1차원 셀룰라 오토마타의 특성다항식에 관한 연구

°조 성 진, 윤 세 영, 최 언 숙
부경대학교 응용수학과

Characteristic polynomials of one-dimensional cellular automata

Sung-Jin Cho, Se-Young Yoon, Un-Sook Choi

Department of Applied Mathematics
Pukyoung National University

세가지 경계조건에 따른 셀룰라 오토마타의 특성다항식을 구하고 이 특성다항식의 성질을 연구한다. 특히 IBCA의 특성다항식과 NBCA의 특성다항식과의 관계를 제시한다.

1. 서론

LFSR의 대안으로서 제시된 CA는 test pattern generation, pseudo-random numbergeneration, cryptography, error correcting codes, signature analysis 등 많은 분야에서 응용된다[1, 3, 5, 7, 8]. 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. 주어진 특성다항식으로부터 그에 대응하는 CA를 역으로 찾아내기 위해서는 CA이차합동식의 풀이가 핵심이며 CA이차합동식의 해에 유클리드 호제법을 적용함으로써 CA를 합성해 낼 수 있다[3]. 본 논문에서는 CA의 경계조건에 따른 세가지 분류에 따라 특성다항식을 구하고, 구해진 특성다항식들의 성질들을 제시한다. 특히 IBCA의 특성다항식이 NBCA의 특성다항식으로서 표현가능하며 NBCA처럼 유클리드 호제법을 만족함을 보인다.

2. NBCA(Null Boundary CA)

$GF(2)$상에서의 CA에 대해서만 고려한다. n개의 셀로 구성된 NBCA의 전이행렬은 다음과 같다. 여기서 d_i는 i번째 셀이 rule 90을 쓰면 0, rule 150을 쓰면 1이다.

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

그리고 NBCA의 특성다항식을

$$|xI - A|$$

라고 정의한다. 여기서 A는 n개의 셀로 이루어진 1-D NBCA의 $n \times n$ 전이행렬이고 I는 n차 단위행렬이다.

M_{ij}는 i번째부터 j번째 셀로 이루어진 NBCA이고 M_{ij}의 특성다항식은 Δ_{ij}로 표시하기로 한다. $\Delta_{1,n-1}$, $\Delta_{2,n}$, $\Delta_{i,j}$을 CA의 subpolynomial이라고 정의한다.
NBCA의 특성다항식은 다음 점화관계식을 만족한다[3].

<정리 2.1>

$$\Delta_{-1} = 0$$

$$\Delta_0 = 1$$

$$\Delta_{1,k} = (x + d_k)\Delta_{1,k-1} + \Delta_{1,k-2}, \quad k > 0$$

이 점화관계식은 유클리드 호제법을 만족한다. 여기서 중요한 사실은 몫이 항상 일차인 것이다. $\Delta_{1,n}$과 $\Delta_{1,n-1}$을 알고 있다고 가정하면 유클리드 호제법의 반복적 적용으로 특성다항식으로부터 CA의 rule을 찾을 수 있다[3]. $\Delta_{1,n-1}$와 $\Delta_{2,n}$은 CA의 서로 다른 subpolynomial들이며 이들은 다음 이차합동식을 만족한다는 것이다[2, 3]. 단, 여기서 $\Delta_{1,n}$은 기약다항식이다.

<정리 2.2> CA 이차합동식
어떤 CA의 특성다항식이 $\Delta_{1,n}$이고 subpolynomial은 $\Delta_{1,n-1}$, $\Delta_{2,n}$이라 하자. 그러면 $y = \Delta_{1,n-1}$과 $y = \Delta_{2,n}$은 다음 이차합동식을 만족한다.

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

3. PBCA(Periodic Boundary CA)

PBCA의 전이행렬은 다음과 같다.

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

다음 정리들은 [3]에 제시되어 있다.

<정리 3.1> PBCA의 특성다항식과 NBCA의 특성다항식의 관계는 다음과 같다.

$$\Phi_{1,n} = \Delta_{1,n} + \Delta_{2,n-1}$$

<정리 3.2> PBCA의 n개의 셀 중 $d_1 = d_n$이면 다음 관계식이 성립한다.

$$\Phi_{1,n} = (x + d_1)\Phi_{2,n} + \Phi_{2,n-1}$$

<정리 3.3> PBCA가 짝수개의 셀로 구성되어 있고 인접한 셀들이 같은 rule을 쓰지 않는다면 다음 관계식이 성립한다.

$$\Phi_{1,n} = x(x + 1)\Phi_{3,n} + \Phi_{5,n}$$

4. IBCA(Intermediate Boundary CA)

CA의 응용분야에서 최대길이를 갖는 CA를 찾는 것이 중요하다. 최대길이를 갖는 CA를 찾는데 있어서 NBCA와 PBCA는 제한점이 있기 때문에 새롭게 제시된 것이 IBCA이다. IBCA의 전이행렬은 다음과 같다.

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

<정리 4.1> IBCA의 특성다항식은 다음과 같이 NBCA의 특성다항식을 이용하여 나타낼 수 있다. 단, IBCA의 셀의 개수는 7개 이상인 것으로 가정한다.

$$\Psi_{1,n} = \Delta_{1,n} + \Delta_{1,n-3} + \Delta_{4,n} + \Delta_{4,n-3}$$

<정리 4.2> IBCA의 첫 번째와 네 번째의 셀이 같은 rule을 사용할 때, 즉 $d_1 = d_4$ 일 때 IBCA의 특성다항식은 다음 관계식을 만족한다.

$$\Psi_{1,n} = a_1 \Psi_{2,n} + \Psi_{3,n}$$

정리 4.2에 의하여 IBCA가 특정한 조건 ($d_1 = d_4$)하에서는 유클리드 호제법을 만족함을 알 수 있다. 이는 IBCA에 대해서도 이차합동식의 해를 구할 수 있음을 보여준다.

<정리 4.3> 각 셀의 rule이 90과 150로만 이루어진 IBCA에서 두 번째 셀과 $n-1$ 번째 셀의 rule이 90이면 같은 특성다항식을 갖는 NBCA가 존재한다.

5. 결론

본 논문에서는 1차원 셀룰라 오토마타의 경계조건에 따른 세 종류의 CA에 대해서 살펴보고 각각의 특성다항식을 구하였다. 그리고 그 특성다항식의 여러 가지 특성들을 살펴보았다. 또, IBCA의 경우에 첫번째와 네번째 셀의 rule이 같다는 조건하에서 그 특성다항식이 유클리드 호제법을 만족함을 밝혔다.

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] P. P. Chaudhuri, D. R. Chowdhury, S. Nandi and S. Chattopadhyay, *Additive cellular automata : Theory and applications*, Vol. 1, IEEE, 1997.

[5] A. K. Das and P. P. Chaudhuri, *"Vector space theoritic analysis of additive cellular automata and its application for pseudo-exhaustive test pattern generation"*, IEEE Trans. Comput., Vol. 42, 1993.

[6] F. R. Gantmatcher, *The theory of matrices*, Vol. 1, Chelsea Publishing Co., New York, 1959.

[7] S. Nandi and P. P. Chaudhuri, *"Analysis of periodic and intermediate boundary 90/150 cellular automata"*, IEEE Trans. Comput, Vol. 45, No. 1, 1996.

[8] M. Serra, T. Slater, J. C. Muzio and D. M. Miller, *"Analysis of one-dimen sional cellular automata and their aliasing properties"*, IEEE Trans. Computer-Aided Design, vol. 9, 1990.