90/150 그룹 셀룰라 오토마타의 합성 및 구조 분석†

김한두*, 김경자**, 허성훈***, 최향희**

최언숙****, 황윤희*****, 조성진******

*인제대학교 컴퓨터응용과학부, **부경대학교 응용수학과

***김해대학 컴퓨터정보과, ****동명대학교 멀티미디어공학과

*****부경대학교 정보보호학과, ******부경대학교 수리과학부

Analysis for Synthesis and Structure of 90/150 Cellular Automata†

Han-Doo Kim*, Kyung-Ja Kim**, Seong-Hun Heo***

Hyang-Hee Choi**, Un-Sook Choi****

Yoon-Hee Hwang*****, Sung-Jin Cho******

*School of Computer Aided Science, Inje Univ.

**Dept. of Applied Mathematics, Pukyong National Univ.

***Dept. of Computer and Information Science, Gimhae College

****Dept. of Multimedia Engineering, Tongmyong Univ.

*****Dept. of Information Security, Pukyong National Univ.

******Division of Mathematical Sciences, Pukyong National Univ.

요 약

본 논문에서는 합성된 90/150 그룹 셀룰라 오토마타의 특성다항식을 분석하고 이러한 셀룰라 오토마타의 구조와 특성다항식의 관계를 살펴본다. 또한 최대길이를 갖는 그룹 셀룰라 오토마타로부터 유도된 여원 셀룰라 오토마타의 구조가 선형 셀룰라 오토마타와 동형임을 밝힌다.

I. 서론

셀룰라 오토마타(이하, CA)는 셀이라 불리는 간단한 메모리의 배열로서 각 셀들의 상태가 국소적인 상호작용에 의해서 동시에 갱신되는 시스템이다[1]. Wolfram[2]은 CA를 각 셀이 0과 1, 두 상태를 가지고 다음 상태가 자기 자신과 인접한 두 이웃에 의해 갱신되는 3-이웃 CA와 상태의 도달 불가능 조건을 확인하기 위한 방법을 제안하였다. Cattell 등[3]에 의해서 LFSR에 대응하는 CA에 대한 연구가 수행되었으며, 테스트 패턴 생성, 의사난수생성기, 오류정정부호, 해싱, 암호시스템 등 많은 분야에 응용되었다[4-7].

본 논문에서는 합성된 90/150 그룹 CA의 특성다항식을 분석하고 이러한 CA의 구조와 특성다항식의 관계를 살펴본다. 또한 최대길이를 갖는 선형 그룹 CA로부터 유도된 여원 CA의 구조가 선형 CA와 동형임을 밝힌다.

II. CA

간단한 구조를 가지는 1차원 CA(1-D CA)에서는 모든 셀들이 선형으로 배열되어 있고 1-D CA 중에서 국소적 상호작용이 세 개의

† 본 연구는 한국과학재단 목적기초연구지원사업 (R01-2006-000-10260-0)에 의해 수행되었습니다.

셀, 즉 자신과 인접한 두 셀에 의해 이루어지는 CA를 3-이웃(3-neighborhood) CA라 한다. 본 논문에서는 3-이웃 1-D CA만 다룬다.

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 셀의 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.

본 논문에서 사용하는 CA의 전이규칙에 대한 결합논리 중 [표1]은 선형규칙을 나타내며, [표2]는 여원규칙을 나타낸다.

[표1] 선형 규칙

전이규칙	전이함수
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	$q_i(t+1) = q_{i+1}(t)$
240	$q_i(t+1) = q_{i-1}(t)$

[표2] 여원 규칙

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

CA는 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 트리구조를 이루며 이전상태가 유일하지 않다. 상태전이행렬이 T인 CA의 특성다항식 $\Delta(x)$는 다음과 같다.

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

상태전이행렬 T의 특성다항식 Δ의 인수 중에서 T를 근으로 갖는 가장 낮은 차수의 다항식을 최소다항식(minimal polynomial)이라 한다.

III. 90/150 그룹 CA의 합성 및 분석

본 논문에서 언급되는 n셀 90/150 CA의 상태전이행렬 T는 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.

한편 90/150 CA로부터 유도되는 여원 CA의 p단계 후의 상태는 $S_{t+p} = \overline{T}S_t = TS_t \oplus F$이다. 여기서 F는 여원벡터이다.

<정리 1[5]> 90/150 CA의 상태전이행렬 T의 특성다항식과 최소다항식은 같다.

n셀 90/150 CA의 상태전이행렬 T의 특성다항식을 $\Delta = \Delta_{1,n} = \Delta_n$이라 하고, $\Delta_{k,m}$은 k번째 셀부터 m번째 셀까지의 전이규칙에 대응하는 T의 부분행렬의 특성다항식을 의미한다.

<예제 1> $R = \langle 1, 1, 0, 0, 1 \rangle$이면 상태전이행렬은 다음과 같다.

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

이때 $\Delta_5 = x^5 + x^4 + x^3 + x^2 + 1$ 이고 $\Delta_{2,4} = x^3 + x^2 + 1$ 이다.

n셀 그룹 CA에서 주기가 $2^n - 1$인 CA를 최대길이를 갖는 CA라 한다. 최대길이를 갖는 임의의 두 90/150 CA인 CA_1과 CA_2에 상태전이행렬을 각각 T_1과 T_2라 하자. 그리고 이 두 CA를 합성한 90/150 CA의 상태전이행렬을 T'이라 하자. <정리 1>에 의하여 T'의 특성다항식과 최소다항식은 같다. 90/150 CA의 합성에는 다음과 같은 두 가지 방법이 있다.

(a) 특성다항식이 서로 다른 CA_1과 CA_2의 합성

(b) 동일한 두 90/150 CA의 합성

합성된 CA의 상태전이행렬 T'은 다음과 같다.

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

특성다항식이 최대길이를 갖는 두 90/150 CA에 대하여 CA_1의 특성다항식을 Δ^1이라 하고 CA_2의 특성다항식을 Δ^2라 하면 합성된 CA의 특성다항식 Δ'은 일반적으로 $\Delta' \neq \Delta^1 \cdot \Delta^2$ 이다.

<예제 2> 전이규칙이 $R = <0,1,0,1>$ 인 CA 두 개를 합성할 때 합성된 CA의 상태전이행렬 T'은 대각성분이 $<0,1,0,1,0,1,0,1>$인 삼중대각행렬이 된다. 그리고 T'의 특성다항식은 다음과 같다.

$$\begin{aligned} \Delta' &= x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + 1 \\ &= (x^2 + x + 1)(x^3 + x + 1)(x^3 + x^2 + 1) \\ &\neq \{\Delta^1\}^2 \end{aligned}$$

다음은 <예제 2>와 같이 동일한 두 90/150 CA를 합성할 때 합성된 90/150 CA의 특성다항식이 원시다항식의 거듭제곱 형태가 되는 90/150 CA의 합성규칙을 제안한다.

<정의 1> 90/150 CA의 규칙이 $R = <a_1, a_2, \cdots, a_n>$ 이라 할 때 다음과 같이 정의된 전이규칙 R'을 합성된 90/150 CA의 **대칭전이규칙**이라 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 의미이다.

<예제 3> 전이규칙이 $R = <0,1,0,1>$ 인 CA의 대칭전이규칙을 갖는 상태전이행렬 T'은 다음과 같다.

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

<정리 2> n차 원시다항식 $f(x)$가 특성다항식인 n셀 90/150 CA의 전이규칙 R에 대하여 대칭전이규칙을 이용하여 k번 합성한 CA의 특성다항식은 $(f(x))^{2^k}$이다.

<예제 4> <예제 4>에서 $R = <0,1,0,1>$ 인 CA의 특성다항식은 $x^4 + x + 1$ 이다. 대칭전이규칙을 이용하여 한 번 합성한 CA의 상태전이행렬 T'의 특성다항식 $\Delta' = \{\Delta^1\}^2 = (x^4 + x + 1)^2$ 이고, 두 번 합성한 CA의 특성다항식은 $(x^4 + x + 1)^{2^2}$ 이 되며, k번 합성하면 특성다항식은 $(x^4 + x + 1)^{2^k}$ 이 된다.

IV. 90/150 그룹 CA 및 여원 CA의 구조 분석

4.1 90/150 그룹 CA

최대 길이를 가지는 n셀 90/150 CA의 상태전이행렬 T에 대한 사이클 구조는 0 을 제외한 $2^n - 1$개의 모든 셀의 상태가 하나의 주기로 이루어지는데, 이를 $[1, 1(2^n - 1)]$로 표현한다. 이 때 대칭전이규칙을 적용하여 합성한 상태전이행렬 T'에 대한 사이클 구조는 다음과 같다.

<정리 3> n차 원시다항식 $f(x)$를 특성다항식으로 갖는 90/150 CA의 전이규칙 R에 대하여 대칭전이규칙을 을 k번 반복 합성한 CA의 사이클 구조는 다음과 같다.

$$\left[1,\ 1(2^n-1),\ \mu_1\left(2(2^n-1)\right),\ \cdots,\ \mu_k\left(2^k(2^n-1)\right)\right]$$

$$\mu_k = \frac{2^{2^k \cdot n} - \left\{2^n + (2^n-1)\sum_{i=0}^{k-1}\mu_i \cdot 2^i\right\}}{2^k(2^n-1)},\ (\mu_0 = 0)$$

<예제 5> 전이규칙이 $R = <0,1,1>$ 인 90/150 CA의 경우, 대칭전이규칙을 이용하여 한 번 합성한 CA의 사이클 구조는 <정리 3>에 의하여 $[1,\ 1(7),\ 4(14)]$이다. 두 번 합성한 CA의 사이클 구조는 $[1, 1(7), 4(14), 144(28)]$이다.

4.2 여원 CA

여원 CA는 비선형이므로 XOR 논리만을 사용하는 선형 CA에 비해 분석이 어렵다. 그래서 여원 CA를 선형 CA로부터 유도된 CA로 분석하는 것이 일반적이다[6]. 일반적으로 선형 그룹 CA와 이로부터 유도된 여원 그룹 CA의 사이클 구조는 다르다. 그러나 최대길이를 가지는 90/150 CA로부터 유도된 여원 CA 또한 최대길이를 갖는 CA가 되어 대응되는 선형 CA와 사이클 구조가 같다[8]. 다음 정리는 대칭전이규칙을 이용하여 합성한 CA와 이로부터 유도된 여원 CA의 사이클 구조를 밝힌다.

<정리 5> 최대길이를 가지는 90/150 그룹 CA를 대칭전이규칙을 이용하여 합성한 CA와, 그로부터 유도된 여원 CA의 사이클 구조는 선형 CA와 동형이다.

<예제 6> 예제 6의 두 번 합성한 CA에 대하여 여원벡터로부터 유도된 여원 CA의 사이클 구조는 $[1, 1(7), 4(14), 144(28)]$ 가 되어서 선형 CA와 동형이다.

V. 결론

본 논문에서는 합성된 90/150 그룹 CA의 특성다항식을 분석하였고 이러한 CA의 구조와 특성다항식의 관계를 살펴보았다. 또한 최대길이를 갖는 그룹 CA로부터 유도된 여원 CA의 구조가 선형 CA와 동형임을 밝혔다.

[참고문헌]

[1]J.V. Neumann, Theory of Self-Reproducing Automata, University of Illinois Press Urbana, 1966.

[2]S. Wolfram, "Statistical Mechanics of Cellular Automata", Rev. Modern Physics, 55(3), 1983.

[3]K. Cattell and J.C. Muzio, "Analysis of One-Dimensional Linear Hybrid Cellular Automata over GF(q)", IEEE Trans. Comput., 45(7), p.p. 782-792, 1996.

[4] A.K. Das, A. Ganguly, A. Dasgupta, S. Bhawmik, P.P. Chaudhuri, "Efficient Characterization of Cellular Automata", Proc. IEEE(part E), 137(1), pp. 81-87, 1990.

[5]S. Nandi and P.P. Chaudhuri, "Analysis of Periodic and Intermediate Boundary 90/150 Cellular Automata", IEEE Trans. Comput., 45, pp. 1-12, 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, Y.H. Hwang, Y.S. Pyo, H.D. Kim, K.S. Kim and S.H. Heo, "Computing Phase Shifts of Maximum-Length 90/150 Cellular Automata Sequences", LNCS 3305, pp. 31-39, 2004.

[8]최언숙, 조성진, "최대길이를 갖는 셀룰라 오토마타의 생성", 정보보호학회논문지, 14(6), pp. 25-30, 2004.