Regular paper | Journal of the KIECS. pp. 357-364, vol. 17, no. 2, Apr. 30. 2022, t. 112, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2022.17.2.357

프로그램 가능한 5-이웃 CA기반의 PRNG

최언숙*

5-Neighbor Programmable CA based PRNG

Un-Sook Choi*

요 약

의사난수 생성기(PRNG)는 많은 양의 난수가 필요할 때 사용되는 프로그램이다. 대칭 키 암호시스템에서 대칭 키를 생성, 공개 키 암호나 디지털 서명에서 공개 키 쌍의 생성, 일회용 패드로 패딩에 사용되는 열을 생성하는 데 사용한다. 다양한 과학 분야에서 비선형 동역학계를 구체적으로 표현하는데 유용한 셀룰라 오토마타(CA)는 이산적이고 추상적인 계산 시스템으로 하드웨어 구현이 가능하여 암호시스템에서 키를 생성하는 PRNG로 응용되고 있다. 본 논문에서는 이웃 셀의 반경을 2로 증가한 5-이웃 CA를 이용하여 비선형 수열을 효과적으로 생성할 수 있는 프로그램 가능한 5-이웃 CA기반의 PRNG를 합성하는 알고리즘을 제안한다.

ABSTRACT

A pseudo-random number generator (PRNG) is a program used when a large amount of random numbers is needed. It is used to generate symmetric keys in symmetric key cryptography systems, generate public key pairs in public key cryptography or digital signatures, and generate columns used for padding with disposable pads. Cellular Automata (CA), which is useful for specific representing nonlinear dynamics in various scientific fields, is a discrete and abstract computational system that can be implemented in hardware and is applied as a PRNG that generates keys in cryptographic systems. In this paper, I propose an algorithm for synthesizing a programmable 5-neighbor CA based PRNG that can effectively generate a nonlinear sequence using 5-neighbor CA with the radius of the neighboring cell increased by 2.

키워드

Pseudo Random Number Generator, Cellular Automata, 5-neighbor, Programmable CA, Nonlinear Sequence
의사 난 수열 생성기, 셀룰라 오토마타, 5-이웃, 프로그램 가능한 CA, 비선형 수열

Ⅰ. 서론

최근 전 세계는 초연결성과 초지능화로 특징되는 디지털 혁신의 제4차 산업혁명 시대 진입으로 사회·경제·문화 전반에 대변혁이 촉발되고 있다. 특히 COVID-19의 대유행은 지금까지 경제적, 사회 문화적 장벽에 가로막혀 도입되지 못했던 혁신적 기술들을 일상에 과감히 도입하게 만드는 효과를 유발하고 있다. 지금까지 이론적 기술적으로 구현되었지만 여러 가지 이유로 확산되지 못했던 4차 산업혁명의 기술 트렌드를 일상 영역에서 비로소 시도하게끔 만드는 동력으로 작용하고 있다. 초연결은 사람과 사물이 서

* 교신저자 : 동명대학교 AI학부
• 접 수 일 : 2022. 02. 24
• 수정완료일 : 2022. 03. 22
• 게재확정일 : 2022. 04. 17
• Received : Feb. 24, 2022, Revised : Mar. 22, 2022, Accepted : Apr. 17, 2022
• Corresponding Author : Un-Sook Choi,
School of Artificial Intelligence, Tongmyong University
Email : choies@tu.ac.kr

로 긴밀히 연결되어 소통하고 상호작용함으로써 경계 없는 미래를 만들어낸다. 초연결로 인한 접점이 늘어나면서 공격 경로도 확대되고 다양해졌으며 이 때문에 사이버범죄, 테러, 인프라 마비 등 초연결 위협에 대응하는 지능형 정보보호 기술이 필요해졌다. 정보보안은 단순히 산업의 영역을 벗어나 국가안보와 국민생명이 직결된 국가기간산업으로서 가치가 강조되는 추세이다.

정보를 보호하는 방법은 다양하다. 이 중 개인정보는 기존의 정형데이터 뿐만이 아니라 각종 이미지 파일, 문서, 로그 데이터 등에도 많이 포함되어 있으며 특히 은행권이나 의료기관은 개인 정보를 스캔한 이미지 파일도 많이 보관하고 있어 이를 암호화해야 할 필요가 있다. 의사난수 생성기(PRNG)는 많은 양의 난수가 필요할 때 사용되는 프로그램이다. 대칭 키 암호시스템에서 대칭 키를 생성, 공개 키 암호나 디지털 서명에서 공개 키 쌍의 생성, 일회용 패드로 패딩에 사용되는 열을 생성하는 데 사용한다. CA는 Wolfram에 의해 암호 시스템에서 난수 발생기로 처음 적용된 이후 암호시스템의 키 생성기 또는 이미지 암호 알고리즘에 적용되고 있다. 지난 30년 간 1차원 CA기반의 PRNG가 광범위하게 연구되었다[1-3].

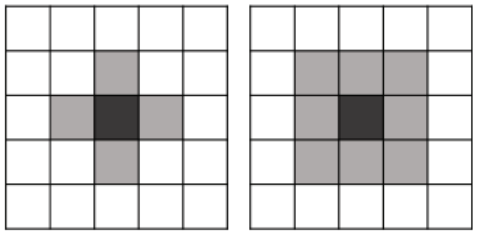
CA는 다양한 과학 분야에서 비선형 동역학계를 구체적으로 표현하는데 유용하다. CA의 고유 특성은 첫 번째 일반적으로 시간과 공간을 이산적으로 다룬다. 셀이라 불리는 일정하고 단순한 단위들의 집합으로 구성된다. 각 시간 단위에서 셀은 유한한 상태를 가지며 이웃으로 정의된 셀 상태와 국소적인 전이규칙에 따라 병렬로 상태가 업데이트 된다. 두 번째 CA는 추상적이다. 순전히 수학적으로 지정할 수 있으며 물리적 구조에서 구현 가능하다. 세 번째 CA는 계산 시스템이다. 기능을 계산하고 알고리즘 문제를 해결할 수 있다. CA는 순수하고 추상적인 환경에서 패턴 형성과 복잡성을 연구하고자 하는 인지 및 자연 과학에까지 응용되고 있다.

본 논문에서는 1차원 CA의 이웃의 반경을 2로 증한 1차원 5-이웃 CA중 특정한 2개의 규칙을 조합하여 만들어진 CA의 특성을 분석하고 이를 이용하여 비선형 수열을 생성하는 PRNG를 합성할 수 있는 알고리즘을 제안한다.

II. 관련 연구

검사 패턴 또는 암호 시스템에서 PRNG로 사용되는 효과적인 CA를 합성하기 위한 연구들이 수행되었다. 최대 주기 수열을 발생시킬 수 있는 최대 주기 CA에 대한 연구가 Cattell 등에 의해 처음 연구되었다[4]. 그들은 1차원 3-이웃 CA에 적용되는 규칙 중 확산과 랜덤성이 우수한 규칙 90과 150을 사용하여 모든 기약다항식에 대응하는 90/150 CA를 합성하였다. 이 후 Cho 등은 참고문헌 [4]에서 제안된 알고리즘을 개선하기 위해 LT(Lanczos Tridiagonalization) 방법을 기반으로 하는 새로운 합성 알고리즘을 제안했다[5]. 제안된 알고리즘은 계산 복잡도를 $O(n^7)$에서 $O(n^2)$으로 크게 줄였으며, 특히 기약다항식뿐 아니라 모든 CA 다항식에 대응하는 90/150 CA를 합성할 수 있는 알고리즘이다. 이를 바탕으로 기약다항식의 거듭제곱형태의 특성다항식에 대응하는 90/150 CA, 해시 함수 설계에 응용되는 비그룹 90/150 CA, 최대 무게 다항식에 대응하는 90/150 CA 등 90/150 CA의 합성 방법이 수학적 이론을 바탕으로 광범위하게 연구되었다[6-9].

최근 2차원 CA PRNG가 관심을 받고 있다[10]. 2차원 CA의 각 셀에 대한 여러 이웃 구조가 제안되었으나 일반적으로 알려진 이웃은 두 가지 유형으로 Neumann 이웃과 Moor 이웃이다[10, 11]. 그림 1은 이웃 반경이 1인 Newman 및 Moor 이웃 구조를 보여준다. 2차원 CA 기반의 PRNG는 무작위성은 1차원 CA PRNG보다 나은 것으로 보이지만 설계의 복잡성과 계산 효율성을 고려할 때 어느 것이 낫다고 단정 짓기는 어렵다. Maiti 등은 5-이웃 CA에 의해 생성된 이진수열의 난수성을 검증하기 위해 24비트 대칭 5-이



(a) Neumann neighborhood (b) Moor neighborhood

그림 1. 2차원 CA의 이웃 구조
Fig. 1 Neighbor structure of 2 dimensional CA

웃 최대 주기 선형 하이브리드 CA를 사용하여 15개의 검사로 구성된 NIST 통계 검증을 수행하였으며 높은 난수성이 있음을 확인하였다[12].

Krylov 행렬을 이용하여 최대 주기를 갖는 대칭 5-이웃 CA합성법이 참고문헌 [13]에서 제안되었으며, Choi 등은 참고문헌 [13]에서 제안된 비선형 방법을 개선한 대칭 5-이웃 합성법을 제안하였다[14].

III. 1차원 선형 5-이웃 CA

1차원 CA는 기본 CA (Elementary CA)로 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. 그림 2는 1차원 CA의 이웃 구조이다.

N_i를 i번째 셀 c_i의 이웃에 대한 집합이라고 할 때, 이웃의 반경인 r CA의 N_i는 식 (1)과 같다.

$$N_i = \{c_k | i-r \le k \le i+r\} \quad (1)$$

(a) 3-neighbor (radius = 1)　　(b) 5-neighbor (radius = 2)

그림 2. 1차원 CA의 이웃 구조
Fig. 2 Neighbor structure of 1 dimensional CA

c_i^t를 시간 t에서 i번째 셀의 상태라 하고, g_i를 i번째 셀의 상태전이 함수라 할 때, 다음상태 c_i^{t+1}를 구하는 기본 CA의 상태전이 함수는 식 (2)와 같다.

$$c_i^{t+1} = g_i(c_{i-1}^t, c_i^t, c_{i+1}^t) \quad (2)$$

5-이웃 CA의 상태전이 함수는 이웃의 반경이 2이므로 이웃의 개수가 5이다. 그러므로 i번째 셀의 상태전이 함수 f_i는 식 (3)과 같다.

$$c_i^{t+1} = f_i(c_{i-2}^t, c_{i-1}^t, c_i^t, c_{i+1}^t, c_{i+2}^t) \quad (3)$$

기본 CA의 전이규칙은 3개의 이웃에 대해 2^3개의 상태가 존재하므로 $2^{2^3} = 256$개의 전이규칙이 존재한다. 또한 전이규칙이 XOR 논리로만 표현되는 전이규칙은 $c_i^{t+1} = p \cdot c_{i-1}^t \oplus q \cdot c_i^t \oplus r \cdot c_{i+1}^t$에서 p, q, r이 0 또는 1이므로 모두 0이 되는 경우를 제외하면 7개의 전이규칙이 존재한다. 표 1은 기본 CA의 선형 전이규칙과 여원 전이규칙의 부울식 표현이다.

표 1. 기본 CA의 선형규칙과 여원규칙의 부울식 표현
Table 1. Boolean expressions of linear rules and complement rules of elementary CA

Rule No.	Boolean expression	Rule Type
15	$c_i^{t+1} = c_{i-1}^t \oplus 1$	Comp.
41	$c_i^{t+1} = c_i^t \oplus 1$	Comp.
60	$c_i^{t+1} = c_{i-1}^t \oplus c_i^t$	Linear
85	$c_i^{t+1} = c_{i+1}^t \oplus 1$	Comp.
90	$c_i^{t+1} = c_{i-1}^t \oplus c_{i+1}^t$	Linear
102	$c_i^{t+1} = c_i^t \oplus c_{i+1}^t$	Linear
105	$c_i^{t+1} = c_{i-1}^t \oplus c_i^t \oplus c_{i+1}^t \oplus 1$	Comp.
150	$c_i^{t+1} = c_{i-1}^t \oplus c_i^t \oplus c_{i+1}^t$	Linear
153	$c_i^{t+1} = c_i^t \oplus c_{i+1}^t \oplus 1$	Comp.
165	$c_i^{t+1} = c_{i-1}^t \oplus c_{i+1}^t \oplus 1$	Comp.
170	$c_i^{t+1} = c_{i+1}^t$	Linear
195	$c_i^{t+1} = c_{i-1}^t \oplus c_i^t \oplus 1$	Comp.
204	$c_i^{t+1} = c_i^t$	Linear
240	$c_i^{t+1} = c_{i-1}^t$	Linear

1차원 5-이웃 CA의 전이규칙은 5개의 이웃에 대해 2^5개의 상태가 존재하므로 $2^{2^5} = 4{,}294{,}967{,}296$개의 전이규칙이 존재한다. 또한 선형 전이규칙의 수와 여원 전이규칙의 수는 각각 31개이다.

선형 CA의 상태전이 함수는 행렬로 나타낼 수 있으며 이 행렬을 상태전이행렬이라고 한다. 기본 CA의 상태전이행렬은 삼중 대각행렬로 표현된다. 선형 기본 CA중 각 셀에 적용된 규칙이 90과 150 (표 1)으로만 이루어진 CA를 90/150 CA라 하는데 n개의 셀로 이루어진 90/150 CA의 상태전이행렬 T_n은 식 (4)와 같다 [15].

$$T_n=(t_{ij})_{n\times n}=\begin{cases}d_i\,, i=j\\ 1\ \ , i=j+1 \text{ or } i=j-1\\ 0\ \ , otherwise\end{cases} \quad (4)$$

여기서 i번째 셀에 적용된 전이규칙이 90인 경우 $d_i=0$ 이고 전이규칙이 150인 경우 $d_i=1$이다. T_n을 주대각선 성분을 이용하여 $<d_1d_2\cdots d_n>$로 간단히 표현한다. 전이규칙이 $<d_1d_2\cdots d_n>$인 n-셀 90/150 CA의 T_n에 대하여 특성다항식 $C_n=|T_n+xI_n|$은 식 (5)를 만족한다[8].

$$C_n=(x+d_n)C_{n-1}+C_{n-2}\,(n\geq 1) \quad (5)$$

여기서 I_n은 n차 단위행렬, C_{n-i}은 $<d_1d_2\cdots d_{n-i}>$로 이루어진 90/150 CA의 특성다항식이고, $C_0=1, C_{-1}=0$이다.

1차원 5-이웃 CA의 모든 셀에 적용되는 f_i $(i=1,2,\cdots)$ 가 XOR논리로 표현될 때 주어진 선형 5-이웃 CA이다. 그림 3은 선형 5-이웃 CA의 구조이다.

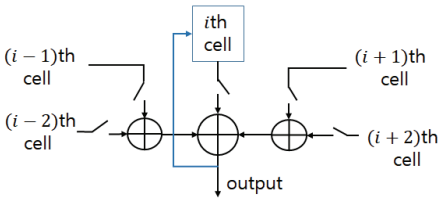


그림 3. 선형 5-이웃 CA의 구조
Fig. 3 Structure of Linear 5-Neighbor CA

1차원 3-이웃 CA의 효과적 합성을 위해 전이규칙을 90과 150으로 제한한 것과 같이 선형 5-이웃 CA의 효과적 합성을 위해 이웃의 의존도를 몇 가지로 제한한다. 이때 셀의 상태전이를 위해 참여하는 이웃의 수를 3-이웃 90/150 CA보다는 크거나 같게 둔다. 표 2은 선형 5-이웃 CA의 이웃의 의존도에 따른 분류와 상태전이 함수의 부울식 표현이다.

전이규칙이 $<r_1,r_2,r_3,\cdots,r_n>$인 n-셀 선형 5-이웃 CA의 특성다항식 $g(x)$를 Γ_n라 하고 Γ_i를 $<r_1,r_2,r_3,\cdots,r_i>$까지 부분 선형 5-이웃 CA의 특성다항식이라고 하자. 표 2에서 유형 II의 선형 5-이웃 CA $\mathbb{F}_n$는 90/150 CA이므로 특성다항식 Γ_n은 $\Gamma_n=(x+u_n)\Gamma_{n-1}+\Gamma_{n-2}$ 이다.

표 2. 1차원 선형 5-이웃 CA의 이웃 의존도에 따른 분류와 부울식 표현
Table 2. Classification and Boolean expression according to neighbor dependence of 1-D linear 5-neighbor CA

Type	Boolean expression
I	$c_i^{t+1}=\ c_{i-2}^t\oplus r_i\cdot c_i^t\oplus c_{i+2}^t$
II	$c_i^{t+1}=\ c_{i-1}^t\oplus r_i\cdot c_i^t\oplus c_{i+1}^t$
III	$c_i^{t+1}=\ c_{i-2}^t\oplus c_{i-1}^t\oplus r_i\cdot c_i^t\oplus c_{i+1}^t\oplus c_{i+2}^t$
IV	$c_i^{t+1}=\ c_{i-1}^t\oplus r_i\cdot c_i^t\oplus c_{i+1}^t\oplus c_{i+2}^t$
V	$c_i^{t+1}=\ c_{i-2}^t\oplus c_{i-1}^t\oplus r_i\cdot c_i^t\oplus c_{i+1}^t$
VI	$c_i^{t+1}=\ c_{i-2}^t\oplus r_i\cdot c_i^t\oplus c_{i+1}^t\oplus c_{i+2}^t$
VII	$c_i^{t+1}=\ c_{i-2}^t\oplus c_{i-1}^t\oplus r_i\cdot c_i^t\oplus c_{i+2}^t$
VIII	$c_i^{t+1}=\ c_{i-2}^t\oplus r_i\cdot c_i^t\oplus c_{i+1}^t$
IX	$c_i^{t+1}=\ c_{i-1}^t\oplus r_i\cdot c_i^t\oplus c_{i+2}^t$

전이규칙이 $<r_1,r_2,r_3,\cdots,r_n>$ 인 유형 III의 선형 5-이웃 CA는 대칭 1차원 5-이웃 CA라 부르며, 상태전이행렬 $M_n=(v_{i,j})_{n\times n}$은 식 (6)과 같고, 특성다항식 Γ_n의 점화관계는 식 (7)과 같다[12,14].

$$v_{ij}=\begin{cases}r_i,\ i=j\\ 1,\ |i-j|=1 \text{ or } 2\\ 0,\ o/w\end{cases} \quad (6)$$

$$\Gamma_n=(x+u_n)\Gamma_{n-1}+\Gamma_{n-2}+(x+u_{n-1})\Gamma_{n-3}+\Gamma_{n-4}\ (n\geq 1) \quad (7)$$

단, $\Gamma_{-3}=\Gamma_{-2}=\Gamma_{-1}=0$,$\Gamma_0=1$ 이다.

본 논문에서는 9가지 유형 중 유형 I의 의존도를 가지는 1차원 선형 5-이웃 CA에 대해 다룬다. 특성다항식의 점화관계 및 특성을 분석하고 이를 이용하여 비선형 수열 생성할 수 있는 PRNG를 설계한다.

IV. 프로그램 가능한 5-이웃 CA 기반 PRNG 합성

전이규칙이 $<r_1,r_2,r_3,\cdots,r_n>$ 이고, 이웃 의존도가 유형 I인 n-셀 선형 5-이웃 CA $\mathbb{P}_n$의 상태전이행렬 $B_n=(b_{i,j})_{n\times n}$는 식 (8)과 같다.

다. 즉 가약 다항식이다.

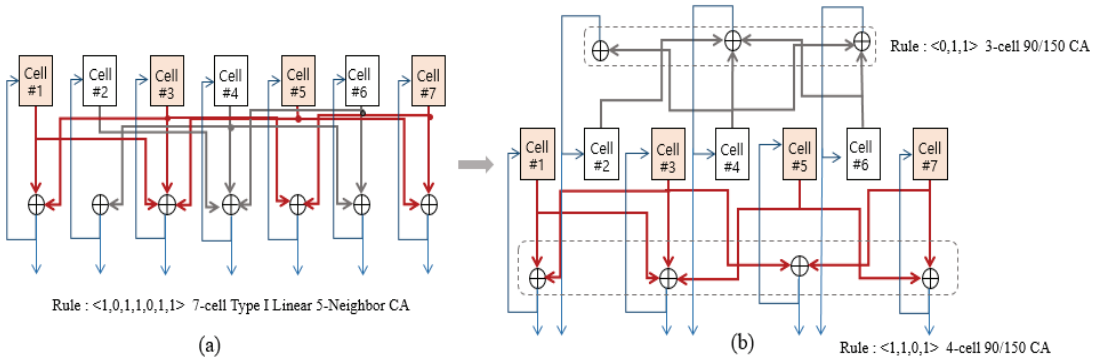


그림 4. 전이규칙 <1,0,1,1,0,1,1>인 7-셀 유형 Ⅰ 선형 5-이웃 CA의 구조와 2개의 90/150 CA로의 분해

Fig. 4 Structure of 7-cell type I linear 5-neighbor CA with transition rule <1,0,1,1,0,1,1> and decomposition into two 90/150 CAs

$$b_{ij}=\begin{cases} r_i, & i=j \\ 1, & j=i-2 \text{ or } j=i+2 \\ 0, & o/w \end{cases} \tag{8}$$

B_n의 특성다항식 Λ_n을 구해보자. $n=1$일 때 $\Lambda_1=x+r_1$ 이고, $n=2$일 때 $\Lambda_2=(x+r_1)(x+r_2)$ 이다. $\Lambda_0=1$, $\Lambda_{-1}=0$라 두면 $\Lambda_2=(x+r_1)\Lambda_1$ 이고 같은 방법으로 Λ_3, Λ_4, $\Lambda_5, \cdots$ 를 정리하면 Λ_n은 식 (9)와 같은 점화 관계를 만족한다.

$$\begin{aligned} \Lambda_3&=(x+r_3)\Lambda_2+(x+r_2)\Lambda_0 \\ \Lambda_4&=(x+r_4)\Lambda_3+(x+r_3)\Lambda_1+\Lambda_0 \\ \Lambda_5&=(x+r_5)\Lambda_4+(x+r_4)\Lambda_2+\Lambda_1 \\ &\vdots \\ \Lambda_n&=(x+r_n)\Lambda_{n-1}+(x+r_{n-1})\Lambda_{n-3}+\Lambda_{n-4} \end{aligned} \tag{9}$$

$(n \geq 3, \Lambda_0=1, \Lambda_{-1}=0)$

유형 I의 선형 5-이웃 CA는 2개의 90/150 CA $\mathbb{C}_1$과 $\mathbb{C}_2$를 결합하여 만든 것으로 해석할 수 있다. 이때 $\mathbb{C}_1$의 크기가 m일 때, $\mathbb{C}_2$의 크기는 m 또는 $m-1$이다. 예를 들어 전이규칙이 <1,0,1,1,0,1,1>인 7-셀 유형 Ⅰ의 선형 5-이웃 CA의 구조는 그림 3(a)과 같다. 이 CA는 그림 3(b)와 같이 전이규칙이 <1,1,1,0,1>인 4-cell 90/150 CA와 전이규칙이 <0,1,1>인 3-셀 90/150 CA로 물리적으로 분해될 수 있다. 그러므로 유형 Ⅰ 선형 5-이웃 CA의 특성다항식은 인수분해 된

<정리 1> m-셀 90/150 CA $\mathbb{C}_1$의 상태전이행렬을 $T_o=<o_1o_2\cdots o_m>$ 라 하고, 그 특성다항식을 O_m이라 하자. 그리고 m-셀 90/150 CA $\mathbb{C}_2$의 상태전이행렬을 $T_e=<e_1e_2\cdots e_m>$ 라 하고, 그 특성다항식을 V_m이라 하자. 그러면 전이규칙이 $B_n=<o_1e_1o_2e_2\cdots o_me_m>$인 $2m$-셀 유형 Ⅰ 선형 5-이웃 CA의 특성다항식 Λ_n은 식 (10)을 만족한다.

$$\Lambda_n=O_m\cdot V_m \tag{10}$$

(증명) $B_n=<o_1e_1o_2e_2\cdots o_me_m>$이라 하면 $n=2m$이다. $B_n=<r_1r_2r_3\cdots r_n>$ 이라 하면 r_i는 식 (11)과 같다.

$$u_i=\begin{cases} o_{\lceil i/2 \rceil}, & i: odd \\ e_{i/2}, & i: even \end{cases} \tag{11}$$

$n=1$일 때 $\Lambda_1=x+r_1=O_1$ 이고, $n=2$일 때 $\Lambda_2=(x+r_1)(x+r_2)=O_1V_1$ 이다. 식 (9)와 식 (10)을 이용하여 Λ_3, Λ_4을 구하면 다음과 같다.

$$\begin{aligned} \Lambda_3&=(x+r_3)\Lambda_2+(x+r_2)=(x+r_3)O_1V_1+V_1 \\ &=V_1\{(x+r_3)O_1+1\}=V_1\{(x+o_2)O_1+1\} \\ &=O_2V_1 \end{aligned}$$

$$\begin{aligned} \Lambda_4&=(x+r_4)\Lambda_3+(x+r_3)\Lambda_1+\Lambda_0 \\ &=(x+r_4)O_2V_1+\{(x+o_2)O_1+1\} \\ &=O_2\{(x+r_4)V_1+1\}=O_2V_2 \end{aligned}$$

같은 방법으로 반복하면 다음과 같다.

$$\begin{aligned}\Lambda_{2m-1} &= (x+r_{2m-1})\Lambda_{2m-2} \\ &\quad +(x+r_{2m-2})\Lambda_{2m-4}+\Lambda_{2m-5} \\ &= (x+r_{2m-1})O_{m-1}V_{m-1} \\ &\quad +(x+r_{2m-2})O_{m-2}V_{m-2}+O_{m-2}V_{m-3} \\ &= (x+r_{2m-1})O_{m-1}V_{m-1} \\ &\quad +O_{m-2}\{(x+e_{m-1})V_{m-2}+V_{m-3}\} \\ &= (x+r_{2m-1})O_{m-1}V_{m-1}+O_{m-2}V_{m-1} \\ &= V_{m-1}\{(x+o_m)O_{m-1}+O_{m-2}\}=O_mV_{m-1}\end{aligned}$$

$$\begin{aligned}\Lambda_{2m} &= (x+r_{2m})\Lambda_{2m-1} \\ &\quad +(x+r_{2m-1})\Lambda_{2m-3}+\Lambda_{2m-4} \\ &= (x+r_{2m})O_mV_{m-1} \\ &\quad +(x+r_{2m-2})O_{m-1}V_{m-2}+O_{m-2}V_{m-2} \\ &= (x+r_{2m})O_mV_{m-1} \\ &\quad +V_{m-2}\{(x+o_m)O_{m-1}+O_{m-2}\} \\ &= (x+e)O_mV_{m-1}+O_mV_{m-2} \\ &= O_m\{(x+e_m)V_{m-1}+V_{m-2}\}=O_mV_m\end{aligned}$$

(증명 끝)

전이규칙이 <1,1,1,0,1>인 4-cell 90/150 CA의 특성다항식이 x^4+x^3+1이고, 전이규칙이 <0,1,1>인 3-셀 90/150 CA의 특성다항식이 x^3+x+1이므로 그림 3의 <1,0,1,1,0,1,1>인 7-셀 유형 I의 선형 5-이웃 CA의 특성다항식은 $(x^4+x^3+1)(x^3+x+1)$이다.

정리 1의 결과는 최대무게 다항식 중 CA다항식이 아닌 경우에 대하여 유형 I의 선형 5-이웃 CA를 이용하여 합성 가능한 경우가 존재함을 의미한다. 여기서 CA다항식이란 90/150 CA로 합성 가능한 다항식이다. 예를 들어 6차 최대무게다항식 $f(x)=x^6+x^5+x^4+x^3+x^2+x+1=(x^3+x+1)(x^3+x^2+1)$이고 $f(x)$는 CA 다항식이 아니다. 그러나 x^3+x+1과 x^3+x^2+1은 CA다항식이므로 유형 I의 선형 5-이웃 CA로는 합성이 가능하다. $f(x)$를 특성다항식으로 갖는 유형 I의 선형 5-이웃 CA의 전이규칙은 <0,0,0,1,1,1>,<0,0,1,0,1,1>,<0,1,0,1,1,0>,<0,1,1,0,1,0>,<1,0,0,1,0,1>,<1,0,1,0,0,1>,<1,1,0,1,0,0>,<1,1,1,0,0,0>으로 다양하게 합성할 수 있다. 따라서 정리 1로부터 따름정리 2를 얻는다.

<따름정리 2> 두 개의 기약다항식의 곱으로 인수분해 되는 가약다항식을 특성다항식으로 갖는 유형 I의 선형 5-이웃 CA는 존재하며 합성가능하다.

표 3는 유형 I 선형 5-이웃 CA를 이용하여 프로그램 가능한 5-이웃 기반의 PRNG를 합성하는 알고리즘이다.

표 3. 두 개의 기약다항식의 곱을 특성다항식으로 가지는 유형 I 선형 5-이웃 CA의 합성 알고리즘
Table 3. Synthesis algorithm of type I linear 5-neighbor CA with product of two irreducible polynomials as characteristic polynomial

Input: Product of two irreducible polynomials
(i) $f_1(x)$ with degree n,
(ii) $f_2(x)$ with degree $n$or $n-1$
Output: Type I 5-neighbor CA
$\mathbb{U}=<u_1u_2\cdots u_{2n}>$ or $<u_1u_2\cdots u_{2n-1}>$

Step 1: for k = 1, 2 do the following
(i) $n_k \leftarrow$ degree of $f_k(x)$
(ii) Make the matrix B_k from $x^{i-1}+x^{2i-1}+x^{2i} \bmod f_k(x)$ $(i=1,2,\cdots,n)$
(iii) Solve the equation $B_kv=(0,0,\cdots,0,1)^t$
(iv) Construct a Krylov matrix $H_k=K(C^t,v)$ by the seed vector v, which is a solution of the equation in (iii).
(v) Compute the LU factorization $H_k=LU$
(vi) Compute CA for f(x) by the matrix U using $r_1=a_1$, $r_i=a_{i-1}\oplus a_i$ $(i=2,3,\cdots,n_k-1)$, $r_{n_k}=a_{n_k-1}\oplus c_{n_k-1}$
(vii) $R_k \leftarrow <r_1r_2\cdots r_{n_k}>$
Step 2: deg $\leftarrow n_1+n_2$
Step 3: for j from 1 to deg do the following
(i) if j mod 2 = 1, idx $\leftarrow (j-1)/2$, $r_j \leftarrow R_1$[idx]
else $r_j \leftarrow R_2[j/2]$

표 4. CA 다항식이 아닌 다항식에 대한 유형 I 선형 5-이웃 CA의 전이규칙
Table 4. Transition Rule of Type I Linear 5-Neighbor CA for Non-CA Polynomials

deg.	Ploy.	Factorization	Type I Rule
5	0,4,5	(0,1,2)(0,1,3)	01101
6	MWP	(0,1,3)(0,2,3)	011010
7	0,2,3,5,7	(0,1,3)(0,1,4)	0011011
8	0,1,2,4,8	(0,3,4)(0,1,2,3,4)	10110010
9	0,1,2,3,4,5,9	(0,1,4)(0,2,5)	101110110
10	0,3,5,6,8,9,10	(0,2,5)(0,3,5)	1010111100
11	0,1,2,3,5,8,11	(0,2,5)(0,1,6)	01010111100
12	0,1,5,6,7,11,1 2	(0,1,6)(0,5,6)	000100111100
13	0,5,7,11,13	(0,5,6)(0,6,7)	0001000111000
40	0,5,10,20,40	(0,15,20)(0,5,10,15,20)	0000010100001001010000111001010010101100
78	MWP	(0,3,4,8,9,10,12,13,14,15,18,19,20,21,23,25,26,28,34, 35,37,38,39)(0,1,2,4,5,11,13,14,16,18,19,20,21,24,25, 26,27,29,30,31,35,36,39)	1001011110101010101101100000111100111001111 11000000101110010100011111011111101001
102	MWP	(0,1,3,8,9,12,13,14,15,17,18,19,20,26,28,29,30,31,32, 35,37,42,43,44,48,49,51)(0,2,3,7,8,9,14,16,19,20,21,2 2,23,25,31,32,33,34,36,37,38,39,42,43,48,50,51)	1011001110001110110000011111010000101001011 1001110100111100001000011011100011001101111 0001001010110011011
200	0,25,75,100, 125,175,200	(0,25,100)(0,75,100)	1111011010111001110000000000100110001000101 1010000110001111010110001100101010110010111 1010010001100100101001001111000010100000011 0011001101110000101101100001111100010101011 110101010100001101101110100111111
294	0,49,98,147, 196,245,294	(0,49,147)(0,98,147)	1100100101011000110110110000101001110101001 1011110010100011011100101100000001010001101 1101111010011000111110011100011101001100101 1101110101111100000110110001101101011001111 1101100000010000111011110100110011110100011 0011011111100010110100011011101101101101110 000101110110100000111001110010010101100011

표 4는 제안된 알고리즘을 이용하여 두 개의 기약다항식으로 인수분해 되는 다항식 중 90/150 CA다항식이 아닌 다항식에 대하여 유형 I 선형 5-이웃 CA로 합성한 결과이다. 표 4에서 'MWP'는 최대 무게 다항식(Maximum Weight Polynomial)을 나타낸다. 6차 MWP는 $x^6+x^5+x^4+x^3+x^2+x+1$이다. 0, 4, 5은 다항식 x^5+x^4+1을 의미한다.

Ⅴ. 결론

본 논문에서는 1차원 5-이웃 CA중 유형 I의 선형 5-이웃 CA에 대한 특성을 분석하였다. 특성다항식의 점화관계를 분석하였으며, 특성다항식을 이용하여 주어진 유형 I의 선형 5-이웃 CA는 두 개의 90/150 CA로 해석할 수 있음을 보였다. 이러한 결과는 6차 최대무게 다항식과 같이 기약다항식 두 개의 곱으로 인수분해 되는 다항식 중 90/150 CA로 합성할 수 없는 다항식에 대해서도 유형 I의 선형 5-이웃 CA로 합성 가능함으로 보였다. 향후 분석하지 않은 이웃 유형 Ⅵ~Ⅸ에 5-이웃 CA에 대한 특성 분석과, 본 논문의 연구결과를 암호 알고리즘에 적용하고자 한다.

이 연구는 Tongmyeong University Research Grants 2021(2021A025)의 지원에 의한 것임.

References

[1] M. Matsumoto, "Simple cellular automata as pseudorandom m-sequence generators for built-in self-test," *ACM Trans. Model. Comput. Simul.* vol. 8, no. 1, 1998, pp. 31–42.

[2] S. Guan and S. Tan, "Pseudorandom number generation with self-programmable cellular automata," *IEEE Trans. Comput-Aided Design Integr. Circuits Syst.*, vol. 23, no. 7, 2004, pp. 1095-1101.
[3] S. Cardell and A. Fuster-Sabater, "Linear models for the self-shrinking generator based on CA," J. Cell. Autom., vol. 11, 2016, pp. 195-211.
[4] K. Cattell and J. Muzio, "Synthesis of one-dimensional linear hybrid cellular automata," *IEEE Trans. Comput-Aided Design Integr. Circuits Syst.*, vol. 19, no. 3, 1996, pp. 325-335.
[5] S. Cho, U. Choi, H. Kim, Y. Hwang, J. Kim, and S. Heo, "New synthesis of one-dimensional 90/150 linear hybrid group cellular automata," *IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems,* vol. 26, no. 9, Sept. 2007, pp. 1720-1724.
[6] S. Cho, U. Choi, H. Kim, and H. An, "Analysis of nonlinear sequences based on shrinking generator," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 5, no. 4, 2010, pp. 412-417.
[7] U. Choi, S. Cho, H. Kim, and J. Kim, "90/150 CA corresponding to polynomial of maximum weight," *J. of Cellular Automata*, vol. 13, no. 4, 2018, pp. 347-358.
[8] U. Choi and S. Cho, "Analysis of Pseudorandom Sequences Generated by Maximum Length Complemented Cellular Automata," *J. of the Korean Institute of Communication Sciences*, vol. 14, no. 5, 2019, pp. 1001-1008.
[9] U. Choi, S. Cho, H. Kim, and M. Kwon, "Analysis of 90/150 CA Corresponding to the Power of Irreducible Polynomials," *J. of Cellular Automata*, vol. 14, no. 5-6, 2019, pp. 417-433.
[10] M. Tomassini, M. Sipper, and M. Perrenoud, "On the generation of high-quality random numbers by two-dimensional cellular automata," *IEEE Trans. Comput.* vol. 49, no. 10, Oct. 2000, pp. 1146-1151.
[11] P. Sarkar, "A Brief History of Cellular Automata," ACM Comput Surveys, vol. 32, no. 1, Mar. 2000, pp. 80-107.
[12] S. Maiti and D. Chowdhury, "Study of five-neighborhood linear hybrid cellular automata and their synthesis," *2017 the 3rd Int. Conf. on Mathematics and Computing,* Haldia, India, Jan. 2017, pp. 68-83.
[13] S. Cho, H. Kim, U. Choi, and S. Kang, "Synthesis of Symmetric 1-D 5-neighborhood CA using Krylov Matrix," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 15, no. 6, Dec. 2020, pp. 1105-1111.
[14] U. Choi, H. Kim, S. Kang, and S. Cho, "Design of Key Sequence Generators Based on Symmetric 1-D 5-Neighborhood CA," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 16, no. 3, June 2021, pp. 533-540.
[15] 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.

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 AI학부 교수
※ 관심분야 : 셀룰라 오토마타론, 정보보호, 사물인터넷, 이미지 암호