두 개의 직전자를 갖는 Nongroup CA

조성진[*]· 최언숙[**]· 김한두[***]· 황윤희[*]· 김진경[*]
[*]부경대학교 ·[**]동명대학교 ·[***]인제대학교

Two Predecessor Nongroup Cellular Automata

Sung-Jin Cho[*] · Un-Sook Choi[**]· Han-Doo Kim[***]
· Yoon-Hee Hwang[*] · Jin-Gyoung Kim[*]
[*]Pukyong National Univ. · [**]Tongmyong Univ. · [***]Inje Univ.
E-mail : sjcho@pknu.ac.kr

요 약

본 논문에서는 두 개의 직전자를 갖는 90/150 비그룹 셀룰라 오토마타(TPNCA)를 생성하는 알고리즘을 제안한다. 특히, $p(x)$가 원시다항식일 때, $xp(x)$와 $x(x+1)p(x)$를 최소다항식으로 갖는 90/150 TPNCA를 주어진 알고리즘을 이용하여 각각 합성한다. 이 CA는 90/150 TPNCA에 기반한 의사난수열 생성 연구에 유용하다. 또한 해쉬을 연구하는데 유용한 TPSACA와 TPMACA를 합성한다.

ABSTRACT

In this paper, we propose an algorithm for finding 90/150 Two Predecessor Nongroup Cellular Automata(TPNCA). Especially, we synthesize TPNCA for the minimal polynomial whose type is of the form $xp(x)$ or $x(x+1)p(x)$ using the proposed algorithm which is useful to study pseudorandom number generation, where $p(x)$ is some primitive polynomial. Also we synthesize Two Predecessor Single Attractor CA and Two Predecessor Multiple Attractor CA which are useful to study hashing.

Ⅰ. 서 론

스스로 조직화하고 재생산할 수 있는 모델로 처음 소개된 셀룰라 오토마타(Cellular Automata, 이하 CA)는 테스트 패턴 생성, 의사난수생성기, 오류정정부호기, 암호, 시그니처 분석 등 많은 분야에 응용되었다[1-6]. 그룹 CA에 대한 연구[4-9]에 비해 비그룹 CA에 대한 연구가 많이 수행되지는 않았지만 최근 해쉬함수나 부울방정식의 해법, 논리회로 검사 등에 응용이 되면서 주목받기 시작하였다[1],[3],[10-11]. 특히 [1], [10]에서 특별한 부류의 D1*CA로 나타내는 비그룹 CA의 연구가 수행되었고, 이 연구에 기반을 두고 D1*CA가 합성 디자인의 테스트 능력을 강화하기 위하여 유한상태기계에 효율적으로 장착될 수 있는 이상적인 테스트 기계로서 제안되었다. 또한 [3]에서 원시다항식 $p(x)$에 대하여 $x(x+1)p(x)$ 형태의 최소다항식을 갖는 90/150 TPNCA를 분석했다. 이런 CA를 사용하면 하드웨어 구현이 간단해지며 이차함수와 관련된 행렬을 얻는데 필요한 복잡한 계산을 하지 않아도 된다는 장점이 있다. [3]에서 CA 길이가 다른 여러 경우를 연구하였지만 각 $n \geq 6$ 에 대하여 n-셀 90/150 TPNCA가 존재한다는 것을 보이지는 못했다. 본 논문에서는 두 개의 직전자를 갖는 90/150 비그룹 셀룰라 오토마타(TPNCA)를 생성하는 알고리즘을 제안한다. 특히, $p(x)$가 원시다항식일 때, $xp(x)$와 $x(x+1)p(x)$를 최소다항식으로 갖는 90/150 TPNCA를 주어진 알고리즘을 이용하여 각각 합

†본 연구는 한국과학재단 목적기초연구지원사업(R01-2006-000-10260-0)에 의해 수행되었습니다.

성한다. 이 CA는 90/150 TPNCA에 기반한 의사난수열 생성 연구에 유용하다. 또한 해성을 연구하는데 유용한 TPSACA와 TPMACA를 합성한다.

II. 셀룰라 오토마타

본 논문에서 다루는 1차원 3-이웃(linear 3-neighbourhood) CA는 모든 셀이 선형으로 배열되어 있고, 국소적 상호작용이 자신과 인접한 두 셀에 의하여 이루어지는 CA이다. CA에 대한 상태전이함수(state transition function)는

$$x_i^{t+1} = f(x_{i-1}^t, x_i^t, x_{i+1}^t)$$

과 같이 나타낸다. 여기서 x_i^t는 시간 t에서 i번째 셀의 상태를 나타낸다. 그리고 이러한 f는 2^{2^3}개가 있으며 이것을 CA의 전이규칙이라 한다. 본 논문에서 사용되는 전이규칙 90과 150은 다음과 같다.

$$\text{전이규칙 } 90 \ : \ x_i^{t+1} = x_{i-1}^t \oplus x_{i+1}^t$$
$$\text{전이규칙 } 150 : \ x_i^{t+1} = x_{i-1}^t \oplus x_i^t \oplus x_{i+1}^t$$

n개의 셀로 이루어진 선형 n-셀 CA의 상태전이함수는 $n \times n$ 행렬로 나타낼 수 있으며, 이를 상태전이행렬(state-transition matrix)이라 한다. 주어진 n-셀 CA의 상태전이행렬 T의 특성다항식(characteristic polynomial) $c(x)$는 $GF(2)$ 위에서 $c(x)=|T \oplus xI|$이다. 여기서, I는 n차 단위행렬이다. 또, 특성다항식의 인수 중 T를 근으로 갖는 차수가 가장 낮은 다항식을 최소다항식(minimal polynomial)이라 한다. 그룹 CA의 상태전이그래프에서 사이클의 구조는 CA의 최소다항식에 의하여 특성화된다. 특히, 90/150 CA는 특성다항식과 최소다항식이 같다[7]. 벡터 $< d_1, d_2, \cdots, d_n >$을 전이규칙 벡터라고 한다. 여기서

$$d_i = \begin{cases} 0, & i\text{번째 셀의 전이규칙} = 90 \\ 1, & i\text{번째 셀의 전이규칙} = 150 \end{cases}$$

이다. 만약 C가 전이규칙 벡터가 $< d_1, d_2, \cdots, d_n >$인 CA라면, C의 상태전이 행렬은 다음과 같은 삼중대각행렬이다.

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

표기상의 편리를 위하여 $T = < d_1, d_2, \cdots, d_n >$로 쓴다.

<정의 2.1[10]> (1) 그룹 CA: T가 CA에 대한 상태전이행렬일 때, $\det(T) = 1$이면 CA를 그룹 CA(group CA)라고 한다. $\det(T) = 0$인 CA를 비그룹 CA(nongroup CA)라 한다.

(2) Attractor: 비그룹 CA의 상태전이그래프에서 순환상태들 중 사이클의 길이가 1인 상태를 attractor라 한다.

(3) 직전자: 상태 x에 대하여 $Ty = x$인 상태 y를 x의 직전자(predecessor)라 한다.

(4) Depth: 비그룹 CA의 상태전이그래프에서 임의의 도달불가능 상태에서 가장 가까운 순환상태까지 가는데 걸리는 최소 단계 수를 depth라 한다.

(5) Multiple attractor CA(MACA): 상태전이그래프가 각 attractor를 root로 하는 서로 분리된 트리들로 구성된 비그룹 CA를 MACA라 한다. 특히 직전자의 수가 두 개인 MACA를 TPMACA라 한다. attractor가 한 개인 MACA를 Single attractor CA(SACA)라 하며 특히 직전자의 수가 두 개인 SACA를 TPSACA라 한다.

(6) TPNCA: 임의의 도달가능한 상태의 직전자의 수가 두 개인 비그룹 CA를 TPNCA라 한다.

III. TPNCA 합성 알고리즘

이 장에서는 [9]의 결과들을 이용하여 90/150 TPNCA를 찾는 알고리즘을 제안한다. 상삼각행렬 U가 다음과 같다고 하자.

$$U = \begin{pmatrix} 1 & a_1 & * & \cdots & * & * & * \\ 0 & 1 & a_2 & \cdots & * & * & * \\ 0 & 0 & 1 & \cdots & * & * & * \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & a_{n-2} & * \\ 0 & 0 & 0 & \cdots & 0 & 1 & a_{n-1} \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix}$$

$f(x) = x^n + c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_1 x + c_0$ $(c_i \in GF(2))$라 할 때 다음과 같은 $n \times n$ 행렬 C를 $f(x)$의 동반행렬(companion matrix)이라 한다.

$$C = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & c_0 \\ 1 & 0 & 0 & \cdots & 0 & c_1 \\ 0 & 1 & 0 & \cdots & 0 & c_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & c_{n-1} \end{pmatrix}$$

<정의 3.1> 주어진 $(2n-1)$-벡터 $< y_1, y_2, \cdots, y_{2n-2}, y_{2n-1} >$에 대해서 Hankel 행렬 H는 다음과 같은 형태이다.

$$H = \begin{pmatrix} y_1 & y_2 & y_3 & \cdots & y_n \\ y_2 & y_3 & y_4 & \cdots & y_{n+1} \\ y_3 & y_4 & y_5 & \cdots & y_{n+2} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ y_n & y_{n+1} & y_{n+2} & \cdots & y_{2n-1} \end{pmatrix}$$

<정의 3.2> 주어진 n-벡터 $\boldsymbol{x}$와 $n\times n$ 행렬 M에 대하여

$$K(M,\boldsymbol{x}) = <\boldsymbol{x}; M\boldsymbol{x}; M^2\boldsymbol{x}; \cdots ; M^{n-1}\boldsymbol{x}>$$

라고 하자. $K(M,\boldsymbol{x})$을 Krylov 행렬이라 한다.

<정리 3.3> $T = <d_1, d_2, \cdots, d_n>$ 라 하고 C를 T의 특성다항식의 동반행렬이라고 하자. U가 $TU = UC$ 를 만족하는 위와 같은 상삼각행렬이면 다음 식이 성립한다.

$$\begin{cases} d_1 = a_1 \\ d_2 = a_1 \oplus a_2 \\ d_3 = a_2 \oplus a_3 \\ \vdots \\ d_{n-1} = a_{n-2} \oplus a_{n-1} \\ d_n = a_{n-1} \oplus c_{n-1} \end{cases}$$

<정의 3.4> 주어진 가약다항식 $f(x)$에 대하여 B가 다음과 같은 n개 다항식의 계수를 오름차순으로 나열한 행벡터로 이루어진 $n\times n$ 행렬이라고 하자.

$$x^{i-1} + x^{2i-1} + x^{2i} \bmod f(x),\ (i = 1,2,\cdots,n)$$

집합 $\{\boldsymbol{v} \mid B\boldsymbol{v} = (0,\cdots,0,1)^t\}$이 공집합이 아닌 경우, $\{\boldsymbol{v} \mid B\boldsymbol{v} = (0,\cdots,0,1)^t\}$의 원소들에 의해 생성된 Krylov 행렬이 LU분해가 가능할 때, 다항식 $f(x)$를 90/150 TPNCA 다항식(TPNCA polynomial)이라 한다.

<예제 3.5> $f(x) = x(x^4 + x^3 + 1)$ 이면

$B = \begin{pmatrix} 1\,1\,1\,0\,0 \\ 0\,1\,0\,1\,1 \\ 0\,0\,0\,0\,0 \\ 0\,0\,0\,1\,1 \\ 0\,1\,1\,0\,0 \end{pmatrix}$ 이고, 방정식 $B\boldsymbol{v} = (0,0,0,0,1)^t$의 해는 $\boldsymbol{v} = (1,0,1,0,0)^t$ 이므로 $H = K(C^t, \boldsymbol{v}) = \begin{pmatrix} 1\,0\,1\,0\,0 \\ 0\,1\,0\,0\,0 \\ 1\,0\,0\,0\,1 \\ 0\,0\,0\,1\,1 \\ 0\,0\,1\,1\,1 \end{pmatrix}$ 이고 $U = \begin{pmatrix} 1\,0\,1\,0\,0 \\ 0\,1\,0\,0\,0 \\ 0\,0\,1\,0\,1 \\ 0\,0\,0\,1\,1 \\ 0\,0\,0\,0\,1 \end{pmatrix}$ 이다. 따라서 $T = <0,0\oplus 0,0\oplus 0,0\oplus 1,1\oplus 1> = <0,0,0,1,0>$이다.

다음 알고리즘은 주어진 가약다항식에 대하여 90/150 TPNCA를 찾는 알고리즘이다.

<알고리즘 90/150 TPNCA의 합성>

Input : 다항식 $f(x)$

Output : 90/150 TPNCA

단계1 : 식(3.2)로부터 행렬 B를 구한다.

단계2 : 방정식 $B\boldsymbol{v} = (0,\cdots,0,1)^t$을 푼다. 만일 해 $\boldsymbol{v}$가 존재하지 않으면 멈춘다.

단계3 : 단계2의 방정식의 해 $\boldsymbol{v}$에 의해 생성된 Krylov 행렬 $H = K(C^t, \boldsymbol{v})$을 구성한다.

단계4 : LU분해 $H = LU$를 계산한다.

단계5 : 식(3.1)을 이용하여 행렬 U에 의해 $f(x)$에 대한 TPNCA를 계산한다.

IV. TPSACA와 TPMACA 합성

이 절에서는 90/150 TPNCA를 분석한다.

<보조정리 4.1> Δ_n이 $<d_1, d_2, \cdots, d_m, d_m, \cdots, d_2, d_1>$의 특성다항식이면 다음 식이 성립한다.$(i = 1,\cdots, 2m-1)$

$$\Delta_{i+1}\Delta_{2m-i-1} + \Delta_i\Delta_{2m-i-2} = \Delta_{i+2}\Delta_{2m-i-2}\Delta_{i+1} + \Delta_{2m-i-3}$$

<정리 4.2> Δ_n이 $<d_1, d_2, \cdots, d_m, d_m, \cdots, d_2, d_1>$의 특성다항식이면 다음 식이 성립한다.

$$\Delta_{2m} = (\Delta_m + \Delta_{m-1})^2$$

<정리 4.3> $f(x)$가 $<d_1, d_2, \cdots, d_m + 1>$의 특성다항식이고 Δ_m이 $<d_1, d_2, \cdots, d_m>$의 특성다항식이면 다음 식이 성립한다.

$$\Delta_m + \Delta_{m-1} = f(x)$$

<따름정리 4.4> $f(x)$가 $<d_1, d_2, \cdots, d_m + 1>$의 특성다항식이고 Δ_{2m}이 $<d_1, d_2, \cdots, d_m, d_m, \cdots, d_2, d_1>$의 특성다항식이면 다음 식이 성립한다.

$$\Delta_{2m} = \{f(x)\}^2$$

<정리 4.5> 모든 양의 정수 n에 대하여 n-셀 90/150 TPSACA가 존재한다.

[참고] n-셀 90/150 TPSACA $\mathbb{C}_n$의 최소다항식이 x^n이므로 2-셀 TPSACA는 $\mathbb{C}_2 = <1,1>$ 임을 알 수 있다. 그러므로 정리 4.5에 의하여 4-셀 TPSACA는 $\mathbb{C}_4 = <1,0,0,1>$가 된다. 또한 1-셀 TPSACA는 $\mathbb{C}_1 = <0>$이 되어 $\mathbb{C}_3 = <0,0,0>$임을 알 수 있다.

<정리 4.6> $N(T_m) = \{(a_1,a_2,\cdots,a_m)^t \mid a_1, a_2, \cdots, a_m \in \{0,1\}\}$ $(:= [(a_1, \cdots, a_m)^t])$ 을 n-셀 90/150 TPSACA의 상태전이행렬 T_n의 영공간(null space)이라 하면 다음이 성립한다.

(i) $n=2m$ $(m \in \mathbb{N})$이고 $N(T_m) = [(a_1, \cdots, a_m)^t]$ 이면 $N(T_n) = [(a_1,a_2,\cdots,a_m,a_m,\cdots,a_2,a_1)^t]$ 이다.

(ii) $n=2m+1$ $(m \in \mathbb{N})$이고 $N(T_m) = [(a_1, \cdots, a_m)^t]$ 이면 $N(T_n) = [(a_1,a_2,\cdots,a_m,0,a_m,\cdots,a_2,a_1)^t]$ 이다.

<예제 4.7> $<0,0,0>$ 은 3-셀 90/150 TPSACA이므로 $<0,0,1,1,0,0>$ 은 6-셀 90/150 TPSACA이고 $<0,0,0,0,0,0,0>$ 은 7-셀 90/150 TPSACA이다.

<정리 4.8> $\mathbb{C}$가 홀수 n에 대하여 n-셀 90/150 TPMACA이면 $\mathbb{C}$의 최소다항식은 $x^{n-1}(x+1)$ 이다.

[참고] 정리 4.8은 n이 짝수일 때 성립하지 않는다.

<정리 4.9> $\mathbb{C}_S^n = <d_1,\cdots,d_n>$ 이 n-셀 90/150 TPSACA이면 $\mathbb{C}_M^{2n+1} = <d_1,\cdots,d_n,1,d_n,\cdots,d_1>$ 은 최소다항식이 $x^{2n}(x+1)$ 인 $(2n+1)$-셀 TPMACA 이다.

V. 결 론

본 논문에서는 두 개의 직전자를 갖는 90/150 비그룹 셀룰라 오토마타(TPNCA)를 생성하는 알고리즘을 제안하였다. 특히, $p(x)$가 원시다항식일 때, $xp(x)$와 $x(x+1)p(x)$를 최소다항식으로 갖는 90/150 TPNCA를 주어진 알고리즘을 이용하여 각각 합성하였다. 이 CA는 90/150 TPNCA에 기반한 의사난수열 생성 연구에 유용하다. 또한 해쉬을 연구하는데 유용한 TPSACA와 TPMACA를 합성하였다.

참고문헌

[1] S. Chakraborty, D.R. Chowdhury and P.P. Chaudhuri, "Theory and application of nongroup cellular automata for synthesis of easily testable finite state machines," IEEE Trans. Computers, Vol. 45, pp. 769-781, 1996.

[2] S. Chattopadhyay and P.P. Chaudhuri, "Theory and application of nongroup cellular automata in pattern classification," IEEE Trans. Computers, communicated.

[3] D. de la Guia Martinez and A. Peinado Dominguez, "Pseudorandom number generation based on nongroup cellular automata," Security Technology, 1999, Proceedings, IEEE 33rd Annual 1999 International Carnahan Conference, 45, pp. 370-376, 1999.

[4] M. Serra, T. Slater, J. C. Muzio and D. M. Miller, "The analysis of one dimensional linear cellular automata and their aliasing properties," IEEE Trans. Comput-Aided Desig,9, pp. 767-778, 1990.

[5] P. D. Hortensius, R. D. McLeod and H. C. Card, "Parallel random number generation for VLSI systems using cellular automata." IEEE Trans. Computers, 38, pp. 1466-1473, 1989.

[6] P. D. Hortensius, R. D. McLeod and H. C. Card, "Cellular automata-based signature analysis for built-in self-test," IEEE Trans. Comput., 39, pp. 1273-1283, 1990.

[7] K. Cattell and J. Muzio, "Synthesis of one-dimensional linear hybrid cellular automata," IEEE Trans. Comput-Aided Des. Integr. Circuits Syst., Vol. 15, pp. 325-335, 1996.

[8] S.J. Cho, U.S. Choi, Y.H. Hwang, Y.S. Pyo, H.D. Kim and S.H. Heo, "Computing Phase Shifts of Maximum-Length 90/150 Cellular Automata Sequences," LNCS, Vol. 3305, pp. 31-39, 2004.

[9] S.J. Cho, U.S. Choi, and H.D. Kim, Y.H. Hwang, J.G. Kim and S.H. Heo, "New synthesis of one-dimensional 90/150 linear hybrid group cellular automata," IEEE Trans. Comput-Aided Des. Integr. Circuits Syst., Accepted.

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

[11] S.J. Cho, U.S. Choi, Y.H. Hwang and H.D. Kim "Analysis of hybrid group cellular automata," ACRI 2006, LNCS, 4173, pp. 222-231, 2006.