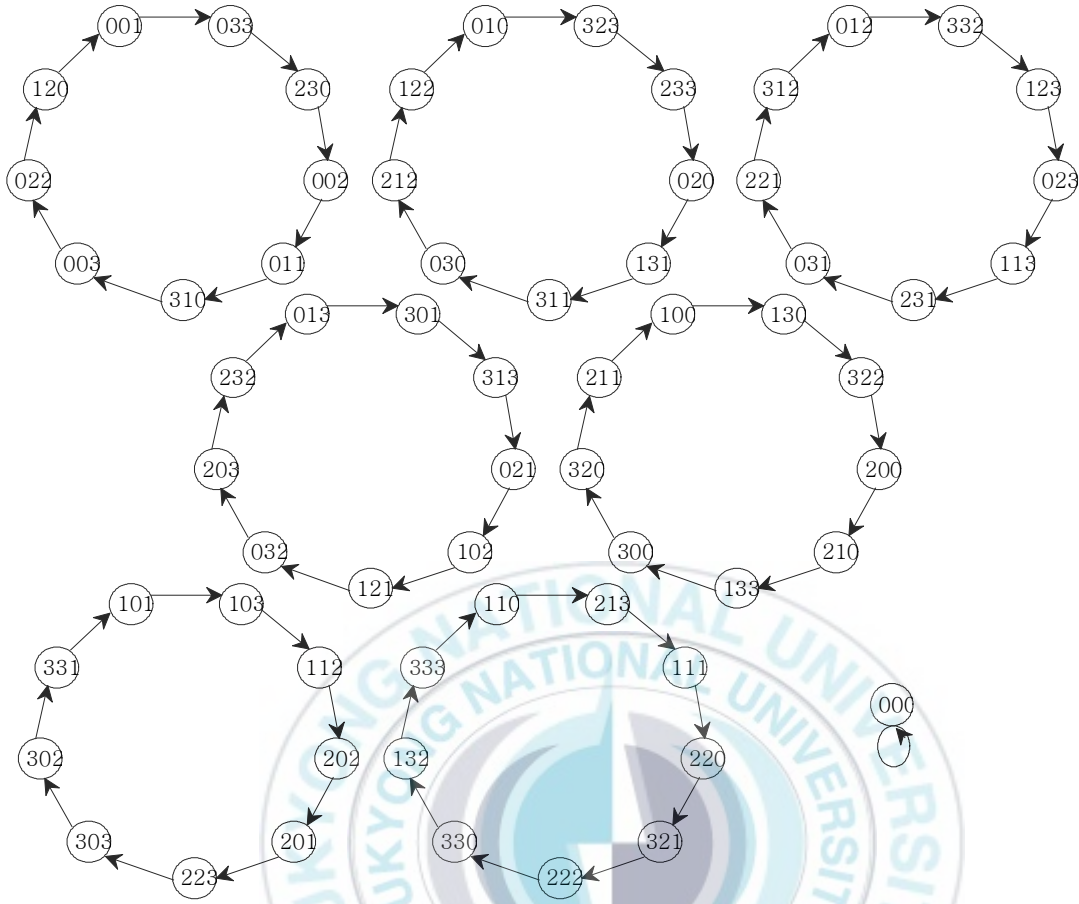
(1) $\phi(x) = f(x)$ ($f(x)$: 기약다항식)

$f(x)$ 의 주기는 $k = \min \{ l : f(x) \mid x^l + 1 \}$ 이고, 이 경우 사이클 구조는

$[1(1), \mu_1(k)]$ 이다. 이 때 $\mu_1 = \frac{2^{np}-1}{k}$ 이다.

<예 5.1> $T = \begin{pmatrix} 1 & 3 & 0 \\ 3 & 2 & 3 \\ 0 & 3 & 3 \end{pmatrix}$ 일 때,

$f(x) = x^3 + 2$ 이고 $x^3 + 2 \mid x^9 + 1$ 이다. 또한 $\mu_1 = \frac{(2^4)^3 - 1}{9} = \frac{63}{9} = 7$ 이다.



<그림 5.1> 3셀 $GF(2^2)$ HCA의 상태전이 그래프

(2) $\phi(x) = [f(x)]^r$ ($f(x)$: 기약다항식)

$2^{r_1-1} < r \leq 2^{r_1}$ 이고, $f(x)$ 의 주기가 k 이면 주어진 HCA의 사이클의 길이는 $1, k, 2k, 2^2k, \dots, 2^{r_1}k$ 가 존재하고 사이클의 구조는 다음과 같다.

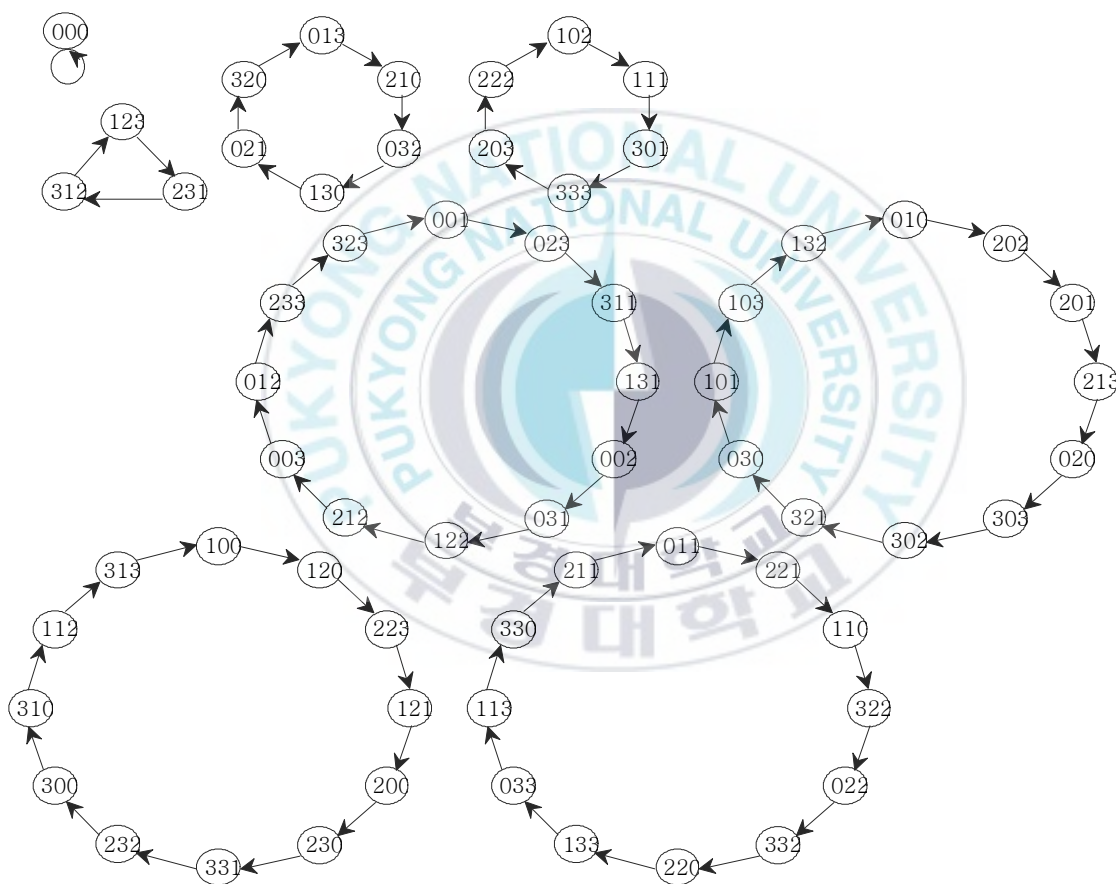
$[1(1), \mu_1(k), \mu_2(2k), \mu_3(2^2k), \dots, \mu_{r_1+1}(2^{r_1}k)](\mu_i(k_i))$ 에서 μ_i 는 주기가 k_i 인 사이클의 개수를 의미한다. $U_i := \{x \mid [f(T)]^i x = 0\}$ 이라 하자.

$x \in U_2 - U_1$ 이면, $[f(T)]^2 x = 0$ 이지만 $f(T)x \neq 0$ 이다. 이러한 상태 x 는

$[f(x)]^2$ 의 주기를 갖는 사이클에 속한다. 따라서 $\mu_i = \frac{n(U_{i-1} - U_{i-2})}{2^{i-1}k}$ 이다.

여기서 $n(A)$ 는 집합 A 의 원소의 개수를 나타낸다.

<예 5.2> $T = \begin{pmatrix} 1 & 2 & 0 \\ 2 & 0 & 2 \\ 0 & 2 & 3 \end{pmatrix}$ 일 때 $f(x) = (x+2)^3$ 이다.



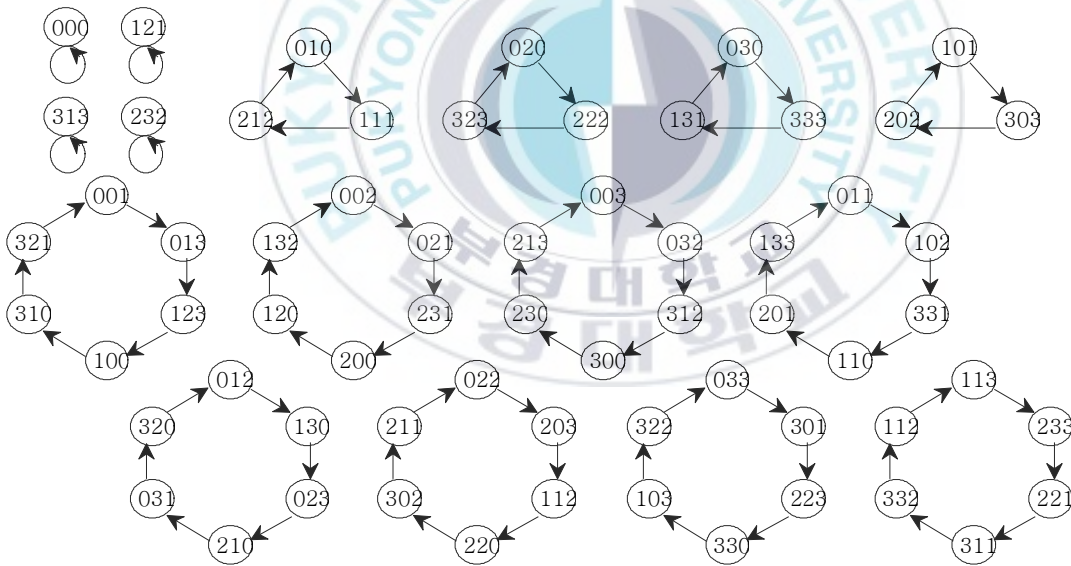
<그림 5.2> 3셀 $GF(2^2)$ HCA의 상태전이 그래프

(3) $\phi(x) = f(x)g(x)$ ($f(x), g(x)$: 기약다항식)

$f(x), g(x)$ 의 차수를 각각 d_1, d_2 라 하고, 주기를 각각 k_1, k_2 라 하자. 그러면 $f(x)$ 에 의해 생성되는 사이클은 $[1(1), \mu_1(k_1)]$ 이고 $g(x)$ 에 의해 생성되는 사이클은 $[1(1), \mu_2(k_2)]$ 이다. 따라서 $f(x)g(x)$ 에 의해 생성되는 사이클의 구조는 $[1(1), \mu_1(k_1)][1(1), \mu_2(k_2)] = [1(1), \mu_1(k_1), \mu_2(k_2), \mu(k)]$ 이다. 여기서 $\mu = \mu_1 \mu_2 \gcd(k_1, k_2)$ 이고 $k = \text{lcm}(k_1, k_2)$ 이다.

<예 5.3> $T = \begin{pmatrix} 3 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 3 \end{pmatrix}$ 에서, 3셀 $\text{GF}(2^2)$ HCA의 최소다항식이 다음과 같이

$m(x) = (x+1)(x+3)^2$ 이라 할 때, 사이클 구조는 <그림 5.3>과 같다.



<그림 5.3> 3셀 $\text{GF}(2^2)$ HCA의 상태전이 그래프

5.2 GF(2^p) HCA의 특성다항식

GF(2^p) HCA의 상태전이행렬에서 오른쪽 이웃과 왼쪽 이웃에 대한 모든 가중치를 동일하게 두는 것은 GF(2)위에서의 90/150 CA에 대한 자연스러운 확장이다. 따라서 가중치를 동일하게 두었을 때 상태전이행렬은 다음과 같다.

$$T = \begin{pmatrix} d_1 & i & 0 & \cdots & 0 \\ i & d_2 & i & \cdots & 0 \\ 0 & i & d_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & d_n \end{pmatrix} \quad (5.4)$$

i 는 가중치로 $\{0, 1, 2, \dots, 2^p - 1\}$ 의 원소이다. 주어진 상태전이행렬을 $T = \langle d_1, d_2, \dots, d_n \rangle_i$ 로 나타내기로 하고 이를 전이규칙이라고 하자. 다음 정리는 n 셀 GF(2^p) HCA의 특성다항식에 관한 점화식으로 GF(2^p) HCA의 전이규칙을 찾을 수 있는 정리이다. 수학적 귀납법으로 간단히 증명할 수 있다.

<정리 5.3> n 셀 GF(2^p) HCA의 전이규칙이 $\langle d_1, d_2, \dots, d_n \rangle_i$ 이고 특성다항식이 $\triangle_n$ 이라 하면 다음 점화식을 만족한다

$$\triangle_k = (x + d_k)\triangle_{k-1} + i^2\triangle_{k-2}, \quad (k > 0) \quad \triangle_{-1} = 0, \quad \triangle_0 = 1 \quad (5.5)$$

n 셀 GF(2^p) HCA의 특성다항식이 점화식 (5.4)를 만족한다면 이 식은 유클리드 알고리즘을 만족한다. 즉, $\triangle_k$ 와 $\triangle_{k-1}$ 가 $x + d_k$ 와 $\triangle_{k-2}$ 을 유일하게 결정한다. 여기서 중요한 것은 몫이 항상 일차이어야 한다. $\triangle_n$ 과 $\triangle_{n-1}$ 을 알고 있다고 가정하면 유클리드 알고리즘에 의하여 $x + d_n$ 과 $\triangle_{n-2}$ 가 유일하게 결정될 것이다.

다시 Δ_{n-1} 과 Δ_{n-2} 에 유클리드 알고리즘을 적용하면 $x + d_{n-1}$ 과 Δ_{n-3} 을 계산할 수 있다. 유클리드 알고리즘의 반복적 적용은 CA의 특성다항식 계산 과정의 역과 같다. 다시 말하면 유클리드 알고리즘을 이용하여 특성다항식으로부터 n 셀 GF(2^p) HCA의 전이규칙을 찾을 수 있다.

다음은 Δ_n 과 Δ_{n-1} 을 알고 있을 때 유클리드 알고리즘을 이용하여 그 주어진 다항식을 특성다항식으로 갖는 GF(2^2) HCA의 전이규칙을 찾는 예이다.

<예 5.3> GF(2^2) HCA의 전이규칙이 $\langle 3, 1, 2, 2 \rangle_3$ 일 때, $\Delta_4 = x^4 + 2x^3 + 2x^2 + 3$ 이고 $\Delta_3 = x^3 + 3$ 이다. 이 다항식에 유클리드 알고리즘을 적용하면 다음과 같다.

피제수	제수	몫	나머지
$x^4 + 2x^3 + 2x^2 + 3$	$x^3 + 3$	$x + 2$	$3^2(x^2 + 2x + 1)$
$x^3 + 3$	$x^2 + 2x + 1$	$x + 2$	$3^2(x + 3)$
$x^2 + 2x + 1$	$x + 3$	$x + 1$	$3^2 \cdot 1$
$x + 3$	1	$x + 3$	0

여기서 몫의 상수만 취해서 역으로 나열하면 3, 1, 2, 2이고 나머지에서 가중치가 3임을 알 수 있다. 그런데 $\Delta_3 = x^3$ 이면 $\langle 0, 0, 0, 2 \rangle_3$ 을 얻고 $\Delta_3 = x^3 + 3x^2 + 2x + 1$ 라면 $\langle 0, 1, 2, 1 \rangle_2$ 을 얻는다. GF(2)위에서 n 차 기약다항식을 특성다항식으로 갖는 90/150 GF(2) CA는 Δ_{n-1} 이 유일하게 존재한다[5]. 이와 달리 위에서 n 차 기약다항식을 특성다항식으로 갖는 n 셀 GF(2^p) HCA는 위의 예처럼 여러 개 존재한다.

또 $x^3 + 2x^2 + 3x + 2$ 에 대응하는 $GF(2^p)$ HCA 규칙은 $\langle 1, 0, 3 \rangle_1$, $\langle 0, 1, 3 \rangle_2$, $\langle 0, 3, 1 \rangle_3$ 도 있지만, 각 셀의 이웃에 대하여 가중치가 다른 HCA도 존재한다.

예를 들어 상태전이행렬이 $T = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 2 \\ 0 & 1 & 2 \end{pmatrix}$ 인 HCA의 특성다항식도 $x^3 + 2x^2 + 3x + 2$

이다. 그러나 이것은 $GF(2)$ 입장에서 볼 때 90/150 CA가 아닌 경우이므로 이러한 경우에 대해서는 배제하기로 한다.

정리 5.1에 의하여 $\triangle_n$ 과 $\triangle_{n-1}$ 을 알 때 HCA의 전이규칙을 찾을 수 있음을 보였으나 $\triangle_{n-1}$ 을 찾을 수 있는 방법이 매우 어렵다. 주어진 다항식에 대한 동반행렬과 HCA의 상태전이행렬이 닮음이라는 사실로부터 다음과 같은 성질을 얻을 수 있다.

<정리 5.4> 원시다항식 $p(x) = x^n + c_{n-1}x^{n-1} + \dots + c_1x + c_0$ 를 특성다항식으로 갖는 n 셀의 상태전이행렬이 $T = \langle d_1, d_2, \dots, d_n \rangle_i$ 이고, 정칙 상삼각행렬 U 와 $p(x)$ 에 대한 동반행렬 C 가 다음과 같다고 하자.

$$U = (u_i) = \begin{cases} u_i & , i = j \\ a_i & , i = j - 1 \\ 0 & , i \geq j \\ x_i (\in GF(2^p)) & , \text{기타} \end{cases}$$

$$C = (s_{ij}) = \begin{cases} 1 & , i = j + 1 (j < n) \\ c_{i-1} & , j = n \\ 0 & , \text{기타} \end{cases}$$

여기서 c_i 는 $p(x)$ 의 계수이다. 그러면 다음이 성립한다.

$$\begin{cases} d_1 = u_1^{-1} a_1 \\ d_k = u_{k-1}^{-1} a_{k-1} + u_k^{-1} a_k \quad (1 < k < n) \\ d_n = u_{n-1}^{-1} a_{n-1} + c_{n-1} \end{cases} \quad (5.6)$$

(증명) 주어진 T 와 C 가 같은 특성다항식을 가지므로 두 행렬은 닮은 행렬이다.
따라서 $TU = UC$ 라 두고 풀면 다음의 결과를 얻는다.

$$\begin{aligned} a_1 &= u_1 d_1 \\ a_k &= i a_{k-1} + u_k d_k \quad (1 < k < n) \\ c_{n-1} u_n &= i a_{n-1} + u_n d_n \\ u_{i+1} &= i u_i \end{aligned}$$

위 식으로부터 $i = u_{k-1}^{-1} u_k$ 를 대입하면 위와 같은 점화식이 성립한다. $\square$

<예 5.4> $T = \langle 1, 3, 3 \rangle_2$ 일 때 U 를 구해보자.

T 의 특성다항식은 $x^3 + x^2 + 2x + 3$ 이므로 동반행렬은 $C = \begin{pmatrix} 0 & 0 & 3 \\ 1 & 0 & 2 \\ 0 & 1 & 1 \end{pmatrix}$ 이다.

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

그러므로 가능한 U 는 다음과 같다.

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

위의 식에 의하여 상태전이행렬 T 의 대각성분을 다음과 같이 구한다.

$$d_1 = 1 \cdot 1 = 1, d_2 = 1 + 2^{-1} \cdot 3 = 3, d_3 = 2 + 1 = 3$$

다음은 $T = \langle 0, 0, 3, 3 \rangle_2$ 일 때, U 를 구하는 방법이다.

<예 5.5> T 의 특성다항식은 $x^4 + x^2 + 2x + 3$ 이므로 $C = \begin{pmatrix} 0 & 0 & 0 & 3 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ 이 된다.

$$U = \begin{pmatrix} u_1 & a_1 & d_1 & d_3 \\ 0 & 2u_1 & a_2 & d_2 \\ 0 & 0 & 3u_1 & a_3 \\ 0 & 0 & 0 & u_1 \end{pmatrix} \text{라 하면 } T = \begin{pmatrix} 0 & 2 & 0 & 0 \\ 2 & 0 & 2 & 0 \\ 0 & 2 & 3 & 2 \\ 0 & 0 & 2 & 3 \end{pmatrix} \text{이므로 } TU = UC \text{를 풀면}$$

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

그러므로 $d_1 = 1 \cdot 0 = 0, d_2 = 0 + 2^{-1} \cdot 0 = 0, d_3 = 0 + 3^{-1} \cdot 2 = 3, d_4 = 3 + 0 = 3$ 이다.

Cho [8] 등은 주어진 $\text{GF}(2)$ 위에서의 기약다항식에 대한 90/150 CA를 찾는 방법을 소개하였다. 이는 기존의 방법보다 훨씬 개선된 방법이다. 그러나 $\text{GF}(2^p)$ 기약다항식에 대한 $\text{GF}(2^p)$ HCA를 구하는 방법은 아직까지 존재하지 않는다.

6. 결 론

CA는 인접한 이웃들과 결합논리로서 서로 연결되어 있고 그 형태가 규칙적인 배열로 구성되어 있고, 난수성이 우수하여 수열을 발생시키는 성질을 가지고 있어 혼돈과 확산의 효과가 뛰어나 암호 알고리즘 설계를 위해 LFSR의 대안으로 제안되고 있다. CA는 LFSR과 비교하여 랜덤성이 우수하다는 것이 알려지면서 의사 난수 패턴 생성기, 해쉬 함수, 스트림 암호 알고리즘 등의 고속화 응용에 많이 활용되고 있다. 하지만 CA는 오랫동안 모델링과 컴퓨팅 패러다임 및 많은 물리계를 모델링하는데 사용되어 왔으나 이런 시스템 모델을 연구함에 있어 물리계의 복잡성이 증가하여 CA를 이용한 모델은 매우 복잡하고 분석적으로 추적하기가 어렵게 되었다.

본 논문은 p 개의 기억소자가 한 개의 셀을 이루는 $GF(2^p)$ 위에서 n 셀 선형 SACA의 특성을 분석하고 선형 SACA로 부터 유도되는 여원 SACA의 상태전이 행동을 분석하였다. 또한 $GF(2^p)$ 위에서 선형 SACA의 기본경로와 여원 SACA의 기본경로를 통하여 SACA의 상태전이 그래프를 분석하는 알고리즘을 제안하였다. 또한 비트단위에서 처리하는 $GF(2)$ 위에서 CA보다 복잡한 시스템을 모델링하기에 적합한 $GF(2^p)$ HCA에 대하여 분석하였다. 특히 그룹 HCA가 되는 여러 가지 전이규칙들을 제시하였고, 최소다항식의 형태에 따른 HCA의 상태전이행동을 분석하였다. 또한 90/150 CA의 자연스런 확장인 $GF(2^p)$ HCA의 특성다항식에 관하여 여러 가지 성질들을 밝혔다.

참 고 문 헌

- [1] V. Aladyev, Survey of research in the theory of homogeneous structures and their application, Mathematical Biosciences, vol. 22, pp. 121-154, 1974.
- [2] E.R. Berlekamp, Factorization, Bell System Technical Journal, no. 46, pp. 1853-1859, 1967
- [3] E. R. Banks, Information Processing and Transmission in Cellular Automata. ph. D. thesis, M. I. T., 1971.
- [4] A. W. Burks, Essays on cellular automata, tech. rep., Univ. of Illinois, Urbana, 1970.
- [5] S.J. Cho, U.S. Choi, Y.H. Hwang, H.D. Kim and Y.S. Pyo, Analysis of state-transition of SACA over $GF(2^p)$, J. Kor. Inst. Info. Security and Cryptology, 15, pp. 105-111, 2005.
- [6] S.J. Cho, U.S. Choi and H.D. Kim, Analysis of complemented CA derived from a linear TPMACA, Computers and Mathematics with Applications, 45, pp. 689-698, 2003.
- [7] S.J. Cho, U.S. Choi and H.D. Kim, Behavior of complemented CA whose complement vector is acyclic in a linear TPMACA, Mathematical and Computer Modelling, 36, pp. 979-986, 2002.
- [8] S.J. Cho, U.S. Choi and H.D. Kim, Y.H. Hwang, J.G.. Kim and S.H. Heo, New synthesis of one-dimensional 90/150 linear hybrid group cellular automata, IEEE Trans. Comput.-Aided Design Integr. Circuits Syst, 26, pp. 1720-1724, 2007.
- [9] S.J. Cho, U.S. Choi, Y.H. Hwang, H.D. Kim and H.H. Choi, Behaviors of Single Attractor Cellular Automata over Galois Field $GF(2^p)$, LNCS 4173, pp. 232-237, 2006.

- [10] K. Cattell and J. Muzio, Synthesis of One-Dimensional Linear Hybrid Cellular Automata, IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Vol. 15(3), pp. 325-335, 1996.
- [11] 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, 45, pp. 769-781, 1996.
- [12] C. Chattopadhyay, Some studies on theory and applications of additive Cellular Automata, Ph. D. Thesis, I.I.T, Kharagpur, India, 2002.
- [13] D.R. Chowdhury, I.S. Gupta and P.P. Chaudhuri, A programmable cellular automata structure for built-in self-test, TENCON '91.1991 IEEE Region International Conference on EC3-Energy, Computer, Communication and Control Systems , Volume: 3, Aug. 23-30, pp. 166-170, 1991.
- [14] E. F. Codd, Cellular Automata. Academic Press Inc., 1968.
- [15] A.K. Das and P.P. Chaudhuri, Vector space theoretic analysis of additive cellular automata and its application for pseudoexhaustive test pattern generation, IEEE Trans. Comput., 42, pp. 340-352, 1993.
- [16] 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.
- [17] A.K. Das and P.P. Chaudhuri, Efficient characterization of cellular automata, Proc. IEE(Part E), 137(1), pp. 81-87, 1990.
- [18] A.K. Das, D. Saha, A.R. Chowdhury, S. Misra and P.P. Chaudhuri, Signature analysers based on additive cellular automata, Fault-Tolerant Computing, FTCS-20. Digest of Papers, 20th International Symposium, 26-28 pp. 265-272, 1990.
- [19] B. Elspas, The Theory of Autonomous Linear Sequential Networks, TRE Trans. on Circuits, CT-6(1), pp. 45-60, 1959.

- [20] I.N. Herstein, Topics in Algebra, Vikas Publishing House Pvt Ltd, 1987.
- [21] M. Harao and S. Naguchi, On some dynamical properties of finite cellular automata, IEEE Trans. on Computers, vol. C-27, no. 1, 1978.
- [22] R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, 1997.
- [23] D. Mukhopadhyay and D.R. Chowdhury, Characterization of a class of complemented group cellular automata, LNCS, 3305, pp. 775-784, 2004.
- [24] S. Nandi and P.P. Chaudhuri, Analysis of periodic and intermediate boundary 90/150 cellular automata, IEEE Trans. Computers, 45(1), pp.1-12, 1996.
- [25] S. Nandi, B.K. Kar and P.P. Chaudhuri, Theory and applications of cellular automata in cryptography, IEEE Trans. Computers, 43, pp. 1346-1357, 1994.
- [26] J. Von Neumann, The Theory of Self-Reproducing Automata, A.W. Burks ed. (Univ. of Illinois Press, Urbana and London), 1966.
- [27] K. Paul, Theory and Application of $GF(2^p)$ Cellular Automata, ph. D. Thesis, B.E. College, Howrah, India, 2002.
- [28] W. Pries, A. Thanailakis and H.C. Card, Group properties of cellular automata and VLSI applications, IEEE Trans, Computers, C-35, pp. 1013-1024, 1986.
- [29] D. Richardson, Tessellations with local transformations, J. Comput. Systems Sci, vol. 6, pp. 373-388, 1972.
- [30] 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, pp. 403-408, 2001.

- [31] B.K. Sikdar, N. Ganguly, P. Majumder, P.P. Chaudhuri, Design of Multiple Attractor $GF(2^p)$ Cellular Automata for Diagnosis of VLSI Circuits, VLSI Design, Fourteenth International Conference on 2001, pp. 454-459, 2001.
- [32] P. Tsalides, T.A. York and A. Thanailakis, Pseudo-random number generators for VLSI systems based on linear cellular automata, IEE Proc. E. Comput. Digit. Tech, 138, pp. 241-249, 1991.
- [33] T. Toffoli, Computation and construction universality of reversible cellular automata, J. Comput. System Sci, vol. 15, p. 213, 1977.
- [34] S. J. Willson, On the ergodic theory of cellular automata, Math. System Theory, vol. 9, pp. 132-141, 1975
- [35] S. Wolfram, Statistical mechanics of cellular automata, Rev. Mod. Phys., 55, pp. 601-644, 1983.



감사의 글

저에게 있어 대학원 8년의 시간은 겸손과 인내를 가르쳐 준 소중한 시간이었습니다. 어느 정도 마음의 각오는 하였지만 과정 중의 중요한 고비마다 나의 부족함을 절실히 느껴 그 때마다 기도하게 되었고, 저에게 지혜와 인내를 주셔서 유종의 미를 거둘 수 있게 이끌어 주신 하나님께 감사드립니다.

이 논문을 완성하기까지 많은 분들의 도움을 받았습니다. 먼저 제자를 마음으로 배려해 주시고, 적절한 시기마다 도움과 따끔한 충고로 오늘이 있게 만드신 조성진 지도교수님께 진심으로 감사를 드립니다. 보다 나은 논문을 위해 조언해 주시고, 끝까지 최선을 다해 지도해 주신 심사위원 김도상 교수님, 표용수 교수님, 박진한 교수님, 인제대 김한두 교수님께 감사드립니다. 만날 때마다 후배를 격려해주셨던 신준용 교수님과 수리과학부의 모든 교수님들께 감사드립니다.

아울러 항상 힘과 의지가 되었던 CA연구실의 최언숙 교수님, 황윤희씨, 김경자 선생님, 숙희, 성훈, 민정, 지미, 진경, 봉수씨께 감사의 마음을 전합니다.

하늘나라에 계시지만 마음속에 더욱 가까이 살아계신 친정부모님께 둘째 딸이 감사의 마음을 드립니다. 몸소 노력하시는 본을 보이며 기도해 주신 사랑하는 시어머니께 깊은 감사를 드리며, 곁에서 위로와 용기를 준 남편과 늘 바빠 제대로 챙겨주지 못했던 두 아들 시은과 규은에게 못 다한 사랑을 마음으로 전합니다.