Regular paper

Journal of the KIECS. pp. 383-390, vol. 13, no. 2, Apr. 30 2018, t. 88, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2018.13.2.383

3항 다항식 $x^{2^n-1}+x+1$에 대응하는 90/150 상태전이행렬의 구성

김한두* · 조성진** · 최언숙***

On the Construction of the 90/150 State Transition Matrix Corresponding to the Trinomial $x^{2^n-1}+x+1$

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

요 약

셀룰라 오토마타(이하 CA)는 LFSR보다 난수성이 우수하여 여러 분야에 LFSR의 대안으로 응용되고 있다. 그러나 주어진 다항식에 대응하는 CA를 구성하는 것이 LFSR보다 어렵다. Cattell 등과 Cho 등은 기약다항식들이 CA-다항식임을 보였다. 그리고 Cho 등과 Sabater 등은 기약다항식의 거듭제곱에 대응하는 90/150 CA의 합성 방법을 제시하였다. 이것은 수축생성기에 적용가능하다. Swan은 유한체 $GF(2)$ 상에서 3항 다항식의 기약인수의 개수의 홀짝성을 분석하였다. 이런 3항 다항식들은 유한체 확장을 구현할 때 실제로 중요한 역할을 한다. 본 논문에서는 3항 다항식들 $x^{2^n-1}+x+1\,(n\geq 2)$이 CA-다항식임을 보인다. 또한 3항 다항식들 $x^{2^a(2^n-1)}+x^{2^a}+1$ $(n\geq 2, a\geq 0)$이 CA-다항식임을 보인다.

ABSTRACT

Since cellular automata(CA) is superior to LFSR in randomness, it is applied as an alternative of LFSR in various fields. However, constructing CA corresponding to a given polynomial is more difficult than LFSR. Cattell et al. and Cho et al. showed that irreducible polynomials are CA-polynomials. And Cho et al. and Sabater et al. gave a synthesis method of 90/150 CA corresponding to the power of an irreducible polynomial, which is applicable as a shrinking generator. Swan characterizes the parity of the number of irreducible factors of a trinomial over the finite field $GF(2)$. These polynomials are of practical importance when implementing finite field extensions. In this paper, we show that the trinomial $x^{2^n-1}+x+1\,(n\geq 2)$ are CA-polynomials. Also the trinomial $x^{2^a(2^n-1)}+x^{2^a}+1$ $(n\geq 2, a\geq 0)$ are CA-polynomials.

키워드

Cellular Automata, 90/150 CA, Trinomial, State Transition Matrix, CA-Polynomial
셀룰라 오토마타, 90/150 CA, 3항 다항식, 상태 전이 행렬, CA-다항식

Ⅰ. 서 론

셀룰라 오토마타(Cellular Automata, 이하 CA)는 1950년대 초반 Von Neumann에 의해 자체 재생산 가능한 모델로 처음 소개되었다[1]. 1980년대 초 Wolfram은 0과 1 두 가지 상태가 있는 3-이웃 1차

* 인제대학교 응용수학과, 기초과학연구소(mathkhd@inje.ac.kr)
** 교신저자: 부경대학교 응용수학과
*** 동명대학교 정보통신공학과 (choies@tu.ac.kr)
· 접 수 일 : 2017. 11. 30
· 수정완료일 : 2018. 02. 06
· 게재확정일 : 2018. 04. 15
· Received : Nov. 30, 2017, Revised : Feb. 06, 2018, Accepted : Apr. 15, 2018
· Corresponding Author : Sung-Jin Cho
Dept. of Applied Math., Pukyong National University,
Email : sjcho@pknu.ac.kr

원 선형 CA를 제안하였다[2]. CA는 셀의 상태가 자기 자신 및 인접한 셀들의 상태의 국소 상호작용에 의해 동시에 갱신되는 시스템으로 간단하고 규칙적이며 작은 단위로 확장 연결할 수 있는 구조이기 때문에 하드웨어 구현에 적합하다. 이러한 특성 때문에 CA는 테스트 패턴 생성, 암호, 오류정정부호, 의사난수 생성기 등 많은 분야에 응용되었다[3-6].

90/150 CA의 특성다항식인 다항식을 CA-다항식(CA-polynomial)이라고 한다[7]. 여러 연구자들이 주어진 다항식들에 대응하는 CA들을 합성하는 방법을 연구하였다. 주어진 다항식이 CA-다항식인지 여부를 식별하는 것은 중요한 문제이며 CA의 합성법 연구 이전에 확인되어야 한다. Cho 등[8]은 최대 길이 90/150 CA를 갖는 90/150 CA를 합성하는 효율적인 방법을 제안하였다. 그들은 $GF(2)$(원소의 개수가 2개인 Galois 체)에서의 Lanczos 삼중대각화 알고리즘과 similarity 변환을 이용하여 주어진 CA-다항식에 대한 90/150 CA를 빠르게 찾는 새로운 방법을 제안하였다. 그들이 제시한 방법은 Cattell 등[7]에 의해 제안된 합성 방법의 시간복잡도 $O(n^7)$를 $O(n^2)$로 감소시켰다. 90/150 CA는 암호 등에 실제 적용 가능한 여러 비선형 키수열 생성기들을 모델링하는데 적용가능하다. Cattell 등[7]은 주어진 기약다항식에 대응하는 90/150 CA를 찾는 방법을 제안하였지만 그들의 방법으로 가약다항식(reducible polynomial)에 대한 90/150 CA를 찾는 것은 불가능하다. Cho 등[3]과 Sabater 등[9]은 가약다항식 $[p(x)]^{2^a}(a \geq 0)$ (여기서 $p(x)$는 2차 이상의 기약다항식)에 대응하는 90/150 CA의 합성 방법을 제안하였다. Choi 등[10]은 다항식의 계수가 모두 1인 자체 상반 다항식(self-reciprocal polynomial) $f_n(x) = x^n + x^{n-1} + \cdots + x + 1$의 CA-다항식 여부를 결정하는 방법을 제안하고 $f_n(x)$에 대응하는 90/150 CA의 개수를 결정하는 방법을 제안하였다. 그리고 일반적인 다항식이 CA-다항식인지를 판정하는 방법들이 연구되고 있다. Swan[11]은 유한체 $GF(2)$ 상에서 3항 다항식의 기약 인수들의 개수의 홀짝성(parity)을 분석하였고, 3항 다항식이 유한체 확장을 구현할 때 실제로 중요한 역할을 한다는 것을 보였다. 본 논문에서 3항 다항식들 $x^{2^n-1} + x + 1 (n \geq 2)$ 와 $x^{2^a(2^n-1)} + x^{2^a} + 1 (n \geq 2, a \geq 0)$이 CA-다항식들임을 보인다.

II. CA 기본 개념

본 논문에서는 1차원 3-이웃 90/150 CA를 다룬다. 90/150 CA는 각 셀에 규칙 90 또는 규칙 150만 적용되는 CA이다. n-셀 90/150 CA의 상태전이행렬(state transition matrix)은 식 (1)과 같은 $n \times n$ 삼중대각 행렬 T_n이다.

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

여기서 d_i는 i번째 셀에 적용된 전이규칙이 90이면 0, 150이면 1이 된다. 이를 간단히 주대각 성분만을 이용하여 $T_n = < d_1, d_2, \cdots, d_n >$으로 나타낸다. n-셀 90/150 CA $\mathbb{C}_n$의 $GF(2)$상의 특성다항식(characteristic polynomial) Δ_n은 $\Delta_n = |T_n \oplus xI_n|$ 이다. 여기서 I_n은 $n \times n$ 단위행렬이다. 상태전이행렬이 T_n인 임의의 n-셀 90/150 CA에 대하여 T_n의 최소다항식(minimal polynomial)은 T_n의 특성다항식과 같다. Δ_n을 T_n의 특성다항식이라고 하자. 그러면 다음과 같은 점화식이 성립한다:

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

여기서 $\Delta_1 = x + d_1$, $\Delta_0 = 1$.

식 (2)는 주어진 90/150 CA의 특성다항식 Δ_n을 구하는 효율적인 알고리즘을 제공해준다.

C_n을 n-셀 90/150의 상태전이행렬 $O_n := < 0, \cdots, 0 >$의 특성다항식이라고 하면 다음과 같은 점화식이 성립한다:

$$C_n = xC_{n-1} + C_{n-2} \tag{3}$$

여기서 $C_1 = x$, $C_0 = 1$.

특히 Δ_n을 n-셀 90/150의 상태전이행렬 $U_n = <1,0,\cdots,0>$ 의 특성다항식이라고 하면 다음과 같은 점화식이 성립한다:

$$\Delta_n = (x+1)C_{n-1} + C_{n-2} \tag{4}$$

여기서 $C_1 = x,\ C_0 = 1.$

그림 1은 1차원 3-이웃 CA의 구조이다. 그림 1에서 전이규칙 90은 왼쪽 셀과 오른쪽 셀의 영향을 받아 다음 셀이 결정되고 전이규칙 150은 왼쪽 셀과 오른쪽 셀 및 셀 자체의 영향을 받아 다음 셀이 결정된다. 표 1은 본 논문에서 사용하는 전이규칙 90과 150에 따른 다음 셀의 상태를 나타내는 표이다.

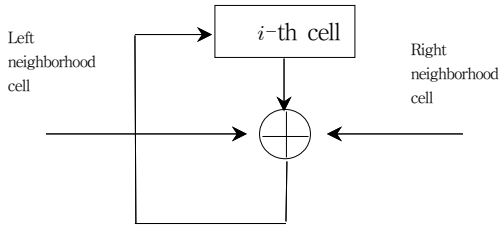

그림 1. 3-이웃 선형 CA의 구조
Fig. 1 The structure of 3-neighborhood linear CA

표 1. 전이규칙에 따른 다음 셀의 상태
Table 1. The next states of cells according to state transition rules

Current States	111	110	101	100	011	010	001	000
rule 90	0	1	0	1	1	0	1	0
rule 150	1	0	0	1	0	1	1	0

III. 3항 다항식 $x^{2^n-1}+x+1$에 대응하는 90/150 CA

이 절에서는 3항 다항식들 $x^{2^n-1}+x+1$ $(n \geq 2)$과 $x^{a(2^n-1)}+x^{2^a}+1\ (n \geq 2, a \geq 0)$이 CA-다항식임을 정리 1과 정리 2를 이용하여 보인다. 다음 정리는 [12]에 있다.

<정리 1> $T_n = <d_1, d_2, \cdots, d_n>$을 n-셀 90/150 CA의 상태전이행렬이라 하고 Δ_n을 T_n의 특성다항식이라 하자. 그러면 Δ_n^2에 대응하는 $2n$-셀 90/150 CA의 상태전이행렬은 다음과 같다:

$$<d_1, d_2, \cdots, d_{n-1}, \overline{d_n}, \overline{d_n}, d_{n-1}, \cdots, d_2, d_1> \tag{5}$$

다음 정리는 [13]에 있다.

<정리 2> $T_n = <a_1, a_2, \cdots, a_n>$을 n-셀 90/150 CA의 상태전이행렬이라 하고 D_3를 상태전이행렬이 $<d_1, d_2, d_3>$인 3-셀 90/150 CA의 특성다항식이라고 하자. $S_{2n+3} = <T_n d_1 d_2 d_3 T_n^*> := <a_1, a_2, \cdots, a_n, d_1, d_2, d_3, a_n, \cdots, a_2, a_1>$을 $(2n+3)$-셀 90/150 CA의 상태전이행렬이라 하자. 그리고 Δ_n(resp. $V_{2n+3}(x)$)을 T_n (resp. $<T_n d_1 d_2 d_3 T_n^*>$)의 특성다항식이라고 하자. 그러면 다음이 성립한다.

$$V_{2n+3}(x) = D_3\Delta_n^2 + (d_1+d_3)(x+d_2)\Delta_n\Delta_{n-1} + (x+d_2)\Delta_{n-1}^2 \tag{6}$$

여기서 D_3는 상태전이행렬 $<d_1, d_2, d_3>$의 특성다항식이다.

<보조정리 3> C_n을 n-셀 90/150 CA의 상태전이행렬 $O_n = <0, \cdots, 0>$ 의 특성다항식이라고 하자. 그러면 다음이 성립한다.

$$C_{2^n-1} = x^{2^n-1} \tag{7}$$

<증명> $\det(O_{2^n-1} + xI_{2^n-1})$의 2^{n-1}번째 행에 따라 여인수 전개(cofactor expansion)를 하면 $C_{2^n-1} = x^{2^n-1}$이 성립한다. 여기서 I_{2^n-1}은 (2^n-1)차 단위행렬이다. □

<보조정리 4> C_n을 n-셀 90/150 CA의 상태전이행렬 $O_n = <0, \cdots, 0>$ 의 특성다항식이라고 하자. 그러면 다음이 성립한다.

$$C_{2^n} = C_{2^{n-1}}^2 + C_{2^{n-1}-1}^2 \quad (8)$$

<증명> $\det(O_{2^n} + xI_{2^n})$의 2^{n-1}번째 행에 따라 여인수 전개를 하면 다음이 성립한다. 여기서 I_{2^n}은 $2^n \times 2^n$ 단위행렬이다.

$$\begin{aligned} C_{2^n-1} &= xC_{2^{n-1}-1} \cdot C_{2^{n-1}} + C_{2^{n-1}-2} \cdot C_{2^{n-1}} \\ &\quad + C_{2^{n-1}-1}^2 \\ &= C_{2^{n-1}}(xC_{2^{n-1}-1} + C_{2^{n-1}-2}) + C_{2^{n-1}-1}^2 \\ &= C_{2^{n-1}}^2 + C_{2^{n-1}-1}^2 \text{ (식 (3) 이용).} \end{aligned}$$ □

보조정리 3과 보조정리 4에 의해 다음 정리를 얻는다.

<정리 5> C_n을 n-셀 90/150 CA의 상태전이행렬 $O_n = <0, \cdots, 0>$의 특성다항식이라고 하자. 그러면 다음이 성립한다.

$$\begin{aligned} C_{2^n} &= x^{2^n} + x^{2(2^{n-1}-1)} + x^{2^2(2^{n-2}-1)} + x^{2^3(2^{n-3}-1)} \\ &\quad + \cdots + x^{2^{n-3}(2^3-1)} + x^{2^{n-2}(2^2-1)} + x^{2^{n-1}} + 1 \end{aligned} \quad (9)$$

<증명> n에 대한 수학적 귀납법으로 증명한다.

$n=1$인 경우 $C_2 = x^2+1$이므로 성립한다. $n=k$인 경우 성립한다고 가정하면 보조정리 3과 보조정리 4에 의해 다음이 성립한다.

$$\begin{aligned} C_{2^{k+1}} &= C_{2^k}^2 + C_{2^k-1}^2 \\ &= \left(x^{2^k} + x^{2(2^{k-1}-1)} + x^{2^2(2^{k-2}-1)} + x^{2^3(2^{k-3}-1)} + \cdots + \right. \\ &\quad \left. x^{2^{k-3}(2^3-1)} + x^{2^{k-2}(2^2-1)} + x^{2^{k-1}} + 1\right)^2 + \left(x^{2^k}-1\right)^2 \\ &= \left(x^{2^{k+1}} + x^{2^2(2^{k-1}-1)} + x^{2^3(2^{k-2}-1)} + x^{2^4(2^{k-3}-1)} + \cdots + \right. \\ &\quad \left. x^{2^{k-2}(2^3-1)} + x^{2^{k-1}(2^2-1)} + x^{2^k} + 1\right) + x^{2(2^k-1)} \\ &= x^{2^{k+1}} + x^{2(2^k-1)} + x^{2^2(2^{k-1}-1)} + x^{2^3(2^{k-2}-1)} + \\ &\quad x^{2^4(2^{k-3}-1)} + \cdots + x^{2^{k-2}(2^3-1)} + x^{2^{k-1}(2^2-1)} + x^{2^k} + 1. \end{aligned}$$

그러므로 $n=k+1$일 때도 참이다. 그러므로 모든 자연수 n에 대하여 성립한다. □

보조정리 3과 보조정리 4와 정리 5를 이용하여 3항 다항식들 $x^{2^n-1}+x+1$ $(n \geq 2)$이 CA-다항식임을 보인다.

<정리 6> 3항 다항식들 $x^{2^n-1}+x+1 (n \geq 2)$은 CA-다항식이다. 특히 $x^{2^n-1}+x+1$에 대응하는 (2^n-1)-셀 CA의 상태전이행렬 R_{2^n-1}은 다음과 같다:

$$R_{2^n-1} = < U_k 011 U_k^* > \quad (10)$$

여기서 $U_k = <1,0,\cdots,0>$, $k = 2^{n-1}-2$이다.

<증명> 상태전이행렬이 $<d_1, d_2, d_3> = <0,1,1>$인 경우 정리 2에 의하면 다음이 성립한다. 보조정리 3, 보조정리 4, 그리고 정리 5를 이용한다.

$$\begin{aligned} V_{2^n-1}(x) &= D_3 \Delta_{2^{n-1}-2}^2 + (x+1)\Delta_{2^{n-1}-2}\Delta_{2^{n-1}-3} \\ &\quad + (x+1)\Delta_{2^{n-1}-3}^2 \\ &= D_3\left\{(x+1)C_{2^{n-1}-3} + C_{2^{n-1}-4}\right\}^2 \\ &\quad + (x+1)\left\{(x+1)C_{2^{n-1}-3} + C_{2^{n-1}-4}\right\} \\ &\quad \left\{(x+1)C_{2^{n-1}-4} + C_{2^{n-1}-5}\right\} \\ &\quad + (x+1)\left\{(x+1)C_{2^{n-1}-4} + C_{2^{n-1}-5}\right\}^2 \text{ (식 (4) 이용)} \\ &= (x^3+x+1)\left(C_{2^{n-1}-2} + C_{2^{n-1}-3}\right)^2 \quad \text{(식 (3) 이용)} \\ &\quad + (x+1)\left(C_{2^{n-1}-2} + C_{2^{n-1}-3}\right)\left(C_{2^{n-1}-3} + C_{2^{n-1}-4}\right) \\ &\quad + (x+1)\left(C_{2^{n-1}-3} + C_{2^{n-1}-4}\right)^2 \\ &= (x^3+x+1)\left(C_{2^{n-1}-2}^2 + C_{2^{n-1}-3}^2\right) \\ &\quad + (x+1)\left(C_{2^{n-1}-3} + C_{2^{n-1}-4}\right)\left(C_{2^{n-1}-2} + C_{2^{n-1}-4}\right) \\ &= x^3 C_{2^{n-1}-2}^2 + x^3 C_{2^{n-1}-3}^2 + xC_{2^{n-1}-2}^2 + C_{2^{n-1}-2}^2 \\ &\quad + C_{2^{n-1}-3}^2 + xC_{2^{n-1}-2}C_{2^{n-1}-3} + xC_{2^{n-1}-2}C_{2^{n-1}-4} \\ &\quad + xC_{2^{n-1}-4}^2 \quad \text{(식 (3) 이용)} \\ &= x^3 C_{2^{n-1}-2}^2 + x^3 C_{2^{n-1}-3}^2 + (x+1)C_{2^{n-1}-2}^2 \\ &\quad + C_{2^{n-1}-3}C_{2^{n-1}-1} + xC_{2^{n-1}-2}(C_{2^{n-1}-2} + xC_{2^{n-1}-3}) \\ &\quad + x\left(C_{2^{n-1}-2} + xC_{2^{n-1}-3}\right)^2 \\ &= x^3 C_{2^{n-1}-2}^2 + C_{2^{n-1}-2}^2 + C_{2^{n-1}-1}C_{2^{n-1}-3} \end{aligned}$$

$$
\begin{aligned}
&+xC_{2^{n-1}-2}^2+x^2C_{2^{n-1}-2}C_{2^{n-1}-3}\\
&=x^3C_{2^{n-1}-2}^2+C_{2^{n-1}-2}^2\\
&+C_{2^{n-1}-1}\left(C_{2^{n-1}-1}+xC_{2^{n-1}-2}\right)\\
&+xC_{2^{n-1}-2}^2+x^2C_{2^{n-1}-2}\left(C_{2^{n-1}-1}+xC_{2^{n-1}-2}\right)\\
&=C_{2^{n-1}-2}^2+C_{2^{n-1}-1}^2+xC_{2^{n-1}-1}C_{2^{n-1}-2}\\
&+xC_{2^{n-1}-2}^2+x^2C_{2^{n-1}-2}C_{2^{n-1}-1}\\
&=\left(C_{2^{n-1}}+xC_{2^{n-1}-1}\right)^2+C_{2^{n-1}-1}^2\\
&+xC_{2^{n-1}-1}\left(C_{2^{n-1}}+xC_{2^{n-1}-1}\right)+x\left(C_{2^{n-1}}+xC_{2^{n-1}-1}\right)^2\\
&+x^2\left(C_{2^{n-1}}+xC_{2^{n-1}-1}\right)C_{2^{n-1}-1}\\
&=C_{2^{n-1}}^2+C_{2^{n-1}-1}^2+xC_{2^{n-1}-1}C_{2^{n-1}}+xC_{2^{n-1}}^2\\
&+x^2C_{2^{n-1}}C_{2^{n-1}-1}\\
&=C_{2^{n-1}}^2+\left(x^{2^{n-1}-1}\right)^2+x\cdot x^{2^{n-1}-1}C_{2^{n-1}}+xC_{2^{n-1}}^2\\
&+x^2\cdot x^{2^{n-1}-1}C_{2^{n-1}}\\
&=(1+x)C_{2^{n-1}}^2+\left(x^{2^{n-1}}+x^{2^{n-1}+1}\right)C_{2^{n-1}}+x^{2^n-2}\\
&=x^{2^n-1}+x+1. \qquad \text{(식 (7) 이용)}
\end{aligned}
$$

마지막 등식은 보조정리 4를 이용하여 C_{2^n}과 $C_{2^{n-1}}$을 각각

$x^{2^n}+x^{2(2^{n-1}-1)}+x^{2^2(2^{n-2}-1)}+x^{2^3(2^{n-3}-1)}+\cdots+x^{2^{n-3}(2^3-1)}+x^{2^{n-2}(2^2-1)}+x^{2^{n-1}}+1$ 와 $x^{2^{n-1}}+x^{2(2^{n-2}-1)}+x^{2^2(2^{n-3}-1)}+x^{2^3(2^{n-4}-1)}+\cdots+x^{2^{n-4}(2^3-1)}+x^{2^{n-3}(2^2-1)}+x^{2^{n-2}}+1$로 대체하였다.

그러므로 $R_{2^n-1}=<U_k011U_k^*>$은 $x^{2^n-1}+x+1$에 대응하는 (2^n-1)-셀 CA의 상태전이행렬이다, 여기서 $U_k=<1,0,\cdots,0>$, $k=2^{n-1}-2$이다. 그러므로 3항 다항식 $x^{2^n-1}+x+1\,(n\geq 2)$은 CA-다항식이다. □

정리 1에 의해 3항 다항식들 $x^{2^a(2^n-1)}+x^{2^a}+1$ $(n\geq 2, a\geq 0)$에 대응하는 90/150 CA를 합성할 수 있다. 표 1은 정리 6에 의해 구한 3항 다항식들 $x^{2^n-1}+x+1$ $(n\geq 3)$의 상태전이행렬들을 나타낸 것이다. 예를 들어 기약다항식 x^7+x+1의 상태전이행렬은 $<10\ \ 011\ \ 01>$이고 가약다항식 $x^{2^5-1}+x+1=(x^3+x+1)(x^7+x^3+1)(x^{21}+x^{19}+x^{18}+x^{15}+x^{14}+x^{11}+x^8+x^7+x^5+x^4+1)$의 상태전이행렬은 <10000000000000 011 00000000000001>이다. 그리고 기약다항식 $x^{32767}+x+1$의 상태전이행렬은 $<U_{16382}\ \ 011\ \ U_{16382}^*>$이다. 여기서 $U_{16382}=<1,0,\cdots,0>$이다.

표 2. 3항 다항식 $x^{2^n-1}+x+1$의 상태전이행렬
Table 2. The state transition matrix of the trinomial $x^{2^n-1}+x+1$

Polynomial	State transition matrix
x^7+x+1	$<10\ \ 011\ \ 01>$
$x^{15}+x+1$	$<100000\ \ 011\ \ 000001>$
$x^{31}+x+1$	$<10000000000000\ \ 011\ \ 00000000000001>$
$x^{63}+x+1$	$<10\cdots 00\ \ 011\ \ 00\cdots 01>$
⋮	⋮
$x^{32767}+x+1$	$<10\cdots 00\ \ 011\ \ 00\cdots 01>$
⋮	⋮

다음 표 3은 3항 다항식들 $x^{2(2^n-1)}+x^2+1\,(n=2,3,4,5)$의 상태전이행렬들이다.

표 3. 3항 다항식 $x^{2(2^n-1)}+x^2+1$의 상태전이행렬
Table 3. The state transition matrix of the trinomial $x^{2(2^n-1)}+x^2+1$

Polynomial	State transition matrix
x^6+x^2+1	$<01\,00\,10>$
$x^{14}+x^2+1$	$<100110\,00\,011001>$
$x^{30}+x^2+1$	$<10000001100000\,11\,00000110000001>$
$x^{62}+x^2+1$	$<1000000000000001100000000000000\ \ 00\ \ 0000000000000011000000000000001>$

Ⅳ. 결론

본 논문에서는 $x^{2^n-1}+x+1$ $(n \geq 2)$ 형태의 3항 다항식이 CA-다항식임을 보였다. 그리고 3항 다항식들 $x^{2^a(2^n-1)}+x^{2^a}+1\,(n \geq 2, a \geq 0)$이 CA-다항식임을 보였다. 향후 CA-다항식이 되는 3항 다항식들에 대하여 연구하고자 한다. 그리고 다항식의 계수가 모두 1인 자체상반다항식의 CA-다항식 여부를 결정하는 효율적인 방법을 연구하고자 한다.

감사의 글

본 논문은 Proceedings, ICEIC 2017 논문[On the state transition matrix of the ternary polynomial $x^{2^n-1}+x+1$]을 확장한 논문임.

References

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

[2] S. Wolfram, "Statistical mechanics of cellular automata," *Rev. Modern Physics,* vol. 12, no. 66, 1983, pp. 601 - 644.

[3] 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, 2007, pp. 1720-1724.

[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, Dec. 2017, pp. 1181-1187.

[6] 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.

[7] 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.

[8] S. Cho, U. Choi, H. Kim, Y. Hwang, and J. Kim, "Analysis of 90/150 Two Predecessor Nongroup Cellular automata," *Int. Conf. on Cellular Automata for Research and Industry(ACRI) 2008, Lecture Notes in Computer Science 5191*, Yokohama, Japan, Sept., 2008, pp. 128-135.

[9] 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.

[10] U. Choi, S. Cho, H. Kim, and J. Kim, "90/150 CA corresponding to polynomial of maximum weight," *J. of Cellular Automata: To appear.*

[11] G. Mullen and D. Panario, *Handbook of finite fields*, New York: CRC Press, 2013.

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

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

저자 소개

김한두 (Han-Doo Kim)

1982년 2월 고려대학교 수학과 졸업 (이학사)
1984년 2월 고려대학교 대학원 수학과 졸업(이학석사)
1988년 2월 고려대학교 대학원 수학과 졸업(이학박사)
1989년~ 현재 인제대학교 응용수학과 교수, 기초과학연구소
※ 관심분야 : 전산수학, 셀룰라 오토마타론

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 대학원 응용수학과 졸업(이학박사)
2009년 부경대학교 대학원 정보보호학과 졸업(공학박사)
2006년 ~ 현재 동명대학교 정보통신공학과 교수
※ 관심분야 : 셀룰라 오토마타론, 정보보호, 암호이론