# 충격반응수열을 이용한 최대길이를 갖는 셀룰라 오토마타의 위상이동차 계산 알고리즘†

최언숙*, 김진경**, 황윤희***, 김한두****, 조성진*****

*동명대학교 멀티미디어공학과, **부경대학교 응용수학과

***부경대학교 정보보호학과, ****인제대학교 컴퓨터응용과학부

*****부경대학교 수리과학부

# Computation Algorithm for the Phase Shifts of Maximum Length Cellular Automata by Using Impulse Response Sequence†

Un-Sook Choi*, Jin-Gyoung Kim**, Yoon-Hee Hwang***

Han-Doo Kim****, Sung-Jin Cho*****

*Dept. of Multimedia Engineering, Tongmyong Univ.

**Dept. of Applied Mathematics, Pukyong National Univ.

***Dept. of Information Security, Pukyong National Univ.

****School of Computer Aided Science, Inje Univ.

*****Division of Mathematical Sciences, Pukyong National Univ.

**요 약**

GF(2)위에서 최대길이를 갖는 $n$-셀 90/150 셀룰라 오토마타의 각 셀은 길이가 $2^n-1$인 수열을 생성한다. 이러한 셀룰라 오토마타의 임의의 셀에 대한 출력수열은 다른 셀에 대한 출력수열의 위치를 이동함으로써 얻을 수 있다. 본 논문에서는 주어진 셀룰라 오토마타의 상태전이행렬의 특성다항식에 의한 동차 선형점화식을 만족하는 충격반응수열을 이용하여 셀들의 위상이동차를 계산하는 알고리즘을 제안한다.

## I. 서론

LFSR의 대안으로 제안된 셀룰라 오토마타(이하 CA)[1]는 LFSR과 달리 고품질의 PN 수열을 생성할 수 있으므로[2,3], 테스트 패턴 생성, 의사 난수열 생성기, 암호 및 서명과 같은 분야에서 응용되고 있다[4-11]. 가산 CA중 GF(2) 위에서 최대길이를 갖는 $n$-셀 90/150 CA의 각 셀들은 주기가 $2^n-1$인 PN 수열을 생성한다. 이러한 CA의 임의의 셀에 대한 출력수열은 다른 셀에 대한 출력수열의 위치를 이동함으로써 얻을 수 있다. 그리고 LFSR과 달리, CA의 셀들에 대한 출력수열들의 위상이동차는 일반적으로 CA의 단계마다 다르다.

Bardell[2]은 로그함수를 이용하여 CA의 셀들 간의 위상이동차를 계산하는 알고리즘을 제안하였다. 이후 Chaudhuri[8]는 CA의 상태전이행렬을 이용하여 CA의 위상이동차를 계산하는 방법을 제안하였으며, Sarkar는 연립방정식의 해를 연이어 구함으로써 CA의 셀들 간의 위상이동차를 구하는 알고리즘을 제안하였고, 이 알고리즘을 스트림 암호의 설계에 응용하였다[5]. Sarkar에 의해 제안된 알고리즘은 Shank의 알고리즘을 바탕으로 하기 때문에 셀의 크기가 50미만이어야 한다. Cho 등[12]은 행위상이동

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

차라는 새로운 개념을 도입하여 위상이동차를 구하는 새로운 알고리즘을 제안하여 Sarkar의 방법을 개선하였다.

본 논문에서는 PN수열을 생성하는 CA의 셀들의 위상이동차를 계산하는 새로운 알고리즘을 제안한다.

## Ⅱ. 90/150 CA의 위상이동차

CA는 규칙적인 방법에 의해 공간적으로 배열된 상호 연결된 셀들로 이루어진다. 여기서, 각 셀의 상태전이는 그 셀의 이웃에 의존한다. Wolfram[1]에 의해 조사된 CA의 구조는 셀들의 이산격자로 간주될 수 있다. 단, 각 셀의 값은 0 또는 1로 가정하고, 한 셀의 다음 상태는 자신과 인접한 두 셀(3-이웃)에 의존한다고 하자. 본 논문에서 다루는 CA의 전이규칙 90과 150은 다음과 같이 주어진다.

$$\text{규칙 } 90 : \ q_i^{t+1} = q_{i-1}^t \oplus q_{i+1}^t$$
$$\text{규칙 } 150 : \ q_i^{t+1} = q_{i-1}^t \oplus q_i^t \oplus q_{i+1}^t$$

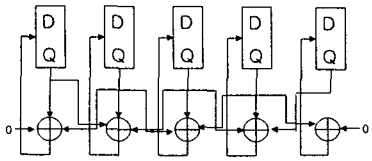
단, $\oplus$는 XOR 논리이고 $q_i^t$는 $t$ 번째 시간에서 $i$ 번째 셀의 상태를 나타내고, $q_{i-1}^t$와 $q_{i+1}^t$는 자신의 왼쪽과 오른쪽 이웃 상태를 나타낸다.

$n$-셀 90/150 CA는 선형 CA로 다음 상태를 나타내는 함수가 다음과 같은 $n \times n$ 삼중대각 행렬 $T_n$으로 표현할 수 있고 이를 상태전이행렬이라 한다.

$$T_n = \begin{pmatrix} a_1 & 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & a_2 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & a_3 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & a_{n-1} & 1 \\ 0 & 0 & 0 & 0 & 0 & \cdots & 1 & a_n \end{pmatrix}$$

단, $a_i$는 $i$ 번째 셀에 대한 규칙이 90인 경우는 0이고, 150인 경우는 1이다. 간단히 $T_n = < a_1, a_2, \cdots, a_n >$으로 나타내기로 한다.

**<예제 1>** $T_5 = < 1,1,1,1,0 >$ 이 주어진 5-셀 90/150 CA의 상태전이행렬이라 하면, 특성다항식은 $f(x) = x^5 + x^2 + 1$ 이고 이는 원시다항식이다. 따라서 최대길이를 갖는 90/150 CA이다. <그림 1>은 주어진 CA의 구조를 보여준다.




<그림 1> 최대길이를 갖는 5-차 90/150 CA의 구조

LFSR을 표현하는 동반행렬은 특성다항식과 최소다항식이 항상 같다. 그러나 LFSR보다 난수성이 우수하다고 알려진 CA는 일반적으로 특성다항식과 최소다항식이 같지 않다. 다음의 정리는 특성다항식과 최소다항식이 항상 같은 CA에 관한 정리이다.

**<정리 1[13]>** 상태전이행렬이 $T_n$인 임의의 $n$-셀 90/150 CA에 대하여, $T_n$의 최소다항식은 $T_n$의 특성다항식과 같다.

**<정의 1[14]>** $s_0, s_1, \cdots$를 GF(2)위의 특성다항식이 $f(x) = x^n + d_{n-1}x^{n-1} + \cdots + d_1 x + 1$ 인 $n$차 선형점화식을 만족하는 동차 선형점화수열들 중에서 다음의 선형점화식에 의하여 유일하게 얻어진 수열을 **충격반응수열**이라 한다.

$$s_{t+n} = d_{n-1} \cdot s_{t+n-1} + d_{n-2} \cdot s_{t+n-2} + \cdots + d_1 \cdot s_{t+1} + s_t$$

여기서 $s_0 = s_1 = \cdots = s_{n-2} = 0$, $s_{n-1} = 1$ 이고 $t = 0, 1, \cdots$ 이다.

예를 들어 선형점화식이 $s_{t+5} = s_{t+2} + s_t$ 인 충격반응수열은 다음과 같다.

0000100101100111110001101110101…

**<예제 2>** <예제 1>의 최대길이를 갖는 5-셀 90/150 CA의 첫 번째 셀에 대한 각 셀들의 위상이동차를 구해 보자. [표 1]은 초기상태 00001에 대한 CA의 상태전이표이며, 첫째 셀에 대한

둘째, 셋째, 넷째, 다섯째 셀의 위상이동차 13, 29, 8, 9는 [표 1]에서 확인할 수 있다.

[표 1] 90/150 CA의 상태전이

| | | | | | |
|---|---|---|---|---|---|
| 0 | 00001 | 11 | 00100 | 22 | 11111 |
| 1 | 00010 | 12 | 01110 | 23 | 01111 |
| 2 | 00111 | 13 | 10101 | 24 | 10111 |
| 3 | 01011 | 14 | 10100 | 25 | 10011 |
| 4 | 11001 | 15 | 10110 | 26 | 11101 |
| 5 | 00110 | 16 | 10001 | 27 | 01000 |
| 6 | 01001 | 17 | 11010 | 28 | 11100 |
| 7 | 11110 | 18 | 00011 | 29 | 01010 |
| 8 | 01101 | 19 | 00101 | 30 | 11011 |
| 9 | 10000 | 20 | 01100 | 31 | 00001 |
| 10 | 11000 | 21 | 10010 | ⋮ | ⋮ |

다음은 충격반응수열을 이용한 최대길이를 갖는 $n$-셀 90/150 CA의 위상이동차를 계산하는 방법을 제시한다.

**<정리 2>** 최대길이를 갖는 $n$차 90/150 CA의 상태전이행렬 $T$의 특성다항식을 $f(x)=x^n+d_{n-1}x^{n-1}+\cdots+d_1x+1$라 하자. CA의 초기상태 벡터$v_0=(00\cdots01)$에 대하여 행렬 $P$를 다음과 같이 정의하자.

$$P=\begin{pmatrix} v_0 \\ v_0T \\ v_0T^2 \\ \vdots \\ v_0T^{n-1} \end{pmatrix}$$

$P$의 $j$열 벡터$(p_{1j},p_{2j},\cdots,p_{nj})^t$ 와 선형점화식 $s_{t+n}=d_{n-1}\cdot s_{t+n-1}+d_{n-2}\cdot s_{t+n-2}+\cdots+d_1\cdot s_{t+1}+1$에 대하여 $(s_{nk},s_{nk+1},\cdots,s_{nk+n-1})^t=(p_{1j},p_{2j},\cdots,p_{nj})^t$ 이 성립할 때, CA의 첫째 셀에 대한 $j$번째 셀의 위상이동차는 $-nk \pmod{2^n-1}$이다.

**<예제 3>** <예제 1>의 최대길이를 갖는 5-셀 90/150 CA에 대한 행렬 $P$는 다음과 같다.

$$P=\begin{pmatrix} 00001 \\ 00010 \\ 00111 \\ 01011 \\ 11001 \end{pmatrix}$$

선형점화식이 $s_{t+5}=s_{t+2}+s_t$ 인 충격반응수열은 [표 2]와 같다. 행렬 $P$의 각 열벡터 $(00011)^t$, $(00100)^t$, $(01110)^t$, $(10111)^t$에 대하여 <정리 2>를 만족하는 $nk$는 80, 95, 85, 115이다. 따라서 <정리 2>에 의하여 각 셀의 위상이동차는 13, 29, 8, 9이다.

[표 2] 선형점화식 $s_{t+5}=s_{t+2}+s_t$ 의 충격반응수열

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 00001 | 00101 | 10011 | 11100 | 01101 | 11010 | 10000 | 10010 |
| 11001 | 11110 | 00110 | 11101 | 01000 | 01001 | 01100 | 11111 |
| 00011 | 01110 | 10100 | 00100 | 10110 | 01111 | 10001 | 10111 |
| 01010 | 00010 | 01011 | 00111 | 11000 | 11011 | 10101 | 00001 |

[표 3]은 충격반응수열을 이용한 최대길이를 갖는 셀룰라 오토마타의 위상이동차 계산 알고리즘이다.

[표 3] CA의 위상이동차 계산 알고리즘

Input : 셀의 수 $n$, CA의 전이행렬 $T_n$
Output : 셀의 위상이동차 PS[$n$]
Step 1. $T_n$과 $v_o$에 의하여 $P$를 구한다.
Step 2. $T_n$의 특성다항식 $m(x)$를 계산한다.
Step 3. $m(x)$를 선형점화식으로 하는 충격반응수열을 구한다.
Step 4. $P$의 $j$열 $(p_{1j},p_{2j},\cdots,p_{nj})$, $j=2,\cdots,n$에 대하여 $(s_{nk},s_{nk+1},\cdots,s_{nk+n-1})=(p_{1j},p_{2j},\cdots,p_{nj})$ 이 성립하는 $nk[j]$를 구한다.
Step 5. PS[1]=0, PS[$j$]=$-nk[j] \pmod{2^n-1}$ $(j=2,\cdots,n)$

## Ⅲ. 결론 및 향후연구과제

본 논문에서는 PN수열을 생성하는 최대길이를 갖는 90/150 CA의 셀들의 위상이동차를 계

산하는 새로운 방법으로, 주어진 CA의 상태전이행렬의 특성다항식에 의한 동차 선형점화식을 만족하는 충격반응수열을 이용하여 계산하는 알고리즘을 제안하였다. 제안한 알고리즘의 계산복잡도는 $O(2^n)$이다. 향후에는 계산복잡도를 줄이는 방법에 대하여 연구할 예정이다.

## [참고문헌]


[1] S. Wolfram, "Statistical Mechanics of Cellular Automata", Rev. Mod. Phys. 55, pp. 601-644, 1983.

[2] P.H. Bardell, "Analysis of Cellular Automata Used as Pseudorandom Pattern Generators", Proc. IEEE Int. Test. Conf. pp. 762-767, 1990.

[3] A.K. Das and P.P. Chaudhuri, "Vector Space Theoretic Analysis of Additive Cellular Automata and its Application for Pseudo-Exhaustive Test Pattern Generation", IEEE Trans. Comput. 42, pp. 340-352, 1993.

[4] S. Tezuka and M. Fushimi, "A Method of Designing Cellular Automata as Pseudorandom Number Generators for Built-In Self-Test for VLSI", Contemporary Mathematica 168, pp. 363-367, 1994.

[5] P. Sarkar, "Computing Shifts in 90/150 Cellular Automata Sequences", Finite Fields Their Appl. 42, pp. 340-352, 2003.

[6] S.J. Cho, U.S. Choi and H.D. Kim, "Analysis of Complemented CA Derived from a Linear TPMACA", Computers and Mathematics with Applications 45, pp. 689-698, 2003.

[7] S.J. Cho, U.S. Choi and H.D. Kim, "Behavior of Complemented CA whose Complement Vector is Acyclic in a Linear TPMACA", Mathematical and Computer Modelling 36, pp. 979-986, 2002.

[8] S. Nandi and P.P. Chaudhuri, "Additive Cellular Automata as an On-Chip Test Pattern Generator", Test Symposium 1993, Proceedings of the Second Asian, IEEE, pp. 166-171, 1993.

[9] P. Sarkar, "The Filter-Combiner Model for Memoryless Synchronous Stream Ciphers", in Proceedings of Crypto 2002, Lecture Notes in Computer Science, Springer, Berlin 2442, pp. 533-548, 2002.

[10] 최언숙, 조성진, "최대길이를 갖는 셀룰라 오토마타의 생성", 정보보호학회논문지, 14(6), pp. 25-30, 2004.

[11] 조성진, 최언숙, 황윤희, 김한두, 표용수, "GF($2^p$) 위에서의 SACA의 상태전이 분석", 정보보호학회논문지, 15(2), pp. 105-111, 2005.

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

[13] 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, 9, pp. 767-778, 1990.

[14] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, 1997.