$GF(q)$에서의 1차원 셀룰라 오토마타의 분석

°조 성 진, 최 언 숙, 윤 세 영
부경대학교 응용수학과

Analysis of one-dimensional cellular automata over $GF(q)$

Sung-Jin Cho, Un-Sook Choi, Se-Young Yoon

Department of Applied Mathematics
Pukyoung National University

q가 소수의 거듭제곱의 형태일 때 $GF(q)$상에서의 1차원 셀룰라 오토마타의 여러 가지 특성들을 연구한다. 이러한 셀룰라 오토마타의 특성다항식에 관한 몇가지 특성들이 제시한다. Intermediate Boundary CA를 정의하고 Null Boundary CA와의 관계를 살펴본다.

1. 서론

LFSR의 대안으로서 제시된 CA는 test pattern generation, pseudo-random numbergeneration, cryptography, error correcting codes, signature analysis 등 많은 분야에서 응용된다[1, 3, 5, 7, 8].

$GF(2)$ 와 $GF(p)$에서의 CA는 널리 연구되었다[4, 6, 11, 12]. 여기서 p는 소수이다. 하나의 LFSM M은 선형연산자 L에 의해 표현되고 L의 특징은 특성다항식에 관한 연구로서 보다 쉽게 알 수 있다.

본 논문에서는 $GF(q)$에서의 1차원 셀룰라 오토마타(1-D CA)의 이론적인 기초에 관하여 연구한다. 여기서 q는 소수의 거듭제곱의 형태이다. 그러한 LFSM의 특성다항식에 관한 결과들이 제시되고 $GF(q)$에서의 IBCA가 $GF(q)$에서의 NBCA와 관련하여 정의된다.

2. 도입

NBCA의 전이행렬은 다음과 같다.

$$\begin{bmatrix} d_1 & b_1 & 0 & \cdots & 0 & 0 & 0 \\ c_2 & d_2 & b_2 & \cdots & 0 & 0 & 0 \\ 0 & c_3 & d_3 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & c_{n-1} & d_{n-1} & b_{n-1} \\ 0 & 0 & 0 & \cdots & 0 & c_n & d_n \end{bmatrix}$$

0아닌 모든 q^n-1개의 상태들이 모두 하나의 주기안에 있을 때 CA는 최대길이를 갖는다고 한다. 또 n차 기약다항식 $p(x)$의 해 α에 대해, $\{\alpha^i : i=0,1,\cdots,q^{n-1}\}$가 $GF(q^n)$의 모든 0아닌 원소들의 집합과 같을 때 $p(x)$는 primitive 라고 한다.

LFSM의 전이행렬을 T_{LFSM}으로 표시하고 I는 T_{LFSM}과 같은 차수의 단위행렬일 때 특성다항식은 다음과 같다.

$$|xI - T_{LFSM}|$$

특성다항식의 primitive일 필요충분조건은 LFSM이 최대길이를 갖는 것이다[8].

M_{ij}는 i번째부터 j번째 셀로 이루어진 LFSM이고 M_{ij}의 특성다항식은 Δ_{ij}로 표시한다. 그리고 $\Delta_{1,n-1}$, $\Delta_{2,n}$, $\Delta_{i,j}$를 CA의 subpolynomial이라고 정의한다.

3. NBCA(Null Boundary CA)

다음 정리들은 [2]에 제시되어 있다.

<정리 3.1> NBCA의 특성다항식은 다음 점화관계식을 만족한다. $(k \geq 1)$

$$\Delta_{-1} = 0$$

$$\Delta_0 = 1$$

$$\Delta_k = (x+d_k)\Delta_{k-1} - b_{k-1}c_k\Delta_{k-2}$$

<따름정리3.2>CA의 특성다항식은 $2n$번의 다항식덧셈과 $2n$번의 다항식 곱셈으로 계산된다.

<정리 3.3> $0 \leq k \leq n$에 대하여 다음이 성립한다.

$$\Delta_{1,n} = \Delta_{1,k}\Delta_{k+1,n} - b_k c_{k+1}\Delta_{1,k-1}\Delta_{k+2,n}$$

<정리 3.4> $0 \leq k \leq n$에 대하여 다음이 성립한다.

$$\Delta_{1,n-1}\Delta_{2,n} - \Delta_{1,n}\Delta_{2,n-1} = \prod_{i=1}^{n-1} b_i \prod_{i=2}^{n} c_i$$

4. Cyclic CA

Cyclic CA의 전이행렬은 다음과 같다.

$$\begin{bmatrix} d_1 & b_1 & 0 & \cdots & 0 & 0 & c_1 \\ c_2 & d_2 & b_2 & \cdots & 0 & 0 & 0 \\ 0 & c_3 & d_3 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & c_{n-1} & d_{n-1} & b_{n-1} \\ b_n & 0 & 0 & \cdots & 0 & c_n & d_n \end{bmatrix}$$

<정리 4.1[2]> Cyclic CA의 특성다항식과 NBCA의 특성다항식의 관계는 다음과 같다.

$$\Phi_{1,n} = \Delta_{1,n} - c_1 b_n \Delta_{2,n-1} + (-1)^{n+1}\left(\prod_{k=1}^{n} b_k + \prod_{k=1}^{n} c_k\right)$$

<정리 4.2> Cyclic CA에서 $a_1 = a_n$, $b_1 = b_n$, $c_1 = c_n$이면 다음 관계식이 성립한다. 여기서 $a_k = x - d_k$이고 $1 \leq k \leq n$ 이다.

$$\Phi_{1,n} = a_n\Phi_{2,n} - c_n b_n \Phi_{2,n-1} + (-1)^{n+1}\left(\prod_{k=1}^{n-1} b_k + \prod_{k=1}^{n-1} c_k\right)(a_n + b_n + c_n)$$

<따름정리 4.3[3]> 정리 4.2에서 $b_k = c_k = 1$, $d_k = 0$ 또는 1, $d_1 = d_n$이면 다음이 성립한다. 여기서 $1 \leq k \leq n$이다.

$$\Phi_{1,n} = (x + d_1)\Phi_{2,n} + \Phi_{2,n-1}$$

만약 $q = 2^n$이면 다음정리를 얻는다.

<정리 4.4> n이 짝수, $b_k = b$, $c_k = c$이고

$d_1 = d_3 = \cdots = d_{n-1}$, $d_2 = d_4 = \cdots = d_n$
이면 다음 관계식이 성립한다.

$$\begin{aligned}\Phi_{1,n} &= a_1 a_2 \Phi_{3,n} + (bc)^2 \Phi_{5,n} \\ &+ (a_1 a_2 + b^2 + c^2)(b^{n-2} + c^{n-2})\end{aligned}$$

5. IBCA(Intermediate Boundary CA)

IBCA의 전이행렬은 다음과 같다.

$$\begin{bmatrix} d_1 & b_1 & c_1 & \cdots & 0 & 0 & 0 \\ c_2 & d_2 & b_2 & \cdots & 0 & 0 & 0 \\ 0 & c_3 & d_3 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & c_{n-1} & d_{n-1} & b_{n-1} \\ 0 & 0 & 0 & \cdots & b_n & c_n & d_n \end{bmatrix}$$

<정리 5.1> $b_2 \neq 0$이고 $c_{n-1} \neq 0$아닌 모든 NBCA에 대하여 같은 특성다항식을 갖는 IBCA가 적어도 하나 존재한다.

정리 5.1에서 $b_k = c_k = 1$ 이고 d_k가 0 또는 1이면 다음 결과를 얻는다[4].

<따름정리 5.2> 모든 90/150 NBCA에 대하여 같은 특성다항식을 갖는 IBCA가 적어도 하나 존재한다.

<정리 5.3> $n \geq 7$일 때 IBCA의 특성다항식은 다음과 같다.

$$\begin{aligned}\Psi_{1,n} &= \Delta_{1,n} + \prod_{k=1}^{3} c_k \Delta_{4,n} + \prod_{k=n-2}^{n} b_k \Delta_{1,n-3} \\ &+ \prod_{k=1}^{3} c_k \prod_{k=n-2}^{n} b_k \Delta_{4,n-3}\end{aligned}$$

<따름정리 5.4[10]> $n \geq 7$이고 $q = 2$라 하자. $b_k = c_k = 1$이고 d_k는 0 또는 1이면 다음이 성립한다.

$$\Psi_{1,n} = \Delta_{1,n} + \Delta_{1,n-3} + \Delta_{4,n} + \Delta_{4,n-3}$$

<정리 5.5> $a_1 = a_4$, $b_1 = b_4$, $c_1 = c_4$, $c_2 = c_5$이고 $n \geq 7$이면 $\Psi_{1,n}$은 다음과 같다.

$$\Psi_{1,n} = a_1 \Psi_{2,n} - b_1 c_2 \Psi_{3,n}$$

<따름정리 5.6[10]> $n \geq 7$이고 $q = 2$라 하자. $b_k = c_k = 1$이고 d_k는 0 또는 1이면 다음이 성립한다.

$$\Psi_{1,n} = a_1 \Psi_{2,n} + \Psi_{3,n}$$

참 고 문 헌

[1] P. H. Bardell, "Analysis of cellular automata used as pseudo-random pattern generators", Proc. IEEE int. Test. Conf., pp. 762-767, 1990.

[2] K. Cattell and J. C. Muzio, "Analysis of one dimensional linear hybrid cellular automata over $GF(q)$, IEEE Trans Computers, Vol. 45, No. 7, pp. 782-792, 1996.

[3] K. M. Cattell and J. C. Muzio, "Synthesis of one-dimensional linear hybrid cellular automata", IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems, Vol. 15, No. 3, pp. 325-335, 1996.

[4] P. P. Chaudhuri, D. R. Chowdhury, S. Nandi and S. Chattopadhyay, Additive cellular automata Theory and applications, Vol. 1, IEEE Computer Society Press, California, 1997.

[5] A. K. Das and P. P. Chaudhuri, "Efficient characterization of cellular automata", Proc. IEE(PartE), Vol. 137, No. 1, pp. 81-87, 1990.

[6] A. K. Das and P. P. Chaudhuri, "Vector space theoritic analysis of additive cellular automata and its appli-cation for pseudo-exhaustive test pattern generation", IEEE Trans. Com

put., Vol. 42, pp. 340-352, 1993.
[7] S. Nandi and P. P. Chaudhuri, "Analysis of periodic and intermediate boundary 90/150 cellular automata", IEEE Trans. Computers, Vol. 45, No. 1, pp. 1-12, 1996.
[8] M. Serra, T. Slater, J. C. Muzio and D. M. Miller, "Analysis of one-dimen sional linear cellular automata and their aliasing properties", IEEE Trans. Computer-Aided Design, vol. 9, pp. 767-778, 1990.
[9] S. Wolfram, Universality and compl -exity in cellular automata, Physica, Vol. 10D, pp. 1-35, 1984.
[10] S.Y. Yoon, Characteristic polynomials of one dimensional cellular automata, Submitted.