Regular paper | Journal of the KIECS. pp. 1019-1026, vol. 19, no. 5, Oct. 31. 2024, t. 127, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2024.19.5.1019

1차원 5-이웃 선형 하이브리드 셀룰라 오토마타의 특성다항식의 점화관계 분석: 이웃 유형 I을 중심으로

최언숙*

Analysis of the Recurrence Relation of the Characteristic Polynomial of One-Dimensional 5-Neighborhood Linear Hybrid Cellular Automata: Focusing on Neighborhood Type I

Un-Sook Choi*

요 약

셀룰러 오토마타(CA)는 자연 컴퓨팅에서 가장 오래된 모델 중 하나이다. 이 논문에서는 1차원 3-이웃 90/150 CA의 확장인 5-이웃 CA의 특성 다항식에 대한 점화 관계를 분석한다. 5-이웃 CA의 선형규칙을 분류하고 선형 5-이웃 하이브리드 CA를 구성하기 위해 이웃 의존도를 유형별로 나눈다. 특별히 이웃 의존도가 유형 I인 5-이웃 CA의 특성 다항식의 점화관계와 합성에 대해 분석한다. 이 연구는 다양한 응용 프로그램을 위해 CA를 보다 효과적으로 합성하기 위해 셀에 적용된 규칙과 특성 다항식 간의 관계를 이해하는 것을 목표로 한다.

ABSTRACT

Cellular Automata (CA) are one of the oldest models in natural computing. In this paper, we analyze the recurrence relations for the characteristic polynomial of a 5-neighbor CA, an extension of the one-dimensional 3-neighbor 90/150 CA. To classify the linear rules of 5-neighbor CA and construct linear 5-neighbor hybrid CA, we categorize the neighborhood dependencies by type. Specifically, we analyze the recurrence relations and composition of the characteristic polynomials for 5-neighbor CA with Type I neighborhood dependencies. This research aims to understand the relationship between the rules applied to cells and their characteristic polynomials to synthesize CA more effectively for various applications.

키워드

5-Neighbor Cellular Automata, Characteristic Polynomial, Linaear Rule, Hybrid Cellular Automata, Irreducible Polynomial
5-이웃 셀룰러 오토마타, 특성다항식, 선형 규칙, 하이브리드 셀룰러 오토마타, 기약다항식

Ⅰ. 서 론

셀룰라 오토마타(Cellular Automata, 이하 CA)는 자연 컴퓨팅의 가장 오래된 모델 중 하나로 자기 복제 가능한 인공 시스템을 설계하고자 하는 목표를 가지고 처음 연구되었다[1]. CA는 셀이라는 기본단위가 선형 또는 평면으로 배열되어 있으며 각 셀의 상태가

* 동명대학교(choies@tu.ac.kr)
* 교신저자 : 동명학교 소프트웨어학과
• 접 수 일 : 2024. 08. 16
• 수정완료일 : 2024. 09. 13
• 게재확정일 : 2024. 10. 12
• Received : Aug. 16, 2024, Revised : Sep. 13, 2024, Accepted : Oct. 12, 2024
• Corresponding Author : Un-Sook Choi
Dept. Software, Tongmyong University
Email : choies@tu.ac.kr

이산시간 단위에서 이웃으로 정의된 셀의 상태와 셀에 정의된 상태전이함수에 따라 동시에 전체 상태가 업데이트되는 동역학계이다.

CA는 무작위성 및 복잡성을 생성할 수 있는 능력 때문에 암호시스템에 응용되며, 유체역학이나 생물의 성장과 같은 자연 현상을 모델링하는데 사용된다. 또한 도시 개발 및 토지 이용 변화 모델링에서 CA는 복잡한 상호작용을 시뮬레이션하는 데 사용된다[2-4]. 최근에는 심층 신경망과의 결합을 통해 CA의 동작 규칙을 학습하고, 복잡한 시스템의 행동을 예측하는 연구가 진행되고 있다. 이러한 접근법은 CA가 단순한 계산 모델을 넘어 인공지능 및 머신러닝 분야에서도 중요한 도구로 자리잡게 하고 있으며 이러한 모델은 셀룰러 학습 오토마타로 분류된다[5,6]. 이처럼 CA는 자연에서 일어나는 많은 일들을 더 쉽게 이해할 수 있게 해 주었으며 단순하고 규칙적인 CA의 구조 및 특성은 다양한 분야의 연구자들과 실무자들의 관심을 받기에 충분했다. CA의 기본 이론적 측면에 대한 연구 분야에서도 연구자들은 CA의 가역성, 보존 법칙, 결정 가능성 문제, 계산적 범용성 및 한계 행동 등을 탐구하고 있다.

본 논문에서는 1차원 3-이웃 90/150 CA를 확장한 5-이웃 CA에 대한 특성다항식에 대한 점화관계에 대해 분석한다. 이를 위해 5-이웃 CA의 선형규칙을 분류하고 선형 5-이웃 하이브리드 CA를 구성하기 위해 이웃 의존도를 유형별로 나눈다. 특별히 이웃 의존도가 유형 I인 5-이웃 CA의 특성다항식의 점화관계와 합성에 대해 분석한다.

II. 기본 CA

1차원 CA는 각 셀이 1비트 메모리 요소인 셀의 1차원 셀 스트링으로 구성되며 가장 가까운 이웃 간의 상호작용에 의해 이산 시간 단계에서 상태가 전이된다. 기본 CA는 1차원 3-이웃 CA이다. 1차원으로 나열된 셀 중 i번째 셀 c_i에 대한 이웃 집합을 N_i라 할 때, 기본 CA의 N_i는 $N_i=\{c_{i-1},c_i,c_{i+1}\}$이다. c_i^t를 시간 t에서 기본 CA의 i번째 셀의 상태라 하고, g_i를 i번째 셀의 상태전이 함수라 할 때 다음상태 c_i^{t+1}는 상태는 (1)과 같다.

$$c_i^{t+1}=g_i(c_{i-1}^t,c_i^t,c_{i+1}^t) \quad \cdots (1)$$

3개의 셀(즉, 주어진 셀과 가장 가까운 이웃)에 대해 총 $2^3(=8)$개의 이진 상태가 있기 때문에 표준 규칙에 따라 0에서 255까지 레이블이 지정된 총 $2^8(=256)$개의 가능한 전이규칙이 존재한다. g_i가 XOR논리로 표현될 때 g_i를 선형 규칙이라 한다. 주어진 CA의 모든 셀에 적용되는 규칙이 선형 규칙으로만 이루어진 CA를 선형 CA라 한다. (2)는 선형규칙을 부울식으로 나타낸 것이다.

$$c_i^{t+1}=p\cdot c_{i-1}^t\oplus q\cdot c_i^t\oplus r\cdot c_{i+1}^t \quad \cdots (2)$$

여기서 $p,q,r\in\{0,1\}$이다. (2)에서 1차원 선형 3-이웃 CA의 각 셀에 적용할 수 있는 전이규칙의 수는 p,q,r이 모두 0인 경우를 제외한 7개가 있다. 1차원 선형 3-이웃 CA중 특히 무작위성이 매우 높은 수열을 생성할 수 있는 1차원 90/150 CA는 각 셀에 적용되는 전이규칙이 90또는 150만 적용되는 CA이다[7]. 표 1은 3개의 이웃의 상태에 대해 다음상태 전이를 보여준다. 표 1에서 규칙 150에 대해 3개의 이웃 상태 $c_{i-1}^t,c_i^t,c_{i+1}^t$가 각각 111, 110, 101, 100, 011, 010, 001, 000에 대해 다음 상태 c_i^{t+1}은 1,0,0,1,0,1,1,0이고 이를 십진수로 표현하면 150이다. 규칙 90도 같은 방법으로 번호를 생성한다.

표 1. 이웃 셀의 상태와 전이규칙 90과 150에 대한 다음 상태 전이
Table 1. Next state transition for neighboring cell states and transition rules 90 and 150

Current Neighborhood State	111	110	101	100	011	010	001	000	Rule
Next State	0	1	0	1	1	0	1	0	90
Next State	1	0	0	1	0	1	1	0	150

선형 CA의 상태전이 함수는 행렬로 나타낼 수 있으며 이 행렬을 상태전이행렬이라고 한다. 기본 CA의 상태전이행렬은 삼중 대각행렬로 표현된다. 특히 n개의 셀로 이루어진 90/150 CA의 상태전이행렬 T_n은 (3)과 같다.

$$T_n=(a_{ij})_{n\times n}=\begin{cases}d_i, i=j\\ 1, i=j+1 \text{ or } i=j-1\\ 0, otherwise\end{cases} \quad \cdots (3)$$

여기서 $d_i \in \{0,1\}$이고 i번째 셀에 적용된 전이규칙이 90인 경우 $d_i = 0$ 이고 전이규칙이 150인 경우 $d_i = 1$이다. T_n을 주대각선 성분을 이용하여 간단히 $< d_1 d_2 \cdots d_n >$로 표현한다.

전이규칙이 $< d_1 d_2 \cdots d_n >$인 n-셀 90/150 CA의 T_n에 대하여 특성다항식 $|T_n + xI_n|$을 C_n이라 할 때 C_n은 (4)와 (5)를 만족한다[8].

$$C_n = (x + d_n) C_{n-1} + C_{n-2} \quad \cdots (4)$$

$$C_n = C_i C_{i+1,n} + C_{i-1} C_{i+2,n} \quad \cdots (5)$$

여기서 I_n은 n차 단위행렬이고, C_i는 전이규칙이 $< d_1 d_2 \cdots d_i >$인 i-셀 90/150 CA의 특성다항식이다. $C_{i+1,n}$은 전이규칙이 $< d_{i+1} d_{i+2} \cdots d_n >$인 $(n-i)$-셀 90/150 CA의 특성다항식이다. 또한 $n \geq 1$ 이고 $C_0 = 1, C_{-1} = C_{-2} = \cdots = 0$.

암호 시스템에서 CA를 키수열 생성기로 사용하기 위해서는 키공간의 크기와 랜덤성은 매우 중요한 부분이다. 키공간과 상태 전이의 무작위성을 증가시키기 위해 1차원 CA의 이웃의 반경을 1에서 2로 확장하여 이웃의 수를 3에서 5로 확장시킨다. 이웃의 반경을 넓혀 이웃의 수를 5개로 증가시키면 1차원 5-이웃 CA의 i번째 셀 s_i의 이웃 집합 N_i는 $N_i = \{s_{i-2}, s_{i-1}, s_i, s_{i+1}, s_{i+2}\}$이 된다. 또한 1차원 5-이웃 CA의 전이규칙은 5개의 이웃에 대해 2^5개의 상태가 존재하므로 $2^{2^5} = 4{,}294{,}967{,}296$개의 전이규칙이 존재한다. f_i를 i번째 셀 s_i의 상태전이 함수라 할 때 다음상태 s_i^{t+1}는 상태는 (6)과 같다.

$$s_i^{t+1} = f_i(s_{i-2}^t, s_{i-1}^t, s_i^t, s_{i+1}^t, s_{i+2}^t) \quad \cdots (6)$$

기본 CA와 마찬가지로 1차원 5-이웃 CA의 모든 셀에 적용되는 $f_i (i = 1,2,\cdots)$ 가 XOR논리로만 표현되는 CA는 선형 CA이다. 1차원 선형 5-이웃 CA의 시간 $(t+1)$에서 i번째 셀의 상태 s_i^{t+1}는 (7)과 같은 부울식을 만족한다.

$$s_i^{t+1} = w_i s_{i-2}^t \oplus x_i s_{i-1}^t \oplus r_i s_i^t \oplus y_i s_{i+1}^t \oplus z_i s_{i+2}^t \quad \cdots (7)$$

여기서 $w_i, x_i, r_i, y_i, z_i \in \{0,1\}$이다. 모든 i에 대해 $w_i = z_i = 0, x_i = y_i = 1, r_i \in \{0,1\}$인 n-셀 CA는 전이규칙이 $< r_1 r_2 \cdots r_n >$ 인 90/150 CA가 된다. (7)에서 선형규칙의 수는 $2^5 - 1 = 31$이다.

III. 이웃 의존도가 유형 I인 1차원 선형 5-이웃 선형 하이브리드 CA의 특성다항식

3.1 1차원 선형 5-이웃 CA의 전이규칙의 분류

1차원 3-이웃 CA의 선형 규칙의 수는 $2^3 - 1 = 7$ 이므로 n개의 셀로 이루어진 1차원 3-이웃 하이브리드 CA 개수는 7^n이다. 이와 비교하여 1차원 5-이웃 CA의 선형 규칙의 수는 31이므로 1차원 선형 5-이웃 하이브리드 CA(Linear Five-neighbor Hybrid CA, LFHCA)의 개수는 31^n으로 1차원 선형 3-이웃 하이브리드 CA보다 훨씬 많이 존재한다. 그러므로 더 다양한 CA를 합성할 수 있으며, 이러한 사실은 암호시스템을 설계할 때 키 공간이 더 크고 복잡해질 수 있으므로 보다 더 안전한 키 수열을 생성할 수 있다. 표 2는 1차원 LFHCA의 전이규칙과 부울함수를 나타낸다. 표 2에서 선형규칙의 번호는 이웃 의존도을 크기가 5인 이진벡터로 나타내었을 때 십진수 값을 나타낸다. 예를 들어 LR 21은 i번째 셀의 다음 상태를 결정하는데 이웃 셀의 의존성은 10101이고 이것을 십진수로 표현하면 21이다.

1차원 3-이웃 90/150 CA의 확장을 위해, 표 2의 1차원 5-이웃 선형 규칙 중 i번째 셀이 다음상태로 전이될 때, 자신의 왼쪽 이웃과 오른쪽 이웃 상태에 모두에 영향을 받는 전이규칙을 선택하면 모두 18개가 된다. 본 논문에서는 선택된 18개의 선형 규칙을 셀 자신이 다음 상태 전이에 영향을 주는 경우와 영향을 주지 않은 경우를 하나로 묶어서 LFHCA를 구성한다. 표 3는 1차원 LFHCA의 이웃 의존도에 따른 분류와 부울식 표현이다. n-셀 1차원 LFHCA의 상태전이함수는 크기가 $n \times n$ 인 5중 대각행렬 M으로 표현할 수 있다. 표 3에서 유형 I, II, III인 1차원 LFHCA의 상태전이행렬 M은 대칭 행렬이 되고, 나머지 유형의 1차원 LFHCA의 상태전이행렬은 대칭행렬이 아니다.

3.2 이웃 의존도가 유형 I인 1차원 선형 5-이웃 선형 하이브리드 CA특성다항식과 합성

본 논문에서는 1차원 LFHCA의 효과적인 합성을 위해 90/150 CA와 같이 1차원 5-이웃 선형 CA에서 상태전이에 참여하는 이웃의 수를 자신을 포함하여 3개로 제한한 이웃 의존도가 유형 I인 1차원 LFHCA의 특성다항식의 접화관계를 분석하고, 합성하는 방법을 제안한다.

표 2. 1차원 선형 5-이웃 CA의 전이규칙과 부울 함수
Table 2. Transition rules and Boolean functions of one-dimensional linear five-neighbor CA

No.	Boolean expression of transition rule	liner rule number	No.	Boolean expression of transition rule	liner rule number
1	$s_i^{t+1}=s_{i-2}^t$	LR 16	16	$s_i^{t+1}=s_{i-2}^t\oplus s_{i-1}^t\oplus s_i^t$	LR 28
2	$s_i^{t+1}=s_{i-1}^t$	LR 8	17	$s_i^{t+1}=s_{i-2}^t\oplus s_{i-1}^t\oplus s_{i+1}^t$	LR 26
3	$s_i^{t+1}=s_i^t$	LR 4	18	$s_i^{t+1}=s_{i-2}^t\oplus s_{i-1}^t\oplus s_{i+2}^t$	LR 25
4	$s_i^{t+1}=s_{i+1}^t$	LR 2	19	$s_i^{t+1}=s_{i-2}^t\oplus s_i^t\oplus s_{i+1}^t$	LR 22
5	$s_i^{t+1}=s_{i+2}^t$	LR 1	20	$s_i^{t+1}=s_{i-2}^t\oplus s_i^t\oplus s_{i+2}^t$	LR 21
6	$s_i^{t+1}=s_{i-2}^t\oplus s_{i-1}^t$	LR 24	21	$s_i^{t+1}=s_{i-2}^t\oplus s_{i+1}^t\oplus s_{i+2}^t$	LR 19
7	$s_i^{t+1}=s_{i-2}^t\oplus s_i^t$	LR 20	22	$s_i^{t+1}=s_{i-1}^t\oplus s_i^t\oplus s_{i+1}^t$	LR 14
8	$s_i^{t+1}=s_{i-2}^t\oplus s_{i+1}^t$	LR 18	23	$s_i^{t+1}=s_{i-1}^t\oplus s_i^t\oplus s_{i+2}^t$	LR 13
9	$s_i^{t+1}=s_{i-2}^t\oplus s_{i+2}^t$	LR 17	24	$s_i^{t+1}=s_{i-1}^t\oplus s_{i+1}^t\oplus s_{i+2}^t$	LR 11
10	$s_i^{t+1}=s_{i-1}^t\oplus s_i^t$	LR 12	25	$s_i^{t+1}=s_i^t\oplus s_{i+1}^t\oplus s_{i+2}^t$	LR 7
11	$s_i^{t+1}=s_{i-1}^t\oplus s_{i+1}^t$	LR 10	26	$s_i^{t+1}=s_{i-2}^t\oplus s_{i-1}^t\oplus s_i^t\oplus s_{i+1}^t$	LR 30
12	$s_i^{t+1}=s_{i-1}^t\oplus s_{i+2}^t$	LR 9	27	$s_i^{t+1}=s_{i-2}^t\oplus s_{i-1}^t\oplus s_i^t\oplus s_{i+2}^t$	LR 29
13	$s_i^{t+1}=s_i^t\oplus s_{i+1}^t$	LR 6	28	$s_i^{t+1}=s_{i-2}^t\oplus s_{i-1}^t\oplus s_{i+1}^t\oplus s_{i+2}^t$	LR 27
14	$s_i^{t+1}=s_i^t\oplus s_{i+2}^t$	LR 5	29	$s_i^{t+1}=s_{i-2}^t\oplus s_{i-1}^t\oplus s_i^t\oplus s_{i+2}^t$	LR 23
15	$s_i^{t+1}=s_{i+1}^t\oplus s_{i+2}^t$	LR 3	30	$s_i^{t+1}=s_{i-1}^t\oplus s_i^t\oplus s_{i+1}^t\oplus s_{i+2}^t$	LR 15
			31	$s_i^{t+1}=s_{i-2}^t\oplus s_{i-1}^t\oplus s_i^t\oplus s_{i+1}^t\oplus s_{i+2}^t$	LR 31

표 3. 1차원 선형 5-이웃 하이브리드 CA의 이웃 의존도에 따른 전이규칙의 분류와 전이규칙의 부울식 표현
Table 3. Classification of transition rules according to neighbor dependence of one-dimensional linear 5-neighbor hybrid CA and Boolean expression of transition rules

Type	Dependency on neighboring cells	Linear Rule Combination	Boolean expression of transition rule $r_i\in\{0,1\}$
Ⅰ	(10*01)	LR 17 & LR 21	$s_i^{t+1}=s_{i-2}^t\oplus r_i s_i^t\oplus s_{i+2}^t$
Ⅱ	(01*10)	LR 10 & LR 14	$s_i^{t+1}=s_{i-1}^t\oplus r_i s_i^t\oplus s_{i+1}^t$
Ⅲ	(11*11)	LR 27 & LR 31	$s_i^{t+1}=s_{i-2}^t\oplus s_{i-1}^t\oplus r_i s_i^t\oplus s_{i+1}^t\oplus s_{i+2}^t$
Ⅳ	(01*11)	LR 11 & LR 15	$s_i^{t+1}=s_{i-1}^t\oplus r_i s_i^t\oplus s_{i+1}^t\oplus s_{i+2}^t$
Ⅴ	(11*10)	LR 26 & LR 30	$s_i^{t+1}=s_{i-2}^t\oplus s_{i-1}^t\oplus r_i s_i^t\oplus s_{i+1}^t$
Ⅵ	(10*11)	LR 19 & LR 23	$s_i^{t+1}=s_{i-2}^t\oplus r_i s_i^t\oplus s_{i+1}^t\oplus s_{i+2}^t$
Ⅶ	(11*01)	LR 25 & LR 29	$s_i^{t+1}=s_{i-2}^t\oplus s_{i-1}^t\oplus r_i s_i^t\oplus s_{i+2}^t$
Ⅷ	(10*10)	LR 18 & LR 22	$s_i^{t+1}=s_{i-2}^t\oplus r_i s_i^t\oplus s_{i+1}^t$
Ⅸ	(01*01)	LR 9 & LR 13	$s_i^{t+1}=s_{i-1}^t\oplus r_i s_i^t\oplus s_{i+2}^t$

전이규칙이 $< r_1 r_2 \cdots r_n >$ 이고, 이웃 의존도가 유형 I인 1-D LFHCA $\mathbb{P}_n$의 상태전이행렬 $M_n = (u_{ij})_{n\times n}$에 대하여 u_{ij}는 (8)과 같다.

$$u_{ij} = \begin{cases} r_i, i = j \\ 1, |i-j| = 2 \\ 0, otherwise \end{cases} \quad \cdots (8)$$

$\mathbb{P}_n$의 물리적 구조를 살펴보면, $\mathbb{P}_n$은 두 개의 90/150 CA $\mathbb{C}_1$과 $\mathbb{C}_2$를 결합하여 만든 것으로 해석할 수 있다. 이때 $n = 2k$이면 $\mathbb{C}_1$의 크기와 $\mathbb{C}_2$의 크기가 각각 k이고, $n = 2k-1$이면 $\mathbb{C}_1$의 크기는 k이고 $\mathbb{C}_2$의 크기는 $k-1$이다.

전이규칙이 $< r_1 r_2 \cdots r_n >$ 이고 이웃 의존도가 유형 I인 1-D LFHCA $\mathbb{P}_n$의 특성다항식 $\Gamma_n = |M_n + xI_n|$은 가약다항식이다. k-셀 90/150 CA $\mathbb{C}_1$의 상태전이행렬을 $T_o = < o_1 o_2 \cdots o_k >$라 하고, 그 특성다항식을 O_k라 하자. k-셀 90/150 CA $\mathbb{C}_2$의 상태전이행렬을 $T_e = < e_1 e_2 \cdots e_k >$이라 하고, 그 특성다항식을 V_k이라하자. 그러면 전이규칙이 $< o_1 e_1 o_2 e_2 \cdots o_k e_k >$인 $\mathbb{P}_{2k}$의 특성다항식 Γ_{2k}는 (9)를 만족하고 $n = 2k-1$인 경우는 (10)을 만족한다[9].

$$\Gamma_{2k} = O_k V_k \quad \cdots (9)$$

$$\Gamma_{2k-1} = O_k V_{k-1} \quad \cdots (10)$$

(9)와 (10)에 의하면 $\mathbb{P}_n$의 특성다항식은 반드시 2개 이상의 기약다항식으로 인수분해된다. 그리고 인수분해된 기약다항식의 차수는 $\lceil n/2 \rceil$ 이하이다. 예를 들어 이웃 의존도가 유형 I인 8-셀 1-D LFHCA 중 특성다항식이 3차 기약다항식과 5차 기약다항식의 곱으로 이루어지거나, 2차 기약다항식과 6차 기약다항식의 곱으로 이루어진 LFHCA는 존재하지 않는다는 의미이다. 그러므로 두 개의 기약다항식의 곱으로 이루어지는 이웃 의존도가 유형 I인 8-셀 1-D LFHCA는 4차 기약다항식들의 곱의 조합으로만 이루어진다.

전이규칙이 $< r_1 r_2 \cdots r_n >$ 이고 이웃 의존도가 유형 I인 1-D LFHCA $\mathbb{P}_n$의 특성다항식 $\Gamma_n = |M_n + xI_n|$은 (11)과 같은 접화관계를 만족한다. [10].

$$\Gamma_n = (x+r_n)\Gamma_{n-1} + (x+r_{n-1})\Gamma_{n-3} + \Gamma_{n-4} \quad \cdots (11)$$
$$(n \geq 3, \Gamma_0 = 1, \Gamma_{-1} = 0)$$

여기서 $\Gamma_1 = x + r_1$이고 $\Gamma_2 = (x+r_2)\Gamma_1$이다.

정리 3.1은 특성다항식이 2개의 기약다항식으로 인수분해되는 이웃 의존도가 유형 I인 n-셀 1-D LFHCA 개수에 대한 정리이며 증명 과정에서 합성하는 방법도 제시된다.

<정리 3.1> 특성다항식이 서로 다른 2개의 기약다항식으로 인수분해되는 이웃 의존도가 유형 I인 n-셀 1-D LFHCA의 개수 $F(n)$은 (12)를 만족한다.

$$F(n) = \begin{cases} 4[I(k)]^2 & , n = 2k \\ 4I(k)I(k-1) & , n = 2k-1 \end{cases} \quad (12)$$

여기서 $I(k)$는 k차 기약다항식의 개수이며 $I(k) = (1/n)\sum_{d|n}\mu(d) \cdot 2^{n/d}$ 이다. 이 때, $\mu(d)$는 뫼비우스 함수로 d가 짝수개의 소인수를 갖는 제곱이 없는 양의 정수인 경우는 1, d가 홀수개의 소인수를 갖는 제곱이 없는 양의 정수인 경우는 -1, d가 제곱된 약수를 가지는 수인 경우는 0이다.

(증명) (i) $n = 2k$일 때, 특성다항식이 서로 다른 두 개의 k차 기약다항식 m_1, m_2로 인수분해되는 경우와 서로 같은 두 개의 k차 기약다항식으로 제곱의 형태 $(m_1)^2$로 인수분해되는 경우를 고려할 수 있다.

① 특성다항식이 $m_1 \cdot m_2$로 인수분해되는 경우 ; m_1에 대응하는 k-셀 90/150 CA $\mathbb{C}_1$의 전이규칙이 R_1, R_1'이고 m_2에 대응하는 k-셀 90/150 CA $\mathbb{C}_1$의 전이규칙이 R_2, R_2'라 둘 수 있다. 여기서 R_1'는 $R_1 = < r_1 r_2 \cdots r_{k-1} r_k >$일 때, $R_1' = < r_k r_{k-1} \cdots r_2 r_1 >$이다. R_1, R_1'과 R_2, R_2'를 이용하여 합성할 수 있는 경우의 수는 8이고, 서로 다른 기약다항식 중에서 2개를 선택하는 방법의 수는 조합이므로 ${}_{I(k)}C_2$이다. 그러므로 특성다항식이 서로 다른 기약다항식 2개로 인수분해되는 이웃 의존도가 유형 1인 $2k$-셀 1-D LFHCA의 개수는 $8\,{}_{I(k)}C_2 = 4I(k)(I(k)-1)$이다.

② 특성다항식이 $(m_1)^2$으로 인수분해되는 경우는 m_1에 대응하는 k-셀 90/150 CA $\mathbb{C}_1$의 전이규칙 R_1, R_1'를 이용하여 합성할 수 있다. 그 경우의 수는 4이다. 또한 k차 기약다항식의 개수는 $I(k)$이므로 특성다항식이 서로 같은 기약다항식 2개로 인수분해되는 이웃 의존도가 유형 1인 $2k$-셀 1-D LFHCA의 개수는 $4I(k)$이다. 그러므로 ①과 ②의 결과에 의해 $F(2k) = 4I(k)[I(k)-1] + 4I(k) = 4[I(k)]^2$ 이다.

(ii) $n = 2k-1$인 경우는 k-셀 90/150 CA $\mathbb{C}_1$와

$(k-1)$-셀 90/150 CA $\mathbb{C}_2$를 이용하여 합성하는데 반드시 길이가 긴 k-셀 CA의 규칙이 선행되어 전이규칙을 교대로 적용하여 합성해야 한다. $\mathbb{C}_1$에 대응하는 전이규칙을 R_1, R_1', $\mathbb{C}_2$에 대응하는 전이규칙을 R_2, R_2'라고 하면 합성할 수 있는 경우의 수는 4이다. k차 기약다항식의 개수는 $I(k)$이고, $(k-1)$차 기약다항식의 개수는 $I(k-1)$이다. 따라서 서로 다른 기약다항식 2개로 인수분해되는 이웃 의존도가 유형 1인 $(2k-1)$-셀 1-D LFHCA의 개수는 $F(2k-1)=4I(k)\,I(k-1)$이다. □

표 4는 4차 기약다항식을 특성다항식으로 갖는 90/150 CA의 전이규칙이며, 표 5는 표 4를 이용하여 특성다항식이 두 개의 기약다항식의 곱으로 이루어진 8-셀 1차원 LFHCA의 특성다항식과 전이규칙과 합성과정을 보여준다. 표 5에서 $m_1(x)=x^4+x+1$이고 $m_2(x)=x^4+x^3+1$, $m_3(x)=x^4+x^3+x^2+x+1$이다. 정리 3.1에 의하면 두 개의 기약다항식의 곱으로 인수분해되는 가약다항식을 특성다항식으로 갖는 이웃 의존도가 유형 I인 1-D LFHCA는 존재하며 합성가능하다.

표 4. 4차 기약다항식을 특성다항식으로 갖는 4-셀 90/150 CA의 전이규칙
Table 4. Transition rule for 4-cell 90/150 CA with irreducible polynomial as characteristic polynomial

irreduc. poly. with degree 4	90/150 CA corresponding to irreducible poly.
x^4+x+1	$T_1 =<0101>$
	$T_2 =<1010>$
x^4+x^3+1	$T_3 =<1011>$
	$T_4 =<1101>$
$x^4+x^3+x^2+x+1$	$T_5 =<0010>$
	$T_6 =<0100>$

다음 정리는 두 개의 작은 크기의 1-D LFHCA를 연결하여 큰 1-D LFHCA를 합성할 때 합성된 1-D LFHCA의 특성다항식은 점화관계를 밝힌다.

<정리 3.2> 전이규칙이 $<r_1, r_2, \cdots, r_i, r_{i+1}, \cdots r_n>$ 인 이웃 의존도가 유형 I인 1-D LFHCA $\mathbb{P}_n$의 특성다항식 Γ_n은 (13)을 만족한다.

$$\begin{aligned}\Gamma_n = {} & (x+r_i)[(x+r_{i+1})\Gamma_{i-1}\Gamma_{i+2,n}+\Gamma_{i-2}\Gamma_{i+2,n} \\ & +\Gamma_{i-1}\Gamma_{i+2,n(i+3)}]+(x+r_{i-1})\Gamma_{i-3}\Gamma_{i+1,n} \\ & +\Gamma_{i-4}\Gamma_{i+1,n}+\Gamma_{i-3}\Gamma_{i+2,n}+(x+r_{i+1})\Gamma_{i-1}\Gamma_{i+3,n} \\ & +\Gamma_{i-2}\Gamma_{i+3,n}+\Gamma_{i-1}\Gamma_{i+4,n} \quad \cdots (13)\end{aligned}$$

표 5. 특성다항식이 두 개의 기약다항식의 곱으로 이루어진 8-셀 1차원 LFHCA의 특성다항식들과 대응하는 전이규칙
Table 5. Transition rules corresponding to characteristic polynomials of 8-cell 1-D LFHCA whose characteristic polynomial is the product of two irreducible polynomials

char. poly.	LFHCA Rule (type I)	Combination of two 90/150 CAs ($\mathbb{C}_1$, $\mathbb{C}_2$)	LFHCA Rule (type I)	Combination of two 90/150 CAs ($\mathbb{C}_1$, $\mathbb{C}_2$)
$m_1(x)m_3(x)$	00100110	$T_1 \& T_5$	00011001	$T_5 \& T_1$
	00110010	$T_1 \& T_6$	00110001	$T_6 \& T_1$
	10001100	$T_2 \& T_5$	01001100	$T_5 \& T_2$
	10011000	$T_2 \& T_6$	01100100	$T_6 \& T_2$
$[m_1(x)]^2$	00110011	$T_1 \& T_1$	10011001	$T_2 \& T_1$
	01100110	$T_1 \& T_2$	11001100	$T_2 \& T_2$
$m_1(x)m_2(x)$	01100111	$T_1 \& T_3$	10011011	$T_3 \& T_1$
	01110011	$T_1 \& T_4$	10110011	$T_4 \& T_1$
	11001101	$T_2 \& T_3$	11001110	$T_3 \& T_2$
	11011001	$T_2 \& T_4$	11100110	$T_4 \& T_2$
$[m_2(x)]^2$	11001111	$T_3 \& T_3$	11100111	$T_4 \& T_3$
	11011011	$T_3 \& T_4$	11110011	$T_4 \& T_4$
$m_2(x)m_3(x)$	10001110	$T_3 \& T_5$	01001101	$T_5 \& T_3$
	10011010	$T_3 \& T_6$	01100101	$T_6 \& T_3$
	10100110	$T_4 \& T_5$	01011001	$T_5 \& T_4$
	10110010	$T_4 \& T_6$	01110001	$T_6 \& T_4$
$[m_3(x)]^2$	00001100	$T_5 \& T_5$	00100100	$T_6 \& T_5$
	00011000	$T_5 \& T_6$	00110000	$T_6 \& T_6$

여기서, $\Gamma_{i+1,n}$은 전이규칙 $<r_{i+1}, \cdots, r_n>$로 이루어진 $\mathbb{P}_n$의 부분 전이행렬에 대한 특성다항식이며, $\Gamma_{i+2,n(i+3)}$은 전이규칙 $<r_{i+2}, \cdots, r_n>$로 이루어진 $\mathbb{P}_n$의 부분 전이행렬에서 2행, 2열을 소거한 행렬의 특성다항식이다.

(증명) $\mathbb{P}_n$의 상태전이행렬 M_n에 대하여 (M_n+xI_n)를 H라 두면 Γ_n은 (14)와 같다.

$$\Gamma_n=(x+r_i)|H_{i,i}|+|H_{i,i-2}|+|H_{i,i+2}| \quad \cdots (14)$$

여기에서 $H_{i,i}$는 H에서 i번째 행과 i번 째 열을 소거

한 소행렬의 행렬식이다. $(H_{i,i})_{k,l}$을 $H_{i,i}$에서 k번째 행과 l번째 열을 소거한 소행렬이라 하면 $|H_{i,i}|$는 (15)와 같다.

$$|H_{i,i}| = (x+r_{i+1})|(H_{i,i})_{i,i}| + |(H_{i,i})_{i,i-1}| + |(H_{i,i})_{i,i+2}| \quad \cdots (15)$$

(15)에서 $|(H_{i,i})_{i,i}| = \Gamma_{i-1}\Gamma_{i+2,n}$이고, $|(H_{i,i})_{i,i-1}| = \Gamma_{i-2}\Gamma_{i+2,n}$이다.

$(H_{i,i})_{i,i+2}$은 $\begin{pmatrix} P_1 & J \\ O & P_2 \end{pmatrix}$와 같은 형태의 블록행렬이다. 따라서 $|(H_{i,i})_{i,i+2}| = |P_1| \cdot |P_2|$이다.

$|P_1| = \Gamma_{i-1}$이고, P_2의 1열은 (2,1)성분만 1이고 나머지 성분은 0이다.

$|P_2|$는 전이규칙이 $< r_{i+2}, r_{i+3}, \cdots, r_n >$인 $\mathbb{P}_n$의 부분 전이행렬에서 2번째 행과 2번째 열을 소거한 행렬의 특성다항식과 같다. 이것을 $\Gamma_{i+2,n(i+3)}$로 표기한다. 그러므로 $|H_{i,i}|$는 (16)과 같다.

$$|H_{i,i}| = (x+r_{i+1})\Gamma_{i-1,i+2,n} + \Gamma_{i-2}\Gamma_{i+2,n} + \Gamma_{i+2,n(i+3)} \quad \cdots (16)$$

(14)에서 $|H_{i,i-2}|$를 구하기 위해 $H_{i,i-2}$의 $(i-1)$번째 열에 대해 여인수 전개 하면 $|H_{i,i-2}| = |(H_{i,i-2})_{i-2,i-1}| + |(H_{i,i-2})_{i+1,i-1}|$이다. $|(H_{i,i-2})_{i+1,i-1}| = 0$이므로 (17)을 만족한다.

$$|H_{i,i-2}| = |(H_{i,i-2})_{i-2,i-1}| = (x+r_{i-1})\Gamma_{i-3}\Gamma_{i+1,n} + \Gamma_{i-4}\Gamma_{i+1,n} + \Gamma_{i-3}\Gamma_{i+2,n} \quad \cdots (17)$$

그리고 유사한 방법으로 $|H_{i,i+2}|$를 구하면 $|H_{i,i+2}| = |(H_{i,i+2})_{i-2,i}| + |(H_{i,i+2})_{i+1,i}|$이고, $|(H_{i,i+2})_{i-2,i}| = 0$이다. 따라서 $|H_{i,i+2}|$은 식 (18)을 만족한다.

$$|H_{i,i+2}| = |(H_{i,i+2})_{i+1,i}| = (x+r_{i+1})\Gamma_{i-1}\Gamma_{i+3,n} + \Gamma_{i-2}\Gamma_{i+3,n} + \Gamma_{i-1}\Gamma_{i+4,n} \quad \cdots (18)$$

그러므로 (14), (16), (17), (18)에 의하여 Γ_n은 (13)을 만족한다. □

이웃 의존도가 유형 I인 1차원 LFHCA의 합성은 작은 크기의 두 개의 이웃 의존도가 유형 I인 1차원 LFHCA를 이용하여 큰 크기의 LFHCA를 합성하는 것이다. 이웃 의존도가 유형 I인 1차원 LFHCA는 그 구조가 90/150 CA에 의해 유도될 수 있음을 (9)와 (10)에 의해 알 수 있다.

전이규칙이 $< r_1, r_2, \cdots, r_i, r_{i+1}, \cdots r_n >$ 인 이웃 의존도가 유형 I인 n-셀 1차원 LFHCA는 $< r_1, r_2, \cdots, r_i >$인 i-셀 1차원 LFHCA $\mathbb{F}_1$과 전이규칙이 $< r_{i+1}, \cdots, r_n >$ 인 $(n-i)$-셀 1차원 LFHCA $\mathbb{F}_2$를 연결하여 만든 것이다. 그리고 $\mathbb{F}_1$의 특성다항식 Γ_i은 전이규칙이 $<\cdots, r_{i-3}, r_{i-1}>$인 k_1-셀 90/150 CA $\mathbb{C}_1$의 특성다항식 O_{k_1}과 전이규칙이 $<\cdots, r_{i-2}, r_i>$인 k_2-셀 90/150 CA $\mathbb{C}_2$의 특성다항식 Δ_{k_2}의 곱으로 표현된다. 즉, $\Gamma_i = O_{k_1}\Delta_{k_2}$이다. 이때 $k_1 = \lfloor i/2 \rfloor$이고 $k_2 = \lceil i/2 \rceil$이다. 마찬가지로 $\mathbb{F}_2$의 특성다항식 $\Gamma_{i+1,n}$은 전이규칙이 $< r_{i+1}, r_{i+3}, \cdots >$인 k_3-셀 90/150 CA $\mathbb{C}_3$의 특성다항식 ∇_{k_3}와 전이규칙이 $< r_{i+2}, r_{i+4}, \cdots >$인 k_4-셀 90/150 CA $\mathbb{C}_4$의 특성다항식 V_{k_4}의 곱인 $\Gamma_{i+1,n} = \nabla_{k_3} V_{k_4}$으로 표현된다. 이때 $k_3 = \lceil (n-i)/2 \rceil$이고 $k_4 = \lfloor (n-i)/2 \rfloor$이다. $\mathbb{F}_1$과 $\mathbb{F}_2$를 연결하는 과정에서 i번째 셀은 $i+2$번째 셀과 연결이 되고, $(i-1)$번째 셀은 $(i+1)$번째 셀과 연결된다. 즉 $\mathbb{C}_1$은 $\mathbb{C}_3$와 연결되고 $\mathbb{C}_2$은 $\mathbb{C}_4$와 연결된다. 그러므로 Γ_n은 (5)에 의해 (19)를 만족한다.

$$\Gamma_n = (O_{k_1}\nabla_{k_3} + O_{k_1-1}\nabla_{2,k_3})(\Delta_{k_2} V_{k_4} + \Delta_{k_2-1} V_{2,k_4}) \quad \cdots (19)$$

Ⅳ. 결 론

본 논문에서는 기본 CA인 3-이웃 선형 하이브리드 CA에서 이웃 반경을 확장한 1차원 5-이웃 선형 하이브리드 CA에 대하여 분석하였다. 먼저 5-이웃 CA의 선형 규칙을 정리하고, 90/150 CA와 같이 무작위성이 높은 규칙들만 선별하여 2개의 선형 규칙을 조합하여 하이브리드 CA를 구성할 수 있도록 이웃 의존도를 유형별로 정리하였다. 특별히 이웃 의존도가 유형 I인 1차원 5-이웃 LFHCA의 특성다항식의 점화관계를 분석하고 작은 단위의 5-이웃 LFHCA 2개를 이용하여 큰 단위의 5-이웃 LFHCA를 합성할 때, 합성된 CA의 특성다항식의 점화관계를 분석하였으며, 복잡한 점화관계를 90/150 CA의 특성다항식을 이용하여 효과적으로 구할 수 있는 방법을 제시하였다. 이러한 결과는 1차원 LFHCA가 의사난수열 생성기로 적용될 때, 시스템의 성질에 맞는 CA를 효과적으로 합성하는데 도움이 될 것으로 사료된다.

감사의 글

본 논문은 20024년도 한국전자통신학회 봄철 학술대회 우수논문을 확장한 논문임.

References

[1] J. Von Neumann, Theory of self-reproducing automata, Urbana and London:University of Illinois Press, , 1966.

[2] G.C. Stanica and P. Anghelescu, "Cryptographic Algorithm Based on Hybrid One-Dimensional Cellular Automata," *Mathematics*, vol. 11, no. 6, 2023, 1481.
https://doi.org/10.3390/math11061481

[3] H. Jeong, S. Cho, and S. Kim, "Medical image encryption based on C-MLCA and 1D CAT," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 14, no. 2, Apr. 2019, pp. 439-446.
https://doi.org/10.13067/JKIECS.2019.14.2.439

[4] K. Islam, M.F. Rahman, M. Jashimuddin, "Modeling land use change using Cellular Automata and Artificial Neural Network: The case of Chunati Wildlife Sanctuary, Bangladesh," *Ecological Indicators*, vol. 88, May 2018, pp. 439-453.
https://doi.org/10.1016/j.ecolind.2018.01.047

[5] W. Gilpin, "Cellular automata as convolutional neural networks," Phys. Rev. E, vol. 100, no. 3, Sept. 2019, 032402(1-11)
https://doi.org/10.1103/PhysRevE.100.032402

[6] M. Ahangaran, N. Taghizadeh and H. Beigy, "Associative cellular learning automata and its applications," *Appl. Soft Comput.* vol. 53, Apr. 2017, pp. 1-18.
https://doi.org/10.1016/j.asoc.2016.12.006

[7] P.P. Chaudhuri, D.R. Chowdhury, S. Nandi and S. Chattopadhyay, *Additive cellular automata, Theory and applications, vol. 1*, Los Alamitos; California; IEEE Computer Society Press, 1997.

[8] U. Choi, S. Cho, H. Kim, M. Kwon, J. Kim and S. Kang, "Analysis of 90/150 CA Concatenated using Inverse Symmetric Transition Rule," *Int. J. Control Autom.*, vol. 10, no. 10, 2017, pp. 217-228.
https://doi.org/10.14257/ijca.2017.10.10.18

[9] U. Choi, "5-Neighbor Programmable CA based PRNG," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 17, no. 2, Apr. 30. 2022. pp. 357-364.
http://doi.org/10.13067/JKIECS.2022.17.2.357

[10] U. Choi, S. Cho, H. Kim and S. Kang "Design and Analysis of Pseudorandom Number Generators Based on Programmable Maximum Length CA," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 15, no. 2, Apr. 2020. pp. 319-326
http://doi.org/10.13067/JKIECS.2020.15.2.319

저자 소개

최언숙(Un-Sook Choi)

1992년 성균관대학교 산업공학과 졸업(공학사)
2000년 부경대학교 대학원 응용수학과 졸업(이학석사)
2004년 부경대학교 응용수학과 졸업(이학박사)
2009년 부경대학교 정보보호학과 졸업(공학박사)
2009년~ 현재 동명대학교 소프트웨어학과 교수
※ 관심분야 : 셀룰라 오토마타론, 정보보호, 사물인터넷, 인공지능