여원벡터에 의해 유도된 여원 그룹 셀룰라 오토마타에 관한 연구†

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

Complemented Group Cellular Automata derived from Complement Vectors

Sung-Jin Cho*, Yoon-Hee Hwang**, Un-Sook Choi***, Yong-Soo Pyo*
*Division of Mathematical Sciences, Pukyong National University
**Department of Information Security, Graduate School, Pukyong National University
***University College of Undeclared Majors, Youngsan University

요 약

셀룰라 오토마타(Cellular Automata, 이하 CA)는 LFSR의 대안으로 제안되었으나 일반화와 분석이 어려워 거의 이뤄지지 않고 있다. 본 논문에서는 특별한 전이규칙을 가지는 그룹 CA에서 각각의 여원벡터에 대응하여 유도되는 여원 그룹 CA의 구조를 분석한다. 여기서 분석하는 그룹 여원 CA는 전체 상태가 그룹 CA의 최대 주기나 그것의 2배가 되는 같은 길이의 사이클들로 분리된다. 이러한 성질은 암호학에서 키 공유 프로토콜에 유용한 성질로 사용될 수 있다.

1. 서론

오늘날 데이터 통신의 성장과 함께 보안과 개인정보 보호에 대한 필요성이 대두되고 있다. 특히 무선 통신의 출현과 PDA, 스마트 카드와 같은 휴대용 장치가 등장하면서 휴대용 장치에 암호학의 적용이 주요 관심사가 되고 있다. 현대 암호에서 중요하게 여겨지고 있는 것 중 하나는 암호화와 복호화를 공유할 수 있는 하드웨어를 구현하는 것이다. 셀룰라 오토마타(Cellular Automata, 이하 CA)는 전용의 하드웨어를 사용하지 않고 실행하도록 프로그램될 수 있어 이에 이용될 수 있다. CA는 Von Neumann에 의하여 스스로 조직화하고 재생산이 가능한 모델로 소개되었다[1]. 이후 CA는 Wolfram에 의해 셀이라 불리는 메모리 배열로 소개되었고, 셀의 상태가 자신을 포함한 인접 이웃 셀 상태의 국소적인 상호작용에 의해 동시에 갱신되는 시스템으로 제안되였다[2]. 또한 CA는 간단하고 규칙적이며 작은 단위로 확장 연결이 가능하여 VLSI 하드웨어 구현이 용이하다. 이러한 CA는 LFSR의 대안으로 제안되었으며, test pattern generation, 의사 난수열 생성기, 오류정정부호, 신호분석기, 암호 등 많은 분야에 응용되고 있다[3-7]. 그러나 이러한 CA는 여러 장점에도 불구하고 LFSR과 달리 일반화와 분석이 어려워 거의 이뤄지지 않고 있다.

Mukhopadhyay 등은 키 공유 프로토콜을 구성하는데 유용한 전이규칙이 102인 uniform CA에서 특

† 본 연구는 2004학년도 부경대학교 기성회 학술연구비에 의해 연구되었음.

별히 여원벡터 $F=(1,1,\cdots,1)$에 의해 유도된 여원 그룹 CA의 상태전이 그래프의 성질을 분석하였다[8].

본 논문에서는 이러한 키 공유 알고리즘을 구성하는데 유용한 특별한 전이규칙과 그에 대응하는 여원벡터를 분석함으로써 기존의 방법을 보다 일반화한 것이다.

본 논문의 구성은 다음과 같다. 2장에서는 그룹 CA의 특별한 전이규칙인 60, 102, 204에 대해 알아보고, 3장에서는 이러한 전이규칙을 가지는 그룹 CA의 구조에 대해 분석한다. 4장에서는 이러한 그룹 CA에서 여원벡터에 의해 유도되는 여원 그룹 CA의 구조를 분석하고 5장에서는 결론을 맺는다.

2. 전이규칙 60, 102, 204

본 절에서는 그룹 CA의 특별한 전이규칙인 60, 102, 204에 대해 알아본다.

CA에서 셀의 다음 상태는 전이규칙에 따라 정해진다. 본 논문에서는 각 셀들은 자기 자신과 이웃 셀의 함수 값에 의해 다음 상태가 결정되는 동시에 갱신되는 3-이웃 CA를 다룬다. 시간 $t+1$에서 i번째 셀의 상태가 x라면 다음과 같이 나타낼 수 있다.

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

여기서 f는 결합논리를 가지는 국소전이 함수로 다음 상태를 결정하는 함수, 즉 전이규칙이라 할 수 있다.

그룹 CA란 모든 셀의 상태가 몇 개의 사이클을 이루며 반복되는 CA이다. 그룹 CA의 전이규칙은 여러 가지가 있다. 본 절에서 분석하고자 하는 그룹 CA의 전이규칙은 다음과 같다.

[표 1] 그룹 CA의 전이규clr

전이규칙	전이함수
60	$x_i(t+1)=x_{i-1}(t)\oplus x_i(t)$
102	$x_i(t+1)=x_i(t)\oplus x_{i+1}(t)$
204	$x_i(t+1)=x_i(t)$

n-셀 CA의 전이규칙이 모두 같으면 uniform CA라 하고 그렇지 않으면 hybrid CA라 한다.

정리 1. 전이규칙이 60, 102 이거나 204인 uniform CA는 그룹 CA이다. □

정리 2. 전이규칙이 60, 102 이거나 204인 hybrid CA 중에서 102와 60의 전이규칙이 나란히 나오지 않으면 그룹 CA이다. □

3. 전이규칙이 60, 102, 204인 그룹 CA의 구조 분석

본 절에서는 전이규칙이 60, 102이거나 204인 n-셀 uniform 그룹 CA와 hybrid 그룹 CA의 구조를 분석한다.

정리 3. 전이규칙이 60, 102이거나 204인 n-셀 uniform 그룹 CA와 hybrid 그룹 CA의 특성다항식 $c(x)$와 최소다항식 $m(x)$는 각각 다음과 같다.(단, $l \leqq n$)

[표 2]. 특성다항식과 최소다항식

	uniform CA			hybrid CA
$c(x)$	60	102	204	$(x+1)^n$
	$(x+1)^n$	$(x+1)^n$	$(x+1)^n$	
$m(x)$	$(x+1)^n$	$(x+1)^n$	$(x+1)$	$(x+1)^l$

□

정리 4. 전이규칙이 60, 102이거나 204인 n-셀 uniform 그룹 CA와 hybrid 그룹 CA의 최소다항식의 차수가 $m(=n$ 또는 $l)$이면 주기(order)는 다음과 같다.

$$\begin{cases} \text{if } m=2^a(a=0,1,2,\cdots), & order=m \\ \text{if } m\neq 2^a(2^{a-1}<m<2^a), & order=2^a \end{cases}$$

□

따름정리 5. 전이규칙이 60, 102이거나 204인 n-셀 uniform 그룹 CA와 hybrid 그룹 CA의 주기는

2^a이다$(a = 0,1,2,\cdots)$. □

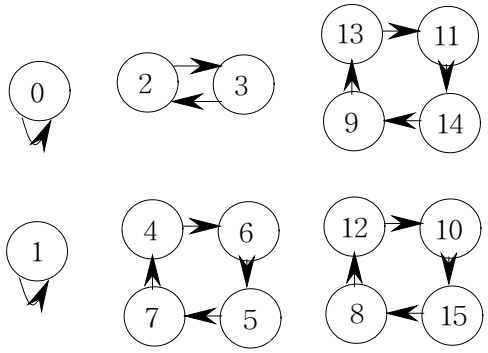
정리 6. 전이규칙이 60, 102이거나 204인 n-셀 uniform 그룹 CA의 상태전이 그래프에서 임의의 상태 X가 다음과 같은 경우에 X는 최대 주기 사이클에 놓인다.

$$\begin{cases} \text{if} \quad R=<60,60,\cdots,60>, \quad X=(1,a_1,\cdots,a_{n-1}) \\ \text{if} \quad R=<102,102,\cdots,102>, \quad X=(b_0,\cdots,b_{n-2},1) \\ \text{if} \quad R=<204,204,\cdots,204>, \quad X=(c_0,\cdots,c_{n-1}) \end{cases}$$

(단, $a_{i,},b_{i,},c_i = 0$ 또는 1)

□

예제 1. $R = <60,60,60,60>$인 4-셀 uniform 그룹 CA의 $\mathbb{C}$의 특성다항식과 최소다항식은 $c(x)=m(x)=(x+1)^4$이고, 최소다항식의 차수 $m=4=2^2$이므로 주기는 4이다. 다음은 $\mathbb{C}$의 상태전이 그래프이다.



[그림 1]. $\mathbb{C}$의 상태전이 그래프

여기서 상태 $X=(1001)=9$에서 $X=(1111)=15$는 최대 주기 사이클에 놓임을 알 수 있다.

4. 여원벡터에 의해 유도된 여원 그룹 CA의 구조 분석

본 절에서는 전이규칙이 60, 102이거나 204인 n-셀 uniform 그룹 CA와 hybrid 그룹 CA에서 각각의 여원벡터에 대응하여 유도되는 여원 그룹 CA의 구조를 분석한다.

정리 7([9]). 선형 그룹 CA의 여원 CA도 그룹 CA이다. □

정리 8. 전이규칙이 60, 102이거나 204인 n-셀 uniform 그룹 CA와 hybrid 그룹 CA의 주기가 k일 때, $\mathbf{0}$이 아닌 여원벡터에 의해 유도된 여원 그룹 CA의 주기는 k이거나 $2k$이다. □

정리 9. 전이규칙이 60, 102이거나 204인 n-셀 uniform 그룹 CA에서 여원벡터 $F(\neq \mathbf{0})$는 다음과 같은 경우에 여원 그룹 CA의 상태전이 그래프는 uniform 그룹 CA의 상태전이 그래프와 형태가 동일하다. □

정리 10. 전이규칙이 60, 102이거나 204인 n-셀 uniform 그룹 CA에서 유도되는 여원 그룹 CA의 상태전이 그래프에서 여원벡터 $F(\neq \mathbf{0})$는 다음과 같은 경우에 사이클들의 주기가 모두 같아진다.

$$\begin{cases} \text{if} \quad R=<60,60,\cdots,60>, \quad F=(1,a_1,\cdots,a_{n-1}) \\ \text{if} \quad R=<102,102,\cdots,102>, \quad F=(b_0,\cdots,b_{n-2},1) \\ \text{if} \quad R=<204,204,\cdots,204>, \quad F=(c_0,\cdots,c_{n-1}) \end{cases}$$

(단, $a_{i,},b_{i,},c_i = 0$ 또는 1)

□

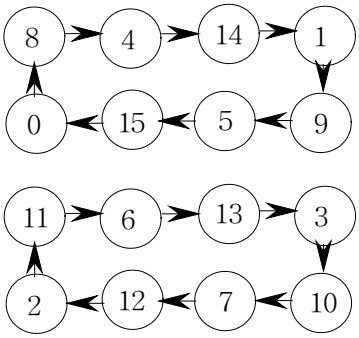
정리 11. i번째 셀의 전이규칙이 204인 $R=<102,\cdots,102,204,60,\cdots,60>$을 전이규칙으로 하는 n-셀 CA에서 유도되는 여원 그룹 CA의 상태전이 그래프에서 여원벡터 $F(\neq \mathbf{0})$가 다음과 같은 경우에 사이클들의 주기가 모두 같아진다.

$$F=(d_0,\cdots,d_i,\cdots,d_{n-1})$$

(단, $d_i = 1, d_j = 0 \ or \ 1, (i \neq j)$)

□

예제 2. 예제1에서 R인 그룹 CA $\mathbb{C}$에서 여원벡터 $F=(1,0,0,0)$에 의 유도되는 여원 그룹 CA $\mathbb{C}'$는 두 개의 주기가 8인 사이클을 이룬다. 다음은 $\mathbb{C}'$의 상태전이 그래프이다.



[그림 2]. $\mathbb{C}$의 상태전이 그래프

정리 12. 정리 6, 8에서 언급한 n-셀 CA에서 유도되는 여원 그룹 CA의 상태전이 그래프에서 사이클들의 주기가 모두 같아지게 하는 여원벡터 $F(\neq \mathbf{0})$는 그룹 CA에서 최대 주기 사이클에 놓인다. □

5. 결론

본 논문은 전이규칙이 60, 102이거나 204인 n-셀 uniform 그룹 CA와 hybrid 그룹 CA에 대해 분석하고 이러한 CA에서 특별한 여원벡터에 의해 유도된 여원 그룹 CA에 대해 분석한 것이다. 이는 키 공유 알고리즘을 구성하는데 유용한 전이규칙과 그에 대응하는 특별한 여원벡터를 분석함으로써 기존의 방법을 보다 일반화였다.

참고문헌

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

[2] S. Wolfram, "Cellular automata and complexity", Addison-Welsly Publishing Company, 1994.

[3] P. Dasgupta, S. Chattopadhyay, P.P. Chaudhuri and I. Sengupta, " Cellular automata-based recursive pseudoexhaustive test pattern generator, IEEE Transactions of Computers, Vol. 50, No. 2, pp. 177-185, 2001.

[4] P.D. Hortensius, R.D. McLeod and H.C. Card, "Cellular automata based pseudorandom number generators for built-in self test, IEEE Trans. on DAS of Integrated Circuits and System, Vol. 8, pp. 842-859, 1989.

[5] C. N. Zang, M. Deng and R. Mason, " Two improved algorithms and hardware implementations for key distribution using extended programmable cellular automata", Computer Security Applications Conference, Proceedings, 14th Annual, pp. 244-249, 1998.

[6] S. Bhattacharjee, S. Sinha, S. Chattopadhyay and P.P. Chaudhuri, " Cellular automata based scheme for solution of Boolean equations, IEEE, Proc.-Comput. Digit. Tech., Vol. 143, No. 3, pp. 174-180, 1996.

[7] S.J. Cho, U.S. Choi, Y.H. Hwang, H.D. Kim, Y.S. Pyo, K.W. Kim & S.H. Heo, "Computing Phase Shifts of Maximum-Length 90/150 Cellular Automata Sequencesf", ACRI 2004, LNCS 3305, pp. 31-39, 2004.

[8] D. Mukhopadhyay and D.R. Chowdhury, " Characterization of a class of complemented Group Cellular Automata", ACRI 2004, LNCS 3305, pp. 775-784, 2004.

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