계층적 셀룰라 오토마타의 특성에 관한 연구

최언숙* · 조성진** · 최향희***

Characterization of Hierarchical Cellular Automata

U.S. Choi* · S.J. Cho** · H.H. Choi***

이 논문은 2006학년도 부경대학교 기성회 학술연구비에 의하여 연구되었음(PK-2006-020)

요 약

셀룰라 오토마타는 오랫동안 모델링과 컴퓨팅 패러다임에 사용되어왔다. 또한 셀룰라 오토마타는 많은 물리계를 모델링하는데 사용되어왔다. 그러한 시스템의 모델을 연구함에 있어서 물리계의 복잡성이 증가하여 셀룰라 오타마타를 이용한 모델은 매우 복잡하고 분석적으로 추적하기가 어렵게 되었다. 또한 그러한 모델들은 물리계의 내재적 계층적 성질의 나타남을 인식할 수 없다. 본 논문에서는 이러한 문제점의 해결의 대안으로 등장한 계층적 셀룰라 오토마타의 특성을 논한다. 특히 전이규칙, 특성다항식과 사이클 구조를 분석한다.

ABSTRACT

Cellular Automata(CA) has been used as modeling and computing paradigm for a long time. And CA has been used to model many physical systems. While studying the models of such systems, it is seen that as the complexity of the physical system increase, the CA based model becomes very complex and becomes to difficult to track analytically. Also such models fail to recognize the presence of inherent hierarchical nature of a physical system. In this paper we give the characterization of Hierarchical Cellular Automata(HCA). Especially we analyze transition rules, characteristic polynomials and cyclic structures of HCA.

키워드

셀룰라 오토마타, HCA, 전이규칙, 상태전이행렬, 주기, 최소다항식, 사이클구조

Ⅰ. 서 론

셀룰라 오토마타(이하, CA)는 셀이라 불리는 간단한 메모리의 배열로서 각 셀들의 상태가 국소적인 상호작용에 의해서 동시에 갱신되는 시스템이다. CA는 간단하고, 규칙적이며 작은 단위로 확장연결이 가능하여 전용의 하드웨어를 사용하지 않고 실행 가능하도록 프로그램화 될 수 있다. CA는 많은 물리계를 모델링하는데 사용되어왔다. 그러한 시스템의 모델을 연구함에 있어서 물리계의 복잡성이 증가하여 CA를 이용한 모델이 매우 복잡하고 분석적으로 추적하기가 어렵게 되었다. 또한 그러한 모델들은 물리계의 내재적 계층적 성질의 나타

* 동명대학교 멀티미디어공학과
** 부경대학교 수리과학부(교신저자)
*** 부경대학교 응용수학과

접수일자 : 2007. 7. 30

남을 인식할 수 없다. 이러한 문제점을 해결하기 위하여 계층적 셀룰라 오토마타(Hierarchical Cellular Automata, 이하 HCA)에 관한 연구를 하기 시작하였다. [1-3] 그러나 HCA의 분석이 어려워 HCA의 특성들이 많이 연구되지 않았으며 또한 HCA 생성방법은 아직까지 연구되지 않고 있다. 1996년에 Cattell과 Muzio[4]는 90/150 CA생성 알고리즘을 제시하였다. 그런데 이 알고리즘에 의하여 90/150 CA를 구함에 있어 요구되는 계산량은 $O(n^7)$으 되어 이 알고리즘은 비효율적이다. 이다. 2007년에 Cho[5] 등은 이 문제점을 보완하여 효과적으로 90/150 CA를 생성하는 알고리즘을 제안하였다. 이 알고리즘에 요구되는 계산량은 $O(n^2)$ 이다. 본 논문에서는 이 연구 결과를 바탕으로 HCA를 생성하기 위하여 HCA의 전이 규칙과 특성다항식, 사이클 구조에 대해 분석한다.

Ⅱ. GF(2^p) Cellular Automata

GF(2) CA는 한 개의 셀이 가질 수 있는 상태는 0, 1로 2개이다. 반면 GF(2^p) CA는 그림 1에서와 같이 p개의 기억소자가 한 개의 셀을 이루기 때문에 하나의 셀이 가질 수 있는 상태는 2^p 개로 {0, 1, 2, ⋯, 2^p-1}의 원소이다. 그림 2는 일반적인 GF(2^p) CA의 구조이다.

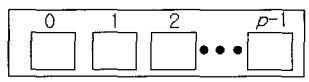

그림 1. $GF(2^p)$ CA의 셀 구조
Fig. 1. Structure of $GF(2^p)$ CA cell

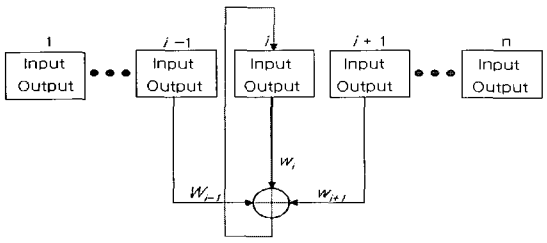

그림 2. $GF(2^p)$ CA의 구조
Fig. 2. Structure of $GF(2^p)$ CA

주어진 i 번 째 셀의 다음 상태는 자신과 이웃하는 두 개의 셀의 상태에 따라 결정되는데 GF(2) CA와 달리 셀의 각 상태에 가중치를 곱한후 XOR하여 다음 상태로 갱신된다. 이러한 CA를 선형 GF(2^p) HCA라 한다[6]. 선형 GF(2^p) HCA의 다음 상태를 전이시키는 상태전이함수를 정의하기 위해 먼저 한 개의 셀이 가지는 2^p개의 상태를 생성해야 한다. 이를 위해 GF(2)의 확장체인 GF(2^p)를 생성하는 다항식을 생성다항식이라 하고 이 생성다항식을 특성다항식으로 갖는 삼중 대각행렬을 생성행렬이라 한다[6].

다음으로 GF(2^p) CA의 다음 상태를 결정하는 상태전이함수는 다음과 같다.

$$q_i(t+1) = \phi\,(w_{i-1}q_{i-1}(t),\ w_iq_i(t),\ w_{i+1}q_{i+1}(t))$$

여기서 $q_i(t)$ 는 시간 t에서 i 번 째 셀의 상태를 나타내며 w_i 는 가중치를 나타낸다. 선형 GF(2^p) CA의 상태전이행렬은 다음과 같은 삼중대각행렬로 이루어진다.

이때 w_{ij}는 j번째 셀의 현재상태가 i번째 셀의 다음 상태에 영향을 주는 정도를 나타내는 가중치이며 GF(2^p)의 원소이다.

$$T=\begin{pmatrix} w_{11} & w_{12} & 0 & \cdots & 0 \\ w_{21} & w_{22} & w_{23} & \cdots & 0 \\ 0 & w_{32} & w_{33} & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & w_{nn} \end{pmatrix} \tag{1}$$

예를 들어 3셀 GF(2^2) CA의 상태전이행렬이 다음과 같다고 하자.

$$T=\begin{pmatrix} 0 & \alpha & 0 \\ \alpha & 0 & \alpha \\ 0 & \alpha^2 & 1 \end{pmatrix} \tag{2}$$

여기서 α는 GF(2^2)를 생성하는 생성자이다. 따라서 GF(2^2)의 원소는 $0,\ 1,\ \alpha,\ \alpha^2$ 이다. 여기서 α는 생성다항식 $g(x) = x^2 + x + 1$ 의 해이며, 생성행렬 M은 다음과 같다.

$$M=\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

n셀 GF(2^p) CA의 현재 상태 x에 대하여 다음 상태 y는 $y = Tx$이다. GF(2^p) HCA의 상태 x는 n개의 GF(2^p)

의 원소인 α^i 로 이루어진 벡터로 표현된다. 유한체 위에서 곱셈과 덧셈을 위해 α^i 와 M^i 의 마지막 열벡터를 대응시킨다. 위 예에서 생성행렬의 M^i 에 대응하는 α^i 는 α=<10>=2, α^2 =<11>=3, α^3=1=<01>=1, 0=<00>=0이다.

따라서 GF(2^2)위에서 덧셈과 곱셈은 표 1과 같다.

표 1. GF(2^2) 위에서의 곱셈과 덧셈
Table 1. Multiplication and addition over GF(2^2)

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

GF(2^p) HCA의 상태전이행렬이 식 (1)과 같을 때, 특성다항식 $\Delta(x)$ 는 $\Delta(x)=|T+xI|$ 이다. 위의 예에서 식 (2)의 상태전이행렬 T의 특성다항식은 x^3+x^2+2x+3 이다.

유한체 GF(2^2)위에서 다항식 x^3+x^2+2x+3 은 원시다항식으로 주기가 63이다. 이와 같이 GF(2^p) HCA는 GF(2) CA와 비교하여 같은 차수의 원시다항식에 대하여 훨씬 주기가 길어지므로 아주 유용하다. 또한 차수가 같은 다항식에 대하여 원시다항식도 더 많이 존재하기 때문에 다양하게 응용할 수 있다. 예를 들어 GF(2) 위에서 3차 다항식은 x^3+x+1 , x^3+x^2+1 로 2개 존재하지만 GF(2^2) 위세서의 원시다항식은 모두 12개로 다음과 같다.

x^3+x^2+x+2 , x^3+3x^2+3x+3 , x^3+x^2+3x+2,
x^3+2x^2+3x+3 , x^3+x^2+2x+3, x^3+3x^2+2x+2,
x^3+x^2+x+3, x^3+2x^2+2x+2, x^3+2x^2+3x+2,
x^3+2x^2+x+3 , x^3+3x^2+x+2, x^3+3x^2+2x+3

GF(2^p)위에서 n차 원시다항식의 개수는 $\phi(2^{np}-1)/n$ 이다. $p=2$, $n=3$ 인 경우에 대하여 원시다항식의 개수는 $\phi(2^{3\cdot 2}-1)/3=12$ 이다. 본 논문에서는 GF(2^p) HCA의 특성다항식에 관하여 분석하고 전이규칙과 특성다항식에 관한 성질들을 분석한다. 또한 그룹 GF(2^p) HCA의 사이클 구조에 대하여 특성화한다.

Ⅲ. 그룹 HCA의 전이규칙과 사이클 구조

GF(2) 위에서의 uniform CA를 GF(2^p)로 확장한 uniform HCA는 각 셀에 대하여 왼쪽이웃에 대한 가중치가 모두 같고 오른 쪽 이웃에 대한 가중치가 모두 같다. 즉 각 셀의 3-이웃에 대한 가중치를 $<\alpha_l, \alpha_s, \alpha_r>$라 하면 식 (1)의 상태전이행렬은 다음과 같다.

$$T=\begin{pmatrix} \alpha_s & \alpha_r & 0 & \cdots & 0 \\ \alpha_l & \alpha_s & \alpha_r & \cdots & 0 \\ 0 & \alpha_l & \alpha_s & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \alpha_s \end{pmatrix}$$

여기서 α_l 은 셀의 왼쪽이웃에 대한 가중치를 나타내고 α_s는 자기 자신에 대한 가중치, α_r은 오른쪽 이웃에 대한 가중치를 나타낸다. 이러한 uniform HCA는 적용하는 전이규칙에 따라 그룹 HCA 또는 비그룹 HCA가 되기도 한다. 그룹 HCA는 상태전이행렬의 행렬식이 0이 아니고 임의의 상태에 대한 이전 상태가 유일하다. 그러나 비그룹 HCA는 상태전이행렬의 행렬식이 0이고, 임의의 상태에 대한 이전 상태가 유일하지 않고 상태전이 그래프는 트리모양이 된다.

<정리 1> 전이규칙이 다음과 같은 n셀 uniform HCA는 다음을 만족한다. 여기서 일반적인 α_i 는 0이 아니다.

(1)$<\alpha_l, \alpha_s, \alpha_r>$가 $<0, \alpha_s, 0>$,$<0, \alpha_s, \alpha_r>$ 또는 $<\alpha_l, \alpha_s, 0>$ 인 모든 크기의 HCA는 그룹이다.

(2) ${\alpha_s}^2=\alpha_l\alpha_r$ 을 만족하며 셀의 크기 n에 대하여 $n \bmod 3 \neq 2$ 인 HCA는 그룹이고 $n \bmod 3 = 2$ 인 HCA는 비그룹이다.

(3) $<\alpha_l, \alpha_s, \alpha_r>$가 $<\alpha_l, 0, \alpha_r>$이고 셀의 수가 짝수인 HCA는 그룹이다.

<증명> (1) $<\alpha_l, \alpha_s, \alpha_r>$가 $<0, \alpha_s, 0>$인 상태전이행렬은 대각성분이 α_s 이고 나머지 성분은 0인 대각행렬이고 $<0, \alpha_s, \alpha_r>$인 경우의 상태전이행렬은 상삼각행렬이며 $<\alpha_l, \alpha_s, 0>$인 경우는 하삼각행렬로 상태전이행렬의 행렬식은 모두 α_s^n이다. 그러므로 주어진 uniform HCA는 그룹이다.

(2) 주어진 규칙을 갖는 n셀 uniform HCA의 상태전이행렬을 $T_{R,n}$ 이라 하자. $T_{R,n}$ 의 행렬식에 대하여 다음

과 같은 점화식이 성립한다.

$$|T_{R,n}| = \alpha_s |T_{R,n-1}| + \alpha_l \alpha_r |T_{R,n-2}| \quad (3)$$

여기서 $T_{R,n-1}$ 은 상태전이행렬 $T_{R,n}$ 에서 n 행과 n 열을 제거한 부분행렬이다. 이를 이용하여 주어진 정리를 수학적 귀납법으로 증명할 수 있다.

$n=1$ 일 때 $|T_{R,1}| = \alpha_s \neq 0$이다. $n=2$일 때 $|T_{R,2}| = \begin{vmatrix} \alpha_s & \alpha_r \\ \alpha_l & \alpha_s \end{vmatrix} = \alpha_s^2 + \alpha_l \alpha_r$ 이고 가정에 의해 0이다. $n=3$ 일 때

$$|T_{R,3}| = \begin{vmatrix} \alpha_s & \alpha_r & 0 \\ \alpha_l & \alpha_s & \alpha_r \\ 0 & \alpha_l & \alpha_s \end{vmatrix} = \alpha_s |T_{R,2}| + \alpha_l \alpha_r |T_{R,1}| = \alpha_l \alpha_s \alpha_r$$

$m=3p$ 또는 $m=3p+1$ 에 대하여 $|T_{R,m}| \neq 0$이고 $m=3p+2$ 에 대하여 $|T_{R,m}| = 0$이라 할 때,

$|T_{R,m+1}|$에 대하여

i) $|T_{R,3(p+1)}| = |T_{R,3p+3}|$
$= \alpha_s |T_{R,3p+2}| + \alpha_l \alpha_r |T_{R,3p+1}|$
$= \alpha_l \alpha_r |T_{R,3p+1}| \neq 0$

ii) $|T_{R,3(p+1)+1}| = |T_{R,3p+4}|$
$= \alpha_s |T_{R,3p+3}| + \alpha_l \alpha_r |T_{R,3p+2}|$
$= \alpha_s |T_{R,3p+3}| \neq 0$

iii) $|T_{R,3(p+1)+2}| = |T_{R,3p+5}|$
$= \alpha_s |T_{R,3p+4}| + \alpha_l \alpha_r |T_{R,3p+3}|$
$= \alpha_s^2 |T_{R,3p+3}| + \alpha_l \alpha_r |T_{R,3p+3}|$
$= |T_{R,3p+3}| (\alpha_s^2 + \alpha_l \alpha_r) = 0$

그러므로 $n \bmod 3 \neq 2$ 인 HCA는 그룹이고 $n \bmod 3 = 2$ 인 HCA는 비그룹이다.

(3) i) $n=2m+1$ 인 경우, $|T_{R,1}| = \alpha_s = 0$ 이므로

$|T_{R,2m+1}| = \alpha_l \alpha_r |T_{R,2m-1}| = (\alpha_l \alpha_r)^2 |T_{R,2m-3}|$
$= \cdots = (\alpha_l \alpha_r)^{m-1} |T_{R,3}| = (\alpha_l \alpha_r)^m |T_{R,1}| = 0$

이고, ii) $n=2m$ 인 경우,

$|T_{R,2}| = \begin{vmatrix} 0 & \alpha_r \\ \alpha_l & 0 \end{vmatrix} = \alpha_l \alpha_r (\neq 0)$ 이므로

$|T_{R,2m}| = \alpha_l \alpha_r |T_{R,2m-2}| = (\alpha_l \alpha_r)^2 |T_{R,2m-4}|$
$= \cdots = (\alpha_l \alpha_r)^{m-1} |T_{R,2}| = (\alpha_l \alpha_r)^m \ (\neq 0)$

이다. 그러므로 $|T_{R,n}|$은 다음과 같다.

$$|T_{R,n}| = \begin{cases} (\alpha_l \alpha_r)^{\frac{n}{2}} & , \ n : even \\ 0 & , \ n : odd \end{cases}$$

주어진 GF(2^p) HCA의 각 셀에 적용되는 전이규칙이 2가지 이상인 CA를 hybrid HCA라 한다. 다음 정리는 특정한 전이규칙이 교대로 사용되는 hybrid HCA에 대한 특성이다.

<정리 2> n셀 GF(2^p) HCA의 각 셀에 적용되는 전이규칙 R_1, R_2 가 다음과 같다고 하자.

$$R_1 = \begin{cases} < \alpha_l, 0, \alpha_r > & , \text{홀수번 째 셀의 규칙} \\ < \alpha_l, \alpha_s, \alpha_r > & , \text{짝수번 째 셀의 규칙} \end{cases}$$

$$R_2 = \begin{cases} < \alpha_l, \alpha_s, \alpha_r > & , \text{홀수번 째 셀의 규칙} \\ < \alpha_l, 0, \alpha_r > & , \text{짝수번 째 셀의 규칙} \end{cases}$$

그러면 다음이 성립한다.

$$|T_{R_1,n}| = \begin{cases} (\alpha_l \alpha_r)^{\frac{n}{2}} & , \ n : even \\ 0 & , \ n : odd \end{cases}$$

$$|T_{R_2,n}| = \begin{cases} (\alpha_l \alpha_r)^{\frac{n}{2}} & , \ n : even \\ \alpha_s (\alpha_l \alpha_r)^{\frac{n-1}{2}} & , \ n \bmod 4 = 1 \\ 0 & , \ o/w \end{cases}$$

<증명> $T_{R,(k,n)}$ 을 $T_{R,n}$ 에서 1행부터 $k-1$행까지, 1열부터 $k-1$열까지 제거한 부분행렬이라 하자. 예를 들어 $T_{R,(2,n)}$ 은 $T_{R,n}$ 에서 1행과 1열을 제거한 부분행렬이다. i) $n=2m$인 경우 전이규칙 R_1, R_2 에 대하여 $|T_{R_1,n}| = 0 \cdot |T_{R,(2,n)}| + \alpha_l \alpha_r |T_{R,(3,n)}| = \alpha_l \alpha_r |T_{R,(3,n)}|$이다. 이를 반복 적용하면 $|T_{R_1,n}| = (\alpha_l \alpha_r)^m$ 이다. 또한 R_2 에 대하여 $|T_{R_1,n}| = \alpha_l \alpha_r |T_{R,n-2}|$이므로 반복하여 적용하면 $|T_{R_1,n}| = (\alpha_l \alpha_r)^m$이다. ii) $n=2m+1$ 일 때, 전이규칙 R_1 에 대하여

$|T_{R_1,2m+1}| = \alpha_l \alpha_r |T_{R_1,2m-1}| = (\alpha_l \alpha_r)^2 |T_{R_1,2m-3}|$
$= \cdots = (\alpha_l \alpha_r)^m |T_{R_1,1}| = (\alpha_l \alpha_r)^m \cdot 0 = 0$

이다. iii) 전이규칙 R_2 에 대하여

$|T_{R_2,n}| = \alpha_s |T_{R,(2,n)}| + \alpha_l \alpha_r |T_{R,(3,n)}|$
$= \alpha_s (0 \cdot |T_{R,(2,n)}| + \alpha_l \alpha_r |T_{R,(3,n)}|$
$+ \alpha_l \alpha_r (\alpha_s \cdot |T_{R,(3,n)}| + \alpha_l \alpha_r |T_{R,(4,n)}|)$
$= (\alpha_l \alpha_r)^2 |T_{R,(4,n)}|$

이므로 $n=4m+1$ 인 경우는 $|T_{R_2,4m+1}| = (\alpha_l \alpha_r)^{2m} \alpha_s$

이고, $n=4m+3$ 인 경우는

$|T_{R_2,4m+3}| = (\alpha_l \alpha_r)^{2m} |T_{R_2,(4m+1,4m+3)}| = 0$이다.

그러므로 셀의 수가 짝수이고 전이규칙 R_1 또는 R_2

를 갖는 hybrid HCA는 그룹이고, 셀의 수가 $n=4m+1$ 이고 전이규칙 R_2 를 갖는 hybrid HCA는 그룹이다.

선형 n셀 GF(2^p) HCA가 그룹인지 비그룹인지를 알 수 있는 방법은 상태전이행렬이 정칙여부에 따라 결정된다. 그러나 이 HCA의 상태전이 행동을 구체적으로 알기에는 부족하다. 본 논문에서는 HCA의 구체적인 상태전이행동을 분석하기 위해서 상태전이행렬의 특성다항식을 이용한다. 그룹 HCA의 상태전이는 임의의 상태에 대한 이전상태가 유일하게 결정되지만, 비그룹 HCA는 그렇지 못하다. HCA의 특성다항식의 인수 $f(x)$ 중 $f(T)=0$ 을 만족하는 최소차수의 다항식을 GF(2^p) HCA의 최소다항식 ($m(x)$)이라 한다. $m(x)=x^d\phi(x)$ 일 때, $d>0$이면 HCA는 비그룹이고 $d=0$이면 HCA는 그룹이다. d는 상태전이그래프에서 트리의 깊이를 결정하며 임의의 도달불가능한 상태에서 가장 가까운 상태에 도달하는데 걸리는 시간이다. $\phi(x)$는 HCA의 사이클 구조를 결정한다[7]. $\phi(x)$는 다음과 같은 형태를 이룬다.

$$\phi(x)=[f_1(x)]^{r_1}[f_2(x)]^{r_2}\cdots[f_h(x)]^{r_h}$$

Elspas는 [7]에서 GF(2)위에서의 사이클 구조를 분석하였는데 이러한 결과는 GF(2^p)에서도 자연스럽게 확장가능하다. GF(2^p) HCA의 사이클 구조를 분석을 위하여 다음과 같은 경우로 간단히 하여 분석한다.

i) $\phi(x)=f(x)$ ($f(x)$:기약다항식)

$f(x)$ 의 주기는 $k=\min\{l:\ f(x)|x^l+1\}$ 이고, 이 경우 사이클 구조는 $[1(1),\mu_1(k)]$ 이다. $\mu_i(k_i)$ 에서 μ_i는 주기가 k_i인 사이클의 개수를 의미한다. $\mu_1=2^{np}-1/k$ 이다.

ii) $\phi(x)=[f(x)]^r$ ($f(x)$:기약다항식)

$2^{r_1-1}<r\le 2^{r_1}$이고, $f(x)$ 의 주기가 k 이면 주어진 HCA의 사이클의 길이는 $1, k, 2k, 2^2k,\cdots,2^{r_1}k$ 가 존재하고 사이클의 구조는 $[1(1), \mu_1(k), \mu_2(2k), \mu_3(2^2k), \cdots, \mu_{r_1+1}(2^{r_1}k)]$ 이다. $U_i:=\{x|[f(T)]^i x=0\}$ 라 하자. $x\in U_2-U_1$ 이면, $[f(T)]^2x=0$ 이지만 $f(T)x\neq 0$ 이다. 이러한 상태 x는 $[f(x)]^2$ 의 주기를 갖는 사이클에 속한다. 따라서 $\mu_i=n(U_{i-1}-U_{i-2})/(2^{i-1}k)$ 이다. 여기서 $n(A)$ 는 집합 A 의 원소의 개수를 나타낸다.

예를 들어 6셀 GF(2^2) HCA의 최소다항식이 $(x^2+x+2)^3$ 라 하자. GF(2^2)위에서 x^2+x+2는 원시다항식이므로 $x^2+x+2|x^{2^2\cdot 2}-1+1(=x^{15}+1)$이다. 또 $2<3\le 2^2$이므로 존재하는 모든 사이클의 길이는 1, 15, 2×15, 2^2×15 즉, 1, 15, 30, 60이다. 각 사이클 길이에 해당하는 사이클 개수를 구하면 먼저 1은 상태 0을 포함은 사이클 1개를 나타낸다. 길이가 15인 사이클의 수는 $(2^2)^2-1/15=1$ 이고, 길이가 30인 사이클의 수는 $(2^2)^4-(2^2)^2/30=8$ 이다. 마지막으로 길이가 60인 사이클의 수는 $(2^2)^6-(2^2)^4/60=64$ 이다.

iii) $\phi(x)=f(x)g(x)$ ($f(x)$, $g(x)$:기약다항식)

$f(x)$, $g(x)$의 차수를 d_1, d_2 라 하고, 주기를 각각 k_1, k_2 라 하자. 그러면 $f(x)$ 에 의해 생성되는 사이클은 [1(1),$\mu_1(k_1)$]이고 $g(x)$ 에 의해 생성되는 사이클은 [1(1),$\mu_2(k_2)$]이다. 따라서 $f(x)g(x)$ 에 의해 생성되는 사이클의 구조는 [1(1),$\mu_1(k_1)$][1(1),$\mu_2(k_2)$]=[1(1), $\mu_1(k_1)$, $\mu_2(k_2)$, $\mu(k)$]이다. 여기서 $\mu=\mu_1\mu_2\gcd(k_1,k_2)$ 이고 $k=lcm(k_1,k_2)$ 이다.

<예제 1> 5셀 GF(2^2) HCA의 최소다항식이 $m(x)=(x+3)(x+2)^4$이라 할 때, 사이클 구조를 분석하면 [1(1), 1(3)][1(1), 1(3), 2(6), 20(12)]=[1(1), 5(3), 8(6), 80(12)]이다.

Ⅳ. HCA의 특성다항식

GF(2^p) HCA의 상태전이행렬에서 오른쪽 이웃과 왼쪽 이웃에 대한 가중치를 동일하게 두는 것은 GF(2) 위에서의 90/150 CA에 대한 자연스러운 확장이다. 따라서 가중치를 동일하게 두었을 때 상태전이행렬은 다음과 같다.

$$T=\begin{pmatrix} d_1 & i & 0 & \cdots & 0\\ i & d_2 & i & \cdots & 0\\ 0 & i & d_3 & \cdots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 0 & 0 & 0 & \cdots & d_n \end{pmatrix}$$

여기서 i 는 가중치로 $\{0, 1, 2, \cdots, 2^p-1\}$ 의 원소이다. 주어진 전이행렬을 $T=<d_1, d_2, \cdots, d_n>_i$ 로 나타내기로 하고 이를 전이규칙이라 하자. 다음 정리는 n셀 GF(2^p) HCA의 특성다항식에 관한 점화식으로 n셀

GF(2^p) HCA의 전이규칙을 찾을 수 있음을 보이는 정리로 수학적 귀납법으로 간단히 증명할 수 있다.

<정리 3> n셀 GF(2^p) HCA의 전이규칙이 $< d_1, d_2, \cdots, d_n >_i$ 이고 특성다항식이 Δ_n 이라 하면 다음 점화식을 만족한다.

$$\Delta_k = (x + d_k)\,\Delta_{k-1} + i^2\,\Delta_{k-2} \quad , (k > 0)$$
$$\Delta_{-1} = 0 \ , \ \Delta_0 = 1$$

n셀 GF(2^p) HCA의 특성다항식의 점화관계식 $\Delta_k = (x + d_k)\,\Delta_{k-1} + i^2\,\Delta_{k-2}$ 에서 Δ_k 를 피제수, Δ_{k-1}을 제수, $x + d_k$ 를 몫, Δ_{k-2}를 나머지라 하면 이 식은 유클리드 호제법을 만족한다. 즉, Δ_k 와 Δ_{k-1}가 $x + d_k$ 와 Δ_{k-2}을 유일하게 결정한다. 여기서 중요한 것은 몫이 항상 일차이어야 한다. Δ_n 과 Δ_{n-1} 을 알고 있다고 가정하면 유클리드 호제법에 의하여 $x + d_n$과 Δ_{n-2}가 유일하게 결정될 것이다. 다시 Δ_{n-1} 과 Δ_{n-2}에 호제법을 적용하면 $x + d_{n-1}$과 Δ_{n-3}을 계산할 수 있다. 유클리드 호제법의 반복적 적용은 CA의 특성다항식 계산의 역과 같다. 다시 말하면 유클리드 호제법을 이용하여 특성다항식으로부터 n셀 GF(2^p) HCA의 전이규칙을 찾을 수 있다. 다음은 Δ_n 과 Δ_{n-1}을 알고 있을 때 유클리드 호제법을 이용하여 그 주어진 다항식을 특성다항식으로 갖는 GF(2^2) HCA의 전이규칙을 찾는 예이다.

GF(2) 위에서 n차 원시다항식을 특성다항식으로 갖는 GF(2) 90/150 CA는 Δ_{n-1}이 유일하게 존재한다[4]. 이와 달리 GF(2^p)위에서 n차 원시다항식을 특성다항식으로 갖는 n셀 GF(2^p) HCA는 위의 예제처럼 여러 개 존재한다. 또 $x^3 + 2x^2 + 3x + 2$ 에 대응하는 GF(2^2) HCA 규칙은 $<1,0,3>_1$, $<0,1,3>_2$, $<0,3,1>_3$ 도 있지만, 각 셀의 이웃에 대하여 가중치가 다른 HCA도 존재한다. 예를 들어 상태전이 행렬이 $T=\begin{pmatrix}0&1&0\\1&0&2\\0&1&2\end{pmatrix}$인 HCA의 특성다항식도 $x^3 + 2x^2 + 3x + 2$ 이다. 그러나 이것은 GF(2) 입장에서 볼 때 90/150 CA가 아닌 경우이므로 이러한 경우에 대하여는 배제하기로 한다.

정리1에 의하여 Δ_n 과 Δ_{n-1}을 알 때 HCA의 전이규칙을 찾을 수 있음을 보였으나 Δ_{n-1}을 찾을 수 있는 방법이 매우 어렵다. 따라서 주어진 다항식에 대한 동반행렬과 HCA의 상태전이행렬이 닮음이라는 사실로부터 다음과 같은 성질을 얻을 수 있다.

<정리 4> 원시다항식 $p(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ 를 특성다항식으로 갖는 n셀 GF(2^p) HCA의 상태전이행렬이 $T = < d_1, d_2, \cdots, d_n >_i$ 이고, 정칙 상삼각행렬 U와 주어진 $p(x)$에 대한 동반행렬 C가 다음과 같다고 하자.

$$U=(u_{ij})=\begin{cases}u_i & , \ i=j\\ a_i & , \ i=j-1\\ 0 & , \ i>j\\ x_{ij}(\in GF(2^p)) & , \ o/w\end{cases}$$

$$C=(s_{ij})=\begin{cases}1 & , \ i=j+1 \ (j<n)\\ c_{i-1} & , \ j=n\\ 0 & , \ o/w\end{cases}$$

여기서 c_i 는 $p(x)$ 의 계수이다. 그러면 다음이 성립한다.

$$\begin{cases}d_1 = u^{-1}a_1\\ d_k = u_{k-1}^{-1}a_{k-1} + u_k^{-1}a_k \quad (1<k<n)\\ d_n = u_{n-1}^{-1}a_{n-1} + c_{n-1}\end{cases} \tag{4}$$

<증명> 주어진 T와 C가 같은 특성다항식을 가지므로 두 행렬은 닮은 행렬이다. 따라서 $TU = UC$라 두고 풀면 다음의 결과를 얻는다.

$$a_1 = u_1 d_1$$
$$a_k = i\,a_{k-1} + u_k d_k \ (1<k<n)$$
$$c_{n-1}u_n = i\,a_{n-1} + u_n d_n$$
$$u_k = i u_{k-1} \quad \cdots\cdots (5)$$

식 (5)로부터 $i = u_{k-1}^{-1}u_k$ 를 대입하면 위와 같은 점화관계식이 성립한다.

<예제 2> T=<1,3,3>$_2$ 일 때 U를 구해보자.

T의 특성다항식은 $x^3 + x^2 + 2x + 3$ 이므로 동반행렬은 $C=\begin{pmatrix}0&0&3\\1&0&2\\0&1&1\end{pmatrix}$이다. $i=2$ 이므로 $U=\begin{pmatrix}u_1&a_1&*\\0&2u_1&a_2\\0&0&3u_1\end{pmatrix}$ 이므로 $TU = UC$를 풀면 U는 다음과 같다.

$$U=\begin{pmatrix}u_1&u_1&2u_1\\0&2u_1&3u_1\\0&0&3u_1\end{pmatrix}=u_1\begin{pmatrix}1&1&2\\0&2&3\\0&0&3\end{pmatrix}, \ u_1(\neq 0)\in GF(2^2)$$

그러므로 가능한 U는 다음과 같다.

$$U_1=\begin{pmatrix}1&1&2\\0&2&3\\0&0&3\end{pmatrix},\ U_2=\begin{pmatrix}2&2&3\\0&3&1\\0&0&1\end{pmatrix},\ U_3=\begin{pmatrix}3&3&1\\0&1&2\\0&0&2\end{pmatrix}$$

식 (4)에 의하여 상태전이행렬 T의 대각성분을 다음과 같이 구한다.

$$d_1=1\cdot 1=1, d_2=1+2^{-1}\cdot 3=3, d_3=2+1=3$$

V. 결론 및 향후 연구방향

본 논문에서는 비트단위에서 처리하는 GF(2) 위에서의 CA보다 복잡한 시스템을 모델링 하기에 적합한 GF(2^p) HCA에 대하여 분석하였다. 특별히 그룹 HCA가 되는 여러 가지 전이규칙들을 제시하였고, 최소다항식의 형태에 따른 HCA의 상태전이행동을 분석하였다. 또한 90/150 CA의 자연스런 확장인 GF(2^p) HCA의 특성다항식에 관하여 여러 가지 성질들을 밝혔다. 이러한 연구결과를 바탕으로 향후 HCA를 생성하는 알고리즘을 개발하고자 한다.

참고문헌

[1] B.K. Sikdar, P. Majumder, M. Mukherjee, N. Ganguly, D.K. Das and P.P. Chaudhuri, "Hierarchical Cellular Automata As An On-Chip Test Pattern Generator", VLSI Design, Fourteenth International Conference on 2001, pp. 403-408, 2001.

[2] B.K. Sikdar, N. Ganguly, P. Majumder, P.P. Chaudhuri, "Design of Multiple Attractor GF(2^p) Cellular Automata for Diagnosis of VLSI Circuits", VLSI Design, Fourteenth International Conference on 2001, pp. 454-459, 2001.

[3] S.J. Cho, U.S. Choi Y.H. Hwang, H.D. Kim, and H.H. Choi, "Behaviors of Single Attractor Cellular Automata over Galois Field GF(2^p)" LNCS 4173, pp. 232-237, 2006.

[4] K. Cattell and J. Muzio, "Synthesis of One-Dimensional Linear Hybrid Cellular Automata", IEEE Transactions on Comptuer-Aided Design of Integrated Circuits and Systems, Vol. 15(3), pp. 325-335, 1996.

[5] S.J. Cho, U.S. Choi Y.H. Hwang, H.D. Kim, J.G Kim and S.H Heo, "New Synthesis of One-Dimensional 90/150 Linear Hybrid Group Cellular Automata", IEEE Transactions on Comptuer-Aided Design of Integrated Circuits and Systems, Vol. 26(9), pp. 1720-1724, 2007.

[6] B.K. Sikdar, N. Ganguly, P. Majumder and P.P. Chaudhuri, "Design of multiple attractor GF(2p) cellular utomata for diagnosis of VLSI circuits, VLSI Design", Fourteenth International Conference on 2001, pp. 454 - .459, 2001.

[7] B. Elspas, "The Theory of Autonomous Linear Sequential Networks", TRE Trans. on Circuit, CT-6, pp.45-60, 1959.

저자소개

최 언 숙 (Un-Sook Choi)

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

조 성 진 (Sung-Jin Cho)

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

최 향 희 (Hyang-Hee Choi)

1985년 부산대학교 수학교육과 학사
2002년 부경대학교 교육대학원 수학과 석사
2008년 부경대학교 응용수학과 박사
※관심분야 : 셀룰라 오토마타론