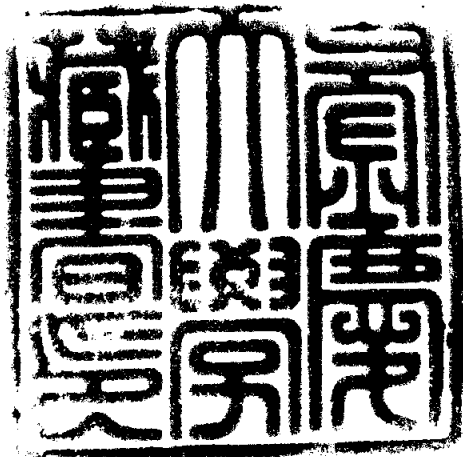


교육학석사 학위논문

# 기약다항식과 셀룰라 오토마타와의 관계

지도교수 조 성 진

이 논문을 교육학석사 학위논문으로 제출함



2003년 8월

부경대학교 교육대학원

수 학 교 육 전 공

이 영 미

# 이영미의 교육학석사 학위논문을 인준함

2003년 6 월 17 일

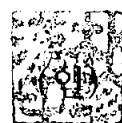
주 심 이학박사

표 용 수



위 원 이학박사

박 진 한



위 원 이학박사

조 성 진



# 목 차

|                                 |    |
|---------------------------------|----|
| Abstract .....                  | 1  |
| 1. 서 론 .....                    | 2  |
| 2. 1차원 셀룰라 오토마타 .....           | 3  |
| 2.1 1차원 셀룰라 오토마타의 정의 및 분류 ..... | 3  |
| 2.2 1-D CA의 경계조건 .....          | 4  |
| 2.3 1-D CA의 전이행렬 .....          | 5  |
| 2.4 1-D CA의 특성다항식과 원시다항식 .....  | 7  |
| 3. 기약다항식 .....                  | 9  |
| 3.1 기약다항식과 원시다항식의 정의 및 성질 ..... | 9  |
| 3.2 기약다항식과 CA의 관계 .....         | 14 |
| 4. Null Boundary CA .....       | 16 |
| 4.1 NBCA의 특성다항식 .....           | 16 |
| 4.2 점화관계식 .....                 | 17 |
| 4.3 이차합동식 .....                 | 18 |
| 5. Trace와 이차합동식 .....           | 20 |
| 5.1 Trace의 정의 및 특성 .....        | 20 |
| 5.2 Trace를 이용한 이차방정식의 풀이 .....  | 26 |
| 5.3 부분다항식을 구하는 알고리즘 .....       | 30 |
| 6. 결론 .....                     | 35 |
| 참고문헌 .....                      | 36 |

# The Relationship of Between Irreducible Polynomials and Cellular Automata

Young-mi Lee

Graduate School of Education  
Pukyong National University

## Abstract

This paper presents a method of obtaining a cellular automata that has a given characteristic polynomial. There is the crucial relationship between Euclid's greatest common divisor algorithm and the characteristic polynomial of a cellular automata. Using this fact, we can get the method for the synthesis of a cellular automata from given characteristic polynomial. The solving quadratic congruence of cellular automata is the heart of the synthesis algorithm. Cellular automata and transition matrices with three boundary conditions are reported. Also some result about irreducible polynomial, primitive polynomial and the relationship between irreducible polynomial and cellular automata are given. The general theory for traces which are very useful analytic tools and the properties of a quadratic congruence are given.

# 1. 서 론

셀룰라 오토마타(Cellular Automata, 이하 CA)는 Von Neumann과 Wolfram에 의해 스스로 조직화하고 재생산할 수 있는 모델로 소개되었다([15, 17]). CA란 동역학계(dynamical system)를 해석하는 한 방법으로 공간과 시간을 이산적으로 다루고, 이산적인 공간인 셀룰라 공간(cellular space)의 기본 단위인 각 셀이 취할 수 있는 상태를 유한하게 처리하며, 각 셀들의 상태가 국소적인 상호작용에 의해서 동시에 갱신되는 시스템이다.

LFSR의 대안으로서 제시된 CA는 test pattern generation, pseudo-random number generation, cryptography, error correcting codes, signature analysis 등 많은 분야에서 응용되고 있다([1, 4, 5, 7-9]).

모든 CA는  $GF(2)$  상에서의 전이행렬에 의해 유일하게 표현되고 모든 전이행렬은 특성다항식을 갖는다. 특성다항식은 CA의 특별한 성질을 나타내어 주기 때문에 주어진 특성다항식으로부터 그에 대응하는 CA를 찾아내는 것은 중요한 문제이다.

최대길이를 갖는 CA의 특성다항식은 원시다항식이며, 특성다항식으로부터 CA를 합성해내기 위해서 일반적으로 기약다항식으로 제한하여 연구한다.

본 논문에서는 CA를 경계조건에 따라 세 가지로 분류하고 CA법칙에 따른 전이행렬의 특성다항식의 성질들을 살펴본다. 또한 CA의 합성뿐만 아니라 곱셈을 수행하는 효과적인 회로의 설계에 실제적으로 응용되기도 하는 trace를  $GF(2)$ 상에서 살펴본다([11, 12, 13]).

본 논문에서는 2장에서 CA에 관한 전반적인 이론과 세 가지 경계조건에 따른 분류 및 그 전이행렬을 알아보고, 3장에서는 기약다항식과 그의 특별한 예인 원시다항식 및 기약다항식과 CA와의 관계에 대해 살펴보았다. 4장에서는 NBCA의 특성다항식, 유클리드 호제법과 이차합동식을 이용하여 CA를 찾는 방법에 관하여 살펴보고 5장에서는 분석적 도구로 활용되는 trace에 관한 일반적인 이론과 이차합동식에 관련된 성질들을 살펴보았다.

## 2. 1차원 셀룰라 오토마타

### 2.1 1차원 셀룰라 오토마타의 정의 및 분류

셀룰라 오토마타(Cellular Automata, 이하 CA)는 동역학계를 해석하는 한 방법으로 공간과 시간을 이산적으로 다루는 시스템이며 셀룰라 공간의 기본 단위는 하나의 셀이다. 각 셀들의 상태는 유한하며, 국소적인 상호작용에 의해서 동시에 갱신된다.

가장 간단한 구조를 가지는 1차원 CA(One-Dimensional CA, 이하 1-D CA)에서는 모든 셀들이 선형으로 배열되어 있으며 1-D CA 중에서 국소적 상호작용이 세 개의 셀, 즉 자신과 인접한 두 셀에 의해 이루어지는 3-이웃(3-neighbourhood) CA가 가장 중요하게 다루어진다.

CA를 설명하기 위해 사용하는 기호들은 다음과 같다.

- $i$  : 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

3-이웃 CA에 대한 상태전이함수(transition function)는 다음과 같이 나타내어진다.

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

여기서  $f$ 는 결합논리를 가지는 국소 전이함수이다.  $f$ 는 3개의 변수를 가지는 Boolean 함수이며, 따라서  $2^{2^3}$ 개의 상태전이함수들이 있다. 이것을 CA의 rule이라고 한다.

3-이웃 CA에서 인접한 세 개의 셀들의 시간  $t$ 에서의 상태와 시간  $t+1$ 에서의 상태의 배열을 나타내어 보면 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       | rule 90  |
| $q_i^{t+1}$                     | 1       | 0       | 0       | 1       | 0       | 1       | 1       | 0       | rule 150 |

위의 rule 에 대한 결합논리는 다음 식으로 표현할 수 있고 여기서  $\oplus$ 는 XOR논리를 나타낸다.

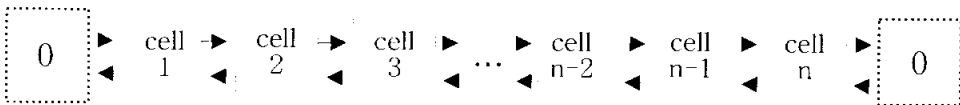
$$\text{rule 90} : q_i(t+1) = q_{i-1}(t) \oplus q_{i+1}(t) \quad (2. 2)$$

$$\text{rule 150} : q_i(t+1) = q_{i-1}(t) \oplus q_i(t) \oplus q_{i+1}(t) \quad (2. 3)$$

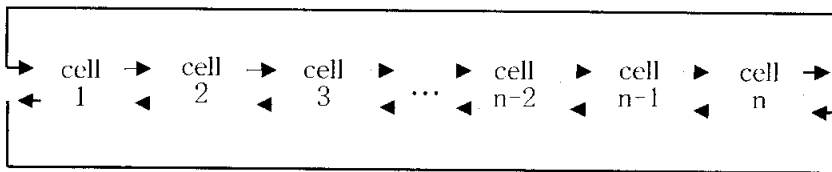
## 2.2 1-D CA의 경계조건

CA의 경계조건이란 두 개의 이웃만 존재하는 제일 왼쪽과 제일 오른쪽의 셀에 대하여 세 번째 이웃의 상태를 결정해 주는 것을 말한다. 일반적으로 경계조건에 따라 CA는 다음과 같이 세 가지로 구분한다.

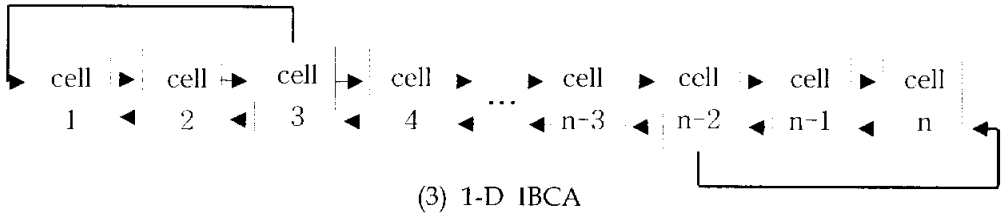
먼저 NBCA(Null Boundary CA)는 제일 왼쪽과 제일 오른쪽의 셀들이 0 상태에 연결되어 있는 경우이다. PBCA(Periodic Boundary CA)는 양끝의 셀들이 서로 연결되어 있는 경우이며 Cyclic CA라고도 한다. 가장 왼쪽(오른쪽) 셀의 다음 상태가 그 자신과 그것의 오른쪽(왼쪽) 이웃, 두 번째 오른쪽(왼쪽) 이웃 셀의 상태에 의존하는 것은 IBCA(Intermediate Boundary CA)이다. <그림2.1>은 각각의 경계조건을 나타낸 것이다.



(1) 1-D NBCA



(2) 1-D PBCA



<그림 2.1> 1-D CA의 경계조건

### 2.3 1-D CA의 전이행렬

$n$  개의 셀을 가지는 1-D CA에서는 현재 상태를 다음 상태로 전이시키는 작용소(operator)를  $n \times n$  행렬로 나타낼 수 있으며 이것을 전이행렬(transition matrix)이라 한다. 전이행렬  $A$ 에서  $i$ 번째 행은  $i$ 번째 셀에 적용되는 rule이며 그 셀의 다음 상태가 현재 상태에 의존하면 1, 그렇지 않으면 0으로 쓴다.

$f_{(t)}(x)$ 가 시간  $t$ 에서 CA의 상태를 나타내면 시간  $t+1$ 에서의 상태는 다음 식으로 표현된다.

$$f_{(t+1)}(x) = A \times f_{(t)}(x) \quad (2.4)$$

$$f_{(t+p)}(x) = A^p \times f_{(t)}(x) \quad (2.5)$$

다음은 CA의 전이행렬과 상태전이에 대한 간단한 예이다.

<예 2.3.1> 네 개의 셀을 가진 1차원 NBCA의 rule이 [150, 90, 150, 90]이면 전이행렬은 다음과 같다.

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

그리고 이 CA의 현재 상태가  $f_{(t)}(x) = [1 \ 1 \ 0 \ 0]^T$  이면 다음 상태는 전이행렬로서 다음과 같이 구할 수 있다.

$$f_{(t+1)}(x) = A \times f_{(t)}(x) = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

본 논문에서는 일반적으로 가장 많이 쓰이는 rule 90과 rule 150만을 사용하는 Linear Hybrid CA(LHCA)에 대해서만 고려한다.

#### 가. 1-D NBCA의 전이행렬

NBCA(Null Boundary CA)는 제일 왼쪽과 제일 오른쪽의 셀들이 0 상태에 연결되는 경계 조건을 가진 CA이다. 따라서  $n$ 개의 셀을 가지는 1-D NBCA의 전이행렬은 다음과 같다. 여기서,  $i$  번째 셀이 rule 90을 사용하면  $d_i$ 의 값은 0이고 rule 150을 사용하면  $d_i$ 의 값은 1이다.

$$\begin{bmatrix} d_1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & d_2 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & d_3 & 1 & \cdots & 0 & 0 \\ \vdots & & & & & & \vdots \\ \vdots & & & \ddots & & & \vdots \\ \vdots & & & & & & \vdots \\ 0 & 0 & \cdots & 1 & d_{n-2} & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 & d_{n-1} & 1 \\ 0 & 0 & \cdots & 0 & 0 & 1 & d_n \end{bmatrix}$$

#### 나. 1-D PBCA의 전이행렬

1-D PBCA에서 전이행렬은 다음과 같다. PBCA에서 첫 번째 셀은 제일 오른쪽의  $n$ 번째 셀의 영향을 받으므로 전이행렬의 1행  $n$ 열의 값이 1이고,  $n$ 번째 셀은 제일 왼쪽인 첫 번째 셀의 영향을 받으므로 전이행렬의  $n$ 행 1열의 값이 1이다.

$$\begin{bmatrix} d_1 & 1 & 0 & 0 & \cdots & 0 & \boxed{1} \\ 1 & d_2 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & d_3 & 1 & \cdots & 0 & 0 \\ \vdots & & & & \ddots & & \vdots \\ \vdots & & & & & & \vdots \\ 0 & 0 & \cdots & 1 & d_{n-2} & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 & d_{n-1} & 1 \\ \boxed{1} & 0 & \cdots & 0 & 0 & 1 & d_n \end{bmatrix}$$

#### 다. 1-D IBCA의 전이행렬

1-D IBCA의 전이행렬은 다음과 같다. IBCA에서 첫 번째 셀은 두 번째 오른쪽 셀의 영향을 받으므로 전이행렬의 1행 3열의 값이 1이고,  $n$  번째 셀은 두 번째 왼쪽 셀의 영향을 받으므로 전이행렬의  $n$  행  $n-2$ 열의 값이 1이다.

$$\begin{bmatrix} d_1 & 1 & \boxed{1} & 0 & \cdots & 0 & 0 \\ 1 & d_2 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & d_3 & 1 & \cdots & 0 & 0 \\ \vdots & & & & \ddots & & \vdots \\ \vdots & & & & & & \vdots \\ 0 & 0 & \cdots & 1 & d_{n-2} & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 & d_{n-1} & 1 \\ 0 & 0 & \cdots & 0 & \boxed{1} & 1 & d_n \end{bmatrix}$$

## 2.4 1-D CA의 특성다항식과 원시다항식

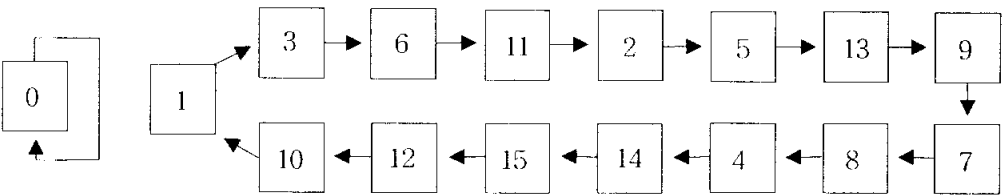
$n$ 개의 셀로 이루어진 CA에 대해서  $A$ 가  $n \times n$  전이행렬이고,  $I$ 가  $n$  차 단위행렬일 때, CA의 특성다항식을 다음과 같이 정의한다.

$$|xI - A| \quad (2.6)$$

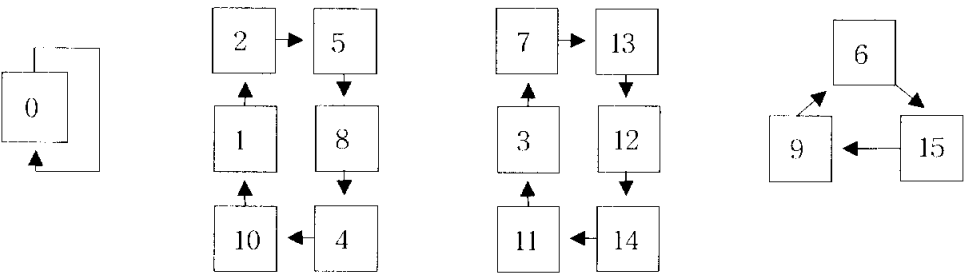
모든 CA는 전이행렬에 의해서 유일하게 표현되고, 모든 전이행렬은 특성다항식을 갖는다. 그리고 이 특성다항식은 CA의 어떤 특정한 성질들을 나타낸다. CA의 전이행렬  $A$ 가 정칙

행렬, 즉  $\det(A)=1$  이면 그 CA를 group CA라 하며 group CA는 최대길이를 갖는 CA와 최대길이를 갖지 않는 CA로 구분할 수 있다.  $n$ 개의 셀로 이루어진 CA에서 셀의 상태가 0 인 경우를 제외하고  $2^n-1$  개의 상태가 모두 하나의 주기 안에 있을 때 최대길이를 갖는다고 한다. 최대 길이를 갖는 CA의 특성다항식은 원시다항식이다 ([10]).  $n$  차 원시다항식  $P(x)$ 는 인수분해 되지 않고  $x^m+1$  을 나누는  $m$ 의 최소값이  $2^n-1$  인 다항식이다.

<그림 2.2>는 특성다항식이  $x^4+x^3+1$  인 최대 길이를 갖는 group CA이고,  
 <그림 2.3>은 특성다항식이  $x^4+x^2+1$  인 최대길이를 갖지 않는 group CA이다.



<그림 2.2> 최대 길이를 갖는 Group CA



<그림 2.3> 최대 길이를 갖지 않는 Group CA

### 3. 기약다항식

#### 3.1 기약다항식과 원시다항식의 정의 및 성질

〈정의 3.1.1〉  $F = GF(p)$  ( $p$ 는 소수) 위의 다항식  $f(x) \in F[x]$ ,  $\deg f(x) \geq 1$ 에 대하여 다음이 성립할 때,  $f(x)$ 를  $F[x]$ 의 기약다항식(irreducible polynomial)이라고 한다.

$$p(x) \mid f(x) \Rightarrow \exists a \in F^*; p(x) = a \text{ 또는 } p(x) = af(x) \quad (3.1)$$

특히, 체  $F$  위의  $n$ 차 기약다항식  $f(x)$ 에 대하여, 다음이 성립할 때,  $f(x)$ 를  $F[x]$ 의 원시다항식(primitive polynomial)이라고 한다.

$$p^n = \min \{ m \mid f(x) \mid x^m - x \} \quad (3.2)$$

〈예 3.1.1〉  $F = GF(2)$  라 하자.  $n=4$ 인 다음 세 가지 다항식을 생각해 보자.

$$f_1(x) = x^4 + x^3 + 1$$

$$f_2(x) = x^4 + x^3 + x^2 + x + 1$$

$$f_3(x) = x^4 + x^2 + 1$$

$f_1(x)$ ,  $f_2(x)$ 는 기약다항식이지만,  $f_3(x)$ 는 기약다항식이 아니다.

특히,  $f_1(x)$ 는 원시다항식이지만,  $f_2(x)$ 는  $f_2(x) \mid x^6 - x$  도 되어 원시다항식이 아니다.

각 차수에 대한 기약다항식과 원시다항식을 정리하면 다음과 같다.

<표 3.1> 기약다항식과 원시다항식

| 차수 | 기약다항식                                                                                                                                                                 | 원시다항식                                                                                                                  |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| 1  | $x, x+1$                                                                                                                                                              | $x+1$                                                                                                                  |
| 2  | $x^2+x+1$                                                                                                                                                             | $x^2+x+1$                                                                                                              |
| 3  | $x^3+x+1, x^3+x^2+1$                                                                                                                                                  | $x^3+x+1, x^3+x^2+1$                                                                                                   |
| 4  | $x^4+x+1, x^4+x^3+1$<br>$x^4+x^3+x^2+x+1$                                                                                                                             | $x^4+x+1, x^4+x^3+1$                                                                                                   |
| 5  | $x^5+x^2+1, x^5+x^3+1$<br>$x^5+x^4+x^2+x+1$<br>$x^5+x^3+x^2+x+1$<br>$x^5+x^4+x^3+x+1$<br>$x^5+x^4+x^3+x^2+1$                                                          | $x^5+x^2+1, x^5+x^3+1$<br>$x^5+x^4+x^2+x+1$<br>$x^5+x^3+x^2+x+1$<br>$x^5+x^4+x^3+x+1$<br>$x^5+x^4+x^3+x^2+1$           |
| 6  | $x^6+x+1, x^6+x^3+1$<br>$x^6+x^5+1$<br>$x^6+x^4+x^2+x+1$<br>$x^6+x^5+x^4+x^2+1$<br>$x^6+x^5+x^4+x+1$<br>$x^6+x^5+x^2+x+1$<br>$x^6+x^5+x^3+x^2+1$<br>$x^6+x^4+x^3+x+1$ | $x^6+x+1$<br>$x^6+x^5+1$<br><br><br>$x^6+x^5+x^4+x+1$<br>$x^6+x^5+x^2+x+1$<br>$x^6+x^5+x^3+x^2+1$<br>$x^6+x^4+x^3+x+1$ |

<정리 3.1.1> 체  $F_p$  위에서 다항식  $x^{p^n}-x$  ( $q=p^n$ )의 모든 기약인수의 차수는  $n$ 의 약수이다. 그리고  $n$ 의 임의의 양의 약수  $d$ 에 대하여 체  $F_p$ 에서의  $d$ 차의 기약다항식은 모두  $x^{p^n}-x$ 의 인수이다.

<증명>  $F_p$ 에 차수  $d \mid n$ 인 임의의 모닉 기약다항식의 한 근  $\alpha$ 를 첨가하면  $F_{p^n}$ 에 포함되는  $F_{p^d}$ 의 동형인 체를 얻는다. 그러면  $\alpha$ 가  $x^q-x=0$ 을 만족하기 때문에 그 모닉 기약다항식은 다항식  $x^q-x$ 을 나누어야 한다. 역으로  $f(x)$ 를  $x^q-x$ 를 나누는 모닉 기약다항식이라 하자. 그러면  $f(x)$ 의 근들은  $F_q$ 에 있어야 한다. ( $x^q-x$ 의 모든 근들이

$F_q$ 에 있기 때문이다.) 그러므로  $f(x)$ 의 차수는  $n$ 의 약수이다. 왜냐하면 한 근을 첨가하면  $F_q$ 의 부분체를 얻기 때문이다. 그러므로  $x^q - x$ 를 나누는 모닉 기약다항식의 차수는  $n$ 의 약수들이다.  $x^q - x$ 가 중근이 없다는 것을 알고 있으므로  $x^q - x$ 는 방금 증명한 바와 같이  $n$ 의 약수인 차수를 갖는 모든 기약다항식의 곱과 같다.

〈보조정리 3.1.2〉  $n$ 가 소수이면  $F_p[x]$ 에는 차수  $n$ 인 모닉 기약다항식이  $\frac{p^n - p}{n}$ 개 존재한다.

<증명> 소수  $n$ 에 대한 Fermat의 작은 정리에 의하면  $p^n \equiv p \pmod n$  이므로  $\frac{p^n - p}{n}$ 는 정수이다. 보조정리를 증명하기 위하여  $l$ 을 차수  $n$ 인 모닉 기약다항식의 개수라 하자. 위의 <정리 3.1.1>에 따르면 차수  $p^n$ 인 다항식  $x^{p^n} - x$ 는 차수  $n$ 인  $l$ 개의 다항식과 차수 1인  $p$ 개의 기약다항식  $x - a$ , ( $a \in F_p$ )의 곱이다. 그러므로 차수를 비교해보면  $p^n = ln + p$ 이다. 이로부터  $l = \frac{p^n - p}{n}$ 이다.

더 일반적으로  $n$ 가 반드시 소수일 필요는 없다고 가정하자.  $l_d$ 를  $F_p$  위에서 차수  $d$ 인 모닉 기약다항식들의 개수라 하면

$$p^n = \sum_{d|n} dl_d = \sum_{\substack{d|n \\ d \neq n}} dl_d + nl_n$$

이다.

왜냐하면  $x^{p^n} - x$  차수가  $n$ 의 약수인  $GF(p)$ 에서의 모든 모닉 기약다항식들의 곱이므로

$$l_n = \frac{p^n - \sum_{\substack{d|n \\ d \neq n}} dl_d}{n} \quad \text{이 성립한다.}$$

〈정리 3.13〉  $F = GF(p)$  라 하자.  $n$  차  $F[x]$ 의 원시다항식은

$$\frac{\phi(p^n - 1)}{n} \quad (4.4)$$

개 존재한다.

<증명>  $n$  차  $F[x]$ 의 원시다항식  $f(x)$ 의 근을  $\alpha$ 라 하면  $\text{ord}(\alpha) = p^n - 1$ 이므로 원시다항식의 근들은  $p^n - 1$ 과 서로소가 되어야 하므로 그러한 원소의 개수는  $\phi(p^n - 1)$ 이다. 또한 각 원시다항식의 차수가  $n$ 이므로 원시다항식들의 개수는  $\frac{\phi(p^n - 1)}{n}$  이 된다.

〈예 3.12〉  $F = GF(2)$  라 하자.  $n = 3$  인 경우 기약다항식의 개수는

$$\frac{p^n - p}{n} = \frac{2^3 - 2}{3} = 2 \text{이고, } n = 4 \text{ 인 경우 원시다항식의 개수는}$$

$$\frac{\phi(2^4 - 1)}{4} = \frac{\phi(15)}{4} = \frac{\phi(3) \cdot \phi(5)}{4} = 2 \text{ 이다.}$$

〈정리 3.14〉 체  $F$  위의 다항식  $p(x)$ 가  $n$ 차 기약다항식이라면  $g(x) := x^n \cdot p(x^{-1})$ 도 기약다항식이다. 역도 성립한다.

<증명>  $g(x)$ 가 기약다항식이 아니라고 가정하면

$$g(x) = h(x) \cdot k(x)$$

을 만족하는 체  $F$  위의 다항식  $h(x)$ ,  $k(x)$ 가 존재하여

$$g(x^{-1}) := x^{-n} \cdot p(x) = h(x^{-1}) \cdot k(x^{-1})$$

이므로

$$p(x) = x^n \cdot h(x^{-1}) \cdot k(x^{-1})$$

이 되어  $p(x)$ 는 기약다항식이 아니다. 역으로,  $p(x)$ 가 기약다항식이 아니라고 가정하면

$$p(x) = u(x) \cdot v(x)$$

을 만족하는 체  $F$  위의 다항식  $u(x)$ ,  $v(x)$  가 존재하여

$$g(x) := x^n \cdot p(x^{-1}) = x^n \cdot u(x^{-1}) \cdot v(x^{-1})$$

이므로

$$g(x) = x^n \cdot u(x^{-1}) \cdot v(x^{-1})$$

이 되어  $g(x)$ 는 기약다항식이 아니다.

**〈정리 3.15〉** 체  $F = GF(2)$  위의 차수가  $n (\geq 3)$ 인 기약다항식  $f(x)$  가 자신의 상반다항식과 같다면  $f(x)$  는 원시다항식이 아니다.

<증명>  $f(x) = x^n f(x^{-1})$  이므로

$f(x) = (x^a)^b + \alpha_1 (x^a)^{b-1} + \alpha_2 (x^a)^{b-2} + \cdots + \alpha_2 (x^a)^2 + \alpha_1 x^a + 1$ ,  $\alpha_1, \alpha_2 \in \{0, 1\}$  이고  $a \cdot b = n$ 이다. 그러므로  $f(x) | (x^a)^{b+1} - 1$ 이며  $a \cdot (b+1) \neq 2^{n-1}$ . 그러므로  $f(x)$ 는 원시다항식이 아니다.

**〈참고〉** 위 정리의 역은 일반적으로 성립하지 않는다. 예를들어  $x^6 + x^5 + x^4 + x^2 + 1$ ,  $x^6 + x^4 + x^2 + x + 1$ 은 자신의 상반다항식과 같지 않으며 원시다항식도 아니다.

**〈예 3.13〉**  $F = GF(2)$ 라 하자.

6차 다항식  $p(x) = x^6 + x^5 + x^4 + x^2 + 1$  은 기약다항식이므로

$$\begin{aligned} g(x) &= x^6 \cdot p(x^{-1}) \\ &= x^6 \cdot \left( \frac{1}{x^6} + \frac{1}{x^5} + \frac{1}{x^4} + \frac{1}{x^2} + 1 \right) \\ &= x^6 + x^4 + x^2 + x + 1 \end{aligned}$$

이 되어  $g(x)$ 도 기약다항식이 된다.

특히,  $x^4 + x^3 + x^2 + x + 1$ 은 원시다항식은 아님을 알 수 있다.

### 3.2 기약다항식과 CA 의 관계

4장에서 특성다항식  $\Delta_n(x)$ 가 기약다항식일 때 rule이 90, 150으로 이루어진 CA는  $\Delta_n(x)$ 와 2:1로 대응됨을 보일 것이다.

〈예 3.2.1〉 CA rule이  $[1, 1, 0, 1]$  일 때, 특성다항식은  $\Delta_n(x) = x^4 + x^3 + 1$ 이다. 여기서 CA rule  $[1, 1, 0, 1]$ 의 역순의 rule  $[1, 0, 1, 1]$ 에 대해 특성다항식  $\Delta_n(x) = x^4 + x^3 + 1$ 가 구해진다.

따라서 각각의 특성다항식에 대하여, CA는 본래의 rule 과 그 의 역순의 rule이 존재하여 1:2로 대응하게 된다.

〈정리 3.2.1〉 주어진 CA의 특성다항식이  $\Delta_n(x)$ 이고, 최소다항식이  $m(x)$  일 때,  $\Delta_n(x)$ 이 기약이면  $m(x) = \Delta_n(x)$  이다.

<증명>  $m(x)$ 는 최소다항식이므로  $m(x) | \Delta_n(x)$ 를 만족한다.

따라서  $\Delta_n$ 가 기약이면  $m(x) = \Delta_n(x)$ 이다.

〈정리 3.2.2〉 주어진  $n \times n$ 행렬  $M$ 의  $(i, j)$ 원소  $M_{ij}$ 가  $M_{ij} = \begin{cases} 0, & |i-j| > 1, \\ a_i, & i=j, \\ c_i, & i=j+1, \\ b_i, & i=j-1 \end{cases}$

이고 어떤  $i$ 에 대하여  $b_i = 0$ 라 가정하자. 그러면  $M$ 의 특성다항식  $\Delta_n$ 은 기약이다.

<증명> 주어진  $n \times n$  행렬  $M$ 의  $(i, j)$  원소  $M_{ij}$ 가  $M_{ij} = \begin{cases} 0, & |i-j| > 1, \\ a_i, & i=j, \\ c_i, & i=j+1, \\ b_i, & i=j-1 \end{cases}$  이고 어떤  $i$ 에

대하여  $b_i = 0$ 라 가정하자.

편의상

$$M_i = \begin{pmatrix} a_j & b_j & \cdots & \cdots & \cdots & \cdots \\ c_{j-1} & a_{j-1} & b_{j-1} & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & c_{i+1} & a_{i+1} & b_{i+1} \\ \cdots & \cdots & \cdots & \cdots & c_i & a_i \end{pmatrix}$$

라 하자. 그러면  $\Delta_n$ 을  $i$  행에 관해 전개하면

$$\Delta_n = c_i \cdot |C_i| + (a_i + x) |A_i|,$$

$$C_i = \begin{pmatrix} M_{i+2}^n + xI & 0 & O \\ 0 \cdots 0 & c_{i+1} & b_{i+1} & 0 \cdots 0 \\ & & c_{i-1} & \\ O & & 0 & M_{i-1} + xI \end{pmatrix}$$

이고

$$A_i = \begin{pmatrix} (M_{i+1}^n + xI) & O \\ O & (M_{i-1} + xI) \end{pmatrix}$$

이다.

그러므로  $|A_i| = \Delta_{i+1}^n \cdot \Delta_{i-1}$ 이고  $|C_i| = \Delta_{i+2}^n \cdot b_{i+1} \cdot \Delta_{i-1}$ 이다.

따라서  $\Delta_n = c_i \cdot b_{i+1} \Delta_{i+2}^n \cdot \Delta_{i-1} + (a_i + x) \Delta_{i+1}^n \cdot \Delta_{i-1}$ 이 되어  $\Delta_n$ 은 가약이 된다.

<정리 3.2.3> rule이 90, 150만으로 이루어진 CA의 전이행렬의 특성다항식은  $m(x) = \Delta_n(x)$ 이다.

<증명>  $M$ 을 위수  $n$ 인 90/150행렬이라 하자.  $M$ 의 최소다항식  $m(x)$ 의 차수가  $n$ 임을 보이면 증명이 끝난다.  $k=0, 1, \dots, n$ 에 대하여  $m_{ij}^k$ 를  $M^k$ 의  $(i, j)$  성분이라 하고

$M^0 = I$ 라 하자. 그러면

$$m_{ij}^1 = \begin{cases} 1, & |i-j|=1 \\ 0, & |i-j| > 1 \end{cases}$$

임을 알 수 있다.

귀납법에 의하여  $k=1, 2, \dots, n$ 에 대하여

$$m_{ij}^k = \begin{cases} 1, & |i-j|=k \\ 0, & |i-j| > k \end{cases}$$

임을 보일 수 있다.

행렬  $I, M, M^2, \dots, M^{n-1}$ 들은  $1 \leq k \leq n-1$ 에 대하여  $m_{ij}^k (\neq 0)$ 가 존재하여  $m_{ij}^r = 0$  ( $0 \leq r < k$ )를 만족한다.

그러므로  $p(M) = 0$ 가 되는  $n$ 보다 차수가 낮은 영이 아닌 다항식  $p(x)$ 는 존재하지 않는다. 따라서  $M$ 의 최소다항식은 차수가  $n$ 이다.

## 4. Null Boundary CA

### 4.1 NBCA의 특성다항식

NBCA의 특성다항식  $\Delta$ 를 다음과 같이 정의한다. 여기서  $A$ 는  $n$ 개의 셀로 이루어진 1-D NBCA의  $n \times n$  전이행렬이고  $I$ 는  $n$ 차 단위행렬이다.

$$\Delta = |xI - A| \quad (4.1)$$

$M_{ij}$ 는  $i$ 번째부터  $j$ 번째 셀로 이루어진 NBCA이고  $M_{ij}$ 의 특성다항식은  $\Delta_{ij}$ 로 표시하기로 한다. 첫번째부터  $n$ 번째 셀까지  $n$ 개의 셀로 이루어진 NBCA는 간단히  $M_{1,n} = M$ 로 쓰고, 그 특성다항식은 간단히  $\Delta_{1,n} = \Delta_n$ 으로 쓴다. 그리고  $\Delta_{1,n-1}$ ,  $\Delta_{2,n}$ ,  $\Delta_{i,j}$ 를 CA의 부분다항식이라고 정의한다.

## 4.2 점화관계식

NBCA의 특성다항식은 다음 점화관계식을 만족한다([3]). 이 점화관계식은  $\Delta_n$ 을  $n$ 번째 행에 관하여 전개하면 증명된다.

〈정리 4.2.1〉

$$\begin{aligned}\Delta_{-1} &= 0 \\ \Delta_0 &= 1 \\ \Delta_k &= (x + d_k)\Delta_{k-1} + \Delta_{k-2}, \quad k \geq 1\end{aligned}\tag{4.2}$$

또한  $\Delta_n$ 을 첫 번째 행에 대해 전개하면 다음 관계식을 만족함을 간단히 보일 수 있다.

$$\Delta_k = (x + d_1)\Delta_{2,k} + \Delta_{3,k}\tag{4.3}$$

NBCA의 점화관계식 (4.2)  $\Delta_k = (x + d_k)\Delta_{k-1} + \Delta_{k-2}$ 에서  $\Delta_k$ 를 피제수,  $\Delta_{k-1}$ 을 제수,  $x + d_k$ 를 몫,  $\Delta_{k-2}$ 를 나머지라고 하면 이 식은 유클리드 호제법을 만족한다.

즉,  $\Delta_k$ 와  $\Delta_{k-1}$ 가  $x + d_k$ 와  $\Delta_{k-2}$ 를 유일하게 결정하게 된다. 여기서 중요한 사실은 몫이 항상 일차인 것이다.

$\Delta_n$ 과  $\Delta_{n-1}$ 을 알고 있다고 가정하면 유클리드 호제법에 의하여  $x + d_n$ 와  $\Delta_{n-2}$ 가 유일하게 결정될 것이다. 다시  $\Delta_{n-1}$ 과  $\Delta_{n-2}$ 에 호제법을 적용하면  $x + d_{n-1}$ 과  $\Delta_{n-3}$ 을 계산할 수 있다. 이 과정을  $x + d_1$ 과  $\Delta_{-1} = 0$ 을 구할 때까지 반복한다. 유클리드 호제법의 반복적 적용은 CA의 특성다항식 계산의 역과 같다. 다시 말하면, 유클리드 호제법을 이용하여 특성다항식으로부터 CA의 rule을 찾을 수 있는 것이다.

다음은  $\Delta_n$ 과  $\Delta_{n-1}$ 을 알고 있을 때 유클리드 호제법을 이용하여 그 특성다항식에 관한 CA의 rule을 찾는 예이다.

〈예 4.2.1〉 CA의 rule이  $[1, 1, 0, 1]$ 일 때, 다음이 성립한다.

$$\Delta_n = x^4 + x^3 + 1, \quad \Delta_{n-1} = x^3 + x + 1$$

| 피제수             | 제수            | 몫       | 나머지     |
|-----------------|---------------|---------|---------|
| $x^4 + x^3 + 1$ | $x^3 + x + 1$ | $x + 1$ | $x^2$   |
| $x^3 + x + 1$   | $x^2$         | $x$     | $x + 1$ |
| $x^2$           | $x + 1$       | $x + 1$ | 1       |
| $x + 1$         | 1             | $x + 1$ | 0       |

여기서 몫의 상수항만 취해서 역으로 세우면  $[1, 1, 0, 1]$  이고 이것은 바로 CA의 rule 이다.

### 4.3 이차합동식

일반적으로 특성다항식만으로 CA를 유일하게 결정할 수는 없다. 즉,  $\Delta_n$  과 CA와는 일대일 대응이 이루어지지 않는다.

그러나 유클리드 호제법에 의하여  $\Delta_n$ 과  $\Delta_{n-1}$ 의 쌍은 CA를 유일하게 결정한다. 즉, 특성다항식 계산에 있어서  $\Delta_n$ 과  $\Delta_{n-1}$ 은 더 낮은 차수의 다항식 뿐만 아니라 전체 CA를 결정하는 것이다.

$\Delta_n$ 과  $\Delta_{n-1}$ 의 쌍을 CA polynomial-subpolynomial pair 라고 하며 이것은 CA와 일대일 대응을 이룬다. 하나의 CA와 그것의 역은 같은 다항식을 갖지만 서로 다른 CA로 간주한다. 예를 들어  $[1, 1, 0, 1, 0]$ 와  $[0, 1, 0, 1, 1]$ 은 같은 특성다항식을 갖는 다른 CA 이다.

따라서  $\Delta_{1,n-1}$ 와  $\Delta_{2,n}$ 은 CA의 서로 다른 부분다항식들이며 이들의 중요한 성질은 다음 이차합동식을 만족한다는 것이다([3]). 단, 여기서  $\Delta_{1,n}$ 은 기약다항식인 경우로 제한한다.

**<정리 4.3.1> (CA 이차합동식)** 어떤 CA의 특성다항식이  $\Delta_{1,n}$ 이고 부분다항식은  $\Delta_{1,n-1}$ ,  $\Delta_{2,n}$ 이라 하자. 그러면  $y = \Delta_{1,n-1}$ 과  $y = \Delta_{2,n}$ 은 다음 이차합동식을 만족한다.

$$y^2 + (x^2 + x)\Delta'_{1,n}y + 1 \equiv 0 \pmod{\Delta_{1,n}} \quad (4.4)$$

(1) 부분다항식들의 합

$$\Delta_{1, n-1} + \Delta_{2, n} \equiv (x^2 + x)\Delta_{1, n}' \pmod{\Delta_{1, n}} \quad (4. 5)$$

(2) 부분다항식들의 곱

$$\Delta_{1, n-1}\Delta_{2, n} = \Delta_{1, n}\Delta_{2, n-1} + 1 \quad (\text{i.e. } \Delta_{1, n-1}\Delta_{2, n} \equiv 1 \pmod{\Delta_{1, n}}) \quad (4. 6)$$

<증명> 부분다항식들의 합에 관한 증명은 [2, 3]에 제시되어 있고 여기서는 부분다항식들의 곱에 대한 증명만 하기로 한다. 증명은 수학적 귀납법에 의한다.

$n=2$  일 때 (4. 2)에 의하여

$$\begin{aligned} \Delta_{1, 2} &= (x + d_2)\Delta_{1, 1} + \Delta_{1, 0} \\ &= (x + d_1)(x + d_2) + 1 \end{aligned}$$

이므로 다음이 성립한다.

$$\begin{aligned} \Delta_{1, 1}\Delta_{2, 2} &= (x + d_1)(x + d_2) \\ &\equiv 1 \pmod{\Delta_{1, 2}} \end{aligned}$$

$n=k$  일 때

$$\Delta_{1, k-1}\Delta_{2, k} + \Delta_{1, k}\Delta_{2, k-1} = 1$$

라고 하자.

그러면  $n=k+1$  일 때 다음이 성립한다.

$$\begin{aligned} &\Delta_{1, k}\Delta_{2, k+1} + \Delta_{1, k+1}\Delta_{2, k} \\ &= \Delta_{1, k}\Delta_{2, k+1} + \{(x + d_{k+1})\Delta_{1, k} + \Delta_{1, k-1}\}\Delta_{2, k} \\ &= \Delta_{1, k-1}\Delta_{2, k} + \Delta_{1, k}\{\Delta_{2, k+1} + (x + d_{k+1})\Delta_{2, k}\} \\ &= \Delta_{1, k-1}\Delta_{2, k} + \Delta_{1, k}\{(x + d_{k+1})\Delta_{2, k} + \Delta_{2, k-1} + (x + d_{k+1})\Delta_{2, k}\} \\ &= \Delta_{1, k-1}\Delta_{2, k} + \Delta_{1, k}\Delta_{2, k-1} \end{aligned}$$

## 5. Trace와 이차합동식

4장에서 다루었던 이차합동식  $y^2 + (x^2 + x)\Delta'_{1,n}y + 1 \equiv 0 \pmod{\Delta_{1,n}}$ 의 해를 구하기 위해서는  $\Delta_{1,n}$ 을 기약다항식으로 제한하고 다항식에 대한 연산은  $\pmod{\Delta_{1,n}}$ 으로 해야한다. 따라서 다항식의 덧셈이나 곱셈은 차수를 증가시키지 않으며, 곱셈과 나눗셈은 연산을 한 후에 modulo 연산을 수행하면 된다. 사실 다항식의 연산은 유한체  $GF(2^n)$ 에서 이루어지는 것이다.

Trace는 유한체에서의 분석적 도구로 활용되며 무한체에서도 계산할 수 있다. 그러나 유한체에서의 정의가 보다 더 정교하고 그 결과들이 더 유용하다. Trace는 4장의 이차합동식의 해를 구하기 위해 필수적인 것일 뿐만 아니라  $GF(2^n)$ 에서 곱셈을 수행하는 효과적인 회로의 설계에 실제적으로 응용되기도 한다([11, 12, 13]).

이 장에서는 trace의 정의와 성질과 몇 가지 예들을 살펴보고 trace를 이용한  $GF(2^n)$ 에서의 곱셈에 대해서도 알아본다. 5장에서  $q$ 는 소수인 경우만 생각하기로 한다.

### 5.1 Trace의 정의 및 특성

〈정의 5.1.1〉  $F = GF(q)$ ,  $K = GF(q^n)$ 이라 하자.  $\alpha$ 가  $K$ 의 원소일 때,  $K$ 에 관한 trace를 다음과 같이 정의한다.

$$Tr_F^K(\alpha) = \alpha + \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}} \quad (5.1)$$

$\alpha$ 를  $GF(2^n)$ 의 원소라 하면 정의에 의하여  $GF(2)$  상에서  $\alpha$ 의 trace는 다음과 같다.

$$Tr_F^K(\alpha) = \alpha + \alpha^2 + \alpha^{2^2} + \cdots + \alpha^{2^{n-1}} \quad (5.2)$$

〈보조정리 5.1.1 [11]〉  $F = GF(q)$ ,  $K = GF(q^n)$ 이고  $\alpha$ 는  $K$ 의 원소라 하자. 그러면 다음이 성립한다.

$$x^{q^n} - x = \prod_{\lambda \in F} (x - \lambda) \quad (5.3)$$

〈보조정리 5.1.2〉 소수  $p$  에 대하여 다음이 성립한다.

$$\{\lambda \mid 0 \leq \lambda \leq p-1\} \equiv \{2\lambda \mid 0 \leq \lambda \leq p-1\} \pmod{p}$$

〈보조정리 5.1.3〉  $q$  가 소수이고  $\lambda$  가  $GF(q)$ 의 원소일 때 다음이 성립한다.

$$\begin{aligned} & \prod_{\lambda \in F} \left( \sum_{j=0}^{m-1} x^{q^{j+1}} - \lambda \right) + \prod_{\lambda \in F} (x - \lambda) \\ &= \begin{cases} \prod_{\lambda \in F} \left( \sum_{j=0}^m x^{q^j} - 2\lambda \right), & q \geq 3 \\ \prod_{\lambda \in F} \left( \sum_{j=0}^m x^{q^j} - \lambda \right), & q = 2 \end{cases} \end{aligned}$$

<증명> 증명은 수학적 귀납법에 의한다.

〈보조정리 5.1.4[12]〉  $m$  차 다항식  $p(x)$ 의 계수가 모두  $GF(q)$ 의 원소이면 방정식  $p(x) = 0$ 는 많아야 서로 다른  $m$ 개의 해를 가진다.

〈정리 5.1.5〉  $F = GF(q)$ ,  $K = GF(q^n)$ 이고  $\lambda$ 는  $F$ 의 원소라 하자. 그러면 다음이 성립한다.

$$x^{q^n} - x = \prod_{\lambda \in F} (x + x^q + \cdots + x^{q^{n-1}} - \lambda) \quad (5.4)$$

<증명> 먼저  $n=1$ 일 때 정리 5.1.1에 의해서

$$x^q - x = \prod_{\lambda \in F} (x - \lambda)$$

이다. 이제  $m > 1$ 에 대해서 다음이 만족한다고 가정하자.

$$x^{q^m} - x = \prod_{\lambda \in F} \left( \sum_{j=0}^{m-1} x^{q^j} - \lambda \right)$$

그러면 <보조정리 5.1.3>에 의해서 다음이 성립한다.

$$\begin{aligned}
 x^{q^{m-1}} - x &= (x^q)^{q^m} - x^q + x^q - x \\
 &= \prod_{\lambda \in F} \left( \sum_{j=0}^{m-1} x^{q^{j+1}} - \lambda \right) + \prod_{\lambda \in F} (x - \lambda) \\
 &= \begin{cases} \prod_{\lambda \in F} \left( \sum_{j=0}^m x^{q^{j+1}} - 2\lambda \right) & q \geq 3 \\ \prod_{\lambda \in F} \left( \sum_{j=0}^m x^{q^{j+1}} - \lambda \right) & q = 2 \end{cases}
 \end{aligned}$$

<정리 5.1.6>  $F = GF(q)$ ,  $K = GF(q^n)$  이라 하자. 그러면  $F$ 의 각 원소  $\lambda$ 에 대하여 다항식  $x + x^q + \cdots + x^{q^{n-1}} - \lambda$ 는  $K$ 에서 꼭  $q^{n-1}$ 개의 해를 갖는다.

<증명>  $x + x^q + \cdots + x^{q^{n-1}} - \lambda$ 를  $G(\lambda)$ 라 두자. 보조정리 5.1.4에 의해서  $G(\lambda)$ 는 많아야  $q^{n-1}$ 개의 서로 다른 해를 가진다.  $G(\lambda)$ 가  $K$ 에서  $j$  ( $< q^{n-1}$ )개의 서로 다른 해를 갖는다고 하자. 그러면 (5.3)과 (5.4)에 의하여  $x^{q^n} - x$ 은

$K$ 에서  $q^n$ 보다 적은 서로 다른 해를 갖는다. 그러나  $x^{q^n} - x$ 는  $q^n$ 개의 서로 다른 해를 가져야 하므로 모순이다. 따라서  $x + x^q + \cdots + x^{q^{n-1}} - \lambda$ 는  $K$ 에서 꼭  $q^{n-1}$ 개의 해를 갖는다.

<정리 5.1.7>  $K$ 의 원소인 모든  $\alpha, \beta$ 에 대해서 다음이 성립한다.

- ①  $Tr(\alpha) \in F$
- ②  $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$
- ③  $Tr(\lambda\alpha) = \lambda Tr(\alpha)$ ,  $\lambda \in F$
- ④  $Tr(\alpha^q) = Tr(\alpha)$
- ⑤ trace는  $K$ 에서  $F$ 로의 전사함수이다.

<증명> ①  $\alpha^{q^n} = \alpha$  이기 때문에

$$\text{Tr}(\alpha)^q = \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}} + \alpha = \text{Tr}(\alpha) \text{ 이다.}$$

$$\forall \beta \in F = GF(q) \Leftrightarrow \beta^q = \beta \text{ 이므로 } \text{Tr}(\alpha) \in F \text{ 이다.}$$

$$\textcircled{2} (\alpha + \beta)^{q^i} = \alpha^{q^i} + \beta^{q^i} \text{ 이므로 } \text{Tr}(\alpha + \beta) = \text{Tr}(\alpha) + \text{Tr}(\beta)$$

$$\textcircled{3} \lambda \in F \text{ 이면 } \lambda^{q^n} = \lambda \text{ 이므로 } \text{Tr}(\lambda \alpha) = \lambda \text{Tr}(\alpha), \quad \lambda \in F$$

$$\textcircled{4} \alpha^{q^n} = \alpha \text{ 이므로}$$

$$\begin{aligned} \text{Tr}(\alpha^q) &= \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}} + \alpha^q \\ &= \alpha^q + \alpha^{q^2} + \cdots + \alpha^{q^{n-1}} + \alpha \\ &= \text{Tr}(\alpha) \end{aligned}$$

$$\therefore \text{Tr}(\alpha^q) = \text{Tr}(\alpha)$$

$$\textcircled{5} \text{ <정리 5.15>에 의하여 } x^{q^n}x = \prod_{\lambda \in F} (x + x^q \cdots + x^{q^{n-1}}\lambda) \text{ 이므로 } V_d(x) \text{ 가 } d$$

$$\text{차 기약다항식일 때, } x^{q^n}x = \prod_{d|n} V_d(x) \text{ 임에 의하여 } x^{q^n}x = \prod_{\alpha \in K} (x - \alpha) \text{ 이기 때}$$

문에  $x + x^q + \cdots + x^{q^{n-1}} - \lambda$ 인 각각의  $q$ 개의 다항식들은  $K$ 에서  $q^{n-1}$ 개의 해를 가지며, 따라서 주어진  $\lambda \in F$ 에 대하여  $\text{Tr}(\alpha) = \lambda$ 인  $\alpha \in K$ 가 존재한다.

다음은  $GF(2^n)$ 의 임의의 원소  $\beta$ 의 trace를 구하는 예이다.

<예 5.1.1>  $F = GF(2)$ ,  $K = GF(2^n)$ 이라 하자. 그리고 확장체  $K$ 를 기약다항식  $f(x) = x^4 + x + 1$ 을 이용하여 구성한다. 또  $\alpha$ 를  $f(x) = 0$ 의 해라고 하자. 이제  $K$ 의 임의의 원소  $\beta$ 의 trace를 구해보자.

$\beta$ 는 다음과 같이 유일하게 표현될 수 있다.

$$\beta = \beta_0 + \beta_1 \alpha + \beta_2 \alpha^{2+\beta_3} \alpha^3$$

그러면  $\beta$ 의 trace는 다음과 같다.

$$\begin{aligned} \text{Tr}(\beta) &= \text{Tr}(\beta_0 + \beta_1 \alpha + \beta_2 \alpha^2 + \beta_3 \alpha^3) \\ &= \beta_0 \text{Tr}(1) + \beta_1 \text{Tr}(\alpha) + \beta_2 \text{Tr}(\alpha^2) + \beta_3 \text{Tr}(\alpha^3) \end{aligned}$$

따라서  $\text{Tr}(\beta)$  를 구하기 위해서는  $\text{Tr}(1), \text{Tr}(\alpha), \text{Tr}(\alpha^2), \text{Tr}(\alpha^3)$ 을 계산하기만 하면 된다. 분명히

$$\text{Tr}(1) = 1 + 1 + 1 + 1 = 0$$

이다. 그런데  $\alpha$ 가  $f(x)$ 의 해이면  $\alpha$ 의 켤레근인  $\alpha^2, \alpha^4, \alpha^8$ 도 또한  $f(x)$ 의 해가 된다. 따라서  $\alpha + \alpha^2 + \alpha^4 + \alpha^8$ 은  $f(x)$ 의 해들의 합이므로

$$\text{Tr}(\alpha) = \alpha + \alpha^2 + \alpha^4 + \alpha^8 = 0$$

이다.

$\text{Tr}(\alpha^2)$ 은 <정리 5.1.7>에 의하여  $\text{Tr}(\alpha)$ 의 값과 같다. 즉

$$\text{Tr}(\alpha^2) = \text{Tr}(\alpha) = 0$$

이다.

$\text{Tr}(\alpha^3)$ 의 값은 다음과 같이 구한다.

$$\begin{aligned} \text{Tr}(\alpha^3) &= \alpha^3 + (\alpha^3)^2 + (\alpha^3)^4 + (\alpha^3)^8 \\ &= \alpha^3 + \alpha^6 + \alpha^{12} + \alpha^{24} \\ &= \alpha^3 + (\alpha^3 + \alpha^2) + (\alpha^3 + \alpha^2 + \alpha + 1) + (\alpha^3 + \alpha) \\ &= 1 \end{aligned}$$

그러므로

$$\beta = (\beta_0, \beta_1, \beta_2, \beta_3) = \beta_0 + \beta_1 \alpha + \beta_2 \alpha^2 + \beta_3 \alpha^3$$

이면  $\text{Tr}(\beta)$ 는 다음과 같다.

$$\begin{aligned} \text{Tr}(\beta) &= \beta_3 \\ &= \beta \cdot (0, 0, 0, 1) \end{aligned}$$

〈보조정리 5.1.8[12]〉  $q$  가 소수이고  $F = GF(q)$ ,  $K = GF(q^n)$  이라 하자. 만약  $\alpha$  가  $F$  의 원소이면  $Tr_E^K(\alpha) = n \cdot \alpha$  이다.

〈정리 5.1.9〉  $F = GF(q)$ ,  $E = GF(q^d)$ ,  $K = GF(q^n)$  이고  $q$  는 소수,  $d$  는  $n$  의 약수라 하자. 그러면  $(x - \alpha)(x - \alpha^q) \cdots (x - \alpha^{q^{d-1}})$  에서  $c_{d-1}$  이  $x$  의 계수일 때, 즉

$$(x - \alpha)(x - \alpha^q) \cdots (x - \alpha^{q^{d-1}}) = x^d + c_1 x^{d-1} + \cdots + c_{d-1} x + c_d \quad (5.5)$$

일 때 다음이 성립한다.

$$Tr_F^K(\alpha^{-1}) = -\frac{n}{d} c_{d-1}$$

<증명>

$$\begin{aligned} (x - \alpha^{-1}) & \{x - (\alpha^{-1})^q\} \cdots \{x - (\alpha^{-1})^{q^{d-1}}\} \\ &= c_d x^d + c_{d-1} x^{d-1} + \cdots + c_1 x + 1 \\ &= x^d + c_{d-1} x^{d-1} + \cdots + c_1 x + 1 \quad (\because c_d = 1) \end{aligned}$$

이다. 그리고 여기서

$$\begin{aligned} c_{d-1} &= -\alpha^{-1} - (\alpha^{-1})^q \cdots - (\alpha^{-1})^{q^{d-1}} \\ &= -Tr_F^E(\alpha^{-1}) \end{aligned}$$

이다. 따라서 〈정리 5.1.7〉의 ③과 〈보조정리 5.1.8〉에 의해서 다음이 성립한다.

$$\begin{aligned} Tr_F^K(\alpha^{-1}) &= Tr_F^E(Tr_E^K(\alpha^{-1})) \\ &= Tr_F^E\left(\frac{n}{d} \alpha^{-1}\right) \\ &= \frac{n}{d} Tr_F^E(\alpha^{-1}) \\ &= \frac{n}{d} (-c_{d-1}) \end{aligned}$$

## 5.2 Trace를 이용한 이차방정식의 풀이

이차방정식  $Ax^2+Bx+C=0$  의 해는 일반적인 공식,

$x = \frac{-B \pm \sqrt{B^2 - 4AC}}{2A}$  을 이용하여 구할 수 있으나  $GF(2)$  에서는 이 공식이 성립하지 않는다. 따라서  $GF(2)$  에서 이차방정식의 해를 구하는 방법을 찾는 것이 필요하며 이것은 trace를 이용하여 알아낼 수 있다.  $GF(2)$  에서의 해를 구하는 방법을 찾기 위해서 먼저  $GF(q)$ 에서의 몇 가지 정리들을 살펴보면 다음과 같다.

〈정리 5.2.1[12]〉  $F=GF(q)$  ,  $K=GF(q^n)$  라 하자.  $Tr(a)=0$  일 필요충분조건은 다음을 만족하는  $K$  의 원소  $\beta$  가 존재하는 것이다.

$$\alpha = \beta - \beta^q \quad (5.6)$$

〈보조정리 5.2.1[12]〉  $\alpha$  ,  $\theta$  가  $K$  의 원소일 때,  $\beta$  가 다음과 같다고 하자.

$$\beta = \alpha \theta^q + (\alpha + \alpha^q) \theta^{q^2} + \dots + (\alpha + \alpha^q + \dots + \alpha^{q^{n-2}}) \theta^{q^{n-1}} \quad (5.7)$$

그러면 다음이 성립한다.

$$\beta - \beta^q = \alpha(Tr(\theta) - \theta) - \theta(Tr(\alpha) - \alpha) \quad (5.8)$$

〈정리 5.2.2[12]〉  $\theta$  를  $Tr(\theta)=1$  인  $K$  의 고정된 원소라 하자.

만약  $Tr(\alpha)=0$  이면  $\beta - \beta^q = \alpha$  이다.

이제,  $F=GF(2)$ ,  $K=GF(2^n)$ 이라 하자. 그러면 식 (5.7)의  $\beta$  는 다음과 같이 표현된다.

$$\begin{aligned}\beta &= \alpha\theta^2 + (\alpha + \alpha^2)\theta^4 + \cdots + (\alpha + \alpha^2 + \cdots + \alpha^{2^{n-2}})\theta^{2^{n-1}} \\ &= \sum_{i=0}^{n-1} \left( \sum_{j=0}^{i-1} \alpha^{2^j} \right) \theta^{2^i}\end{aligned}\quad (5.9)$$

그리고 홀수인 모든  $n$ 에 대하여  $\text{Tr}(1)=1$ 이므로 (5.9)에서  $\theta=1$ 이라 둘 수 있다.

이때  $\beta$ 는 다음과 같이 간단해 진다.

$$\begin{aligned}\beta &= \alpha^2 + \alpha^8 + \cdots + \alpha^{2^{n-2}} \\ &= \sum_{i=0}^{(n-1)/2} \alpha^{2^{2i-1}}\end{aligned}\quad (5.10)$$

또한  $\alpha$ 가  $K$ 의 고정된 원소일 때, 방정식  $x^2+x=\alpha$ 가 해를 가질 필요충분조건은  $\text{Tr}(\alpha)=0$ 인 것이다. 그리고 하나의 해가  $\beta$ 라면 분명히 다른 하나의 해는  $\beta+1$ 이다.

다음은 trace를 이용하여 이차합동식의 해를 구하는 예이다.

〈예 5.2.1〉  $K=GF(2^4)$ 라 하자. 그리고  $\alpha$ 는  $f(x)=x^4+x+1$ 을 만족하는 하나의 해라고 하자. 그러면 이 체의 구조는 다음과 같다.

<표 5.1> GF(24)의 구조

| $i$ | $\alpha^i$ |
|-----|------------|
| 0   | 0 0 0 1    |
| 1   | 0 0 1 0    |
| 2   | 0 1 0 0    |
| 3   | 1 0 0 0    |
| 4   | 0 0 1 1    |
| 5   | 0 1 1 0    |
| 6   | 1 1 0 0    |
| 7   | 1 0 1 1    |
| 8   | 0 1 0 1    |
| 9   | 1 0 1 0    |
| 10  | 0 1 1 1    |
| 11  | 1 1 1 0    |
| 12  | 1 1 1 1    |
| 13  | 1 1 0 1    |
| 14  | 1 0 0 1    |

이제, 방정식

$$y^2 + y = \gamma$$

를 생각하자. 여기서  $\gamma$ 는 주어진  $K$ 의 원소이다.

이 방정식이 해를 가질 필요충분조건은  $Tr(\gamma) = 0$ 인 것이다. 만약,  $\gamma_i$ 가  $GF(2)$ 의 원소이면

$$\begin{aligned}\gamma &= \gamma_3 \alpha^3 + \gamma_2 \alpha^2 + \gamma_1 \alpha + \gamma_0 \\ &= (\gamma_3, \gamma_2, \gamma_1, \gamma_0)\end{aligned}$$

이다. <예 5.1.1>에서

$$Tr(1) = 0$$

$$Tr(\alpha) = Tr(\alpha^2) = 0$$

$$Tr(\alpha^3) = 1$$

이므로

$$Tr(\gamma) = \gamma_3$$

이다. 따라서 주어진 방정식은

$\gamma_3 = 0$ 일 때 즉,  $\gamma = 0$ 이거나  $\gamma = \alpha^0, \alpha^1, \alpha^2, \alpha^4, \alpha^5, \alpha^8, \alpha^{10}$ 일 때 해를 갖는다.

방정식을 풀기 위해 trace가 1인 원소  $\theta$ 가 필요하다. [표 5.1]에서  $Tr(\alpha^3) = 1$ 이므로  $\theta = \alpha^3$ 라 두자. 그러면,

$$\begin{aligned}y &= \gamma \theta^2 + (\gamma + \gamma^2) \theta^4 + (\gamma + \gamma^2 + \gamma^4) \theta^8 \\ &= \gamma(\theta^2 + \theta^4 + \theta^8) + \gamma^2(\theta^4 + \theta^8) + \gamma^4 \theta^8\end{aligned}$$

이다.  $\theta = \alpha^3$ 이므로

$$\begin{aligned}\theta^2 + \theta^4 + \theta^8 &= \alpha^6 + \alpha^{12} + \alpha^{24} = \alpha^6 + \alpha^{12} + \alpha^9 = \alpha^3 + 1 \\ \theta^4 + \theta^8 &= \alpha^{12} + \alpha^{24} = \alpha^{12} + \alpha^9 = \alpha^2 + 1 \\ \theta^8 &= \alpha^{24} = \alpha^9 = \alpha^3 + \alpha\end{aligned}$$

이다.

그러므로  $T\gamma(\gamma)=0$  일 때

$$y = \gamma(\alpha^3 + 1) + \gamma^2(\alpha^2 + 1) + \gamma^4(\alpha^3 + \alpha)$$

이다.

$\gamma$ 에서  $y$ 로의 사상은 선형이므로 일반적인 행동을 기술하기 위해서는 basis인  $1, \alpha, \alpha^2, \alpha^3$ 에서의 행동만 기술하면 된다.

$$\gamma = 1 : y = \alpha^2 + \alpha = (0, 1, 1, 0)$$

$$\gamma = \alpha : y = \alpha^3 + \alpha + 1 = (1, 0, 1, 1)$$

$$\gamma = \alpha^2 : y = \alpha^3 + 1 = (1, 0, 0, 1)$$

$$\gamma = \alpha^3 : y = 1 = (0, 0, 0, 1)$$

그러므로  $\gamma = (\gamma_3, \gamma_2, \gamma_1, \gamma_0)$  일 때,  $y^2 + y = \gamma$ 의 해는 다음과 같다.

$$y = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \cdot \begin{pmatrix} \gamma_3 \\ \gamma_2 \\ \gamma_1 \\ \gamma_0 \end{pmatrix}$$

예를 들어,  $y^2 + y = \alpha^{10} = (0, 1, 1, 1)$ 의 해는

$$y = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \cdot \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \alpha^2$$

이다. 구한 해가 맞는지 확인해 보자.

$$y^2 + y = \alpha^4 + \alpha^2 = \alpha^{10}$$

$y^2 + y = \alpha^{10}$ 의 나머지 한 해는 다음과 같다.

$$\alpha^2 + 1 = (0, 1, 0, 1) = \alpha^8$$

### 5.3 부분다항식을 구하는 알고리즘

이제 trace를 이용하여 4장에서의 이차함동식 (4. 4)의 해  $\Delta_{1, n-1}$ 을 실제적으로 구하는 방법을 살펴본다.  $\Delta_{1, n-1}$ 을 구하는 알고리즘은 다음과 같다.

$p(x)$ 가 주어진 특성다항식이다.

제 1단계 :  $f = (x^2 + x)p'(x)$ 와  $\alpha = (\frac{1}{f})^2$ 를 계산한다.

제 2단계 :  $n$ 이 짝수이면

trace가 1인  $\theta$ 를 찾는다

식 (5. 9)을 통해서  $\beta$ 를 계산한다

$n$ 이 홀수이면

식 (5. 10)을 통해서  $\beta$ 를 계산한다

제 3단계 :  $q = \beta f$ 라 하고  $\gcd(p, q)$ 를 계산한다

제 4단계 : 몫의 상수항만 취하여 역으로 둔다.

다음은 trace를 이용하여  $\Delta_{1, n-1}$ 을 실제로 구하는 예이다.

〈예 5.3.1〉

①  $p = x^5 + x^2 + 1$  이라 하자( $n=5$ ). 그러면

$$p' = 5x^4 + 2x^2 = x^4$$

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

$$\frac{1}{f} = x^3 + x^2 + 1$$

$$\alpha = (\frac{1}{f})^2 = (x^3 + x^2 + 1)^2 = x^6 + x^4 + 1 = x^4 + x^3 + x + 1$$

이다. 여기서  $n=5$  이므로  $\beta$ 는 다음과 같다.

$$\begin{aligned}\beta &= \sum_{i=0}^2 a^{2^{i+1}} = a^2 + a^8 \\ &= x^4 + x\end{aligned}$$

따라서

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

이다. 이제  $p$  와  $q$  에 유클리드 호제법을 적용하면 된다.

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

여기서 뺀  $[x, x+1, x+1, x+1, x+1]$  이고 상수항만 취해서 역으로 세우면 CA의 rule인  $[1, 1, 1, 1, 0]$  이 구해진다.

②  $p = x^6 + x + 1$  이라 하자 ( $n=6$ ). 그러면

$$\begin{aligned}p' &= 1 \\ f &= (x^2 + x)(1) = x^2 + x \\ \frac{1}{f} &= x^4 + x^3 + x^2 + x + 1\end{aligned}$$

$$\begin{aligned}
\alpha &= \left(\frac{1}{f}\right)^2 = (x^4 + x^3 + x^2 + x + 1)^2 \\
&= x^8 + x^6 + x^4 + x^2 + 1 \\
&= x^4 + x^3 + x
\end{aligned}$$

이다. 여기서  $n=6$ 이므로  $\beta$ 는 다음과 같다.

$$Tr(\alpha^5) = 1 \text{ 이므로 } \theta = \alpha^5 \text{ 라 두자.}$$

그러면, <예 4.2.1>과 같은 방법으로

$$\begin{aligned}
\beta &= \begin{vmatrix} 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \end{vmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} \\
&= x^4 + x + 1
\end{aligned}$$

따라서

$$\begin{aligned}
q &= \beta f \\
&= (x^4 + x + 1)(x^2 + x) \\
&= x^5 + x^3 + 1
\end{aligned}$$

이다.

이제  $p$ 와  $q$ 에 유클리드 호제법을 적용하면 된다.

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

여기서 뭉은  $[x, x, x, x+1, x+1, x]$  이고 상수항만 취해서 역으로 세우면 CA의 rule인  $[0, 1, 1, 0, 0, 0]$ 이 구해진다.

③  $p = x^4 + x^3 + x^2 + x + 1$  이라 하자 ( $n=4$ ). 여기서,  $p$ 는 원시다항식이 아니다. 따라서  $\alpha$ 는 원시근이 아니다. 원시근을 구하기 위하여 가우스 알고리즘을 사용하게 되는데 다음과 같다.

### 가우스 알고리즘

1.  $i = 1, \alpha_i \in F, \text{ord}(\alpha_i) = t_i$
2. 만약  $t_i \neq q-1$ 이라면 그때의  $\alpha_i$ 는 원시근이다.
3. 이면  $\alpha_i$ 의 거듭제곱이 아닌  $\omega (\neq 0) \in F$ 를 선택하여  $\text{ord}(\omega) = s$ 라 두자.  
 $s = q-1$ 이면  $\alpha_{i+1} = \omega$ 라 두면 된다.
4.  $s \neq q-1$ 이라면  $\gcd(d, e) = 1, d \cdot e = \text{lcm}(t_i, s)$ 인  $d|t_i$ 이고  $e|s$ 를 찾는다.  
 $t_{i+1} = \text{lcm}(t_i, s), \alpha_{i+1} = \alpha^{t_i/d} \cdot \omega^{s/e}$ 라 두고  $i$ 를 1씩 증가시킨다.

가우스 알고리즘에 의해 원시근을  $\omega = \alpha + 1$ 로 하여 체를 구성하면 다음과 같이 원시다항식으로 구성된 체의 형태가 된다.

<표 5.2> GF(24)의 구조

| $i$ | $\alpha^i$ | $\omega^i$ |
|-----|------------|------------|
| 0   | 0 0 0 1    | 0 0 0 1    |
| 1   | 0 0 1 0    | 0 0 1 1    |
| 2   | 0 1 0 0    | 0 1 0 1    |
| 3   | 1 0 0 0    | 1 1 1 1    |
| 4   | 1 1 1 1    | 1 1 1 0    |
| 5   | 0 0 0 1    | 1 1 0 1    |
| 6   | 0 0 1 0    | 1 0 0 0    |
| 7   | 0 1 0 0    | 0 1 1 1    |
| 8   | 1 0 0 0    | 1 0 0 1    |
| 9   | 1 1 1 1    | 0 1 0 0    |
| 10  | 0 0 0 1    | 1 1 0 0    |
| 11  | 0 0 1 0    | 1 0 1 1    |
| 12  | 0 1 0 0    | 0 0 1 0    |
| 13  | 1 0 0 0    | 0 1 1 0    |
| 14  | 1 1 1 1    | 1 0 1 0    |

$$p' = x^2 + 1$$

$$f = (x^2 + x)(x^2 + 1) = 1$$

$$\frac{1}{f} = 1$$

$$\alpha = \left(\frac{1}{f}\right)^2 = 1$$

이다. 여기서  $n=4$  이므로  $\beta$  는 다음과 같다.

$$Tr(\omega) = 1 \text{ 이므로}$$

$$\begin{aligned} \beta &= \alpha\theta^2 + (\alpha + \alpha^2)\theta^4 + (\alpha + \alpha^2 + \alpha^4)\theta^8 \\ &= \omega^2 + \omega^8 \\ &= x^3 + x^2 \end{aligned}$$

따라서

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

이다.

이제  $p$  와  $q$  에 유클리드 호제법을 적용하면 된다.

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

여기서 뺀  $[x, x, x+1, x]$  이고 상수항만 취해서 역으로 세우면 CA의 rule인  $[0, 1, 0, 0]$  이 구해진다.

## 6. 결론

본 논문에서는 1차원 셀룰라 오토마타의 경계조건에 따른 세 종류의 CA에 대해서 살펴보고 각각의 특성다항식을 구하였으며, 그 특성다항식의 여러 가지 성질들을 조사하였다.

그리고, 기약다항식에 관한 성질과 CA와의 관련성에 대해서도 살펴보았다.

이차합동식을 만족하는 부분다항식을 구하면 주어진 특성다항식과 부분다항식에 유클리드 호제법을 반복적으로 적용하여 CA의 rule을 합성해 낼 수 있음을 알 수 있었으며, 이차합동식을 만족하는 부분다항식을 구하기 위하여 trace를 이용한 몇 가지 정리를 얻고 부분다항식을 구하는 알고리즘과 그 예를 제시하였다.

## 참 고 문 헌

- [1] P.H. Bardell, "Analysis of cellular automata used as pseudo-random pattern generators", Proc. IEEE int. Test. Conf., 1990.
- [2] K.M. Cattell and J.C. Muzio, "A linear cellular automata algorithm : Theory", 1991.
- [3] K.M. Cattell and J.C. Muzio, "Synthesis of one-dimensional linear hybrid cellular automata", IEEE Trans. Computer-Aided Design, Vol. 15, No. 3, 1996.
- [4] S.J. Cho, H.D. Kim and U.S. Choi, "Behavior of Complemented CA Whose Complement Vector is Acyclic in a Linear TPMACA", Mathematical and Computer Modelling, Vol. 36, 2002, pp. 980-986.
- [5] S.J. Cho, H.D. Kim and U.S. Choi, "Analysis of complemented CA derived from a linear TPMACA" Computers & Mathematics with Applications, Vol. 45, 2003, pp. 689-698.
- [6] P.P. Chaudhuri, D.R. Chowdhury, S. Nandi and S. Chattopadhyay, Additive cellular automata : Theory and applications, Vol. 1, IEEE, 1997.
- [7] D.R. Chowdhury, S. Basu, I.S. Gupta and P.P. Chaudhuri, "Design of CAUCC-cellular automata based error correcting code", IEEE Trans. Comput., Vol. 43, 1994.
- [8] T. Damala and A. Sathaye, "Application of one-dimensional cellular automata and linear feedback shift registers for pseudo-exhaustive testing", IEEE Trans. Computer-Aided Design, Vol. 12, 1993.
- [9] A.K. Das and P.P. Chaudhuri, "Vector space theoretic analysis of additive cellular automata and its application for pseudo-exhaustive test pattern generation", IEEE Trans. Comput., Vol. 42, 1993.
- [10] F.R. Gantmacher, "The theory of matrices, Vol. 1, Chelsea Publishing Co.", New York, 1959
- [11] R. Lidl and H. Niederreiter, "Introduction to finite fields and their applications", Cambridge University Press, 1994.
- [12] R.J. McEliece, "Finite fields for computer scientists and engineers", Kluwer Academic

Publishers, 1987.

- [13] A.J. Menezes, "Applications of finite fields, Kluwer Academic Publishers", 1993.
- [14] S. Nandi and P.P. Chaudhuri, "Analysis of periodic and intermediate boundary 90/150 cellular automata", IEEE Trans. Comput, Vol. 45, No. 1, 1996.
- [15] J.V. Neumann, "Theory of self-reproducing automata", University of Illinois Press Urbana, 1966.
- [16] M. Serra, T. Slater, J.C. Muzio and D.M. Miller, "Analysis of one-dimensional cellular automata and their aliasing properties", IEEE Trans. Computer-Aided Design, vol. 9, 1990.
- [17] S. Wolfram, "Statistical mechanics of cellular automata", Rev. Modern Physics, Vol.55, No. 3, 1983.