Regular paper | Journal of the KIECS. pp. 1301-1308, vol. 13, no. 6, Dec. 31 2018, t. 92, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2018.13.6.1301

# 90/150 CA 〈10 … 0〉의 특성다항식

김진경* · 조성진** · 최언숙*** · 김한두**** · 강성원*

## Characteristic Polynomials of 90/150 CA 〈10 … 0〉

Jin-Gyoung Kim* · Sung-Jin Cho** · Un-Sook Choi*** · Han-Doo Kim**** · Sung-Won Kang*

요 약

암호 시스템의 키 생성기로 응용되는 90/150 CA는 LFSR보다 난수성이 뛰어나지만 합성법이 어렵기 때문에 CA 합성법에 대한 연구가 많은 연구자에 의해 진행되어 왔다. 적합한 CA를 합성하기 위해 90/150 CA의 특성다항식에 대한 분석이 선행되어야 한다. 일반적으로 $n$셀 90/150 CA의 특성다항식 $\Delta_n$는 $\Delta_{n-1}$와 $\Delta_{n-2}$을 이용하여 구한다. 본 논문에서는 $n$셀 90/150 CA 〈10 … 0〉의 특성다항식 $H_n(x)$을 $(n-1)$셀 90/150 CA 〈10 … 0〉의 특성다항식 $H_{n-1}(x)$로부터 구하는 방법과 이 방법을 이용하여 $H_{2^n}(x)$로부터 $H_{2^n+i}(x)$와 $H_{2^n-i}(x)$ $(1 \le i \le 2^{n-1})$을 효과적으로 구하는 알고리즘을 제안한다.

ABSTRACT

90/150 CA which are used as key generators of the cipher system have more randomness than LFSRs, but synthesis methods of 90/150 CA are difficult. Therefore, 90/150 CA synthesis methods have been studied by many researchers. In order to synthesize a suitable CA, the analysis of the characteristic polynomial of 90/150 CA should be preceded. In general, the characteristic of polynomial $\Delta_n$ of $n$ cell 90/150 CA is obtained by using $\Delta_{n-1}$ and $\Delta_{n-2}$. Choi et al. analyzed $H_{2^n}(x)$ and $H_{2^n-1}(x)$, where $H_k(x)$ is the characteristic polynomial of $k$ cell 90/150 CA with state transition rule 〈10 … 0〉. In this paper, we propose an efficient method to obtain $H_n(x)$ from $H_{n-1}(x)$ and an efficient algorithm to obtain $H_{2^n+i}(x)$ and $H_{2^n-i}(x)(1 \le i \le 2^{n-1})$ from $H_{2^n}(x)$ by using this method.

키워드

Characteristic Polynomial, Fractal Structure, Cellular Automata, Transition Rule, 90/150 CA
특성 다항식, 프랙탈 구조, 셀룰라 오토마타, 전이 규칙, 90/150 CA

## Ⅰ. 서 론

Wolfram은 1980년대에 3-이웃 1차원 셀룰라 오토마타(CA : Cellular Automata)를 제안하였다[1]. 이러한 CA는 모든 셀이 선형으로 배열되어 있고 각 셀은 자기 자신과 왼쪽과 오른쪽에 인접한 두 개의 셀 상

* 부경대학교 응용수학과 (5892587@hanmail.net, jsm2371@hanmail.net)
** 교신저자 : 부경대학교 응용수학과
*** 동명대학교 정보통신공학과 (choies@tu.ac.kr)
**** 인제대학교 응용수학과 (mathkhd@inje.ac.kr)
· 접 수 일 : 2018. 09. 07
· 수정완료일 : 2018. 10. 26
· 게재확정일 : 2018. 12. 15
· Received : Sep. 07, 2018, Revised : Oct. 26, 2018, Accepted : Dec. 15, 2018
· Corresponding Author : Sung-Jin Cho
Dept. of Applied Math. Pukyong National University,
Email : sjcho@pknu.ac.kr

태에 의해 다음 상태로 갱신되는 시스템이다[2]. 각 셀의 국소적 상호작용에 의해 동시에 갱신되는 CA는 간단하고 규칙적이며 작은 단위로 확장 연결할 수 있기 때문에 하드웨어 구현에 적합하다[3]. 이러한 이유로 CA는 테스트 패턴 생성, 의사난수 생성, 패턴분류, 암호화 및 오류정정부호 등의 많은 분야에서 응용되고 있다[4-8].

CA 중 가장 랜덤성이 뛰어난 것은 90/150 CA이므로 응용에 적합한 90/150 CA를 합성하기 위하여 90/150 CA의 특성다항식인 CA다항식(CA polynomial)에 대한 연구가 진행되어왔다[9-14]. 주어진 CA다항식에 대응하는 90/150 CA의 합성방법을 여러 연구자들이 연구하고 있다. Cho 등은 그룹 CA와 비그룹 CA의 특성다항식을 분석하였고, 그 후에 그들은 최대길이 90/150 CA를 갖는 효율적인 합성방법을 제안하였으며, 그들이 제안한 방법은 기존에 제안된 방법보다 계산 복잡도를 $O(n^7)$에서 $O(n^2)$로 크게 낮추는 효율적인 방법이다[10,11].

Choi 등은 $2^n$셀 90/150 CA $\langle 10\cdots 0\rangle$의 특성다항식 $H_{2^n}(x)$와 $(2^n-1)$셀 90/150 CA $\langle 10\cdots 0\rangle$의 특성다항식 $H_{2^n-1}(x)$을 분석했다[12,13]. 본 논문에서는 $n$셀 90/150 CA $\langle 10\cdots 0\rangle$의 특성다항식 $H_n(x)$을 $(n-1)$셀 90/150 CA $\langle 10\cdots 0\rangle$의 특성다항식 $H_{n-1}(x)$와 $(n-2)$셀 90/150 CA $\langle 10\cdots 0\rangle$의 특성다항식 $H_{n-2}(x)$를 이용한 점화식으로 구하는 방법이 아닌 $(n-1)$셀 90/150 CA $\langle 10\cdots 0\rangle$의 특성다항식 $H_{n-1}(x)$로부터 구하는 방법과 이 방법을 이용하여 $H_{2^n}(x)$로부터 $H_{2^n+i}(x)$와 $H_{2^n-i}(x)$ $(1\le i\le 2^{n-1})$을 효과적으로 구하는 알고리즘을 제안한다. 또한 $H_n(x)$의 계수들을 순차적으로 나열하였을 때 그 배열이 시어핀스키 삼각형 형태의 프랙탈 구조를 가지고 있다는 것을 보인다[15].

## II. 기본 지식

$s_i^t$를 $t$시간에 $i$번째 셀의 상태라 할 때 $s_i^{t+1}$는 다음과 같이 나타낸다. 여기서 $f_i$는 다음 상태를 구하는 전이함수이다.

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

그림 1은 전이규칙 90과 전이규칙 150에 대하여 Wolfram의 표기법으로 나타낸 것이다.


그림 1. Wolfram의 표기법으로 나타낸 전이규칙 90과 전이규칙 150
Fig. 1 The transition rules 90 and 150 represented by Wolfram's notation

본 논문에서 사용하는 전이규칙 90과 전이규칙 150은 다음과 같이 부울함수로 표현된다.

$$\text{전이규칙 90}\quad s_i^{t+1}=s_{i-1}^t\oplus s_{i+1}^t$$
$$\text{전이규칙 150}\quad s_i^{t+1}=s_{i-1}^t\oplus s_i^t\oplus s_{i+1}^t$$

부울함수가 XOR로만 표현되는 규칙을 선형규칙이라 하고, 모든 전이규칙이 선형규칙으로 이루어진 CA를 선형 CA(linear CA)라 한다. 이러한 선형 CA는 상태전이행렬로 표현이 가능하다. 전이규칙 90과 150만으로 이루어진 $n$셀 90/150 선형 CA의 상태전이행렬 $T_n$는 식 (1)과 같다.

$$T_n=\begin{pmatrix} d_1 & 1 & 0 & \cdots & 0 & 0\\ 1 & d_2 & 1 & \cdots & 0 & 0\\ 0 & 1 & d_3 & \cdots & 0 & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots\\ 0 & 0 & 0 & \cdots & d_{n-1} & 1\\ 0 & 0 & 0 & \cdots & 1 & d_n \end{pmatrix} \tag{1}$$

이때 $T_n$를 간단히 주대각 성분만을 이용하여 $<d_1\ d_2\cdots\ d_n>$로 나타낸다. 여기서 전이규칙이 90이면 $d_i=0$, 150이면 $d_i=1$이다.

$n$셀 90/150 CA의 $GF(2)$상의 특성다항식(characteristic polynomial) $\Delta_n$은 $\Delta_n=|T_n\oplus xI_n|$ 이고 식 (2)를 만족한다. 여기서 $I_n$은 $n\times n$ 단위행렬이다.

$$\Delta_n = (x+d_n)\Delta_{n-1} + \Delta_{n-2} \quad (2)$$

여기서 $\Delta_1 = x+1$, $\Delta_0 = 1$이다[3]. $\Delta_n$은 $T_n$의 최소 다항식(minimal polynomial)과 같다[3].

그림 2는 127셀 CA의 상태전이행렬 $<0\cdots 0>$에 대하여 초기상태가 64번째 셀만 1이고 나머지 셀은 0인 $(0\cdots 010\cdots 0)$를 이용하여 64번 상태전이를 시켜 시간에 따라 변해가는 전체 패턴을 나타낸 결과이다. 이 결과는 시어핀스키 삼각형 형태의 프랙탈 구조를 갖는다.

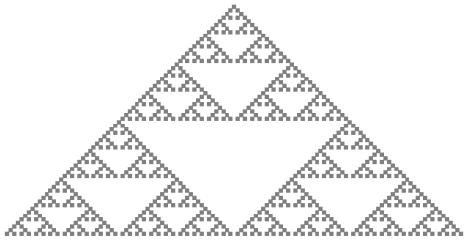

그림 2. 90 UCA의 상태전이에 대응하는 시어핀스키 삼각형 형태의 프랙탈 구조
Fig. 2 Fractal structure in the form of Sierpinski's triangle corresponding to state transition of 90 UCA

전이규칙이 〈10 … 00〉인 $n$셀 90/150 CA의 특성다항식 $H_n(x)$은 식 (3)과 같은 점화식이 성립한다.

$$H_n(x) = x\ H_{n-1}(x) + H_{n-2}(x) (n \geq 2) \quad (3)$$

여기서 $H_1(x) = x+1$, $H_0(x) = 1$ 이다.

식 (4), 식 (5), 식 (6)은 $H_n(x)$에 대한 [12,13]의 연구결과이다.

$$H_{2^n-1}(x) = x^{2^n-1} + \left[H_{2^{n-1}-1}(x)\right]^2 \quad (4)$$

$$H_{2^n}(x) = x^{2^n-1} + \left[H_{2^{n-1}}(x)\right]^2 \quad (5)$$

$$H_{2^n}(x) = x^{2^n} + H_{2^n-1}(x) \quad (6)$$

## III. 전이규칙이 〈10 … 0〉인 90/150 CA의 특성다항식

$H_{2^n-1}(x)$와 $H_{2^n}(x)$의 형태는 식 (4), 식 (5), 식 (6)로부터 식 (7), 식 (8)과 같이 나타낼 수 있다.

$$H_{2^n-1}(x) = x^{2^n-1} + x^{2^n-2^1} + x^{2^n-2^2} + \cdots + x^{2^n-2^{n-1}} + 1 \quad (7)$$

$$H_{2^n}(x) = x^{2^n} + x^{2^n-2^0} + x^{2^n-2^1} + x^{2^n-2^2} + \cdots + x^{2^n-2^{n-1}} + 1 \quad (8)$$

또한 $H_{2^n}(x) \cdot H_{2^n-1}(x) = x^{2^{n+1}-1} + 1$ 는 $x$를 제외한 차수가 $n+1$의 약수인 모든 기약다항식들의 곱이다[13].

$H_i(x)$를 다음과 같이 나타내었다고 하자.

$$H_i(x) = c_{i,0} + c_{i,1}x + \cdots + c_{i,j}x^j + \cdots + c_{i,i-2}x^{i-2} + x^{i-1} + x^i$$

그러면 식 (3)에 의해 식 (9)가 성립한다.

$$c_{i,j} = c_{i-1,j-1} + c_{i-2,j}, (i \geq 2,\ 1 \leq j \leq i,\ c_{0,1} := 0) \quad (9)$$

식 (9)에 $c_{i,0} = c_{i,i-1} = c_{i,i} = 1$은 분명하다.

**정리 1>** 전이규칙이 〈10 … 0〉인 $2l$셀 90/150 CA의 특성다항식 $H_{2l}(x)$의 계수 $c_{2l,k}\ (1 \leq k \leq 2l-2)$는 식 (10)과 같다.

$$c_{2l,k} = \begin{cases} c_{2l-1,2j-1}, & \text{if } k = 2j-1 \\ c_{2l-1,2j-1} + c_{2l-1,2j}, & \text{if } k = 2j \end{cases} \quad (10)$$

여기서 $1 \leq j \leq l-1\ (l \geq 2)$이고 $c_{i,j} := 0 (i < j)$이다.

(증명) $l = 2$일 때 $H_4(x) = 1 + x^2 + x^3 + x^4$이다. 따라서 $c_{4,0} = 1$, $c_{4,1} = 0$, $c_{4,2} = c_{4,3} = c_{4,4} = 1$ 이다.

$c_{4,1} = c_{3,1} = 0, c_{4,2} = c_{3,2} + c_{3,1} = 1$이므로 성립한다. $l = k (k \geq 3)$일 때 식 (10)이 성립한다고 가정하자.

(i) 식 (9)와 귀납가정을 이용하면 $c_{2(k+1),2j-1}$은 다음과 같다.

$$\begin{aligned} & c_{2(k+1),2j-1} \\ &= c_{2k+1,2j-2} + c_{2k,2j-1} \\ &= (c_{2k,2j-3} + c_{2k-1,2j-2}) + c_{2k-1,2j-1} \end{aligned}$$

$= c_{2k,2j-3} + (c_{2k,2(j-1)} + c_{2k-1,2(j-1)-1}) + c_{2k-1,2j-1}$
$= c_{2k,2(j-1)} + c_{2k-1,2j-1}$
$= c_{2(k+1)-1,2j-1}$

(ii) $c_{2(k+1),2j}$도 (i)과 유사한 방법으로 증명하면 다음과 같은 결과를 얻을 수 있다.

$c_{2(k+1),2j} = c_{2(k+1)-1,2j-1} + c_{2(k+1)-1.2j}$

따라서 모든 $l(\geq 2)$, $1 \leq j \leq l-1$에 대하여 식 (10)이 성립한다. (Q.E.D.)

식 (10)을 이용하여 다음 따름정리를 얻는다.

**따름정리 2>** $H_{2l-1}(x)$의 계수 $c_{2l-1,k}$ $(1 \leq k \leq 2l-2)$는 식 (11)과 같다.

$$c_{2l-1,k} = \begin{cases} c_{2l,2j-1}, & \text{if } k = 2j-1 \\ c_{2l,2j-1} + c_{2l,2j}, & \text{if } k = 2j \end{cases} \quad (11)$$

여기서 $1 \leq j \leq l-1 (l \geq 2)$이고 $c_{i,j} := 0 (i < j)$이다.

**정리 3>** 전이규칙이 〈10 … 0〉인 $(2k+1)$셀 90/150 CA의 특성다항식 $H_{2k+1}(x)$의 계수 $c_{2k+1,s}$ $(0 \leq s \leq 2k-1)$는 식 (12)와 같다.

$$c_{2k+1,s} = \begin{cases} c_{2k,2i}, & \text{if } s = 2i \\ c_{2k,2i} + c_{2k,2i+1}, & \text{if } s = 2i+1 \end{cases} \quad (12)$$

여기서 $0 \leq i \leq k-1 (k \geq 1)$이고 $c_{i,j} := 0 (i < j)$이다.

(증명) $k=1$일 때 $H_3(x) = 1 + x^2 + x^3$이다. 따라서 $c_{3,0} = 1$, $c_{3,1} = 0$, $c_{3,2} = c_{3,3} = 1$ 이다.

$c_{3,0} = c_{2,0} = 1, c_{3,1} = c_{2,1} + c_{2,2} = 0$이므로 성립한다. $k = h (h \geq 2)$일 때 식 (12)가 성립한다고 가정하자.

(i) 식 (9)와 귀납가정을 이용하면 $c_{2(h+1)+1,2i}$은 다음과 같다.

$c_{2(h+1)+1,2i}$
$= c_{2h+2,2i-1} + c_{2h+1,2i}$
$= (c_{2h+1,2i-2} + c_{2h,2i-1}) + c_{2h+1,2i}$
$= c_{2h+1,2i-2} + (c_{2h+1,2i-1} + c_{2h,2i-2}) + c_{2h+1,2i}$
$= c_{2h+1,2i-1} + c_{2h+1,2i}$
$= c_{2(h+1),2i}$

(ii) $c_{2(h+1)+1,2i+1}$도 (i)과 유사한 방법으로 증명하면 다음과 같은 결과를 얻을 수 있다.

$c_{2(h+1)+1,2i+1} = c_{2(h+1),2i} + c_{2(h+1).2i+1}$

따라서 모든 $k(\geq 1)$, $0 \leq i \leq k-1$에 대하여 식 (12)가 성립한다. (Q.E.D.)

식 (12)를 이용하여 다음 따름정리를 얻는다.

**따름정리 4>** $H_{2k}(x)$의 계수 $c_{2k,s} (0 \leq s \leq 2k-1)$는 식 (13)과 같다.

$$c_{2k,s} = \begin{cases} c_{2k+1,2i}, & \text{if } s = 2i \\ c_{2k+1,2i} + c_{2k+1,2i+1}, & \text{if } s = 2i+1 \end{cases} \quad (13)$$

여기서 $0 \leq i \leq k-1 (k \geq 1)$이고 $c_{i,j} := 0 (i < j)$이다.

$H_m(x)$는 다음과 같은 2가지 경우로 나누어 구한다.

$n = \lfloor \log_2 m \rfloor$ 일 때,

i) $\min\{m - 2^n, 2^{n+1} - 1 - m\} = m - 2^n$인 경우: 식 (8)에 의해 $H_{2^n}(x)$로부터 식 (10)과 식 (12)를 이용하여 $H_m(x)$를 구한다.

ii) $\min\{m - 2^n, 2^{n+1} - 1 - m\} = 2^{n+1} - 1 - m$인 경우: 식 (7)에 의해 $H_{2^{n+1}-1}(x)$로부터 식 (11)과 식 (13)을 이용하여 $H_m(x)$를 구한다.

**예제 5>** i) $H_{18}(x)$는 $\min\{18 - 2^4, 2^5 - 1 - 18\} = \min\{2, 13\} = 2$이므로 $H_{2^4}(x)$로부터 구한다. 식 (8)에 의해 $H_{2^4}(x) = x^{16} + x^{15} + x^{14} + x^{12} + x^8 + 1$이다. $H_{17}(x)$은 식 (12)를 이용하여 다음과 같이 구할 수 있다.

$c_{17,0} = c_{17,1} = c_{17,8} = c_{17,9} = c_{17,12} = c_{17,13}$
$= c_{17,14} = c_{17,16} = c_{17,17} = 1,$

$c_{17,2} = c_{17,3} = c_{17,4} = c_{17,5} = c_{17,6} = c_{17,7}$
$= c_{17,10} = c_{17,11} = c_{17,15} = 0$

$H_{18}(x)$은 식 (10)을 이용하여 다음과 같이 구할 수 있다.

$c_{18,0} = c_{18,1} = c_{18,2} = c_{18,8} = c_{18,9} = c_{18,10} = c_{18,12}$
$= c_{18,13} = c_{18,16} = c_{18,17} = c_{18,18} = 1,$

$c_{18,3} = c_{18,4} = c_{18,5} = c_{18,6} = c_{18,7}$
$= c_{18,11} = c_{18,14} = c_{18,15} = 0$

따라서 $H_{18}(x)$은 다음과 같다.

$$H_{18}(x)=x^{18}+x^{17}+x^{16}+x^{13}+x^{12}+x^{10}+x^9+x^8+x^2+x+1$$

ii) $H_{13}(x)$는 $\min\{13-2^3, 2^4-1-13\}=\min\{5, 2\}=2$이므로 $H_{2^4-1}(x)$로부터 구한다. 식 (7)에 의해 $H_{2^4-1}(x)=x^{15}+x^{14}+x^{12}+x^8+1$이다. $H_{14}(x)$은 식 (13)을 이용하여 $H_{13}(x)$은 식 (11)을 이용하여 구할 수 있다. 따라서 $H_{13}(x)$은 다음과 같다.

$$H_{13}(x)=x^{13}+x^{12}+x^{10}+x^9+x^8+x^2+x+1$$

그림 3은 $H_n(x)$을 효과적으로 구하는 알고리즘이다.

Input : Degree $n$ of $H_n(x)$
Output : The characteristic polynomial $H_n(x)$
Step1 : Compute $m=\lfloor \log_2 n \rfloor$ .
Step2 : $K=\min(n-2^m, 2^{m+1}-n)$
  switch $K$
  case $K=n-2^m$
   Make $H_{2^m}(x)=x^{2^m}+x^{2^m-1}+\cdots+x^{2^m-2^{m-1}}+1$
   if $K\neq 0$ then
    for $i$ from 1 to $k$
     switch $i$
     case $i\equiv 1 \pmod 2$
      $\begin{cases} c_{2k+1,2i}=c_{2k,2i} \\ c_{2k+1,2i+1}=c_{2k,2i}+c_{2k,2i+1} \end{cases}$
      break
     case $i\equiv 0 \pmod 2$
      $\begin{cases} c_{2l,2j-1}=c_{2l-1,2j-1} \\ c_{2l,2j}=c_{2l-1,2j-1}+c_{2l-1,2j} \end{cases}$
    STOP
   else STOP
  case $K=2^{m+1}-n$
   Make $H_{2^m}(x)=x^{2^m}+x^{2^m-1}+\cdots+x^{2^m-2^{m-1}}+1$
   for $i$ from 1 to $k$
    switch $i$
    case $i\equiv 1 \pmod 2$
     $\begin{cases} c_{2l-1,2j-1}=c_{2l,2j-1} \\ c_{2l-1,2j}=c_{2l,2j-1}+c_{2l,2j} \end{cases}$
     break
    case $i\equiv 0 \pmod 2$
     $\begin{cases} c_{2k,2i}=c_{2k+1,2i} \\ c_{2k,2i+1}=c_{2k+1,2i}+c_{2k+1,2i+1} \end{cases}$
  STOP

그림 3. $H_n(x)$을 구하는 알고리즘
Fig. 3 Algorithm for finding $H_n(x)$

**정리 6>** 전이규칙이 〈10⋯00〉인 $(2^n+i)$셀 90/150 CA의 특성다항식을 $H_{2^n+i}(x)$라 하면 식 (14)가 성립한다.

$$H_{2^n+i}(x)=H_{2^n-1-i}(x)+x^{2^n}H_i(x) \quad (0\le i\le 2^n-1) \tag{14}$$

(증명) 모든 $i$ $(0\le i\le 2^n-1)$에 대하여 식 (14)가 성립함을 수학적 귀납법으로 증명한다.

$i=0$일 때 $H_{2^n}(x)=H_{2^n-1}(x)+x^{2^n}$ 은 식 (6)에 의해 성립한다. $0\le k\le 2^n-2$인 $k$에 대하여

$H_{2^n+k}(x)=H_{2^n-1-k}(x)+x^{2^n}H_k(x)$ 가 성립한다고 가정하자. 그러면

$$\begin{aligned}
&H_{2^n-1-(k+1)}(x)+x^{2^n}H_{k+1}(x)\\
&=H_{2^n-1-(k+1)}(x)+x^{2^n}\left(xH_k(x)+H_{k-1}(x)\right)\\
&=H_{2^n-1-(k+1)}(x)+x\left(x^{2^n}H_k(x)\right)+x^{2^n}H_{k-1}(x)\\
&=H_{2^n-k}(x)+xH_{2^n+k}(x)+x^{2^n}H_{k-1}(x)\\
&=\left(H_{2^n-1-(k-1)}(x)+x^{2^n}H_{k-1}(x)\right)+xH_{2^n+k}(x)\\
&=H_{2^n+(k-1)}(x)+xH_{2^n+k}(x)\\
&=H_{2^n+k+1}(x).
\end{aligned}$$

따라서 모든 $i$ $(0\le i\le 2^n-1)$에 대하여

$H_{2^n+i}(x)=H_{2^n-1-i}(x)+x^{2^n}H_i(x)$ 가 성립한다.

(Q.E.D.)

그림 4는 $H_0(x)\sim H_{230}(x)$의 계수들을 1이면 검은색으로 0이면 흰색으로 나타낸 것이다. 그 결과는 그림 4와 같이 시어핀스키 삼각형 형태의 프랙탈 구조를 갖는다.

## Ⅳ. 결 론

본 논문에서는 $n$셀 90/150 CA 〈10⋯0〉의 특성다항식 $H_n(x)$을 $(n-1)$셀 90/150 CA 〈10⋯0〉의 특성다항식 $H_{n-1}(x)$로부터 구하는 방법과 이 방법을 이용하여 $H_{2^n}(x)$로부터 $H_{2^n+i}(x)$와 $H_{2^n-i}(x)$ $(1\le i\le 2^{n-1})$을 효과적으로 구하는 알고리즘을 제안하였다. 또한 $H_n(x)$의 계수들을 순차적으로 나열하였을 때 그 배열이 시어핀스키 삼각형 형태의 프랙

탈 구조를 가지고 있다는 것을 보였다.

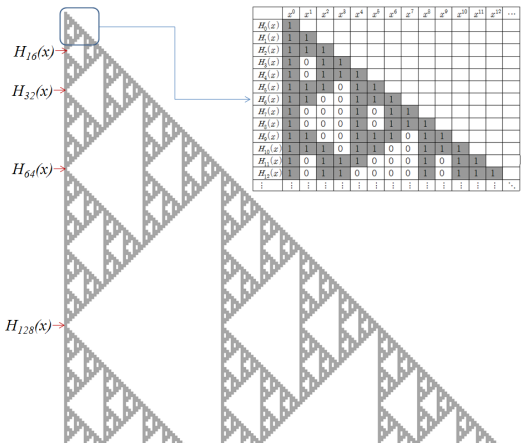


그림 4. $H_0(x) \sim H_{230}(x)$의 계수들로 이루어진 시어핀스키 삼각형 형태의 프랙탈 구조
Fig. 4 Fractal structure in the form of Sierpinski's triangle composed of coefficients from $H_0(x)$ to $H_{230}(x)$

감사의 글

위 논문은 "2018년 한국전자통신학회 봄철학술대회 우수논문"입니다.

## References

[1] S. Wolfram, "Statistical mechanics of cellular automata," *Rev. Modern Physics*, vol. 12, no. 55, 1983, pp. 601-644.

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

[3] P. P. Chaudhuri, D. R. Chowdhury, S. Nandi, and S. Chattopadhyay, *Additive cellular automata theory and applications,* Los Alamitos, Califomia: IEEE Computer Society Press, 1997.

[4] M. Song, Y. Kang, and H. Kim, "Performance evaluation of big stream based high speed data storage," *J. of the Korea Institute of Electronic Communication Sciences,* vol. 11, no. 5, Oct. 2017, pp. 817-827.

[5] Y. Kim, "On efficient algorithms for generating fundamental units and their H/W implementations over number fields," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 6, 2017, pp. 1181-1187.

[6] A. Sabater and P. Gil, "Synthesis of cryptographic interleaved sequences by means of linear cellular automata," *Applied Mathematics Letters*, vol. 22, no. 12, 2009, pp. 1518-1524.

[7] U. Choi, S. Cho, and G. Kong, "Analysis of Characteristic Polynomial of Cellular Automata with Symmetrical Transition Rules," *Proceedings of the Jangjeon Mathematical Society,* vol. 18, no. 1, 2015, pp. 85-93.

[8] H. Kim, S. Cho, U. Choi, and M. Kwon, "Analysis of 90/150 cellular automata with extended symmetrical transition rules," *Proceedings of the Jangjeon Mathematical Society,* vol. 20, no. 2, 2017, pp. 193-201.

[9] K. Cattell and J. Muzio, "Synthesis of one-dimensional linear hybrid cellular automata," *IEEE Trans. Comput-Aided Design Integrated Circuits and Systems,* vol. 15, no. 3, 1996, pp. 325-335.

[10] 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. Comput-Aided Design Integr. Circuits Syst.*, vol. 26, no. 9, 2007, pp. 1720-1724.

[11] 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.

[12] H. Kim, S. Cho, U. Choi, M. Kwon, and G. Kong, "Synthesis of Uniform CA and 90/150 Hybrid CA," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 3, Mar. 2016, pp. 293-302.

[13] U. Choi and S. Cho, "Characteristic Polynomial of 90 UCA and Synthesis of CA using Transition Rule Blocks," *J. of the Korea Institute of Electronic Communication Sciences,* vol. 13, no. 3, 2018, pp. 593-600.

[14] 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,* Accepted.
[15] R. Lidl and H. Niederreiter, *Finite fields : Encyclopedia of Mathematics and its Applications 20.* New York: Cambridge University Press, 1997.

## 저자 소개

**김진경(Jin-Gyoung Kim)**

2008년 부경대학교 대학원 응용수학과 졸업(이학석사)
2013년 부경대학교 대학원 응용수학과 졸업(이학박사)
※ 관심분야 : 셀룰라 오토마타론, 유한체

**조성진(Sung-Jin Cho)**

1979년 강원대학교 수학교육과 졸업(이학사)
1981년 고려대학교 대학원 수학과 졸업(이학석사)
1988년 고려대학교 대학원 수학과 졸업(이학박사)
1988년~ 현재 부경대학교 응용수학과 교수
※ 관심분야 : 셀룰라 오토마타론, 정보보호

**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 정보통신공학과 교수
※ 관심분야 : 셀룰라 오토마타론, 정보보호, 암호이론

**김한두(Han-Doo Kim)**

1982년 고려대학교 수학과 졸업(이학사)
1984년 고려대학교 대학원 수학과 졸업(이학석사)
1988년 고려대학교 대학원 수학과 졸업(이학박사)
1989년~ 현재 인제대학교 응용수학과 정교수
※ 관심분야 : 셀룰라 오토마타론, 정보보호, 인공지능

**강성원(Sung-Won Kang)**

2017년 부경대학교 응용수학과 졸업(이학사)
2017년~ 현재 부경대학교 대학원 응용수학과 석사과정 재학
※ 관심분야 : 셀룰라 오토마타론, 유한체