J. KSIAM **Vol.4**, No.2, 21-32, 2000

Analysis of One-dimensional cellular automata over $GF(q)$

Sung-Jin Cho, Han-Doo Kim and Un-Sook Choi

Abstract

We study theoretical aspects of one-dimensional cellular automata over $GF(q)$, where q is a power of a prime. Some results about the characteristic polynomials of such cellular automata are given. Intermediate boundary cellular automata are defined and related to the more common null boundary cellular automata.

1 Introduction

One-dimensional linear hybrid cellular automata(CA) have been proposed as an alternative to linear feedback shift registers(LFSRs), in applications such as test pattern generation, pseudorandom number generation, cryptography and signature analysis. Uniform CA have been studied extensively, both over $GF(2)$ and the more general setting of $GF(q)$ ([4], [6], [10], [11]). An LFSM M is an implementation of a linear operator L, and many properties of M can be expressed as properties of L. Some properties of linear operators, and hence of LFSMs, are easier to identify by the study of minimal polynomials than by direct examination of linear operators. Determining the minimal polynomial of a linear operator is sometimes complicated, whereas deriving the characteristic polynomial of a linear operator is straightforward. Fortunately, the classes of linear operators that we study often have the property that their minimal polynomials equal their characteristic polynomials. Cattel and Muzio ([2]) studied theoretical aspects of one-dimensional linear hybrid cellular automata over a finite field, and they presented general results concerning the characteristic polynomials of such CA. Also they defined cyclic boundary CA and gave relations to the more common null boundary CA. In this paper we study theoretical foundation of one-dimensional cellular automata over a finite field. Some results about the characteristic polynomials of such cellular automata are given. Intermediate boundary cellular automata are defined and related to the more common null boundary cellular automata.

1991 Mathematics Subject Classification: 94

Key Words and Phrases: Cellular automata, null boundary cellular automata, cyclic cellular automata, intermediate boundary cellular automata, characteristic polynomials, minimal polynomials.

This work was supported by the 2000 Inje University Research Grant

2 Preliminaries

The structures under consideration are a particular type of linear machine defined over the finite field $GF(q)$, where q is a power of a prime. For background on CA, see [1], [2], [3], [4], [5], [6], [7], [8], [9]. The transition matrix of a null boundary CA has the form

$$T_{NBCA} = \begin{pmatrix} d_1 & b_1 & 0 & \cdots & 0 & 0 & 0 \\ c_2 & d_2 & b_2 & \cdots & 0 & 0 & 0 \\ 0 & c_3 & d_3 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & c_{n-1} & d_{n-1} & b_{n-1} \\ 0 & 0 & 0 & \cdots & 0 & c_n & d_n \end{pmatrix}$$

A CA has a maximal length cycle if the sequence of states includes all $q^n - 1$ nonzero states for any nonzero starting state.

Example 2.1. *Consider the three cell CA over $GF(2^2)$ with transition matrix*

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

where $\alpha^2 + \alpha + 1 = 0$. This machine has a maximal length cycle of 63 distinct nonzero states.

An irreducible polynomial $p(x)$ of degree n is primitive if it has a root α such that the set $\{\alpha^i : i = 0, 1, \cdots, q^{n-2}\}$ equals the set of nonzero elements of $GF(q^n)$. Let the transition matrix of an LFSM be denoted T_{LFSM}. The characteristic polynomial of the LFSM is defined to

$$|xI - T_{LFSM}|$$

where x is an indeterminate and I is the identity matrix with the same dimension as T_{LFSM}. The characteristic polynomial is primitive if and only if the LFSM has a maximal length cycle([8]). We use $\Delta_{i,j}$ to denote the characteristic polynomial of $M_{i,j}$ and abbreviate $\Delta_{1,j}$ as Δ_j. $\Delta_{i,j}$ is called a *subpolynomial*. The machine $M_{1,n}$ is written as M with corresponding characteristic polynomial Δ.

3 Null Boundary CA(NBCA) characteristic polynomials

Cattel and Muzio([2]) presented several theroems that show interrelationships among the subpolynomials of a NBCA. The following theorems and corollary are in [2].

Theorem 3.1. *Δ_k satisfies the following recurrence:*

$$\begin{aligned}\Delta_{-1} &= 0,\\ \Delta_0 &= 1,\\ \Delta_k &= (x-d_k)\Delta_{k-1} - b_{k-1}c_k\Delta_{k-2}, \quad k \geq 1.\end{aligned}$$

Corollary 3.2. *The characteristic polynomial of a CA can be computed with $2n$ polynomial additions and $2n$ scalar polynomial multiplications.*

Example 3.3. *Consider the three cell CA over $GF(2^2)$ from Example 2.1, with transition matrix*

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

We have

$$\begin{aligned}\Delta_{-1} &= 0,\\ \Delta_0 &= 1,\\ \Delta_1 &= (x-1)\cdot 1 + 0 = x+1,\\ \Delta_2 &= (x-1)(x+1) - 1\cdot\alpha^2\cdot 1 = x^2+\alpha^2+1,\\ \Delta_3 &= x^3+\alpha x^2+\alpha^2 x+\alpha\end{aligned}$$

Theorem 3.4. *For any k with $0 \leq k \leq n$,*

$$\Delta_{1,n} = \Delta_{1,k}\Delta_{k+1,n} - b_k c_{k+1}\Delta_{1,k-1}\Delta_{k+2,n}.$$

Theorem 3.5.

$$\Delta_{1,n-1}\Delta_{2n} - \Delta_{1,n}\Delta_{2,n-1} = \prod_{i=1}^{n-1} b_i \prod_{i=2}^{n} c_i.$$

4 Cyclic CA

Cattel and Muzio ([2]) considered cyclic CA which is a generalization of NBCA. The transition matrix of a cyclic CA has the form

$$T = \begin{pmatrix} d_1 & b_1 & 0 & \cdots & 0 & 0 & c_1 \\ c_2 & d_2 & b_2 & \cdots & 0 & 0 & 0 \\ 0 & c_3 & d_3 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & c_{n-1} & d_{n-1} & b_{n-1} \\ b_n & 0 & 0 & \cdots & 0 & c_n & d_n \end{pmatrix}$$

They defined the notion of a *submachine* $C_{i,j}$. $\Phi_{i,j}$ denotes the characteristic polynomial of the submachine $C_{i,j}$ with $\Phi = \Phi_{1,n}$. The following theorem is in [2].

Theorem 4.1. *Let T be a cyclic CA, with Φ and $\Delta_{i,j}$ as defined above. Then*

$$\Phi_{1,n} = \Delta_{1,n} - c_1 b_n \Delta_{2,n-1} + (-1)^{n+1}(\prod_{k=1}^{n} b_k + \prod_{k=1}^{n} c_k).$$

We obtain the following theorem from Theorem 4.1.

Theorem 4.2. *Let T be a cyclic CA, with Φ and $\Delta_{i,j}$ as defined above. Then*

$$\Phi_{1,n} = a_n \Phi_{2,n} - c_n b_n \Phi_{2,n-1} + (-1)^{n+1}(\prod_{k=1}^{n-1} b_k + \prod_{k=1}^{n-1} c_k)(a_n + b_n + c_n),$$

where $a_k = x - d_k, k = 1, \cdots, n, a_1 = a_n, b_1 = b_n$ and $c_1 = c_n$.

Proof. ¿From Theorem 4.1 we know

$$\Phi_{2,n} = \Delta_{2,n} - c_2 b_n \Delta_{3,n-1} + (-1)^{n}(\prod_{k=2}^{n} b_k + \prod_{k=2}^{n} c_k).$$

$$\Phi_{2,n-1} = \Delta_{2,n-1} - c_2 b_{n-1} \Delta_{3,n-2} + (-1)^{n-1}(\prod_{k=2}^{n-1} b_k + \prod_{k=2}^{n-1} c_k).$$

Using the above two results

$$\begin{aligned}
\Phi_{1,n} &= a_1\Delta_{2,n} - b_1c_2\Delta_{3,n} - c_1b_n\Delta_{2,n-1} + (-1)^{n+1}(\prod_{k=1}^{n} b_k + \prod_{k=1}^{n} c_k) \\
&= a_1(\Phi_{2,n} + c_2b_n\Delta_{3,n-1} + (-1)^{n+1}(\prod_{k=2}^{n} b_k + \prod_{k=2}^{n} c_k)) - b_1c_2\Delta_{3,n} \\
&\quad -c_1b_n(\Phi_{2,n-1} + c_2b_{n-1}\Delta_{3,n-2} + (-1)^{n}(\prod_{k=2}^{n-1} b_k + \prod_{k=2}^{n-1} c_k)) + (-1)^{n+1}(\prod_{k=1}^{n} b_k + \prod_{k=1}^{n} c_k) \\
&= a_n\Phi_{2,n} - c_nb_n\Phi_{2,n-1} + c_2b_n(a_n\Delta_{3,n-1} - b_{n-1}c_n\Delta_{3,n-2} - \Delta_{3,n}) \\
&\quad +(-1)^{n+1}a_n(\prod_{k=2}^{n} b_k + \prod_{k=2}^{n} c_k) + (-1)^{n+1}b_nc_n(\prod_{k=2}^{n-1} b_k + \prod_{k=2}^{n-1} c_k) \\
&\quad +(-1)^{n+1}(\prod_{k=1}^{n} b_k + \prod_{k=1}^{n} c_k) \quad \text{because } a_1 = a_n, c_1 = c_n \\
&= a_n\Phi_{2,n} - c_nb_n\Phi_{2,n-1} + (-1)^{n+1}(a_n + b_n + c_n)(\prod_{k=1}^{n-1} b_k + \prod_{k=1}^{n-1} c_k)
\end{aligned}$$

□

As a corollary we obtain the following result which is in [3].

Corollary 4.3. *Let $b_k = c_k = 1, d_k = 0$ or 1 and $d_1 = d_n$ for $k = 1, \cdots, n$ in Theorem 4.2. Then*

$$\Phi_{1,n} = (x + d_1)\Phi_{2,n} + \Phi_{2,n-1}.$$

If $q = 2^n$, then we obtain the following result.

Theorem 4.4.

$$\Phi_{1,n} = a_1a_2\Phi_{3,n} + (bc)^2\Phi_{5,n} + (a_1a_2 + b^2 + c^2)(b^{n-2} + c^{n-2})$$

where n is even and $b_k = b, c_k = c, d_1 = d_3 = \cdots = d_{n-1}$ and $d_2 = d_4 = \cdots = d_n$.

Proof.

$$\begin{aligned}
\Phi_{1,n} &= a_1\Delta_{2,n} - b_1c_2\Delta_{3,n} - b_nc_1\Delta_{2,n-1} + (-1)^{n+1}(\prod_{k=1}^{n} b_k + \prod_{k=1}^{n} c_k) \\
&= a_1\Delta_{2,n} - bc\Delta_{3,n} - bc\Delta_{2,n-1} + b^n + c^n \\
&= a_1\Delta_{2,n} + b^n + c^n \quad \text{because } \Delta_{3,n} = \Delta_{2,n-1} \\
&= a_1(a_2\Delta_{3,n} + bc\Delta_{4,n}) + b^n + c^n \\
&= a_1a_2\Delta_{3,n} + a_1bc\Delta_{4,n} + b^n + c^n \\
&= a_1a_2(\Phi_{3,n} + bc\Delta_{4,n-1} + b^{n-2} + c^{n-2}) + a_1bc\Delta_{4,n} + b^n + c^n \\
&= a_1a_2\Phi_{3,n} + a_1a_2bc\Delta_{4,n-1} + a_1bc\Delta_{4,n} + a_1a_2b^{n-2} + a_1a_2c^{n-2} + b^n + c^n \\
&= a_1a_2\Phi_{3,n} + a_1bc(a_2\Delta_{4,n-1} + \Delta_{4,n}) + a_1a_2b^{n-2} + a_1a_2c^{n-2} + b^n + c^n \\
&= a_1a_2\Phi_{3,n} + (bc)^2a_1\Delta_{4,n-2} + a_1a_2b^{n-2} + a_1a_2c^{n-2} + b^n + c^n \\
&\quad \text{because } a_2 = a_n \text{ and } a_n\Delta_{4.n-1} + \Delta_{4,n} = bc\Delta_{4,n-2} \\
&= a_1a_2\Phi_{3,n} + (bc)^2\{\Phi_{5,n} + b^{n-4} + c^{n-4}\} + a_1a_2b^{n-2} + a_1a_2c^{n-2} + b^n + c^n \\
&\quad \text{because } a_1 = a_5, \Delta_{4,n-2} = \Delta_{5,n-1} = \Delta_{6,n} \text{ and } \Phi_{5,n} = a_5\Delta_{6,n} + (b^{n-4} + c^{n-4}) \\
&= a_1a_2\Phi_{3,n} + (bc)^2\Phi_{5,n} + (a_1a_2 + b^2 + c^2)(b^{n-2} + c^{n-2})
\end{aligned}$$

□

5 Intermediate Boundary CA

In this section we consider Intermediate Boundary CA(IBCA) and the relations with NBCA and study the related properties. The transition matrix of an IBCA has the form

$$T_{IBCA} = \begin{pmatrix}
d_1 & b_1 & c_1 & \cdots & 0 & 0 & 0 \\
c_2 & d_2 & b_2 & \cdots & 0 & 0 & 0 \\
0 & c_3 & d_3 & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \dots & c_{n-1} & d_{n-1} & b_{n-1} \\
0 & 0 & \cdots & \cdots & b_n & c_n & d_n
\end{pmatrix}$$

$\Psi_{i,j}$ denotes the characteristic polynomial of the submachine $B_{i,j}$ with $\Psi = \Psi_{1,n}$.

Theorem 5.1. *For every NBCA such that $b_2 \neq 0$ and $c_{n-1} \neq 0$ there exist at least one IBCA having the same characteristic polynomial.*

Proof. The characteristic matrix of a NBCA can be represented as

$$T_{NBCA} = \begin{pmatrix} d_1 & b_1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ c_2 & d_2 & b_2 & 0 & \cdots & 0 & 0 & 0 \\ 0 & c_3 & d_3 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & d_{n-2} & b_{n-2} & 0 \\ 0 & 0 & 0 & 0 & \cdots & c_{n-1} & d_{n-1} & b_{n-1} \\ 0 & 0 & 0 & 0 & \cdots & 0 & c_n & d_n \end{pmatrix}$$

The characteristic polynomial of this is $|xI - T_{NBCA}|$.

$$xI - T_{NBCA} = \begin{pmatrix} x-d_1 & b_1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ c_2 & x-d_2 & b_2 & 0 & \cdots & 0 & 0 & 0 \\ 0 & c_3 & x-d_3 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & x-d_{n-2} & b_{n-2} & 0 \\ 0 & 0 & 0 & 0 & \cdots & c_{n-1} & x-d_{n-1} & b_{n-1} \\ 0 & 0 & 0 & 0 & \cdots & 0 & c_n & x-d_n \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} x-d_1+c_2 & x-d_2+b_1 & b_2 & 0 & \cdots & 0 & 0 & 0 \\ c_2 & x-d_2 & b_2 & 0 & \cdots & 0 & 0 & 0 \\ 0 & c_3 & x-d_3 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & x-d_{n-2} & b_{n-2} & 0 \\ 0 & 0 & 0 & 0 & \cdots & c_{n-1} & x-d_{n-1} & b_{n-1} \\ 0 & 0 & 0 & 0 & \cdots & c_{n-1} & x-d_{n-1}+c_n & x-d_n+b_{n-1} \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} x-u & u-d_2+b_1 & b_2 & \cdots & 0 & 0 & 0 \\ c_2 & x-d_2-c_2 & b_2 & \cdots & 0 & 0 & 0 \\ 0 & c_3 & x-d_3 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & x-d_{n-2} & b_{n-2} & 0 \\ 0 & 0 & 0 & \cdots & c_{n-1} & x-d_{n-1}-b_{n-1} & b_{n-1} \\ 0 & 0 & 0 & \cdots & c_{n-1} & v-d_{n-1}+c_n & x-v \end{pmatrix}$$

where $u = d_1 - c_2$ and $v = d_n - b_{n-1}$

$$\Rightarrow xI - \begin{pmatrix} d_1 - c_2 & d_2 - d_1 + c_2 - b_1 & -b_2 & 0 & \cdots & 0 & 0 & 0 \\ -c_2 & d_2 + c_2 & -b_2 & 0 & \cdots & 0 & 0 & 0 \\ 0 & -c_3 & d_3 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & d_{n-2} & -b_{n-2} & 0 \\ 0 & 0 & 0 & 0 & \cdots & -c_{n-1} & d_{n-1} + b_{n-1} & -b_{n-1} \\ 0 & 0 & 0 & 0 & \cdots & -c_{n-1} & d_{n-1} - d_n + b_{n-1} - c_n & d_n - b_{n-1} \end{pmatrix}$$

$\Rightarrow xI - T_{IBCA}$ T_{IBCA} is the matrix representation of IBCA. □

Let $b_k = c_k = 1$ and $d_k = 0$ or 1 in Theorem 5.1. Then we obtain the following result which is in [4].

Corollary 5.2. *For every* 90/150 *NBCA there exists at least one IBCA having the same characteristic polynomial.*

Theorem 5.3. *Let* $n \geq 7$. *Then*

$$\Psi_{1,n} = \Delta_{1,n} + \prod_{k=1}^{3} c_k \Delta_{4,n} + \prod_{k=n-2}^{n} b_k \Delta_{1,n-3} + \prod_{k=1}^{3} c_k \prod_{k=n-2}^{n} b_k \Delta_{4,n-3}.$$

Proof. Let $a_i = x - d_i$. Then

$$\Psi = \begin{vmatrix} a_1 & b_1 & c_1 & \cdots & 0 & 0 & 0 \\ c_2 & a_2 & b_2 & \cdots & 0 & 0 & 0 \\ 0 & c_3 & a_3 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & c_{n-1} & a_{n-1} & b_{n-1} \\ 0 & 0 & 0 & \cdots & b_n & c_n & a_n \end{vmatrix}$$

By expanding the determinant along the first row, we have

$$\begin{aligned} \Psi_{1,n} &= a_1|A| - b_1|B| + c_1|C| \\ &= a_1(a_n\Delta_{2,n-1} - c_n|D| + b_n|E|) - b_1c_2|F| + c_1c_2c_3|G|, \end{aligned}$$

where

$$A = \begin{pmatrix} a_2 & b_2 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ c_3 & a_3 & b_3 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & c_4 & a_4 & b_4 & \cdots & 0 & 0 & 0 & 0 & 0 \\ & & & & \ddots & & & & & \\ & & & & & \ddots & & & & \\ 0 & 0 & 0 & 0 & \cdots & c_{n-3} & a_{n-3} & b_{n-3} & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & c_{n-2} & a_{n-2} & b_{n-2} & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & c_{n-1} & a_{n-1} & b_{n-1} \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & b_n & c_n & a_n \end{pmatrix}$$

$$B = \begin{pmatrix} c_2 & b_2 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & a_3 & b_3 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & c_4 & a_4 & b_4 & \cdots & 0 & 0 & 0 & 0 & 0 \\ & & & & \ddots & & & & & \\ & & & & & \ddots & & & & \\ 0 & 0 & 0 & 0 & \cdots & c_{n-3} & a_{n-3} & b_{n-3} & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & c_{n-2} & a_{n-2} & b_{n-2} & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & c_{n-1} & a_{n-1} & b_{n-1} \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & b_n & c_n & a_n \end{pmatrix}$$

$$C = \begin{pmatrix} c_2 & a_2 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & c_3 & b_3 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a_4 & b_4 & \cdots & 0 & 0 & 0 & 0 & 0 \\ & & & \ddots & & & & & & \\ & & & & & \ddots & & & & \\ 0 & 0 & 0 & 0 & \cdots & c_{n-3} & a_{n-3} & b_{n-3} & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & c_{n-2} & a_{n-2} & b_{n-2} & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & c_{n-1} & a_{n-1} & b_{n-1} \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & b_n & c_n & a_n \end{pmatrix}$$

$$D = \begin{pmatrix} a_2 & b_2 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ c_3 & a_3 & b_3 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & c_4 & a_4 & b_4 & \cdots & 0 & 0 & 0 & 0 \\ & & & & \ddots & & & & \\ & & & & & \ddots & & & \\ 0 & 0 & 0 & 0 & \cdots & c_{n-3} & a_{n-3} & b_{n-3} & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & c_{n-2} & a_{n-2} & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & c_{n-1} & b_{n-1} \end{pmatrix}$$

$$E = \begin{pmatrix} a_2 & b_2 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ c_3 & a_3 & b_3 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & c_4 & a_4 & b_4 & \cdots & 0 & 0 & 0 & 0 \\ & & & & \ddots & & & & \\ & & & & & \ddots & & & \\ 0 & 0 & 0 & 0 & \cdots & c_{n-3} & a_{n-3} & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & c_{n-2} & b_{n-2} & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & a_{n-1} & b_{n-1} \end{pmatrix}$$

$$F = \begin{pmatrix} a_3 & b_3 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ c_4 & a_4 & b_4 & \cdots & 0 & 0 & 0 & 0 & 0 \\ & & & \ddots & & & & & \\ & & & & \ddots & & & & \\ 0 & 0 & 0 & \cdots & c_{n-3} & a_{n-3} & b_{n-3} & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & c_{n-2} & a_{n-2} & b_{n-2} & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & c_{n-1} & a_{n-1} & b_{n-1} \\ 0 & 0 & 0 & \cdots & 0 & 0 & b_n & c_n & a_n \end{pmatrix}$$

$$G = \begin{pmatrix} a_4 & b_4 & \cdots & 0 & 0 & 0 & 0 & 0 \\ & & \ddots & & & & & \\ & & & \ddots & & & & \\ 0 & 0 & \cdots & c_{n-3} & a_{n-3} & b_{n-3} & 0 & 0 \\ 0 & 0 & \cdots & 0 & c_{n-2} & a_{n-2} & b_{n-2} & 0 \\ 0 & 0 & \cdots & 0 & 0 & c_{n-1} & a_{n-1} & b_{n-1} \\ 0 & 0 & \cdots & 0 & 0 & b_n & c_n & a_n \end{pmatrix}$$

Since $|A| = a_n\Delta_{2,n-1} - c_n|D| + b_n|E|$, $|D| = b_{n-1}\Delta_{2,n-2}$ and $|E| = b_{n-1}b_{n-2}\Delta_{2,n-3}$, by Theorem 3.1 we have

$$\begin{aligned} \Psi_{1,n} &= a_1\{a_n\Delta_{2,n-1} - c_nb_{n-1}\Delta_{2,n-2} + b_nb_{n-1}b_{n-2}\Delta_{2,n-3}\} \\ &\quad -b_1b_2(a_n\Delta_{3,n-1} - c_nb_{n-1}\Delta_{3,n-2} + b_nb_{n-1}b_{n-2}\Delta_{3,n-3}) \\ &\quad +c_1c_2c_3(a_n\Delta_{4,n-1} - c_nb_{n-1}\Delta_{4,n-2} + b_nb_{n-1}b_{n-2}\Delta_{4,n-3}) \\ &= (a_1\Delta_{2,n} - b_1c_2\Delta_{3,n} + c_1c_2c_3\Delta_{4,n}) \\ &\quad +(a_1\Delta_{2,n-3} - b_1c_2\Delta_{3,n-3} + c_1c_2c_3\Delta_{4,n-3})b_nb_{n-1}b_{n-2} \\ &= \Delta_{1,n} + c_1c_2c_3\Delta_{4,n} + b_nb_{n-1}b_{n-2}\Delta_{1,n-3} + c_1c_2c_3b_nb_{n-1}b_{n-2}\Delta_{4,n-3} \\ &= \Delta_{1,n} + \prod_{k=1}^{3} c_k\Delta_{4,n} + \prod_{k+n-2}^{n} b_k\Delta_{1,n-3} + \prod_{k=1}^{3} c_k \prod_{k+n-2}^{n} b_k\Delta_{4,n-3} \end{aligned}$$

□

Corollary 5.4. [12] *Let $q = 2$, $n \geq 7$ and $b_k = c_k = 1, d_k = 0$ or 1, where $k = 1, \cdots, n$. Then*

$$\Psi_{1,n} = \Delta_{1,n} + \Delta_{4,n} + \Delta_{1,n-3} + \Delta_{4,n-3}.$$

Theorem 5.5. *Let $a_1 = a_4, b_1 = b_4, c_1 = c_4$, $c_2 = c_5$ and $n \geq 7$. Then*

$$\Psi_{1,n} = a_1\Psi_{2,n} - b_1c_2\Psi_{3,n}.$$

Proof.

$$\begin{aligned}
\Psi_{1,n} &= a_1\Delta_{2,n} - b_1c_2\Delta_{3,n} + c_1c_2c_3\Delta_{4,n} + a_1b_nb_{n-1}b_{n-2}\Delta_{2,n-3} \\
&\quad -b_1c_2b_nb_{n-1}b_{n-2}\Delta_{3,n-3} + c_1c_2c_3b_nb_{n-1}b_{n-2}\Delta_{4,n-3} \\
&= a_1(\Delta_{2,n} + \prod_{k=n-2}^{n} b_k\Delta_{2,n-3}) - b_1c_2(\Delta_{3,n} + \prod_{k=n-2}^{n} b_k\Delta_{3,n-3}) \\
&\quad + \prod_{k=1}^{3} c_k(\Delta_{4,n} + \prod_{k=n-2}^{n} b_k\Delta_{4,n-3}) \\
&= a_1(\Psi_{2,n} - \prod_{k=1}^{3} c_k\Delta_{5,n} - \prod_{k=n-2}^{n} b_k \prod_{k=1}^{3} c_k\Delta_{5,n-3}) - b_1c_2(\Psi_{3,n} - \prod_{k=1}^{3} c_k\Delta_{6,n} \\
&\quad - \prod_{k=n-2}^{n} b_k \prod_{k=1}^{3} c_k\Delta_{6,n-3}) + \prod_{k=1}^{3} c_k(\Delta_{4,n} + \prod_{k=n-2}^{n} b_k\Delta_{4,n-3}) \\
&\qquad \text{because } c_1 = c_4, c_2 = c_5 \text{ and} \Psi_{j,n} = \Delta_{j,n} + \prod_{k=n-2}^{n} b_k\Delta_{j,n-3} + \prod_{k=j}^{j+2} c_k\Delta_{j+3,n} \\
&\quad + \prod_{k=n-2}^{n} b_k \prod_{k=j}^{j+2} c_k\Delta_{j+3,n-3}, j = 2, 3 \\
&= a_1\Psi_{2,n} - b_1c_2\Psi_{3,n} - \prod_{k=1}^{3} c_k(a_1\Delta_{5,n} - b_1c_2\Delta_{6,n} - \Delta_{4,n}) \\
&\quad - \prod_{k=n-2}^{n} b_k \prod_{k=1}^{3} c_k(a_1\Delta_{5,n-3} - b_1c_2\Delta_{6,n-3} - \Delta_{4,n-3}) \text{ by Theorem 3.1} \\
&= a_1\Psi_{2,n} - b_1c_2\Psi_{3,n}
\end{aligned}$$

□

Corollary 5.6. [12] *Let $q = 2$ and $b_k = c_k = 1, d_k = 0$ or 1, where $k = 1, \cdots, n$ and $n \geq 7$. Then*

$$\Psi_{1,n} = \Psi_{2,n} + \Psi_{3,n}.$$

References

[1] P.H. Bardell, "Analysis of cellular automata used as pseudorandom pattern generators", *Proc. IEEE int. Test. Conf.*, 1990, pp. 762-767.

[2] Kevin Cattell and Jon C. Muzio, "Analysis of one-dimensional linear hybrid cellular automata over $GF(q)$", *IEEE Trans. Computers*, **Vol. 45, No. 7**, 1996, pp. 782-792.

[3] Kevin Cattell and Jon C. Muzio, "Synthesis of One-Dimensional Linear Hybrid Cellular Automata", *IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems*, **Vol. 15, No. 3**, 1996, pp. 325-335.

[4] P.P. Chaudhuri, D.R. Chowdhury, S. Nandy and Chattopadhyay, *Additive Cellular Automata Theory and Applications*, **1**, IEEE Computer Society Press, California, 1997.

[5] A.K. Das and P.P. Chaudhuri, "Efficient characterization of cellular automata", *Proc. IEE(Part E)*, **Vol. 137, No. 1**, 1990, pp. 81-87.

[6] A. K. Das and P. P. Chaudhuri, "Vector space theoritic analysis of additive cellular automata and its application for pseudo-exhaustive test pattern generation", *IEEE Trans. Comput.*, **Vol. 42**, 1993, pp. 340-352.

[7] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, **Cambridge, U.K.**, Cambridge Univ. Press, 1987.

[8] R.J. McEliece, *Finite fields for computer scientists and engineers*, **Boston**, Kluwer, 1987.

[9] 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.

[10] S. Wolfram, *Universality and complexity in cellular automata, Physica*, **Vol. 10D**, 1984, pp. 1-35.

[11] S. Wolfram, *Statistical mechanics of cellular automata, Rev. Modern Physics*, **Vol. 55, No. 3**, 1983.

[12] S.Y. Yoon, *Characterizations of one-dimensional cellular automata*, **To be submitted**, 2000.

Department of Applied Mathematics
Pukyong National University
Pusan 608-737

KOREA
e-mail: sjcho@dolphin.pknu.ac.kr

Department of Computational Mathematics
Inje University
Kimhae 621-749
KOREA
e-mail: mathkhd@ijnc.inje.ac.kr