J. Appl. Math. & Informatics Vol. **37***(2019), No. 1 - 2, pp. 23 - 35*
https://doi.org/10.14317/jami.2019.023

ANALYSIS OF THE 90/150 CA GENERATED BY LINEAR RULE BLOCKS

SUNG-JIN CHO, HAN-DOO KIM*, UN-SOOK CHOI, JIN-GYOUNG KIM AND SUNG-WON KANG

Abstract. Self-reciprocal polynomials are important because it is possible to specify only half of the coefficients. The special case of the self-reciprocal polynomial, the maximum weight polynomial, is particularly important. In this paper, we analyze even cell 90/150 cellular automata with linear rule blocks of the form $< a_1, \cdots, a_n, d_1, d_2, b_n, \cdots, b_1 >$. Also we show that there is no 90/150 CA of the form $< U_n|R_2|U_n^* >$ or $< \overline{U_n}|R_2|\overline{U_n^*} >$ whose characteristic polynomial is $f_{2n+2}(x) = x^{2n+2} + \cdots + x + 1$ where $R_2 =< d_1, d_2 >$ and $U_n =< 0, \cdots, 0 >$, and $\overline{U_n} =< 1, \cdots, 1 >$.

AMS Mathematics Subject Classification : 97N70, 11G25, 94A55, 68Q87.
Key words and phrases : CA-polynomial, Self-reciprocal polynomial, Symmetric transition rule, Maximum weight polynomial, Linear rule blocks.

1. Introduction

Cellular Automata(CA) were originally introduced by Von Neumann in early 1950's in order to study the logical properties of self-reproducing machines. Wolfram in early 1980's suggested a simplified two-state three-neighborhood 1-D CA with cells arranged linearly in one dimension [1]. CA has a simple, regular, modular and cascadable structure with logical neighborhood interconnection. The simple structure of CA with logical interconnections is ideally suited for hardware implementation [2]. For these reasons CA have been used for various applications such as pattern classification, cryptography, and pseudorandom-number generation, etc. ([3] $\sim$ [7]). In this paper, we analyze 90/150 cellular automata with transition rules of the form $< T_n|R_2|B_n >$, where $T_n =< a_1, a_2, \cdots, a_n >$ and $R_2 =< d_1, d_2 >$, and $B_n =< b_n, b_{n-1}, \cdots, b_1 >$. Also we show that there

Received August 30, 2018. Revised October 25, 2018. Accepted November 2, 2018.
*Corresponding author.

is no 90/150 CA of the form $< U_n|R_2|U_n^* >$ or $< \overline{U_n}|R_2|\overline{U_n^*} >$ whose characteristic polynomial is $f_{2n+2}(x) = x^{2n+2} + \cdots + x + 1$ where $R_2 =< d_1, d_2 >$ and $U_n =< 0, \cdots, 0 >$, and $\overline{U_n} =< 1, \cdots, 1 >$.

2. Preliminaries

A CA consists of a number of interconnected cells arranged spatially in a regular manner [1]. In most simple case, a CA cell can exhibit two different states(0 or 1) and the next state of each cell depends on the present states of its three neighborhoods including itself. The state s_i^{t+1} of the ith cell at time $(t+1)$ is denoted as

$$s_i^{t+1} = f_i(s_{i-1}^t, s_i^t, s_{i+1}^t),$$

where s_i^t denotes the state of the ith cell at time t and f_i is the next state function called the rule of the CA. If the next state generating logic employs only XOR logic then it is called a *linear rule*. And a CA with all the cells having linear rules is called a *linear CA* [2]. Since a linear CA employs XOR logic only as the next state function, it can be represented as a matrix referred to as the *state transition matrix* over $GF(2)$. An n-cell CA is characterized by an $n \times n$ state transition matrix. The state transition matrix T is constructed as

$$T = \begin{pmatrix} d_1 & a_{1,2} & 0 & \cdots & 0 & 0 \\ a_{2,1} & d_2 & a_{2,3} & \cdots & 0 & 0 \\ 0 & a_{3,2} & d_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & a_{n,n-1} & d_n \end{pmatrix}$$

$$a_{i,j} = \begin{cases} 1, & if\ the\ next\ state\ of\ the\ ith\ cell\ depends\ on\ the\ present\ state \\ & of\ the\ jth\ cell \\ 0, & otherwise. \end{cases}$$

And $a_{i,i} = d_i$, $i = 1, 2, \cdots, n$.

In this paper, a CA is a null-boundary 90/150 CA fully specified by which cells use 90 and 150. The transition rules 90 and 150 are defined as follows:

$$\begin{array}{rcl} \text{Rule 90} & : & s_i^{t+1} = s_{i-1}^t \oplus s_{i+1}^t \\ \text{Rule 150} & : & s_i^{t+1} = s_{i-1}^t \oplus s_i^t \oplus s_{i+1}^t \end{array}$$

According to rule 90, the value of a particular site s_i^{t+1} is the sum modulo 2 of the values of its two neighboring sites on the previous time step t. Rule 150 also includes the value of site s_i^t. A natural form for the specification of 90/150 CA is an n-tuple $< d_1, d_2, \cdots, d_n >$, called the *linear rule block*, where $d_i = 0$ (resp. 1) if ith cell uses rule 90(resp. 150).

A polynomial is said to be a *CA-polynomial* if it is the characteristic polynomial of some 90/150 CA. All irreducible polynomials are CA-polynomials [3] and reducible polynomials which are power of irreducible polynomial are also

CA-polynomials [8]. However, there is no criterion for whether a reducible polynomial is a CA-polynomial or not.

In [3], Cattell et al. proposed a method for the synthesis of one-dimensional 90/150 Linear Hybrid Group CA(LHGCA) for irreducible polynomial. Cho et al. [9] proposed a new efficient method for the synthesis of one-dimensional 90/150 LHGCA for any CA-polynomial as well as irreducible polynomial by using Lanczos tridiagonalization algorithm. Sabater et al. [4] and Cho et al. [6] proposed a method of constructing a linear 90/150 CA with characteristic polynomial $f(x)^{2^m}$ by concatenating the basic automaton whose characteristic polynomial is $f(x)$, which is irreducible. In this paper, we give a simpler proof of the result of Sabater et al. [4] and Cho et al. [6].

3. Characteristic polynomial of the linear rule block $< T_n|R_2|B_n >$

Let $GF(2)$ be the finite field with two elements. Throughout, all polynomials are assumed to be in $GF(2)[x]$. The characteristic polynomial Δ_n of an n-cell 90/150 CA $\mathbf{C}_n$ is defined by $\Delta_n = |T_n \oplus xI_n|$ where x is an indeterminate, I_n is the $n \times n$ identity matrix and T_n is the linear rule block of $\mathbf{C}_n$. Then the following recurrence relation holds:

$$\Delta_n = (x + d_n)\Delta_{n-1} + \Delta_{n-2} \tag{3.1}$$

where $\Delta_1 = x + d_1$, $\Delta_0 = 1$ [3]. Eq. (3.1) provides an efficient algorithm to compute Δ_n of a given n-cell 90/150 CA. We denote the characteristic polynomial of *sub-CA* consisting of cells i through j by $\Delta_{i,j}$, where $i \leq j$. We simply denote $\Delta_{1,i}$ by Δ_i. Δ_i is said to be a *CA-subpolynomial.* Let T_n^* be the linear rule block corresponding to the linear rule block T_n of an n-cell 90/150 CA as the following $T_n^* =< a_n, \cdots , a_2, a_1 >$ and let Δ_n^* be the characteristic polynomial of T_n^*. Then $\Delta_n^* = \Delta_n$.
For any n-cell 90/150 CA whose linear rule block is T_n, the minimal polynomial for T_n is the same as the characteristic polynomial for T_n [2].

Definition 3.1 ([10])**.** Let $T_n =< a_1, a_2, \cdots , a_n >$ be the linear rule block of an n-cell 90/150 CA. Then $< T_n|T_n^* >=< a_1, a_2, \cdots , a_n, a_n, \cdots , a_2, a_1 >$ is called the *CA with symmetric transition rule.*

If A, B, and M differ only in the ith row (or column), and the ith row (or column) of M is the sum of the ith rows (or columns) of A and B, then

$$|M| = |A| + |B| \tag{3.2}$$

Hereafter, we denote the linear rule block $< a_1, a_2, \cdots , a_n >$ of an n-cell 90/150 CA $\mathbf{C}$ by T_n.

Lemma 3.2 ([10])**.** *Let V_{2n} be the characteristic polynomial of $< T_n|T_n^* >$. Then*

(i) $V_{2n} = (\Delta_n + \Delta_{n-1})^2$.
(ii) Let $T_{\overline{n}} =< a_1, \cdots, a_{n-1}, \overline{a_n} >$ *be the linear rule block of an* n*-cell 90/150 CA and let* $\Delta_{\overline{n}}$ *be the characteristic polynomial of* $T_{\overline{n}}$*. Then* $V_{2n} = (\Delta_{\overline{n}})^2$.
(iii) Let D_1 *be the characteristic polynomial of the 1-cell 90/150 CA* $< d >$*. Let* $M_{2n+1} =< a_1, a_2, \cdots, a_n|d|a_n, \cdots, a_2, a_1 >$ *be the linear rule block of a* $(2n+1)$*-cell 90/150 CA* $\mathbf{C}_{2n+1}$*. And let* V_{2n+1} *be the characteristic polynomial of* M_{2n+1}*. Then* $V_{2n+1} = D_1\Delta_n^2$.

Hereafter, we denote the characteristic polynomial of the n-cell 90/150 CA $< 0, \cdots, 0 >$ by $U_n(x)$. And we denote the characteristic polynomial of the n-cell 90/150 CA $< 1, 0, \cdots, 0 >$ by $h_n(x)$.

Lemma 3.3 ([11])**.** *We have*

$$\begin{aligned} U_n(x) &= x^{2^n} + x^{2(2^{n-1}-1)} + x^{2^2(2^{n-2}-1)} + x^{2^3(2^{n-3}-1)} + \cdots + x^{2^{n-3}(2^3-1)} \\ &\quad + x^{2^{n-2}(2^2-1)} + x^{2^{n-1}} + 1. \end{aligned}$$

The following lemma is the result of [12]. Here, the result is represented by a relation between $U_n(x)$ and $h_n(x)$.

Lemma 3.4. *We have*

$$U_n(x) = \begin{cases} \{h_{n/2}(x)\}^2, & n \text{ is even} \\ x\{U_{\frac{n-1}{2}}(x)\}^2, & n \text{ is odd.} \end{cases}$$

Lemma 3.5. *We have*
(i) $h_n(x) = xh_{n-1}(x) + h_{n-2}(x)$ $(n \geq 1), (h_0(x) := 1, h_{-1}(x) := 1)$.
(ii) $h_n(x) = (x+1)U_{n-1}(x) + U_{n-2}(x)$ $(n \geq 1), (U_0(x) := 1, U_{-1}(x) := 0)$.
(iii) $h_n(x) = U_n(x) + U_{n-1}(x)$ $(n \geq 1)$.
(iv) $h_0(x) + h_1(x) + \cdots + h_n(x) = U_n(x)$ $(n \geq 1)$.

Proof. Part (i) and Part (ii) are the basic properties of the recurrence relation. Using Eq. (3.2) we have

$$\begin{aligned} h_n(x) &= \begin{vmatrix} x+1 & 1 & 0 & \cdots & 0 & 0 \\ 1 & x & 1 & \cdots & 0 & 0 \\ 0 & 1 & x & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & x \end{vmatrix} \\ &= \begin{vmatrix} x & 1 & 0 & \cdots & 0 & 0 \\ 1 & x & 1 & \cdots & 0 & 0 \\ 0 & 1 & x & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & x \end{vmatrix} + \begin{vmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & x & 1 & \cdots & 0 & 0 \\ 0 & 1 & x & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & x \end{vmatrix} \\ &= U_n(x) + U_{n-1}(x) \end{aligned}$$

Part (iv) follows from Part (iii).

□

For the polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ over $GF(2)$ of degree n, the *weight* $w(f)$ of $f(x)$ is defined to be the number of nonzero coefficients of $f(x)$. The polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ over $GF(2)$ of degree n with $w(f) = n+1$ is called the *maximum weight polynomial.* Hereafter, we denote the polynomial of degree n with maximum weight by $f_n(x)$. The *reciprocal* $f^*(x)$ of a polynomial $f(x)$ of degree n over $GF(2)$ is defined by $f^*(x) = x^n f(x^{-1})$. The polynomial $f(x)$ is called *self-reciprocal* if $f^*(x) = f(x)$. The fact that self-reciprocal polynomials are given by specifying only half of their coefficients is of importance [5]. Self-reciprocal irreducible polynomials over finite fields have been studied by many authors. In [13], Meyn studied the construction of self-reciprocal irreducible polynomials over binary fields. The self-reciprocal polynomial applies to the design of reversible error correcting codes with a reverse read property and to the efficient implementation of LFSRs. Such reversible codes are advantageous in certain data storage systems that can read data in bi-direction.

Baum et al. [14] showed the following fact: For a given polynomial $q(x)$ over $GF(2)$, the number of polynomials $p(x)$ over $GF(2)$ for which $\frac{p(x)}{q(x)} = [0; a_1, a_2, \cdots, a_n]$ with $deg(a_i) = 1$ for all i is either 0 or a power of two where $[0; a_1, a_2, \cdots, a_n]$ is the continued fraction of $p(x)/q(x)$. Using results of Baum et al. [14], Mesirov et al. [15] showed the following fact: If a polynomial $q(x)$ over $GF(2)$ has k distinct irreducible factors different from x and $x+1$, and if there is a polynomial $p(x)$ over $GF(2)$ for which $\frac{p(x)}{q(x)} = [0; a_1, a_2, \cdots, a_n]$ with $deg(a_i) = 1$ for all i, then there are 2^k such $p(x)$. Since $f'_{2m}(x) = \{f_{m-1}(x)\}^2 \neq 0$, $f_{2m}(x)$ is square-free. And $f_{2m}(x)$ does not have x or $x+1$ as a factor. Choi et al. [8] proved the following theorem by associating continued fraction $[0; a_n, a_{n-1}, \cdots, a_1]$ with n-cell 90/150 CA $< a_1, a_2, \cdots, a_n >$.

Example 3.1. For the CA-polynomial $f_{14}(x) = (x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1)$, there are 2^4 90/150 CA with the characteristic polynomial $f_{14}(x)$:

$$\begin{array}{lcl}
< 0,0,0,1,1,0|0,1|0,1,1,0,0,0 > & , & < 0,0,1,0,1,0|0,1|0,1,0,1,0,0 > \\
< 0,1,0,0,1,0|0,1|0,1,0,0,1,0 > & , & < 0,1,1,0,1,1|0,1|1,1,0,1,1,0 > \\
< 1,0,0,1,0,0|0,1|0,0,1,0,0,1 > & , & < 1,0,1,1,0,1|0,1|1,0,1,1,0,1 > \\
< 1,1,0,1,0,1|0,1|1,0,1,0,1,1 > & , & < 1,1,1,0,0,1|0,1|1,0,0,1,1,1 > \\
< 0,0,0,1,1,0|1,0|0,1,1,0,0,0 > & , & < 0,0,1,0,1,0|1,0|0,1,0,1,0,0 > \\
< 0,1,0,0,1,0|1,0|0,1,0,0,1,0 > & , & < 0,1,1,0,1,1|1,0|1,1,0,1,1,0 > \\
< 1,0,0,1,0,0|1,0|0,0,1,0,0,1 > & , & < 1,0,1,1,0,1|1,0|1,0,1,1,0,1 > \\
< 1,1,0,1,0,1|1,0|1,0,1,0,1,1 > & , & < 1,1,1,0,0,1|1,0|1,0,0,1,1,1 >.
\end{array}$$

Theorem 3.6. *If $f_n(x)$ (n is even) is a CA-polynomial and has k distinct irreducible factors, then there are 2^k 90/150 CA whose characteristic polynomial is $f_n(x)$.*

From now on, the characteristic polynomial of the n-cell 90/150 CA $< a_1, \cdots, a_n >$ may simply be expressed as $< a_1, \cdots, a_n >$ if necessary.

Lemma 3.7. *Let $V_{2n+2}(x)$ be the characteristic polynomial of $< T_n|d_1, d_2|T_n^* >$. If $V_{2n+2}(x) = f_{2n+2}(x)$, then $d_1 \neq d_2$.*

Proof. Suppose that $d_1 = d_2$. Then $< T_n|d_1, d_2|T_n^* >=< T_{n+1}|T_{n+1}^* >$ where $T_{n+1} =< T_n|d_1 >$. By Lemma 3.2 (ii), the characteristic polynomial of $< T_n|d_1, d_2|T_n^* >$ is $< T_n|\overline{d_1} >^2$. But $V_{2n+2}(x) =< T_n|\overline{d_1} >^2$ is not equal to $f_{2n+2}(x)$ because $f_{2n+2}(x)$ is square-free. □

Corollary 3.8. *Characteristic polynomials of $< T_n|0, 0|T_n^* >$ and $< T_n|1, 1|T_n^* >$ are not equal to $f_{2n+2}(x)$.*

Thus the transition rule of the CA with the characteristic polynomial $f_{2n+2}(x)$ may be only in $< T_n|0, 1|T_n^* >$ or $< T_n|1, 0|T_n^* >$. Since the characteristic polynomials of $< T_n|0, 1|T_n^* >$ and $< T_n|1, 0|T_n^* >$ are the same, only the linear rule block $< T_n|0, 1|T_n^* >$ needs to be investigated.
Sabater et al. [4] and Cho et al. [6] analyzed the linear rule block $< T_n|T_n^* >$ and Cho et al. ([10], [16]) analyzed various extended forms of $< T_n|T_n^* >$. Here we analyze the characteristic polynomial of the most general linear rule block $< T_n|R_2|B_n >$. The calculation of the characteristic polynomial of linear rule block is usually performed by cofactor expansion for the last row, but as in the proof of the following theorem, the cofactor expansion for the row corresponding to the last cell of the second rule block simplifies the calculation of the characteristic polynomial.

Theorem 3.9. *Let $B_n =< b_n, \cdots, b_2, b_1 >$ be the linear rule block of an n-cell 90/150 CA. Let $< T_n|R_2|B_n >$ be the linear rule block of a $(2n+2)$-cell 90/150 CA $\mathbf{C_{2n+2}}$ where $R_2 =< d_1, d_2 >$. Let $V_{2n+2}(x)$ be the characteristic polynomial of $< T_n|R_2|B_n >$. Then*

$$V_{2n+2}(x) = D_2\Delta_n\nabla_n + (x + d_1)\Delta_n\nabla_{n-1} + (x + d_2)\Delta_{n-1}\nabla_n + \Delta_{n-1}\nabla_{n-1}$$

, where D_2 is the characteristic polynomial of the 2-cell 90/150 CA R_2 and Δ_{n-1} is the characteristic polynomial of $< a_1, a_2, \cdots, a_{n-1} >$ and Δ_n is the characteristic polynomial of T_n and ∇_{n-1} is the characteristic polynomial of $< b_{n-1}, \cdots, b_2, b_1 >$, and ∇_n is the characteristic polynomial of B_n.

Proof. Let $M(i : j)$ denote the submatrix obtained by removing the ith row and the jth column of M. By cofactor expansion along the $(n + 2)$th row, we have

$$\begin{aligned} V_{2n+2}(x) &= \{(x+d_1)\Delta_n + \Delta_{n-1}\}(x+d_2)\nabla_n \\ &\quad +1\cdot|M(n+2:n+1)| + 1\cdot|M(n+2:n+3)| \\ &= \{(x+d_1)\Delta_n + \Delta_{n-1}\}(x+d_2)\nabla_n + \Delta_n\nabla_n \\ &\quad +\{(x+d_1)\Delta_n + \Delta_{n-1}\}\nabla_{n-1} \\ &= \{(x+d_1)(x+d_2)+1\}\Delta_n\nabla_n + (x+d_1)\Delta_n\nabla_{n-1} \\ &\quad +(x+d_2)\Delta_{n-1}\nabla_n + \Delta_{n-1}\nabla_{n-1} \\ &= D_2\Delta_n\nabla_n + (x+d_1)\Delta_n\nabla_{n-1} + (x+d_2)\Delta_{n-1}\nabla_n + \Delta_{n-1}\nabla_{n-1}, \end{aligned}$$

where $M =< T_n, R_2, B_n > +xI_{2n+2}$. □

Corollary 3.10. *Let $B_n =< b_n, \cdots, b_2, b_1 >$ be the linear rule block of an n-cell 90/150 CA. Then the characteristic polynomial $V_{2n+2}(x)$ of $< T_n|R_2|B_n >$ is as follows:*

$$V_{2n+2}(x) = \Delta_{n+1}\nabla_{n+1} + \Delta_n\nabla_n$$

, where $R_2 =< d_1, d_2 >$ and $\Delta_{n+1} =< T_n|d_1 >$, and $\nabla_{n+1} =< d_2|B_n >$.

Now we investigate the characteristic polynomial of $< T_n|R_2|B_n >$ where $B_n = T_n^*$. Using Theorem 3.9 we can prove

Theorem 3.11 ([16]). *The characteristic polynomial $V_{2n+2}(x)$ of $< T_n|R_2|T_n^* >$ is $V_{2n+2}(x) = D_2\Delta_n^2 + (d_1+d_2)\Delta_n\Delta_{n-1} + \Delta_{n-1}^2$, where D_2 is the characteristic polynomial of the 2-cell 90/150 CA $R_2 =< d_1, d_2 >$.*

Theorem 3.11 provides the more simple proof of the following Sabater' result [4]:

Corollary 3.12. *We have*

$$< a_1, a_2, \cdots, a_n, \overline{a_{n+1}}, \overline{a_{n+1}}, a_n, \cdots, a_1 >=< a_1, \cdots, a_n, a_{n+1} >^2 .$$

Proof. For $< d_1, d_2 >=< \overline{a_{n+1}}, \overline{a_{n+1}} >$, since $D_2 = x^2 + a_{n+1}$, using Theorem 3.11 we have

$$\begin{aligned} &< a_1, a_2, \cdots, a_n, \overline{a_{n+1}}, \overline{a_{n+1}}, a_n, \cdots, a_1 > \\ =\ & (x^2 + a_{n+1})\Delta_n^2 + \Delta_{n-1}^2 \\ =\ & \{(x + a_{n+1})\Delta_n + \Delta_{n-1}\}^2 \\ =\ & < a_1, \cdots, a_n, a_{n+1} >^2. \end{aligned}$$

□

Corollary 3.13. *The characteristic polynomial $V_{2n+2}(x)$ of $< T_n|0,1|T_n^* >$ is $(\Delta_{n+1} + \Delta_n)^2 + \Delta_{n+1}\Delta_n$ where $\Delta_{n+1} =< T_n|0 >= x\Delta_n + \Delta_{n-1}$.*

Proof. Using Theorem 3.11 we have

$$\begin{aligned} V_{2n+2}(x) &= (x^2+x+1)\Delta_n^2 + \Delta_n\Delta_{n-1} + \Delta_{n-1}^2 \\ &= (x\Delta_n + \Delta_{n-1})^2 + (x\Delta_n + \Delta_{n-1})\Delta_n + \Delta_n^2 \\ &= \Delta_{n+1}^2 + \Delta_n^2 + \Delta_{n+1}\Delta_n \\ &= (\Delta_{n+1} + \Delta_n)^2 + \Delta_{n+1}\Delta_n \end{aligned}$$

where $\Delta_{n+1} =< T_n|0 >= x\Delta_n + \Delta_{n-1}$.

□

Example 3.2. (i) $< 0, 0, 0, 0, 0, 0, 0, 0 >= (x^4 + x^3 + x^2 + 1)^2 = \{h_4(x)\}^2$.
(ii) $< 0, 0, 0, 0, 0, 0, 0, 0, 0, 0 >= (x^5 + x^4 + x^2 + x + 1)^2 = \{h_5(x)\}^2$.

4. Analysis of the n-cell 90/150 CA corresponding to $f_n(x)$

In [8], we performed several studies on 90/150 CA corresponding to $f_n(x)$. In [17], we gave a necessary and sufficient condition for finding a 90/150 CA whose characteristic polynomial is $f_n(x)$. In this section, we use this condition to show that there is no 90/150 CA of the form $< U_n|R_2|U_n^* >$ or $< \overline{U_n}|R_2|\overline{U_n^*} >$ whose characteristic polynomial is $f_{2n+2}(x) = x^{2n+2} + \cdots + x + 1$ where $R_2 =< d_1, d_2 >$ and $U_n =< 0, \cdots, 0 >$, and $\overline{U_n} =< 1, \cdots, 1 >$.

Theorem 4.1 ([17])**.** *Let Δ_n be the characteristic polynomial of an n-cell 90/150 CA $T_n =< a_1, a_2, \cdots, a_n >$ and let $V_{2n+2}(x)$ be the characteristic polynomial of the $(2n + 2)$-cell 90/150 CA $< T_n|0, 1|T_n^* >$. Then the following are equivalent:*
(1) $V_{2n+2}(x) = f_{2n+2}(x)$.
(2) $(\Delta_{n+1}\Delta_n)' = \{f_n(x)\}^2$.
(3) $f_n(x) = \sum_{i=0}^{n} \Delta_i$.

Theorem 4.1 shows that if $f_n(x) = \sum_{i=0}^{n} \Delta_i$, then $< T_n|0, 1|T_n^* >$ is 90/150 CA corresponding to $f_{2n+2}(x)$ where Δ_n is the characteristic polynomial of $T_n =< a_1, a_2, \cdots, a_n >$. Using Theorem 4.1 we can prove

Corollary 4.2. *Let $< T_n|0, 1|T_n^* >= f_{2n+2}(x)$. Then $a_1 + a_2 + \cdots + a_n \equiv 0$ $(mod\ 2)$.*

Proof. By Theorem 4.1, $f_n(x) = \sum_{i=0}^{n} \Delta_i$. Since the coefficient of x^{n-1} in Δ_n is $a_1 + a_2 + \cdots + a_n$, we have $a_1 + a_2 + \cdots + a_n \equiv 0$ $(mod\ 2)$ because $f_n(x) = \sum_{i=0}^{n} \Delta_i$. □

Corollary 4.3. *If there is no n-cell 90/150 CA $T_n =< a_1, a_2, \cdots, a_n >$ with $f_n(x) = \sum_{i=0}^{n} \Delta_i$, then the transition rule of $f_{2n+2}(x)$ is not of the form $< T_n|0, 1|T_n^* >$.*

From now on, we analyze the n-cell 90/150 CA $T_n =< a_1, a_2, \cdots, a_n >$ with $f_n(x) = \sum_{i=0}^{n} \Delta_i$.

Example 4.1. There is no 2-cell 90/150 CA $T_2 =< a_1, a_2 >$ of $f_6(x)$ of the form $< T_2|0, 1|T_2^* >=< a_1, a_2, 0, 1, a_2, a_1 >$.
For each $a_1, a_2 \in \{0, 1\}^2$, the following holds:

$$\begin{aligned} \sum_{i=0}^{2} \Delta_i &= (x + \overline{a_2})\Delta_1 = (x + \overline{a_2})(x + a_1) \\ &= x^2 + (a_1 + \overline{a_2})x + a_1\overline{a_2} \\ &\neq f_2(x). \end{aligned}$$

From Theorem 4.1, $V_6(x) \neq f_6(x)$.

Remark 4.1. There is no 2-cell 90/150 CA $T_2 =< a_1, a_2 >$ of $f_6(x)$ of the form $< T_2|d_1, d_2|T_2^* >=< a_1, a_2, d_1, d_2, a_2, a_1 >$.

Example 4.2. Since the CA-polynomial $f_8(x)$ is $(x^2+x+1)(x^6+x^3+1)$, by Theorem 3.6, there are 2^2 90/150 CA with the characteristic polynomial $f_8(x)$. We can find those four 90/150 CA using Theorem 4.1.

For each $a_1, a_2, a_3 \in \{0, 1\}^3$, suppose that $\sum_{i=0}^{3} \Delta_i = f_3(x)$ holds:
Now, we have

$$\begin{array}{rcl} \sum_{i=0}^{3} \Delta_i &=& x^3 + (a_1 + a_2 + \overline{a_3})x^2 + \{a_1a_2 + (a_1 + a_2)\overline{a_3} + 1\}x \\ &+& a_1a_2\overline{a_3} + a_3. \end{array}$$

This implies $a_1 + a_2 + \overline{a_3} = 1, a_1a_2 + (a_1 + a_2)\overline{a_3} = 0, a_1a_2\overline{a_3} + a_3 = 1$.
It follows directly that the solution (a_1, a_2, a_3) is $(0, 1, 1)$ or $(1, 0, 1)$.
Hence there are only four 8-cell 90/150 CA with the characteristic polynomial $f_8(x)$:

$$\begin{array}{ccc} < 0,1,1,0,1,1,1,0 > & , & < 0,1,1,1,0,1,1,0 > \\ < 1,0,1,0,1,1,0,1 > & , & < 1,0,1,1,0,1,0,1 > \end{array}$$

Theorem 4.4. *For $n \geq 2$, the characteristic polynomial $V_{2n+2}(x)$ of the $(2n+2)$-cell 90/150 CA $< U_n|0, 1|U_n^* >$ is not equal to $f_{2n+2}(x)$.*

Proof. For $n = 2$ we showed that $< 0, 0, d_1, d_2, 0, 0 >$ is not equal to $f_6(x)$ in Example 4.1.

(i) For the case $n = 2m (m \geq 2)$:
By Lemma 3.4, we have

$$\begin{array}{rl} & \Delta_{2m} + \Delta_{2m-1} + \cdots + \Delta_1 + \Delta_0 \\ = & (\Delta_{2m} + \Delta_{2m-2} + \cdots + \Delta_2 + \Delta_0) \\ + & (\Delta_{2m-1} + \Delta_{2m-3} + \cdots + \Delta_3 + \Delta_1) \\ = & \{h_m(x) + h_{m-1}(x) + \cdots + h_1(x) + h_0(x)\}^2 \\ + & x\{U_{m-1}(x) + U_{m-2}(x) + \cdots + U_1(x) + U_0(x)\}^2. \end{array}$$

Suppose that $f_{2m}(x) = \sum_{i=0}^{2m} \Delta_i$. Then

$$\begin{array}{rl} & \{h_m(x) + h_{m-1}(x) + \cdots + h_1(x) + h_0(x)\}^2 \\ = & x^{2m} + x^{2m-2} + \cdots + x^2 + 1 \\ = & (x^m + x^{m-1} + \cdots + x + 1)^2 \\ = & \{f_m(x)\}^2 \end{array}$$

and

$$\begin{array}{rl} & x\{U_{m-1}(x) + U_{m-2}(x) + \cdots + U_1(x) + U_0(x)\}^2 \\ = & x^{2m-1} + x^{2m-3} + \cdots + x^3 + x \\ = & x(x^{m-1} + x^{m-2} + \cdots + x + 1)^2 \\ = & x\{f_{m-1}(x)\}^2. \end{array}$$

Thus $h_m(x)+h_{m-1}(x)+\cdots+h_1(x)+h_0(x) = f_m(x)$ and $U_{m-1}(x)+U_{m-2}(x)+\cdots + U_1(x) + U_0(x) = f_{m-1}(x)$. Now, by Lemma 3.5(ii) we have

$$\begin{array}{rcl} h_m(x) & = & (x+1)U_{m-1}(x) + U_{m-2}(x) \\ h_{m-1}(x) & = & (x+1)U_{m-2}(x) + U_{m-3}(x) \\ & \vdots & \\ h_2(x) & = & (x+1)U_1(x) + U_0(x) \\ h_1(x) & = & (x+1)U_0(x) \\ h_0(x) & = & 1. \end{array} \tag{4.1}$$

If we add each term of the above equations, then the sum of the left side is $f_m(x)$, so we obtain

$$\begin{array}{rcl} f_m(x) & = & (x+1)\{U_{m-1}(x) + U_{m-2}(x) + \cdots + U_1(x) + U_0(x)\} \\ & & +U_{m-2}(x) + U_{m-3}(x) + \cdots + U_1(x) \\ & = & (x+1)f_{m-1}(x) + \{U_{m-1}(x) + U_0(x) + f_{m-1}(x)\}. \end{array}$$

Thus $f_m(x) = xf_{m-1}(x)+U_{m-1}(x)+1 = f_m(x)+U_{m-1}(x)$. Hence $U_{m-1}(x) = 0$. This is a contradiction for $m \geq 2$. Hence by Theorem 4.1 $V_{2n+2}(x) \neq f_{2n+2}(x)$.

(ii) For the case $n = 2m-1 (m \geq 2)$:
By Lemma 3.4, we have

$$\begin{array}{rl} & \Delta_{2m-1} + \Delta_{2m-2} + \cdots + \Delta_1 + \Delta_0 \\ = & (\Delta_{2m-1} + \Delta_{2m-3} + \cdots + \Delta_3 + \Delta_1) \\ & +(\Delta_{2m-2} + \Delta_{2m-4} + \cdots + \Delta_2 + \Delta_0) \\ = & \{U_{2m-1}(x) + U_{2m-3}(x) + \cdots + U_3(x) + U_1(x)\} \\ & +\{U_{2m-2}(x) + U_{2m-4}(x) + \cdots + U_2(x) + U_0(x)\} \\ = & x\{U_{m-1}(x) + U_{m-2}(x) + \cdots + U_1(x) + U_0(x)\}^2 \\ & +\{h_{m-1}(x) + h_{m-2}(x) + \cdots + h_1(x) + h_0(x)\}^2. \end{array}$$

Suppose that $f_{2m-1}(x) = \sum_{i=0}^{2m-1} \Delta_i$. Then
$h_{m-1}(x)+h_{m-2}(x)+\cdots+h_1(x)+h_0(x) = f_{m-1}(x)$ and $U_{m-1}(x)+U_{m-2}(x)+\cdots+U_1(x)+U_0(x) = f_{m-1}(x)$.

Using Lemma 3.5, we have
$U_{m-1}(x) = f_{m-1}(x)$ and $U_{m-1}(x)+U_{m-2}(x)+\cdots+U_1(x)+U_0(x) = f_{m-1}(x)$. Thus $U_{m-2}(x) + \cdots + U_1(x) + U_0(x) = 0$. This is a contradiction for $m \geq 2$. Hence by Theorem 4.1 $V_{2n+2}(x) \neq f_{2n+2}(x)$. □

Remark 4.2. (i) In Theorem 4.4, we showed that $V_{2n+2}(x) = f_{2n+2}(x)$ when $n \geq 2$. However, the characteristic polynomial of the 4-cell 90/150 CA $< 0, 0, 1, 0 >$ is $f_4(x)$.
(ii) The characteristic polynomial of the form $< U_n|d_1, d_2|U_n^* >$ $(n \geq 2)$ is not equal to $f_{2n+2}(x)$.

Theorem 4.5. *For $n \geq 1$, the characteristic polynomial $V_{2n+2}(x)$ of the $(2n+2)$-cell 90/150 CA $< \overline{U_n}|0, 1|\overline{U_n^*} >$ is not equal to $f_{2n+2}(x)$ where $\overline{U_n} =< 1, \cdots, 1 >$.*

Proof. The characteristic polynomial $x^4 + x^3 + 1$ of the 4-cell 90/150 CA $< 1, 0, 1, 1 >$ is not equal to $f_4(x)$. For $n = 2$ we showed that $< 1, 1, d_1, d_2, 1, 1 >$

is not equal to $f_6(x)$ in Example 4.1.

(i) For the case $n = 2m (m \geq 2)$:
By Lemma 3.4, we have

$$\begin{aligned}
& \Delta_{2m} + \Delta_{2m-1} + \cdots + \Delta_1 + \Delta_0 \\
= \ & (\Delta_{2m} + \Delta_{2m-2} + \cdots + \Delta_2 + \Delta_0) \\
& + (\Delta_{2m-1} + \Delta_{2m-3} + \cdots + \Delta_3 + \Delta_1) \\
= \ & (\overline{U_{2m}}(x) + \overline{U_{2m-2}}(x) + \cdots + \overline{U_2}(x) + \overline{U_0}(x)) \\
& + (\overline{U_{2m-1}}(x) + \overline{U_{2m-3}}(x) + \cdots + \overline{U_3}(x) + \overline{U_1}(x)) \\
= \ & \{h_m(x+1) + h_{m-1}(x+1) + \cdots + h_1(x+1) + h_0(x+1)\}^2 \\
& + (x+1)\{U_{m-1}(x+1) + U_{m-2}(x+1) + \cdots + U_1(x+1) + U_0(x+1)\}^2 \ .
\end{aligned}$$

Suppose that $f_{2m}(x) = \sum_{i=0}^{2m-1} \Delta_i$. Then
$U_{m-1}(x+1) + U_{m-2}(x+1) + \cdots + U_1(x+1) + U_0(x+1) = f_{m-1}(x)$ and

$$\begin{aligned}
& (U_{m-1}(x+1) + U_{m-2}(x+1) + \cdots + U_1(x+1) + U_0(x+1)) \\
& + (h_{m-1}(x+1) + \cdots + h_1(x+1) + h_0(x+1)) \\
= \ & f_{m-1}(x).
\end{aligned}$$

Thus $U_{m-1}(x+1) = 0$. This is a contradiction for $m \geq 2$. Hence by Theorem 4.1 $V_{2n+2}(x) \neq f_{2n+2}(x)$.

(ii) For the case $n = 2m - 1 (m \geq 2)$:
By Lemma 3.4, we have

$$\begin{aligned}
& \Delta_{2m-1} + \Delta_{2m-2} + \cdots + \Delta_1 + \Delta_0 \\
= \ & (\Delta_{2m-1} + \Delta_{2m-3} + \cdots + \Delta_3 + \Delta_1) \\
& + (\Delta_{2m-2} + \Delta_{2m-4} + \cdots + \Delta_2 + \Delta_0) \\
= \ & (\overline{U_{2m-1}}(x) + \overline{U_{2m-3}}(x) + \cdots + \overline{U_3}(x) + \overline{U_1}(x)) \\
& + (\overline{U_{2m-2}}(x) + \overline{U_{2m-4}}(x) + \cdots + \overline{U_2}(x) + \overline{U_0}(x)) \\
= \ & (x+1)\{U_{m-1}(x+1) + U_{m-2}(x+1) + \cdots + U_1(x+1) + U_0(x+1)\}^2 \\
& + \{h_{m-1}(x+1) + h_{m-2}(x+1) + \cdots + h_1(x+1) + h_0(x+1)\}^2 \\
= \ & (x+1)\{U_{m-1}(x+1) + U_{m-2}(x+1) + \cdots + U_1(x+1) + U_0(x+1)\}^2 \\
& + \{h_m(x+1) + h_{m-1}(x+1) + \cdots + h_1(x+1) + h_0(x+1)\}^2.
\end{aligned}$$

Suppose that $f_{2m-1}(x) = \sum_{i=0}^{2m-1} \Delta_i$. Then
$U_{m-1}(x+1) + \cdots + U_1(x+1) + U_0(x+1) = f_{m-1}(x)$ and $U_{m-2}(x+1) + \cdots + U_1(x+1) + U_0(x+1) = f_{m-1}(x)$.

Thus $U_{m-1}(x+1) = 0$. This is a contradiction for $m \geq 2$. Hence by Theorem 4.1 $V_{2n+2}(x) \neq f_{2n+2}(x)$. □

Remark 4.3. The characteristic polynomial of the form $< \overline{U_n} | d_1, d_2 | \overline{U_n^*} >$ $(n \geq 1)$ is not equal to $f_{2n+2}(x)$.

5. Conclusion

Maximum weight polynomials over $GF(2)$ are important both in the theoretical and practical applications. In this paper, we analyzed 90/150 cellular automata with linear rule blocks of the form $< a_1, \cdots, a_n | d_1, d_2 | b_n, \cdots, b_1 >$.

This is an extension of the results of [16]. Also we showed that there is no 90/150 CA of the form $< U_n|R_2|U_n^* >$ or $< \overline{U_n}|R_2|\overline{U_n^*} >$ whose characteristic polynomial is $f_{2n+2}(x) = x^{2n+2} + \cdots + x + 1$ where $R_2 =< d_1, d_2 >$ and $U_n =< 0, \cdots, 0 >$, and $\overline{U_n} =< 1, \cdots, 1 >$.

References

1. S. Wolfram, *Statistical mechanics of cellular automata*, Rev. Modern Physics. **55** (1983), 601-644.
2. P.P. Chaudhuri, D.R. Chowdhury, S. Nandi and S. Chatterjee, *Additive Cellular Automata*, Theory and Applications **1**, Los Alamitos, California: IEEE Computer Society Press, 1997.
3. K. Cattell and J.C. Muzio, *Synthesis of one-dimensional linear hybrid cellular automata*, IEEE Trans. Comput-Aided Design Integr. Circuits Syst. **19**(2) (1996), 325-335.
4. P. C-Gil, A. F-Sabater and M.E. P-Robles, *Using linear difference equations to model nonlinear cryptographic sequences*, International Journal of Nonlinear Sciences & Numerical Simulation **11**(3) (2010), 165-172.
5. E.R. Berlekamp, *Bit-serial Reed-Solomon encoders*, IEEE Trans. Inform. Theory IT-28 (1982), 869-874.
6. S.J. Cho, U.S. Choi, H.D. Kim, Y.H. Hwang and J.G. Kim, *Analysis of 90/150 two predecessor nongroup cellular automata*, ACRI 2008, LNCS 5191 (2008), 128-135.
7. M.J. Kwon, S.J. Cho, H.D. Kim, U.S. Choi, and G.T. Kong, *Analysis of complemented group CA derived from 90/150 group CA*, J. of Applied Mathematics and Informatics **34**(3-4) (2016), 239-247.
8. U.S. Choi, S.J. Cho, H.D. Kim and J.G. Kim, *90/150 CA corresponding to polynomial of maximum weight*, J. of Cellular Automata **13**(4) (2018), 347-358.
9. S.J. Cho, U.S. Choi, H.D. Kim, Y.H. Hwang, J.G. Kim and S.H. Heo, *New synthesis of one-dimensional 90/150 linear hybrid group cellular automata*, IEEE Trans. Comput-Aided Design Integr. Circuits Syst. **26**(9) (2007), 1720-1724.
10. U.S. Choi, S.J. Cho and Gil-Tak Kong, *Analysis of characteristic polynomial of cellular automata with symmetrical transition rules*, Proceedings of the Jangjeon Mathematical Society, **18**(1) (2015), 85-93.
11. H.D. Kim, S.J. Cho and U.S. Choi, *On the construction of the 90/150 state transition matrix corresponding to the trinomial $x^{2^n-1} + x + 1$*, J. of the Korea Institute of Electronic Communication Sciences **13**(2) (2017), 383-389.
12. U.S. Choi, S.J. Cho and J.M. Yim, *Synthesis of 90/150 uniform CA and computation of characteristic polynomial corresponding to uniform CA*, J. of the Korea Institute of Electronic Communication Sciences **5**(1) (2010), 10-16.
13. H. Meyn, *On the construction of irreducible self-reciprocal polynomials over finite fields*, Appl. Alg. in Eng., Comm., and Comp. **1** (1990), 43-50.
14. E. Baum and M.M. Sweet, *Badly approximable power series in characteristic 2*, Ann. of Math. **105** (1977), 573-580.
15. J.P. Mesirov and M.M. Sweet, *Continued fraction expansions of rational expressions with irreducible denominators in characteristic 2*, Journal of Number Theory **27** (1987), 144-148.
16. H.D. Kim, S.J. Cho, U.S. Choi and J.M. Yim, *Analysis of 90/150 cellular automata with extended symmetrical transition rules*, Proc. of the Jangjeon Mathematical Society **20**(2) (2017), 193-201.
17. S.W. Kang, U.S. Choi, S.J. Cho, H.D. Kim and J.G. Kim, *Synthesis of 90/150 CA corresponding to maximum weight polynomials of even degree*, Advanced Science and Technology Letters **152** (NGCIT 2018), 125-128.

Sung-Jin Cho received the M.S. degree and the Ph.D degree at Korea University. He is currently a professor at Pukyong University since 1988. His research interests include finite field theory, discrete mathematics and cellular automata.

Department of Applied Mathematics, Pukyong National University, Busan 48513, Korea.
e-mail: sjcho@pknu.ac.kr

Han-Doo Kim received the M.S. degree and the Ph.D degree at Korea University. He is currently a professor at Inje University since 1989. His research interests include discrete mathematics and cellular automata.

Department of Computer Engineering and Institute of Basic Sciences, Inje University, Kyeongnam 50834, Korea.
e-mail: mathkhd@inje.ac.kr

Un-Sook Choi received the M.S. degree and the Ph.D degree at Pukyong National University. She is currently a professor at Tongmyong University since 2006. Her research interests include cryptography, cellular automata and its applications.

Department of Information and Communications Engineering, Tongmyong University, Busan 48520, Korea.
e-mail: choies@tu.ac.kr

Jin-Gyoung Kim received the M.S. degree and the Ph.D degree at Pukyong National University. Her research interests include cryptography, cellular automata.

Department of Applied Mathematics, Pukyong National University, Busan 48513, Korea.
e-mail: 5892587@hanmail.net

Sung-Won Kang is currently on the course for the M.S. degree at Pukyong National University. His research interests include cryptography, cellular automata.

Department of Applied Mathematics, Pukyong National University, Busan 48513, Korea.
e-mail: jsm2371@hanmail.net