최대길이를 갖는 가산 셀룰라 오토마타의 생성†

조성진*, 최언숙**
*부경대학교 수리과학부
**영산대학교 자유전공학부
e-mail : sjcho@pknu.ac.kr

Generation of Additive Maximum Length Cellular Automata†

Sung-Jin Cho*, Un-Sook Choi**
*Division of Mathematical Sciences, Pukyong National University
**University College of Undeclared Majors, Youngsan University

요 약

최대길이를 갖는 선형유한상태기계(LFSM)가 패턴생성, 신호분석, 암호, 오류정정 부호에 응용되면서 n차 원시다항식을 특성다항식으로 갖는 선형유한상태기계에 관한 연구가 활발하게 이루어지고 있다. 본 논문은 최대길이를 갖는 다양한 셀룰라 오토마타의 효과적인 생성방법을 제안한다. 특성다항식이 n차 원시다항식인 선형 MLCA로부터 유도된 여원 CA가 MLCA임을 밝히며 여원 MLCA의 여러 가지 성질들을 분석한다. 또한 n-셀 MLCA를 $\phi(2^n-1)\,2^{n+1}/n$ 개 생성할 수 있음을 보인다.

1. 서론

셀룰라 오토마타(CA)는 Von Neumann[1]에 의하여 스스로 조직화하고 재 생산할 수 있는 모델로 처음 소개되었다. 이후 1980년대에 Wolfram[2]은 CA를 셀이라 불리는 메모리의 배열로 소개하고, 셀의 상태가 자기 자신 및 인접한 셀 상태의 국소적인 상호작용에 의해서 동시에 갱신되는 시스템으로 제안하였다. 또한 CA는 간단하고, 규칙적이며, 작은 단위로 확장 연결할 수 있는 구조이기 때문에 하드웨어 구현에 알맞다. VLSI 하드웨어 구현의 용이성과 렌덤성의 우수함으로 인해 LFSR의 대안으로 제안된 CA중, 특히 최대길이를 갖는 CA는 test pattern generation, 의사난수열 생성기, 오류정정부호, 신호분석 등 많은 분야에서 응용되고 있다.

† 본 연구는 한국과학재단 특정기초연구 (R01-2003-000-10663-0)지원으로 수행되었음.

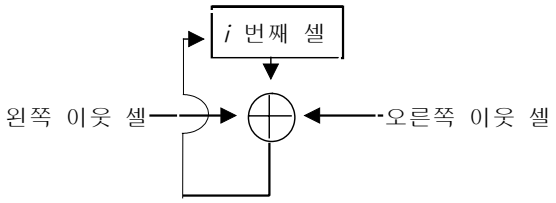
Chang 등[3]은 최대길이의 선형 이진 LFSR 수열을 90/150 NBCA를 이용하여 생성할 수 있음을 보였다. Cattel과 Muzio[4]는 주어진 원시다항식을 특성다항식으로 갖는 LFSR은 하나 존재하는데 비하여 90/150 NBCA는 두 개가 있음을 보이고 이러한 CA의 합성법을 유클리드의 알고리즘과 이차 합동식을 이용하여 제안하였다. Nandi와 Chaudhuri[5]는 최대길이를 갖는 CA를 다양하게 생성하기 위하여 90/150 IBCA를 제안하고, 이 CA를 이용하여 한 원시다항식에 대응하는 최대길이를 갖는 CA가 최대 18개까지 존재할 것이라고 추측하였다. 보다 우수한 랜덤성을 갖는 CA의 생성을 위하여 최대길이를 갖는 CA에 관한 연구는 1차원뿐만 아니라 2차원 CA에서도 연구되어왔다. Chowdhury 등[6]은 랜덤패턴 생성에 2차원 CA를 도입하였고, Cho 등[7]은 최대길이를 갖는 2차원 CA의 다양한 생성을 위하여 2-D IBCA를 제안하였다. Cho 등[8, 9]은 선형 CA로부터 유도되는 여원 CA의 행동을 분석하였다.

본 논문은 최대길이를 갖는 다양한 셀룰라 오토마타의 효과적인 생성방법을 제안한다. 특성다항식이

n차 원시다항식인 선형 MLCA로부터 유도되는 여원 CA가 MLCA임을 밝히며 여원 MLCA의 여러 가지 성질들을 분석한다. 또한 n-셀 MLCA를 $\phi(2^n-1)\,2^{n+1}/n$개 생성할 수 있음을 보인다.

2. 셀룰라 오토마타

CA란 동역학계를 해석하는 한 방법으로 공간과 시간을 이산적으로 다루는 시스템이며, 셀룰라 공간(cellular space)의 기본 단위인 각 셀(cell)이 취할 수 있는 상태를 유한하게 처리하며, 각 셀들의 상태가 국소적인 상호작용에 의해서 동시에 갱신되는 시스템이다. 가장 간단한 구조를 가지는 1차원 CA(1-D CA)에서는 모든 셀들이 선형으로 배열되어 있고 1-D CA 중에서 국소적 상호작용이 세 개의 셀, 즉 자신과 인접한 두 셀에 의해 이루어지는 CA를 3-이웃(3-neighborhood) CA라 한다. 본 논문에서 다루는 CA는 3-이웃 1-D CA에 국한시킨다. 그림 1은 3-이웃 선형 CA의 셀 구조이다.



<그림 1> 3-이웃 선형 CA의 셀 구조

세 개의 이웃을 가지는 CA에 대하여 시간 t에서 다음 시간에서 i번째 셀의 상태를 구하는 전이함수는 다음과 같다.

$$q_i(t+1) = f[\,q_{i-1}(t)\,,\,q_i(t)\,,\,q_{i+1}(t)\,]$$

여기서 f는 결합논리를 가지는 국소 전이함수이다. 본 논문에서 사용되는 rule 90과 rule 150은 다음과 같은 논리결합으로 전이함수를 표현할 수 있다.

rule 90: $q_i(t+1) = q_{i-1}(t) \oplus q_{i+1}(t)$
rule 150: $q_i(t+1) = q_{i-1}(t) \oplus q_i(t) \oplus q_{i+1}(t)$

CA는 적용되는 rule의 논리의 종류에 따라 선형 CA(Linear CA), 가산 CA(Additive CA), 비가산 CA(Nonadditive CA)로 분류되는데 각 셀에 적용된 rule이 XOR 논리로만 이루어진 CA는 선형 CA이다. 선형 CA의 상태 전이 함수는 행렬로 표현 될 수 있고 이 행렬을 전이행렬이라 한다. 또한 셀에 적용되는 rule이 XNOR과 XOR논리로 이루어진 CA를 여원 CA(Complemented CA)라 하고 선형 CA와 여원 CA를 가산 CA라 한다. 셀들의 rule이 AND-OR논리로 이루어진 CA를 비가산 CA라 한다.

CA의 rule에 의해 변화되는 상태를 나타낸 상태 전이 그래프의 형태에 따라 Group CA와 Nongroup CA로 분류할 수 있다. Group CA는 모든 셀들의 상태가 몇 개의 사이클을 이루며 반복되는 CA로 임의의 한 상태에 대한 이전상태가 유일하다.

CA에서 가장 왼쪽과 오른쪽의 셀은 2개의 이웃만을 가지므로 세 번째 이웃의 상태를 결정해 주어야 한다. 이것을 CA의 경계조건이라 하고 일반적으로 다음 세 가지의 경계조건을 이용한다. 제일 왼쪽과 오른쪽의 셀들이 0상태에 연결되어 있는 NBCA (Null Boundary CA), 양끝의 셀들이 서로 연결되어 있는 PBCA(Periodic Boundary CA), 가장 왼쪽(오른쪽) 셀의 다음 상태가 그 자신과 그것의 오른쪽(왼쪽) 이웃, 두 번째 오른쪽(왼쪽) 이웃 셀의 상태에 의존하는 IBCA(Intermediate Boundary CA)이다.

90과 150 rule로만 이루어진 선형 CA를 90/150 CA라고 하는데, 본 논문에서 언급되는 n-셀 90/150 NBCA의 전이행렬은 다음과 같은 삼중대각 행렬(tridiagonal matrix)로 나타낼 수 있다.

$$T = \begin{pmatrix} a_1 & 1 & 0 & \cdots & 0 \\ 1 & a_2 & 1 & \cdots & 0 \\ 0 & 1 & a_3 & \cdots & 0 \\ & & \cdots & & \\ 0 & 0 & 0 & \cdots & a_n \end{pmatrix}$$

여기서 a_i는 i번째 셀에 적용된 rule이 90인 경우는 0이고, 150인 경우는 1이다. S_t가 시간 t에서 CA의 상태를 나타내면, 시간 $t+1$에서 CA의 상태는 $S_{t+1} = TS_t$이다. 또한 p단계 후의 CA의 상태는 $S_{t+p} = T^pS_t$이다.

여원 CA의 다음 상태를 구하는 연산자를 $\overline{T}$라 하면, 다음 상태는 $S_{t+1} = \overline{T}S_t = TS_t \oplus F$이다. 여기서 F는 여원벡터로, 여원 규칙에 대응하는 선형규칙으로 표현한 전이행렬을 T라 할 때, 결과 값

을 역으로 바꾸어야 하는 셀을 나타내는 위치의 성분 값이 1이고 나머지는 0인 n차원 벡터이다. $\overline{T}^p$를 여원 CA의 연산자인 $\overline{T}$를 p번 적용한 것이라 하면 p시간 단계 후의 여원 CA의 상태는 다음과 같다.

$$S_{t+p} = \overline{T}^p S_t = T^p S_t \oplus (I \oplus T \oplus \cdots \oplus T^{p-1})F$$

3. 최대길이를 갖는 CA

전이행렬 T에 대하여 $|T+xI|$를 CA의 특성다항식이라 한다. 90/150 NBCA는 특성다항식과 최소다항식이 같다[10]. n차 다항식 $p(x)$가 x^m+1을 나누는 최소의 m값이 2^n-1일 때, $p(x)$를 원시다항식이라 한다. 계수가 GF(2)의 원소인 n차 원시다항식의 개수는 $\phi(2^n-1)/n$이다[11].

<정의> 상태 전이그래프에서 주기가 2^n-1인 n-셀 CA를 최대길이를 갖는 CA(Maximum Length CA, 이하 MLCA)라 한다. □

<정리 1> n차 원시다항식을 특성다항식으로 갖는 선형 CA는 선형 MLCA이다. □

임의의 원시다항식에 대응되는 최대길이를 갖는 선형 90/150 CA는 2개 존재한다[4]. 이러한 제약을 극복하고 보다 많은 MLCA를 찾기 위해 여원 CA를 고려한다. 여원 CA에서 여원 벡터 F는 CA의 크기와 같은 n차원 벡터이다. 그러므로 F는 모든 성분이 0인 0 벡터를 제외한 2^n-1개를 만들 수 있고, 이것은 CA가 생성하는 상태들과 일대일 대응시킬 수 있다. 이러한 여원 CA는 모두 같은 전이행렬 T의 영향을 받는다. 이렇게 같은 전이행렬을 가지는 선형 CA를 여원 CA에 대응하는 선형 CA라하고, 여원 CA는 선형 CA로부터 유도된 여원 CA라 한다. 다음의 정리에 의해 선형 MLCA로부터 유도된 여원 CA는 MLCA가 됨을 알 수 있다.

<정리 2> n셀 선형 MLCA로부터 유도되는 여원 CA의 상태전이그래프에서 상태 0은 길이가 2^n-1인 사이클에 놓인다. □

n셀 CA의 상태의 개수는 2^n이다. 여원 MLCA의 상태전이 그래프는 주기의 길이가 2^n-1인 사이클 1개와, 주기가 1인 사이클 1개로 이루어진다. 다음 두 정리는 주기가 1인 상태를 구할 수 있음을 보이며, 또한 이러한 상태의 성질을 밝힌다.

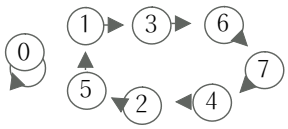
<정리 3> 특성다항식이 원시다항식인 선형 MLCA로 부터 유도되는 여원 MLCA에 대하여 $\overline{T}(T^kF) = T^kF$인 k가 존재한다. 여기서 T^kF는 주기가 1인 순환상태이다. □

<정리 4> 한 선형 MLCA로부터 유도되는 2^n-1개의 여원 MLCA에 대하여 $\overline{T}(T^kF) = T^kF$를 만족하는 k가 유일하다. □

<예> 3-셀 CA의 rule이 <90, 90, 150>일 때 전이행렬과 특성다항식 $m(x)$은 다음과 같다.

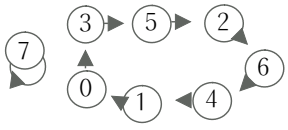
$$T = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \; m(x) = x^3+x^2+1$$

$m(x)$가 원시다항식이므로 이 CA는 선형 MLCA이다.



<그림 2> 선형 MLCA

그림 2는 주어진 선형 MLCA의 상태전이 그래프이다. 여기서 상태 3을 여원벡터 F라 할 때, 선형 MLCA에 의해 유도된 여원 CA의 상태전이 그래프는 그림 3과 같다.



<그림 3> 여원 MLCA

선형 MLCA의 특성다항식은 원시다항식이므로 특성다항식과 최소다항식이 같다. 그림 3의 주기가 1인 상태 T^kF는 다음을 만족한다.

$\overline{T}(T^kF) = T^kF \Leftrightarrow T(T^kF) \oplus F = T^kF (F \neq 0)$

$\Leftrightarrow (T^{k+1} \oplus T^k \oplus I)F = 0 \Leftrightarrow T^k(T \oplus I) = I$

$m(T) = T^3 + T^2 + I = 0$이다. $T^3 = T^2 + I$이므로 $T^5 = T^2(T^2 + I) = T(T^2 + I) + T^2 = T + I$이다. 그러므로 $T^2(T + I) = T^7 = I$을 만족한다. 그러므로 $k = 2$이다. □

한 선형 MLCA로부터 유도되는 $2^n - 1$개의 여원 MLCA에 대하여 주기가 1인 순환상태가 모두 다르므로 서로 다른 $2^n - 1$개의 여원 MLCA를 구성할 수 있다. 그러므로 n차 원시다항식의 개수는 $\phi(2^n - 1)/n$이고, 한 원시다항식에 대응하는 MLCA의 개수는 선형 90/150 MLCA 2개와 이로부터 유도되는 여원 MLCA $2(2^n - 1)$개이므로 n-셀 MLCA의 개수는 $\phi(2^n - 1)\, 2^{n+1}/n$이다.

4. 결론 및 향후 연구방향

최대길이를 갖는 유한상태기계는 패턴생성, 신호분석, 암호, 오류정정 부호에 응용되므로, n차 원시다항식을 특성다항식으로 갖는 MLCA를 구성하는 것은 매우 중요하다. 본 논문은 보다 다양한 MLCA를 구성하기 위해 여원 MLCA를 이용하여, $\phi(2^n - 1)\, 2^{n+1}/n$개까지 구성할 수 있음을 보였다. 이는 n차 원시다항식을 특성다항식으로 갖는 MLCA가 2개 존재한다는 기존의 연구결과 보다 향상된 결과이다. 또한 분석의 용이성을 위해 선형 MLCA로부터 여원 MLCA를 유도하였다. 향후 연구계획은 최대길이를 갖는 90/150 IBCA로부터 여원 CA를 유도하여 더욱 다양한 MLCA를 구성하고 이를 분석하고자 한다.

참고문헌

[1] J. Von Neumann, “Theory of self-reproducing automata”, University of Illinois Press Urbana, 1966.

[2] S. Wolfram, “Statistical mechanics of cellular automata”, Rev. Modern Physics, Vol. 55, No. 3, 1983.

[3] T.J. Chang, I.H. Song, J.S. Bae and K.S. Kim, "Maximum length cellular automata sequences and its application", Signal Processing Vol. 56, 1997, pp. 199-203.

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

[5] S. Nandi and P.P. Chaudhuri, "Analysis of periodic and intermediate boundary 90/150 cellular automata", IEEE Trans. Comput., Vol. 45, 1996, pp. 1-12.

[6] D.R. Chowdhury, I.S. Gupta and P.P. Chaudhuri, " A class of two-dimensional cellular automata and applications in random pattern testing", J. Electronic Testing: Theory & Applications, Vol. 5, 1944, pp. 65-80.

[7] S.J. Cho, S.T. Kim, J.G. Kim, H.D. Kim and U.S. Choi, "Algorithm for generating traffic distributions in ATM networks using 2-D LHCA"

[8] S.J. Cho, U.S. Choi and H.D. Kim, “Analysis of complemented CA derived from a linear TPMACA”, Comput. & Math. Appl., Vol. 45, 2003, pp. 689-698.

[9] S.J. Cho, H.D. Kim and U.S. Choi, “Behavior of complemented cellular automata derived from a linear cellular automata”, Mathematical and Computer Modelling, Vol. 36, 2002, pp. 979-986.

[10] 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. Computer-Aided Design, Vol. 9, 1990. pp. 767-778.

[11] B. Elspas, "The Theory of Autonomous Linear Sequential Networks", TRE Trans. Circuits, Vol. CT-6, Mar. 1959, pp. 45-60.