90/150 그룹 CA의 특성다항식 분석

조성진*· 김경자* · 최언숙** ·황윤희* · 김한두***

*부경대학교 · **동명대학교 · ***인제대학교

Analysis of Characteristic Polynomials of 90/150 Group CA

Sung-Jin Cho* · Kyung-Ja Kim* · Un-Sook Choi** · Yoon-Hee Hwang* · Han-Doo Kim***

*Pukyong National Univ. · **Tongmyong Univ. · ***Inje Univ.

E-mail : sjcho@pknu.ac.kr

요 약

본 논문에서는 전이규칙으로 90, 150 규칙만을 사용하는 90/150 셀룰라 오토마타의 특성다항식을 분석한다. 특히 최대길이를 갖는 90/150 CA를 합성하여 CA의 특성다항식이 원시다항식의 지수승 형태를 갖는 방법을 제안한다.

ABSTRACT

In this paper, we analyze the characteristic polynomials of 90/150 cellular automata which uses only 90, 150 rules as state-transition rules. In particular, we propose the method which the characteristic polynomial is represented as the exponential type of a primitive polynomial by synthesizing 90/150 CA.

키워드

셀룰라 오토마타, 특성다항식, 전이규칙, 원시다항식, 전이행렬

I. 서 론

셀룰라 오토마타(CA)는 셀이라 불리는 메모리의 배열로서, 셀의 상태가 자기 자신 및 인접한 셀 상태의 국소적인 상호작용에 의해서 동시에 갱신되는 시스템이다. 간단하고, 규칙적이며, 작은 단위로 확장 연결할 수 있는 구조를 가진 CA는 스스로 조직화하고 재생산할 수 있는 모델로 von Neumann[1]에 의해 처음 소개되었고, 1980년대에 Wolfram[2]은 처음으로 암호학에 CA를 도입하였다. 이후 Das[3] 등에 의해서 행렬 대수학으로 분석이 이루어 졌다. 특히 Chaudhuri 등은 여러 가지 경계조건을 가지는 90/150 CA에 대해 분석하였으며[4], Cattell 등은 1차원 CA의 합성에 관한 연구를 하였다[5].
특히 Cho 등은 CA의 상태행동분석에 대하여 연구를 하였고[6,7], 90/150 CA의 위상이동차에 대한 연구를 하였다[8].

* 본 연구는 한국과학재단 목적기초연구지원 사업(R01-2006-000-10260-0)에 의해 수행되었음.

II. 셀룰라 오토마타의 소개

CA란 동역학계를 해석하는 한 방법으로 공간과 시간을 이산적으로 다루는 시스템이며, 셀룰라 공간(cellular space)의 기본 단위인 각 셀(cell)이 취할 수 있는 상태를 유한하게 처리하며, 각 셀들의 상태가 국소적인 상호작용에 의해서 동시에 갱신되는 시스템이다. 가장 간단한 구조를 가지는

1차원 CA(1-D CA)에서는 모든 셀들이 선형으로 배열되어 있고 1-D CA 중에서 국소적 상호작용이 세 개의 셀, 즉 자신과 인접한 두 셀에 의해 이루어지는 CA를 3-이웃(3-neighborhood) CA라 한다. 본 논문에서 다루는 CA는 3-이웃 1-D CA이다.

CA의 3-이웃 상태전이 함수는 다음과 같다.

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

여기서 f는 결합 논리를 가지는 국소전이 함수이다. i는 일차원으로 배열되어 있는 각 셀들의 위치이고 t는 시간 단계이며 $q_i(t)$는 시간 t에서 i번째 셀의 상태, $q_i(t+1)$는 시간 $t+1$에서 i번째 셀의 상태를 말한다.

[CA의 Rule]

GF(2) 상에서 3-이웃 CA에는 서로 다른 2^3개의 이웃의 배열상태가 있으며 그러한 CA에 대응하는 상태전이 함수는 2^{2^3}개이다. 본 논문에서 사용하는 CA의 전이규칙에 대한 결합논리는 다음 표와 같은 식으로 표현될 수 있다.

표1. CA 전이규칙

전이규칙	선형 CA의 전이규칙
60	$q_i(t+1) = q_{i-1}(t) \oplus q_i(t)$
90	$q_i(t+1) = q_{i-1}(t) \oplus q_{i+1}(t)$
102	$q_i(t+1) = q_i(t) \oplus q_{i+1}(t)$
150	$q_i(t+1) = q_{i-1}(t) \oplus q_i(t) \oplus q_{i+1}(t)$
170	$q_i(t+1) = q_{i+1}(t)$
204	$q_i(t+1) = q_i(t)$
240	$q_i(t+1) = q_{i-1}(t)$

[CA의 종류]

CA는 적용되는 전이규칙의 논리에 따라 가산 CA(Additive CA), 비가산 CA(Nonadditive CA)로 분류된다. 각 셀에 적용된 전이규칙이 XOR 논리로만 이루어진 CA를 선형 CA라고 한다. 선형 CA의 상태전이 함수는 행렬로 표현될 수 있는데 이 행렬을 전이행렬이라 한다. 또한 셀에 적용되는 전이규칙이 XNOR과 XOR논리로 이루어진 CA를 여원 CA(Complemented CA)라 하고 선형 CA와 여원 CA를 가산 CA라 한다. 셀들의 전이규칙이 AND-OR논리로 이루어진 CA를 비가산 CA라 한다.

CA의 전이규칙에 의해 변화되는 상태를 나타낸 상태전이 그래프의 형태에 따라 그룹 CA와 비그룹 CA로 분류할 수 있다. 그룹 CA는 모든 셀들의 상태가 몇 개의 사이클을 이루며 반복되는 CA로 임의의 한 상태에 대한 이전상태가 유일하다. 비그룹 CA는 한 개, 또는 몇 개의 트리구조를 이루며 이전상태가 유일하지 않다.

CA에서 가장 왼쪽과 오른쪽 셀은 2개의 이웃만 가지므로 세 번째 이웃의 상태인 경계조건을 결정해 주어야 한다. 본 논문에서는 제일 왼쪽과 오른쪽 셀들이 0상태에 연결되어 있는 NBCA (Null Boundary CA)에 대해서만 다룬다.

[특성다항식과 최소다항식]

선형 CA는 전이규칙에 따라 행렬로 표현할 수 있는데 그러한 행렬을 T 라고 하자. 전이행렬이 T 인 CA의 특성다항식 $c(x)$는 다음과 같다.

$$c(x) = |T + xI| \quad (I\text{는 단위행렬})$$

전이행렬 T 의 특성다항식 $c(x)$의 인수 중에서 T 를 근으로 갖는 가장 낮은 차수의 다항식을 최소다항식(minimal polynomial)이라 한다.

III. 합성된 90/150 CA의 특성다항식 분석

전이규칙 90과 150으로만 이루어진 선형 CA를 90/150 CA라 하고, 본 논문에서 언급되는 n셀 90/150 NBCA의 전이행렬은 다음과 같은 삼중대각행렬(tridiagonal matrix)로 나타낼 수 있다.

$$T = \begin{pmatrix} a_1 & 1 & 0 & \cdots & 0 & 0 \\ 1 & a_2 & 1 & \cdots & 0 & 0 \\ 0 & 1 & a_3 & \cdots & 0 & 0 \\ & & \cdots & & & \\ 0 & 0 & 0 & \cdots & 1 & a_n \end{pmatrix}$$

$$(a_1, a_2, \cdots, a_n \in \{0,1\})$$

여기서 a_i는 i번째 셀에 적용된 전이규칙이 90인 경우는 0이고, 150인 경우는 1이다.

$R = \langle a_1, a_2, \cdots, a_n \rangle$를 CA의 전이규칙이라 한다.

S_t가 시간 t에서 CA의 상태라 하면, 시간 $t+1$에서 CA의 상태는 $S_{t+1} = TS_t$이다. 또한 p단계 후의 CA의 상태는 $S_{t+p} = T^p S_t$이다.

<정리 1[5]> 90/150 CA의 전이행렬 T 에 대한 특성다항식과 최소다항식은 같다.

<Remark> n셀 90/150 CA의 전이행렬 T에 대한 특성다항식을 $\Delta_{1,n}$이라 표기한다. $\Delta_{k,m}$은 k번째 셀부터 m번째 셀까지의 전이규칙에 대

응하는 T의 부분행렬에 대한 특성다항식을 나타낸다. R은 주어진 CA의 전이규칙이다.

<예1> $R=\langle 0,0,1,0,1\rangle$이면 전이행렬은 다음과 같다.

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

이때 $\Delta_n = x^5+x^3+x^2$이고 $\Delta_{2,4}=x^3+x^2$이다.

n셀 그룹 CA에서 주기가 2^n-1인 CA를 최대길이를 갖는 CA라 한다. 최대길이를 갖는 임의의 두 90/150 CA CA_1과 CA_2에 대하여 대응하는 전이행렬을 각각 T_1과 T_2라 하자. 그리고 이 두 CA를 합성한 90/150 CA의 전이행렬을 T'이라 하자. 정리 1에 의해 T'의 특성다항식과 최소다항식은 같다. 90/150 CA의 합성에는 다음과 같은 경우들을 고려할 수 있다.

ⓐ 크기가 서로 다른 CA_1과 CA_2의 합성
ⓑ 크기는 같고 특성다항식이 다른 CA_1과 CA_2의 합성
ⓒ 동일한 두 90/150 CA의 합성

또한 두 90/150 CA를 합성할 때, CA_1과 CA_2의 전이규칙을 바꾸지 않고 합성하는 경우와 CA_1의 마지막 셀의 전이규칙을 90(150)에서 240(60)으로 바꾸거나 CA_2의 첫 번째 셀의 규칙을 90(150)에서 170(102)으로 바꾸어 합성하는 경우가 있다.

합성된 CA의 전이행렬 T'은 다음과 같은 형태를 갖는다.

$$T'=\begin{pmatrix}T_1 & A\\ B & T_2\end{pmatrix}$$

두 CA의 전이행렬을 바꾸지 않은 경우는 T'이 삼중대각행렬이고, CA_1의 마지막 셀의 전이규칙을 바꾸게 되면 $A=O$이고, CA_2의 처음 셀의 전이규칙을 바꾸게 되면 $B=O$이다. 합성된 90/150 CA의 전이행렬 T'의 특성다항식을 Δ'이라 하면 다음 정리는 ⓐ,ⓑ의 경우에 대한 Δ'을 특성화한다.

<정리 2> 특성다항식이 서로 다른 최대길이를 갖는 두 90/150 CA에 대하여 CA_1의 특성다항식을 Δ^1이라 하고 CA_2의 특성다항식을 Δ^2라 하면 합성된 CA의 특성다항식 Δ'은 다음과 같다.

$$\Delta' = \Delta^1 \cdot \Delta^2$$

<예2> 크기가 다른 CA_1과 CA_2의 합성 CA_1의 전이규칙이 $R_1=\langle 1,1,0\rangle$이고, CA_2의 전이규칙이 $R_2=<1,0,1,0>$이라 하자. 그러면 두 CA의 특성다항식은 다음과 같다.

$$\Delta^1 = x^3+x+1,\ \Delta^2 = x^4+x+1$$

또한 합성된 CA의 특성다항식 Δ'은 다음과 같다.

$$\begin{aligned}\Delta' &= x^7+x^4+x^3+x^2+1\\ &= (x^3+x+1)(x^4+x+1)\\ &= \Delta^1\cdot\Delta^2\end{aligned}$$

이제, ⓒ의 경우인 동일한 두 90/150 CA의 합성의 경우에 대해 살펴보자. 예를 들어 전이규칙이 $R=\langle 1,0,1,1\rangle$인 CA 두 개를 합성할 때 전이규칙을 바꾸지 않고 합성하게 되면 합성된 CA의 전이행렬 T'은 대각성분이 <1, 0, 1, 1, 1, 0, 1, 1>인 삼중대각행렬이 된다. 그리고 T'의 특성다항식은 다음과 같다.

$$\Delta' = x^8+x^3+x^2+x+1$$

만약 CA_1의 마지막 셀의 규칙 또는 CA_2의 첫 번째 셀의 규칙을 바꾸었을 때 T'에서 블록 행렬 A와 B중 적어도 하나가 영행렬이 되고 특성다항식은 $\Delta' = (x^4+x^3+1)^2$이다. 여기서 $\Delta^1=\Delta^2=x^4+x^3+1$이다.

다음은 위 예와 같이 합성된 CA의 특성다항식이 원시다항식의 거듭제곱 형태가 되도록 하는 90/150 CA의 합성규칙을 제안한다.

<정의> CA의 규칙이 $R=\langle a_1,a_2,\cdots,a_n\rangle$이라 할 때 합성 CA의 규칙 R'은 다음과 같고 이를 **대칭전이규칙**이라고 한다.

$$R'=<a_1,a_2,\cdots,a_{n-1},\overline{a_n},\overline{a_n},a_{n-1},\cdots,a_1>$$

여기서 $\overline{a_n}=a_n\oplus 1$이고, 이것은 n번째 셀의 전이규칙이 90인 경우는 150으로, 반대로 150인 경우는 90으로 바꾸는 의미가 된다.

<예3> 전이규칙이 $R=\langle 1,0,1,1\rangle$인 CA의 대칭전이규칙을 갖는 전이행렬 T'은 다음과 같다.

$$T' = \left(\begin{array}{c|c} \begin{matrix}1&1&0&0\\1&0&1&0\\0&1&1&1\end{matrix} & \begin{matrix}0&0&0&0\\0&0&0&0\\0&0&0&0\end{matrix} \\ \hline \begin{matrix}0&0&1&0\\0&0&0&0\\0&0&0&0\end{matrix} & \begin{matrix}1&0&0&0\\0&1&0&0\\0&0&1&1\end{matrix} \\ \hline \begin{matrix}0&0&0&1\\0&0&0&0\\0&0&0&0\end{matrix} & \begin{matrix}0&1&0&0\\1&1&1&0\\0&1&0&1\end{matrix} \\ \hline \begin{matrix}0&0&0&0\\0&0&0&0\\0&0&0&0\end{matrix} & \begin{matrix}0&0&0&0\\0&0&1&1\\1&1&0&1\end{matrix} \end{array}\right)$$

<정리 3> n차 원시다항식 $f(x)$를 특성다항식으로 갖는 n셀 90/150 CA의 전이규칙 R에 대하여 대칭전이규칙을 갖는 합성 90/150 CA의 특성다항식 Δ'은 다음과 같다.

$$\Delta' = \{\Delta_n\}^2 = (f(x))^2$$

<예4> 예3에서 $R = \langle 1,0,1,1\rangle$ 인 CA의 특성다항식은 x^4+x^3+1 이다. 이 규칙을 이용하여 대칭전이규칙을 갖는 합성된 CA의 전이행렬 T'의 특성다항식은 다음과 같다.

$$\Delta' = \{\Delta^1\}^2 = (x^4+x^3+1)^2$$

V. 결 론

전이규칙으로 90, 150만을 사용하는 90/150 셀룰라 오토마타의 특성다항식을 분석하였으며 최대길이를 갖는 임의의 두 90/150 CA의 합성을 통해 그 CA의 특성다항식을 분석하였다. 특히 같은 원시다항식을 가지는 두 90/150 CA를 합성할 때 전이규칙을 변화시키지 않고 특성다항식이 원시다항식의 지수승 형태를 가지도록 하는 방법으로 대칭전이규칙을 제안하였다.

참고문헌

[1] J. von Neumann, *Theory of self-reproducing automata*, University of Illinois Press Urbana, 1966.

[2] S. Wolfram, *Statistical mechanics of cellular automata*, Rev. Modern Physics, Vol. 55, No. 3, 1983.

[3] A.K Das and P.P Chaudhuri, *Efficient characterization of cellular automata*, Proc. IEEE(part E), Vol. 137, No. 1, pp. 81-87, 1990.

[4] S. Nandi and P.P. Chaudhuri, *Analysis of periodic and intermediate boundary 90/150 cellular automata, IEEE Trans. Comput.*, Vol. 45, pp. 1-12, 1996.

[5] K. Cattell and J.C. Muzio, *Analysis of one-dimensional linear hybrid cellular automata over GF(q), IEEE Transactions of* Computers, Vol. 45 (7), 782-792, 1996.

[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, *Phase Shifts of Sequences by a Maximum-Length 90/150 Cellular Automata*, LNCS 3305, pp. 32-39, 2004.