3-이웃 셀룰라 오토마타의 도달 가능/불가능 상태 분석

황윤희* · 최언숙** · 권숙희* · 김경자* · 김한두*** · 조성진*[1]

Analysis of Reachable/Nonreachable States of 3-neighborhood Cellular Automata

Yoon-Hee Hwang* · Un-Sook Choi** · Suk-Hee Kwon* · Kyung-Ja Kim* · Han-Doo Kim*** · Sung-Jin Cho*[1]

요 약

본 논문에서는 3-이웃 셀룰라 오토마타의 도달 가능/불가능한 상태를 분석하고 도달가능 상태의 직전자를 구하는 알고리즘을 제안한다.

ABSTRACT

In this paper, we analyze reachable/nonreachable states of 3-neighborhood cellular automata and propose the algorithm finding the predecessor of a reachable state.

키워드

셀룰라 오토마타, 전이규칙, 직전자, 도달가능 상태 트리

Ⅰ. 서 론

셀룰라 오토마타(Cellular Automata; 이하 CA)는 von Neumann에 의하여 자체 재생산 할 수 있는 모델로 처음 소개되었다. 이후 Wolfram은 다음 상태가 스스로 조직화되고 갱신되는 3-이웃 상호연결을 만족하는 간단한 구조를 소개하였다[1]. Cattell 등에 의해서 LFSR에 대응하는 CA에 대한 연구와 최대 길이를 갖는 CA를 찾는 연구가 수행되었다[2]. 또, Cho 등은 nongroup CA의 특성에 관한 연구를 하였다[3-6]. CA는 이산 시간의 동적 시스템으로 셀의 기본 단위 메모리의 배열로 이루어진다. 즉, 각 셀들은 자기 자신과 이웃 셀들의 함수값에 의해 다음 상태가 동시에 갱신된다.

본 논문에서는 3-이웃 셀룰라 오토마타의 상태가 도달가능한지, 불가능한지를 판별하고 도달가능 상태의 직전자를 구하는 알고리즘을 제안한다.

Ⅱ. 셀룰라 오토마타

본 논문에서 사용되는 3-이웃 CA 상태전이함수는 $s_i^{t+1} = f(s_{i-1}^t, s_i^t, s_{i+1}^t)$이다. s_i^t는 시간 t에서 i번째 셀의 상태를 나타내고, f는 결합논리를 가지는 함수이다. 예를 들면, 규칙 105는 다음과 같다.

현재상태	111	110	101	100	011	010	001	000
다음상태	0	1	1	0	1	0	0	1

01101001(이진 표현) ⇒ 105(십진 표현)

규칙 105처럼 다음 상태의 8-비트 이진표현에서 0과 1의 개수가 같은 규칙을 균형이 잡힌 규칙(balanced rule)이라 하고, 그렇지 않은 경우 균형이 깨진 규칙(unbalanced

* 부경대학교, ** 동명대학교
*** 인제대학교, *1 교신저자

접수일자 : 2006. 5. 26

rule)이라 한다. 시간 t 에서 셀들의 상태 $s^t=(s_1^t, s_2^t, \cdots, s_n^t)$ 의 다음 상태는 다음과 같다.

$$s^{t+1}=(f_1(s_0^t,s_1^t,s_2^t),f_2(s_1^t,s_2^t,s_3^t), \cdots,f_n(s_{n-1}^t,s_n^t,s_{n+1}^t))$$

여기서 사용되는 CA는 NBCA(Null Boundary CA)로서, $s_0^t=s_{n+1}^t=0$ 이다.

CA는 상태전이그래프의 형태에 따라 모든 셀의 상태가 몇 개의 사이클을 이루며 반복되는 그룹 CA와 그렇지 않은 비그룹 CA로 나뉜다. 그룹 CA는 임의의 한 상태에 대한 직전자가 유일하므로 모든 상태가 도달가능하다. 이와 달리 비그룹 CA는 상태전이그래프가 트리 구조를 이루고 있으며, 상태전이 함수에 의해 얻어질 수 있는 상태인 도달가능 상태와 상태전이함수에 의해 나타날 수 없는 도달불가능 상태로 나누어진다.

Ⅲ. 도달 가능/불가능 상태

이 장에서는 주어진 CA에 대하여 상태가 도달가능 상태인지 도달불가능 상태인지를 판별한다. 그리고 직전자를 구하고 도달가능한 상태의 트리를 구성한다.

예를 들어, 규칙이 <83, 51, 105, 25>인 CA에서 상태 0011(3)가 도달가능 상태라고 가정하고, 표 1에서의 규칙들의 RMT(Rule Min Term; 현재상태의 십진표현)로부터 0011의 직전자를 구해보자. 본 논문에서 사용되는 CA는 NBCA이기 때문에 RMT들의 일부가 다음 상태에 영향을 주지 않으므로 'X'를 이용하여 표현한다[7].

표 1. 규칙 <83, 51, 105, 25>에 대한 진리표
Table. 1 Truth table of the CA with Rule <83, 51, 105, 25>

현재상태	111	110	101	100	011	010	001	000	규칙
첫번째 셀	X	X	X	X	0	0	1	1	83
두번째 셀	0	0	1	1	0	0	1	1	51
세번째 셀	0	1	1	0	1	0	0	1	105
네번째 셀	X	0	X	1	X	0	X	1	25

상태 0011의 첫 번째 비트 0을 얻기 위해서는 CA의 첫 번째 셀인 규칙 83의 2번째와 3번째 즉, RMT=2와 3에서 0으로 주어졌기 때문에, 2번째 또는 3번째 RMT에서 유도된다. 이러한 두 개의 RMT를 $x_1=\{2,3\}$ 이라 적는다. 다음으로, 규칙 51에서 두 번째 비트 0을 얻으려면, 가능한 RMT의 집합은 $P_2=100(4),101(5),110(6),111(7)\}$ 이다. 또한 규칙 51에서 얻고자 하는 상태 0에 대응하는 RMT의 집합 R_2 는 $R_2=010(2),011(3),110(6),111(7)$ 이다. 따라서 가능한 RMT의 집합 x_2 는 $P_2 \cap R_2=6,7$ 이다. 마찬가지로 규칙 105인 경우는 $P_3=4,5,6,7$ 이고 $R_3=0,3,5,6$ 이므로 $x_3=\{5,6\}$ 이다. 마지막으로 규칙 25인 경우는 $P_4=2,4$ 이고, $R_4=\{0,4\}$ 이므로 $x_4=\{4\}$ 이다. 상태 0011(3)의 경우 $x_4=\{4\}$ 는 x_3 의 6에서 유도되고, x_2 는 6에서 같은 방법으로 7에서 유도되고, x_1 은 3에서 유도되므로 0011의 직전자가 1110이고 따라서 0011은 도달가능 상태이다.

이제 도달가능 상태를 나타내는 도달가능 상태 트리를 구성하는 방법에 대해 알아보고, 이 트리를 이용하여 몇 가지 정리를 얻는다. 도달가능 트리의 각 노드는 최대 2개의 자식 노드를 가질 수 있다. n-셀 CA에서의 레벨의 수는 n 이다. 단노드의 수는 도달가능 상태의 개수를 나타낸다. n 비트 이진 문자열을 나타내는 근노드에서부터 단노드까지의 자식 노드들로 이루어진 수열은 도달가능 상태를 나타낸다. 즉, 규칙 <83, 51, 105, 25>인 CA의 도달가능 상태 트리를 만들면 그림 1과 같다.

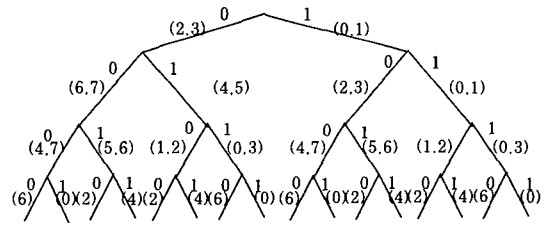

그림 1. 규칙이 <83, 51, 105, 25>인 CA의 도달가능 상태 트리
Fig. 1 Reachable state tree of the CA with Rule <83, 51, 105, 25>

<정리 1> n-셀 CA $\mathbb{C}$ 의 도달가능 상태 트리를 T라 할 때, $\mathbb{C}$가 그룹 CA일 필요충분조건은 T는 완전 이진트리이다.

<따름정리 2> CA의 도달가능 상태 트리 T의 단노드를 제외한 각 노드가 정확히 두 개의 RMT를 가지면, T는 완전 이진트리이다.

<정의 1> CA의 도달가능 상태 트리 T에 대하여 근노드를 중심으로 왼쪽 부트리와 오른쪽 부트리가 대칭이거나 같은 모양을 가질 때, T를 대칭트리(symmetric tree)라고 한다.

<정의 2> 하나의 CA C가 다음과 같은 세 조건 중에서 적어도 하나를 만족할 때, C를 균형이 깨진 규칙을 갖는 (having unbalanced rule) CA라고 정의한다.

(i) 첫 번째 셀의 RMT들 0, 1, 2와 3이 균형이 깨진 경우,
(ii) 마지막 셀의 RMT들 0, 2, 4와 6의 다음 상태의 0과 1의 개수가 다른 경우,
(iii) 첫 번째와 마지막을 제외한 셀 중에는 적어도 하나의 균형이 깨진 규칙이 있는 경우

이와는 반대로, 균형이 깨진 규칙을 갖지 않는 CA를 균형이 잡힌 규칙을 갖는 CA라고 정의한다. 즉, 정의 2의 세 조건을 모두 만족하지 않는 CA를 균형이 잡힌 규칙을 갖는 CA라고 한다.

규칙이 <83, 51, 105, 25>인 CA는 표 1에서와 같이 균형이 잡힌 규칙을 갖는 CA이다. 그러나 규칙이 <49, 105, 90, 73>인 CA는 표 2에서와 같이 균형이 깨진 규칙을 갖는 CA이다.

표 2. 규칙이 <49, 105, 90, 73>인 CA의 진리표
Table. 2 Truth table of the CA with **Rule** <49, 105, 90, 73>

현재상태	111	110	101	100	011	010	001	000	규칙
첫번째 셀	X	X	X	X	0	0	0	1	49
두번째 셀	0	1	1	0	1	0	0	1	105
세번째 셀	0	1	0	1	1	0	1	0	90
네번째 셀	X	1	X	0	X	0	X	1	73

규칙이 <25, 195, 85, 37>인 CA의 진리표는 표 3과 같이 균형이 잡힌 규칙을 갖는 CA이다. 이 CA의 도달가능 상태 트리를 그려보면 그림 2와 같이 CA의 도달가능 상태 트리가 대칭이지만 완전 이진트리는 아니다. 그림 2는 01과 10으로 시작하는 모든 상태가 직전자를 갖지 않음을 보여준다.

표 3. 규칙이 <25, 195, 85, 37>인 CA의 진리표
Table. 3 Truth table of the CA with **Rule** <25, 195, 85, 37>

현재상태	111	110	101	100	011	010	001	000	규칙
첫번째 셀	X	X	X	X	1	0	0	1	25
두번째 셀	1	1	0	0	0	0	1	1	195
세번째 셀	0	1	0	1	0	1	0	1	85
네번째 셀	X	1	X	0	X	0	X	1	37

<정리 3> 균형이 깨진 규칙을 갖는 CA는 비그룹 CA이다.

정리 3의 역은 일반적으로 성립하지 않는다. 예를 들어 규칙 <25, 195, 85, 37>을 갖는 CA는 비그룹 CA이지만 균형이 잡힌 규칙을 갖는 CA이다.

<정리 4> 균형이 잡힌 규칙을 갖는 CA의 도달가능 상태 트리는 항상 대칭트리이다.

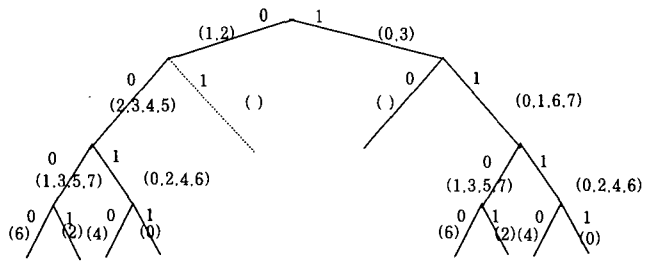

그림 2. 규칙이 <25, 195, 85, 37>인 CA의 도달가능 상태 트리
Fig. 2 Reachable state tree of the CA with Rule <25, 195, 85, 37>

VI. 도달가능 상태의 직전자

이 장에서는 CA가 도달가능한지 불가능한지를 판정하고 도달가능한 경우 직전자를 구한다. 표 4에 따르면 i 번째 셀 규칙에서 선택된 RMT가 k 이면, $(i+1)$ 번째 셀은 다음과 같은 규칙을 가진다.

표 4. $(i+1)$ 번째 규칙의 RMT
Table. 4 RMT at the $(i+1)^{th}$ rule

RMT	0	1	2	3	4	5	6	7	
$2k$	0	2	4	6	0	2	4	6	짝수
$2k+1$	1	3	5	7	1	3	5	7	홀수

표 4를 이용하여 CA 상태 x 가 도달 가능/불가능한지를 알아보고 x 가 도달가능한 상태일 때, x 의 직전자를 찾는 알고리즘은 표 5와 같다.

표 5. 도달가능 상태의 직전자를 찾는 알고리즘
Table. 5 Algorithm for computing predecessor of reachable state

INPUT : 규칙$[n]\{8\}$, 상태$[n]$, n.
OUTPUT1 : 도달불가능이면 1, 나머지는 0
OUTPUT2 : 도달가능한 상태의 직전자

Step1: 규칙$[1][j]=$ 상태$[1]$, $j=0,1,2,3$을 만족하는 x_1을 구한다.

If $x_1=\varnothing$ then OUTPUT1=1 END.

Step2: $i=2$ 에서 $n-1$ 까지
(a) $P_i=2k, 2k+1 \pmod 8 \mid k \in x_{i-1}$
(b) $R_i=\{j\}$, j는 다음을 만족한다.
규칙$[i][j]=$ 상태$[j]$, $j=0,1,\cdots,7$
(c) $x_i=P_i \cap R_i$
(d) If $x_i=\varnothing$ then OUTPUT1=1 END.

Step 3: (a) $P_n=2k, 2k+1 \pmod 8 \mid k \in x_{n-1}$
(b) $R_n=\{j\}$, j는 다음을 만족한다.
규칙$[i][j]=$ 상태$[j]$, $j=0,2,4,6$
(c) $x_n=P_n \cap R_n$을 구한다.
(d) If $x_n=\varnothing$ then OUTPUT1=1
else OUTPUT1=0 END.

Step 4: x_n에 대하여 다음을 구한다.
(a) $S_n=\{\left[\frac{a}{2}\right],\left[\frac{a+8}{2}\right] \mid a \in x_n\}$
(b) $y_{n-1}=S_n \cap x_{n-1}$
(c) $\left[\frac{y_{n-1}}{2}\right]$를 이진수 $n-1$과 n번째 셀에 채운다.

Step 5: $x_j, j=n-1$ 부터 2까지,
(a) $S_j=\{\left[\frac{a}{2}\right],\left[\frac{a+8}{2}\right] \mid a \in y_{n-1}\}$
(b) $y_{j-1}=S_j \cap x_{j-1}$
(c) If $y>4$
then ($n-j+1$번째 셀에 1을 채운다)
else ($n-j+1$번째 셀에 0을 채운다)

END.

V. 결 론

본 논문에서는 3-이웃 셀룰라 오토마타의 도달 가능/불가능한 상태를 판별하고 도달가능 상태에 대해서 직전자를 구하는 알고리즘을 제안하였다. 또한 도달가능 상태의 트리를 구성하여 CA가 그룹인지 비그룹인지를 판별하였다.

참고문헌

[1] S. Wolfram, O. Martin and A. M. Odlyzko, *Algebraic properties of cellular automata* Communications in Mathematical Physics, 3, pp. 219-258, 1984.

[2] K. Cattell and J. Muzio, *Analysis of one-dimensional linear hybrid cellular automata over $GF(q)$*, IEEE Transactions of Computers, Vol. 45(7), pp. 782-792, 1996.

[3] S.J. Cho, U.S. Choi, and H.D. Kim, *Analysis of complemented CA derived from a linear TPMACA*, Computers and Mathematics with Applications, Vol.45, pp. 689-698, 2003.

[4] S.J. Cho, U.S. Choi, Y.H. Hwang, H.D. Kim and Y.S. Pyo, *Analysis of state-transition of SACA over $GF(2^p)$*, J. Kor. Info. Security and Cryptology, Vol.15 , pp. 105-111, 2005.

[5] S.T. Kim, S.K. Lee, U.S. Choi and S.J. Cho, TPSACA를 이용한 완전 해싱 알고리즘, 한국해양정보통신학회, 제8권 제6호, pp. 1047-1054, 2004.

[6] S.J. Cho, S.T. Kim and U.S. Choi, Complemented CA derived from linear Two-Predecessor MACA, 한국해양정보통신학회, 제5권 제2호, pp. 365-370, 2001.

[7] S. Das, B. K. Sikdar and P. P. Chaudhuri, *Characterization of reachable/ nonreachable cellular automata states*, LNCS 3305, pp. 813-822, 2004.

저자소개

황 윤 희(Yoon-Hee Hwang)

2002년 2월 부경대학교 통계학과 학사
2004년 2월 부경대학교 응용수학과 석사
2006년 2월 부경대학교 정보보호학과 박사과정 수료
※ 관심분야 : 셀룰라 오토마타론, 정보보호, 유한체, 컴퓨터 구조론

최 언 숙(Un-Sook Choi)

1992년 2월 성균관대학교 산업공학과 학사
2000년 2월 부경대학교 응용수학과 석사
2004년 2월 부경대학교 응용수학과 박사
2004년 3월 ~ 2006년 2월 영산대학교 자유전공학부 단임교수
2006년 3월 ~ 현재 동명대학교 멀티미디어공학과 전임강사
※ 관심분야 : 셀룰라 오토마타론, 정보보호, 부호이론, 컴퓨터 구조론

권 숙 희(Suk-Hee Kwon)

1989년 2월 경북대학교 조경학과 학사
2005년 3월 ~ 부경대학교 응용수학과 석사 과정
※ 관심분야 : 셀룰라 오토마타론, 컴퓨터 구조론

김 경 자 (Kyung-Ja Kim)

약력
2005년 2월 : 방송통신대학교 경제학과 학사
2005년 3월 ~ : 부경대학교 응용수학과 석사 과정
※관심분야 : 셀룰라 오토마타론, 컴퓨터 구조론

김 한 두 (Han-Doo Kim)

1982년 2월 고려대학교 수학과 학사
1984년 2월 고려대학교 수학과 석사
1988년 2월 고려대학교 수학과 박사
1989년 ~ 현재 : 인제대학교 컴퓨터 응용과학부 정교수
※ 관심분야 : 전산수학, 셀룰라 오토마타론, 컴퓨터 구조론

조 성 진 (Sung-Jin Cho)

1979년 2월 강원대학교 수학교육과 학사
1981년 2월 고려대학교 수학과 석사
1988년 2월 고려대학교 수학과 박사
1988년 ~ 현재 부경대학교 수리과학부 정교수
※ 관심분야 : 셀룰라 오토마타론, 정보보호, 부호이론, 컴퓨터 구조론