Journal of Cellular Automata, Vol. 13, pp. 347–358
Reprints available directly from the publisher
Photocopying permitted by license only

90/150 CA Corresponding to Polynomial of Maximum Weight

UN-SOOK CHOI[1], SUNG-JIN CHO[2,*], HAN-DOO KIM[3] AND
JIN-GYOUNG KIM[4]

[1]*Department of Information and Communications Engineering, Tongmyong University,*
Busan 48520, Korea
E-mail: choies@tu.ac.kr

[2]*Department of Applied Mathematics, Pukyong National University, Busan 48513, Korea*

[3]*Institute of Basic Sciences and Department of Applied Mathematics, Inje University,*
Gimhae 50834, Korea

[4]*Department of Applied Mathematics, Pukyong National University, Busan 48513, Korea*

Received: May 2, 2017. Accepted: September 4, 2017.

In this paper, we analyze the 90/150 CA **C** corresponding to self-reciprocal polynomial $f_n(x) = x^n + x^{n-1} + \cdots + x + 1$ of maximum weight and give a method of determining whether $f_n(x)$ is a CA-polynomial or not. Also we give a method of determining the number of 90/150 CA corresponding to $f_n(x)$ and propose the synthesis method for **C** using the synthesis algorithm proposed by Cho *et al.* [4].

Keywords: Cellular automata, polynomial of maximum weight, state transition matrix, symmetric transition rule, irreducible polynomial, self-reciprocal polynomial.

1 INTRODUCTION

Let $\mathbf{F_2}$ denote the finite field containing 2 elements. The reciprocal $f^*(x)$ of a polynomial $f(x)$ of degree n over $\mathbf{F_2}$ is defined by $f^*(x) = x^n f(1/x)$. The polynomial $f(x)$ is called *self-reciprocal* if $f^*(x) = f(x)$. For many years, many researchers have analyzed several self-reciprocal irreducible polynomials over finite fields [8, 10]. The self-reciprocal polynomials over finite fields

[*] Corresponding author: E-mail: sjcho@pknu.ac.kr

This work was supported by a Research Grant of Pukyong National University(2017 year)

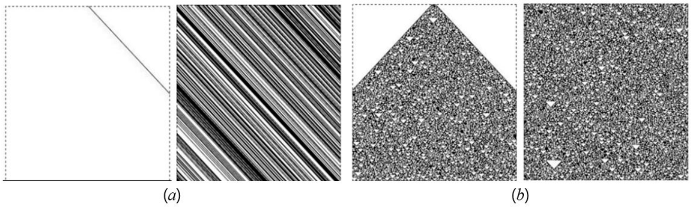

FIGURE 1
State transition of LFSR and 90/150 CA with maximum length

are useful in several applications such as cyclic error correcting codes and reversible codes with read-backward properties [7, 12].

Cellular Automata(CA) were originally introduced by Von Neumann in early 1950's in order to study the logical properties of self-reproducing machines [11]. Wolfram in early 1980's suggested a simplified two-state three-neighborhood 1-D CA with cells arranged linearly in one dimension [14]. 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. The bit sequences generated by 90/150 CA are superior to the bit sequences generated by LFSR in that there is no correlation. Figure 1 shows the state transition of LFSR and 90/150 CA corresponding to the characteristic polynomial $x^{256} + x^{10} + x^5 + x^2 + 1$ over $\mathbf{F_2}$ which is primitive. Figure 1 (*a*) shows the state transition of LFSR and Figure 1 (*b*) shows the state transition of 90/150 CA. In Figure 1, sites with value 1 are represented by black, and those with value 0 by white. Figure 1 shows that the state transition of the 90/150 CA with the same characteristic polynomial as the LFSR is superior to the LFSR in randomness and diffusion properties. CA has better randomness than LFSR, but its synthesis method is more difficult than that of LFSR. For this reason, many researchers have proposed methods to synthesize CA suitable for various applications [1, 13]. Cattell *et al.* [3] studied the synthesis of 90/150 linear CA corresponding to irreducible polynomials suitable for test pattern generation. Cho *et al.* [4] then proposed a more efficient synthesis algorithm. And Cho *et al.* studied the synthesis of 90/150 CA corresponding to the power of irreducible polynomials applicable to the keystream generator in the stream cryptosystem.

In this paper, we analyze 90/150 CA $\mathbf{C}$ corresponding to self-reciprocal polynomial $f_n(x) = x^n + x^{n-1} + \cdots + x + 1$ over $\mathbf{F_2}$ of maximum weight and give a method of determining whether $f_n(x)$ is a CA-polynomial or not. Also we give a method of determining the number of 90/150 CA corresponding to $f_n(x)$ and propose the synthesis method for $\mathbf{C}$ using the synthesis algorithm proposed by Cho *et al.* [4].

rule number	Linear transition rule
60	$s_i^{t+1} = s_{i-1}^t \oplus s_i^t$
90	$s_i^{t+1} = s_{i-1}^t \oplus s_{i+1}^t$
102	$s_i^{t+1} = s_i^t \oplus s_{i+1}^t$
150	$s_i^{t+1} = s_{i-1}^t \oplus s_i^t \oplus s_{i+1}^t$
170	$s_i^{t+1} = s_{i+1}^t$
204	$s_i^{t+1} = s_i^t$
240	$s_i^{t+1} = s_{i-1}^t$

TABLE 1
Linear rule with XOR logic

2 CA PRELIMINARIES

When the state transition function R_i applied to the ith cell of a CA is represented by XOR logic, R_i is referred to as a *linear transition rule.*

$$s_i^{t+1} = R_i(s_{i-1}^t, s_i^t, s_{i+1}^t) = as_{i-1}^t \oplus bs_i^t \oplus cs_{i+1}^t \ (a, b, c \in \{0, 1\}) \qquad (2.1)$$

Table 1 shows the linear transition rules. In Table 1, s_i^t denotes the state of the ith CA cell at the time of instant t, s_{i-1}^t and s_{i+1}^t refer to the state of the left and right neighbors. A CA with all the cells having linear rules is called a *linear CA.* A linear CA can represent a state transition function as a matrix, which is called a *state transition matrix.*

In particular, the state transition matrix of 90/150 CA is a tridiagonal matrix as shown in Equation (2.2) and is simply expressed as $T =< d_1, d_2, \cdots, d_n >$, where

$$d_i = \begin{cases} 0, & \text{if cell } i \text{ uses rule 90} \\ 1, & \text{if cell } i \text{ uses rule 150} \end{cases}$$

$$T = \begin{pmatrix} d_1 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & d_2 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & d_3 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & d_{n-1} & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & d_n \end{pmatrix} \qquad (2.2)$$

The characteristic polynomial $c(x)$ over $\mathbf{F_2}$ of an n-cell linear CA $\mathbf{C}$ is defined by $c(x) = |T \oplus xI_n|$, where T is the state transition matrix of the CA. The minimal polynomial of $\mathbf{C}$ is the polynomial $m(x)$ of least degree such that

$m(T) = O$. A polynomial is said to be a *CA-polynomial* if it is the characteristic polynomial of some 90/150 CA [3]. The following is well known.

Theorem 2.1 [2].

(i) For any n-cell 90/150 CA whose state transition matrix is T_n, the minimal polynomial of T_n is the same as the characteristic polynomial over $\mathbf{F_2}$ of T_n.

(ii) All irreducible polynomials over $\mathbf{F_2}$ are CA-polynomials. And there are exactly two 90/150 CA corresponding to any irreducible polynomial.

Cattell et al. [3] proposed a method to find 90/150 CA corresponding to a given irreducible polynomial. However, their method is limited to irreducible polynomials only. So it is impossible to generate 90/150 CA corresponding to reducible polynomials by their method. Cho et al. [4] proposed an efficient method for the synthesis of 90/150 linear CA. They reduced the complexity of the synthesis algorithm from $O(n^7)$ to $O(n^2)$. Algorithm 1 is the 90/150 CA synthesis algorithm proposed in [4].

In the proposed algorithm, $TU = UC$ since the state transition matrix T of a 90/150 CA and the companion matrix C corresponding to characteristic polynomial $f(x)$ over $\mathbf{F_2}$ of T are similar. In Step 2, for a solution $\mathbf{v}$ of $B\mathbf{v} = (0, \cdots, 0, 1)^T$, $f(x)$ is a CA-polynomial if $H = K(C^T, \mathbf{v})$ has an LU decomposition.

Algorithm 1 SynthesisOf90/150LinearHybridCA

Input : The characteristic polynomial $f(x) = x^n + q_{n-1}x^{n-1} + \cdots + q_1x + q_0$ over $\mathbf{F_2}$ of degree n

Output : 90/150 CA rule

Step1 : Make the matrix B which is the $n \times n$ matrix obtained by reducing the n polynomials $x^{i-1} + x^{2i-1} + x^{2i} (mod\ \ f(x))$ $(i = 1, 2, \cdots, n)$.

Step2 : Solve the equation $B\mathbf{v} = (0, \cdots, 0, 1)^T$. If the equation has no solution, then $f(x)$ is not a CA-polynomial. STOP.

Step3 : Construct a Krylov matrix $H = K(C^T, \mathbf{v})$ by the seed vector $\mathbf{v} = (v_1, v_2, \cdots, v_n)^T$ which is a solution of the equation in Step 2.

Step4 : Compute the LU decomposition $H = LU$. If the first entry v_1 of the solution $\mathbf{v}$ is 0, then LU decomposition is impossible. Stop.

Step5 : Compute 90/150 CA for $f(x)$ by the matrix $U = (u_{i,j})_{n\times n}$.

$$\begin{cases} d_1 = u_{1,2} \\ d_i = u_{i-1,i} + u_{i,i+1} (i = 2, 3, \cdots, n-1) \\ d_n = u_{n-1,n} + q_{n-1} \end{cases} \tag{2.3}$$

The self-reciprocal polynomial may or may not be a CA-polynomial.

Example 2.2.

(i) *For the irreducible polynomial* $f_4(x) = x^4 + x^3 + x^2 + x + 1$ *over* $\mathbf{F_2}$*, let* B *be the* 4×4 *matrix obtained by coefficients of the 4 polynomials* $x^{i-1} + x^{2i-1} + x^{2i}(mod \quad f_4(x))$ $(i = 1, 2, 3, 4)$. *Then* $B = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$. *The two solutions of* $B\mathbf{v} = (0, 0, 0, 1)^T$ *are* $\mathbf{v_1} = (1, 0, 1, 0)^T$ *and* $\mathbf{v_2} = (1, 0, 1, 1)^T$. *The Krylov matrix* $H = K(C^T, \mathbf{v_1})$ *by the seed vector* $\mathbf{v_1} = (1, 0, 1, 0)^T$ *is* $H = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$. *The LU decomposition of* H *is* $H = LU$*, where*

$$L = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \text{ and } U = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Every first superdiagonal entries of U *are* $(u_{12}, u_{23}, u_{34}) = (0, 0, 1)$. *Thus* $d_1 = u_{12} = 0, d_2 = u_{12} + u_{23} = 0, d_3 = u_{23} + u_{34} = 1, d_4 = u_{34} + q_3 = 0$. *Here* q_3 *is the coefficient of* x^3 *for* $f_4(x)$. *Thus the 90/150 CA corresponding to* $f_4(x)$ *is* $T =< 0, 0, 1, 0 >$. *Using the seed vector* $\mathbf{v_2} = (1, 0, 1, 1)^T$*, the 90/150 CA corresponding to* $f_4(x)$ *is* $T =< 0, 1, 0, 0 >$. *Thus two 90/150 CA corresponding to* $f_4(x)$ *are* $< 0, 0, 1, 0 >$ *and* $< 0, 1, 0, 0 >$.

(ii) *For reducible polynomial* $f_6(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ *over* $\mathbf{F_2}$*, let* B *be the* 6×6 *matrix obtained by coefficients of the 6 polynomials* $x^{i-1} + x^{2i-1} + x^{2i}(mod \quad f_6(x))$ $(i = 1, 2, 3, 4, 5, 6)$. *Then*

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

Since there is no $\mathbf{v}$ *such that* $B\mathbf{v} = (0, 0, 0, 0, 0, 1)^T$, $f_6(x)$ *is not a CA-polynomial.*

Definition 2.3 [5]. *Let* $T_n =< d_1, d_2, \cdots, d_n >$ *be the state transition matrix of an n-cell 90/150 CA. Then the m-cell 90/150 CA with the following two* *state transition matrices are called the 90/150 CA with symmetrical transition rule.*

$$\begin{cases} T_{2n} =< d_1, \cdots, d_{n-1}, d_n, d_n, d_{n-1}, \cdots, d_1 >, \ m = 2n \\ T_{2n+1} =< d_1, d_2, \cdots, d_n, d, d_n, \cdots, d_2, d_1 >, \ m = 2n+1 \end{cases}$$

Definition 2.4 [9]. *For the polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ over $\mathbf{F_2}$ of degree n, the weight $w(f)$ of f is defined to be the number of terms with nonzero coefficients in $f(x)$.*

The polynomial $f(x) = x^n + x^{n-1} + \cdots + x + 1$ over $\mathbf{F_2}$ of degree n with $w(f) = n+1$ is called the *polynomial of maximum weight*. Hereafter, we denote the polynomial of degree n of maximum weight by $f_n(x)$.

Theorem 2.5 [6]. *The polynomial $f_n(x) = x^n + x^{n-1} + \cdots + x + 1$, which is of weight $n+1$, is irreducible over $\mathbf{F_2}$ if and only if $n+1$ is a prime number and 2 is a primitive root modulo $n+1$.*

Example 2.6. *Consider the polynomial $f_4(x)$ of degree 4. In this case $n+1 = 5$ is prime. Since $2^1 \equiv 2(mod\ 5), 2^2 \equiv 4(mod\ 5), 2^3 \equiv 3(mod\ 5)$ and $2^4 \equiv 1(mod\ 5)$, 2 is a primitive root modulo 5. For the polynomial $f_6(x)$ of degree 6, $n+1 = 7$ is prime. Since $2^3 \equiv 1(mod\ 7)$, 2 is not a primitive root modulo 7. Thus $f_6(x) = (x^3 + x + 1)(x^3 + x^2 + 1)$ is reducible. Table 2 shows the irreducibility of the polynomial $f_n(x)$ of degree n when $n+1$ is*

degree n	Irreducibility of $f_n(x)$
2	irreducible
4	irreducible
6	(3,2,0)(3,1,0)
10	irreducible
12	irreducible
16	(8,5,4,3,0)(8,7,6,4,2,1,0)
18	irreducible
22	(11,9,7,6,5,1,0)(11,10,6,5,4,2,0)
28	irreducible
30	(5,2,0)(5,3,0)(5,4,3,2,0)(5,4,3,1,0)(5,4,2,1,0)(5,3,2,1,0)
36	irreducible
40	(20,18,17,16,15,14,11,10,9,6,5,4,3,2,0) (20,19,17,16,14,11,10,9,6,4,3,1,0)
42	(14,11,10,9,8,7,6,5,4,3,0)(14,12,10,7,4,2,0)(14,13,11,7,3,1,0)
46	(23,19,18,14,13,12,10,9,7,6,5,3,2,1,0) (23,22,21,20,18,17,16,14,13,11,10,9,5,4,0)

TABLE 2
Factorization of polynomial of degree n of maximum weight

prime, where $n \leq 50$. The polynomials are represented by listing their nonzero coefficients. For example, (3,2,0) *represents the polynomial* x^3+x^2+1. *Also* (3, 2, 0)(3, 1, 0) *represents the polynomial* $(x^3+x^2+1)(x^3+x+1)$.

3 ANALYSIS OF 90/150 CA CORRESPONDING TO POLYNOMIAL OF MAXIMUM WEIGHT

First, we analyze the characteristic polynomial of 90/150 CA synthesized by 90/150 CA with symmetric transition rule by the following theorem.

Lemma 3.1 [5]. *Let Δ_n be the characteristic polynomial over $\mathbf{F_2}$ of $T_n =< d_1, d_2, \cdots, d_n >$. Then the characteristic polynomial $c_{2n+1}(x)$ of $(2n+1)$-cell 90/150 CA $T_{2n+1} =< d_1, d_2, \cdots, d_n, d, d_n, \cdots, d_2, d_1 >$ with symmetric transition rule is $(x+d)\Delta_n^2$.*

Proof. By cofactor expansion along the $(n+1)$th row of $c_{2n+1}(x) = |T_{2n+1} \oplus xI_{2n+1}|$, we have

$$c_{2n+1}(x) = 1 \cdot \Delta_{n-1}\Delta_n + (x+d)\Delta_n^2 + 1 \cdot \Delta_n\Delta_{n-1} = (x+d)\Delta_n^2. \qquad \square$$

Theorem 3.2. *$f_n(x)$ is a CA-polynomial if and only if $f_{2n+1}(x)$ is a CA-polynomial.*

Proof. If $f_n(x)$ is a CA-polynomial, then there exists a 90/150 CA T_n corresponding to $f_n(x)$. Since $f_{2n+1}(x) = (x+1)[f_n(x)]^2$, we can construct the $(2n+1)-$cell 90/150 CA $< T_n, 1, T_n^* >$ whose characteristic polynomial is $f_{2n+1}(x) = (x+1)[f_n(x)]^2$ by Lemma 3.1. Thus $f_{2n+1}(x)$ is a CA-polynomial. Conversely, let $f_{2n+1}(x)$ be a CA-polynomial. Then there exists a $(2n+1)-$cell 90/150 CA $< a_1, \cdots a_n, d, b_n, \cdots, b_1 >$. The characteristic polynomial of $< a_1, \cdots a_n, d, b_n, \cdots, b_1 >$ is $V_{2n+1}(x) = \Delta_{n-1}\nabla_n + (x+d)\Delta_n\nabla_n + \Delta_n\nabla_{n-1}$, where Δ_n is the characteristic polynomial of $< a_1, \cdots, a_n >$ and ∇_n is the characteristic polynomial of $< b_1, \cdots, b_n >$. Since $f_{2n+1}(x) = (x+1)[f_n(x)]^2$, $d = 1$ and $\Delta_n = \nabla_n$. Therefore $a_i = b_i$ $(i = 1, \cdots, n)$. Thus $< a_1, \cdots, a_n >$ is an n-cell 90/150 CA corresponding to $f_n(x)$. Hence $f_n(x)$ is a CA-polynomial. □

Corollary 3.3. *The number of 90/150 CA corresponding to $f_{2n+1}(x)$ is the same as the number of 90/150 CA corresponding to $f_n(x)$.*

By Theorem 3.2, we can reduce the time to synthesize a CA from $O(n^2)$ to $O(log_2 n)$ by synthesizing the $(2n+1)$-cell 90/150 CA with symmetric transition rule using the n-cell 90/150 CA. In Example 2.2(ii), since $f_6(x)$ is not a CA-polynomial, $f_{13}(x)$, $f_{27}(x)$, $f_{55}(x), \cdots$ are not CA-polynomials.

Now we give a method of determining whether $f_n(x)$ over $\mathbf{F_2}$ is a CA-polynomial or not. Also we give a method of determining the number of 90/150 CA corresponding to $f_n(x)$.

Case (i): $n = 2m + 1$:
In this case, if $f_m(x)$ is a CA-polynomial, then $f_n(x)$ is a CA-polynomial and $T_n =< T_m, 1, T_m^* >$ by Theorem 3.2, where $T_m =< d_1, d_2, \cdots, d_m >$ is the 90/150 CA corresponding to $f_m(x)$ and $T_m^* =< d_m, \cdots, d_2, d_1 >$. Thus the number of 90/150 CA corresponding to $f_n(x)$ is the same as the number of 90/150 CA corresponding to $f_m(x)$ by Corollary 3.3.

In Example 2.2(i), since 90/150 CA corresponding to $f_4(x)$ are $< 0, 0, 1, 0 >$ and $< 0, 1, 0, 0 >$, 90/150 CA corresponding to $f_9(x)$ are $< 0, 0, 1, 0, 1, 0, 1, 0, 0 >$ and $< 0, 1, 0, 0, 1, 0, 0, 1, 0 >$.

Specifically, when $n = 2^k - 1$, the 90/150 CA corresponding to $f_n(x)$ can be synthesized from the 90/150 CA $T_1 =< 1 >$ corresponding to $f_1(x) = x + 1$. That is, $T_n = T_{2^k-1} =< 1, \cdots, 1 >$. Thus the 90/150 CA corresponding to $f_{2^k-1}(x) = (1 + x)^{2^k-1} (k = 1, 2, \cdots)$ is unique.

Case (ii): $n = 2m$:
For the characteristic polynomial Δ_n over $\mathbf{F_2}$ of the state transition matrix $T =< d_1, d_2, \cdots, d_n >$ of an n-cell 90/150 CA, the following recurrence relation holds [3]:

$$\Delta_n = (x + d_n)\Delta_{n-1} + \Delta_{n-2}, (\Delta_0 = 1, \Delta_{-1} = 0) \tag{3.1}$$

The relation between the 90/150 CA rule and the continued fraction is as follows. Using Euclid's algorithm for Δ_n and Δ_{n-1}, we can express equation (3.1) as a finite continued fraction of $\frac{\Delta_{n-1}}{\Delta_n}$ as equation (3.2):

$$\frac{\Delta_{n-1}}{\Delta_n} = \cfrac{1}{(x + d_n) + \cfrac{1}{(x+d_{n-1}) + \cfrac{1}{\ddots}}} \tag{3.2}$$

Here, $x + d_i$ is the partial quotient of the finite continued fraction and the constant term of the partial quotient is the transition rule of the ith cell of the 90/150 CA. As an example, the 90/150 CA corresponding to $f_4(x)(:= \Delta_4)$ is $< 0, 1, 0, 0 >$ and $\Delta_3 = x^3 + x^2$. The continued fraction of $\frac{\Delta_3}{\Delta_4}$ is as follows:

$$\frac{\Delta_3}{\Delta_4} = \frac{x^3 + x^2}{x^4 + x^3 + x^2 + x + 1} = \cfrac{1}{x + \cfrac{1}{x + \cfrac{1}{(x+1) + \frac{1}{x}}}}$$

For $f_n(x)$ to be a CA-polynomial, there must be a polynomial Δ_{n-1} of degree $n-1$ for which the partial quotients of the continued fraction expansion of $f_n(x)$ all have degree one. But it is very difficult to find such a Δ_{n-1}.

A method for determining whether $f_n(x)$ is a CA-polynomial or not is as follows. (i) For the case $f_n(x)$ $(n = 2m)$ is irreducible, $f_n(x)$ is a CA-polynomial [2,4].

(ii) For the case $f_n(x)$ $(n = 2m)$ is reducible:

To obtain the 90/150 CA for the given $f_n(x)$, we make the $n \times n$ matrix B obtained by coefficients of the n polynomials $x^{i-1} + x^{2i-1} + x^{2i}$ $(mod\ f_n(x))$ $(i = 1, 2, \cdots, n)$ and solve the equation $B\mathbf{v} = (0, \cdots, 0, 1)^T$. In addition, we construct the Krylov matrix $H = K(C^T, \mathbf{v})$ using the solution $\mathbf{v}$ of the equation $B\mathbf{v} = (0, \cdots, 0, 1)^T$. In this case, $H = K(C^T, \mathbf{v})$ has an LU decomposition provided that the first component of $\mathbf{v} = (v_1, v_2, \cdots, v_n)^T$ is always 1. Thus we obtain $u_{i,i+1}(i = 1, \cdots, n-1)$ from U and thus obtain $< d_1, \cdots, d_n >$ using (2.3). Therefore to be $f_n(x)$ a CA-polynomial, $B\mathbf{v} = (0, \cdots, 0, 1)^T$ must have a solution. This means that $rank(B) = rank(B|\mathbf{e}_n)$, where $\mathbf{e}_n = (0, \cdots, 0, 1)^T$.

In Example 2.2, since $rank(B) = rank(B|\mathbf{e}_4) = 3$, $f_4(x)$ is a CA-polynomial. But since $rank(B) = 4 \neq 5 = rank(B|\mathbf{e}_6)$, $f_6(x)$ is not a CA-polynomial.

Now we propose the method of finding the number of 90/150 CA corresponding to a given CA-polynomial $f_n(x)$.

Theorem 3.4. *Let $f_{2m}(x)$ be a reducible polynomial. Then $f_{2m}(x)$ is the product of different irreducible polynomials.*

Proof. Since $x^{2m+1} - 1 = \prod_{d|2m+1} \Phi_d(x)$ where $\Phi_d(x)$ is a d-th cyclotomic polynomial [9] and $x^{2m+1} - 1 = (x+1) f_{2m}(x)$,

$$f_{2m}(x) = \prod_{d|2m+1, d\neq 1} \Phi_d(x)$$

It is well-known that $\Phi_d(x)$ is an irreducible polynomial or the product of different irreducible polynomials. Also, if $d_1 \neq d_2$ $(d_1|2m+1, d_2|2m+1)$, then the factors of $\Phi_{d_1}(x)$ and $\Phi_{d_2}(x)$ are all different irreducible polynomials. Hence $f_{2m}(x)$ is the product of different irreducible polynomials. □

Example 3.5. *Let $n = 32$. Then $x^{33} - 1 = \prod_{d|33} \Phi_d(x)$. Since $33 = 3 \times 11$, $f_{32}(x) = \Phi_3(x) \cdot \Phi_{11}(x) \cdot \Phi_{33}(x)$. Here $\Phi_3(x) = f_2(x)$ and $\Phi_{11}(x) = f_{10}(x)$ are irreducible polynomials, and $\Phi_{33}(x) = (x^{10} + x^9 + x^5 + x + 1)(x^{10} + x^7 + x^5 + x^3 + 1)$. Hence $f_{32}(x)$ is the product of 4 different irreducible polynomials.*

Theorem 3.6. *Let $f_n(x)(n : even)$ be a CA-polynomial and let $f_n(x) = \prod_{i=1}^{k} h_i(x)$, where $h_i(x)$ is an irreducible polynomial $(i = 1, 2, \cdots, k)$. Then the number of 90/150 CA corresponding to $f_n(x)$ is 2^k.*

Proof. Since n is even, $f_n(0) \neq 0$ and $f_n(1) \neq 0$. Thus $h_i(x)$ is a polynomial of degree at least two. Also for $i,\ j(i \neq j)$, $h_i(x)$ and $h_j(x)$ are different irreducible polynomials by Theorem 3.4. Let $deg(h_i(x)) = d_i$ and B_i be the $d_i \times d_i$ matrix obtained by reducing the d_i polynomials $x^{a-1} + x^{2a-1} + x^{2a}$ $(mod\ \ h_i(x))$ $(a = 1, \cdots, d_i)$. Let $\mathbf{u_i} = (u_1^i, u_2^i, \cdots, u_{d_i}^i)$ be the solution of $\mathbf{u_i}B_i = O$ and $r_i(x) = u_1^i + u_2^i x + \cdots + u_{d_i}^i x^{d_i - 1}$. Then $r_i(x)\{1 + r_i(x)(x^2 + x)\} \equiv 0(mod\ \ h_i(x))$. Since $h_i(x)$ is irreducible $(i = 1, \cdots, k)$, $r_i(x) \equiv 0(mod\ \ h_i(x))$ or $r_i(x)$ is the inverse of $x^2 + x(mod\ \ h_i(x))$. Let $H_i(x) = h_1(x) \cdots h_{i-1}(x)h_{i+1}(x) \cdots h_k(x)$. Then $gcd(h_i(x), H_i(x)) = 1$ for each i. Let $r(x) = \sum_{i=1}^{k} r_i(x)H_i(x)H_i(x)^{-1}$. Then $r(x)\{1 + r(x)(x^2 + x)\} \equiv 0$ $(mod\ \ f_n(x))$ by Chinese Remainder Theorem. Therefore the number of $r(x)$ is 2^k. By the hypothesis, $f_n(x)$ is a CA-polynomial. Thus $B\mathbf{v} = \mathbf{e_n}$ must have solutions where B is the $n \times n$ matrix obtained by reducing the n polynomials $x^{a-1} + x^{2a-1} + x^{2a}$ $(mod\ \ f_n(x))$ $(a = 1, \cdots, n)$. Now the number of $\mathbf{v}$ is equal to the number of $\mathbf{u}$ where $\mathbf{u} = (u_1, u_2, \cdots, u_n)$ is the solution of $\mathbf{u}B = O$. Also the number of $\mathbf{u}$ is equal to the number of $r(x)$. Hence the number of the 90/150 CA corresponding to $f_n(x)$ is 2^k. □

Corollary 3.7. *Let $f_n(x)(n : even)$ be a CA-polynomial and let $f_n(x) = \prod_{i=1}^{k} h_i(x)$, where $h_i(x)$ is an irreducible polynomial of $deg(h_i(x)) \geq 2$ $(i = 1, 2, \cdots, k)$. And let B be the $n \times n$ matrix obtained by coefficients of the n polynomials $x^{i-1} + x^{2i-1} + x^{2i}$ $(mod\ \ f_n(x))$ $(i = 1, 2, \cdots, n)$. Then $rank(B) = n - k$.*

Example 3.8. *Consider $f_8(x) = x^8 + \cdots + x + 1$. The 8×8 matrix B obtained by coefficients of the 8 polynomials $x^{i-1} + x^{2i-1} + x^{2i}$ $(mod\ \ f_8(x))$ $(i = 1, 2, \cdots, 8)$ is*

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

Since $f_8(x) = (x^2 + x + 1)(x^6 + x^3 + 1)$, $rank(B) = 8 - 2 = 6$ by Corollary 3.7. The solution of $B\mathbf{v} = (0, 0, 0, 0, 0, 0, 0, 1)^T$ is $\mathbf{v} = (1, \alpha, 1 +$

α	β	$\mathbf{v} = (1, \alpha, 1+\alpha, 1, 1+\alpha, \alpha, 1, \beta)^T$	90/150 CA
0	0	$\mathbf{v_0} = (1, 0, 1, 1, 1, 0, 1, 0)^T$	$< 01110110 >$
0	1	$\mathbf{v_1} = (1, 0, 1, 1, 1, 0, 1, 1)^T$	$< 01101110 >$
1	0	$\mathbf{v_2} = (1, 1, 0, 1, 0, 1, 1, 0)^T$	$< 10110101 >$
1	1	$\mathbf{v_3} = (1, 1, 0, 1, 0, 1, 1, 1)^T$	$< 10101101 >$

TABLE 3
90/150 CA corresponding to $f_8(x)$

$\alpha, 1, 1+\alpha, \alpha, 1, \beta)^T$, *where* $\alpha, \beta \in \{0, 1\}$. *By Algorithm 1, we obtain the 90/150 CA corresponding to* α *and* β *which are shown in Table 3.*

4 CONCLUSION

The self-reciprocal polynomials over $\mathbf{F_2}$ are useful in several applications. In this paper, we analyzed the 90/150 CA **C** corresponding to self-reciprocal polynomial $f_n(x) = x^n + x^{n-1} + \cdots + x + 1$ of maximum weight and gave a method of determining whether $f_n(x)$ is a CA-polynomial or not using the rank of the matrix obtained by reducing the n polynomials $x^{i-1} + x^{2i-1} + x^{2i}(mod\ \ f_n(x))\,(i = 1, 2, \cdots, n)$. Also we gave a method of determining the number of 90/150 CA corresponding to $f_n(x)$ by using factorization of $f_n(x)$ and Chinese Remainder Theorem. And we proposed the synthesis method for **C** using the synthesis algorithm proposed by Cho *et al.* [4].

REFERENCES

[1] A.F-Sabater and P.C-Gil. (2009). Synthesis of cryptographic interleaved sequences by means of linear cellular automata. *Applied Mathematics Letters*, 22:1518–1524.

[2] K.M. Cattell and J.C. Muzio. (1996). Analysis of one-dimensional linear hybrid cellular automata over GF(q). *IEEE Trans. Comput-Aided Design Integr. Circuits Syst.*, 45:782–792.

[3] K.M. Cattell and J.C. Muzio. (1996). Synthesis of one-dimensional linear hybrid cellular automata. *IEEE Trans. Comput-Aided Design Integr. Circuits Syst.*, 19:325–335.

[4] S.J. Cho, U.S. Choi, H.D. Kim, Y.H. Hwang, J.G. Kim, and S.H. Heo. (2007). New synthesis of one-dimensional 90/150 linear hybrid group cellular automata. *IEEE Trans. Comput-Aided Design Integr. Circuits Syst.*, 26:1720–1724.

[5] U.S. Choi, S.J. Cho, and Gil-Tak Kong. (2015). Analysis of characteristic polynomial of cellular automata with symmetrical transition rules. *Proceedings of the Jangjeon Mathematical Society*, 18:85–93.

[6] L.E. Dickson. (1958). *Linear Groups: With an Exposition of the Galois Field Theory*. Dover Publications Inc., New York.

[7] S.J. Hong and D.C. Bossen. (1975). On some properties of self-reciprocal polynomials. *IEEE Trans. Infor. Thy.*, IT-21:462–464.

[8] J.L.Yucas and G.L. Mullen. (2004). Self-reciprocal irreducible polynomials over finite fields. *Design, Codes and Cryptography*, 33:275–281.

[9] R. Lidl and H. Niederreiter. (1997). *Finite fields, 2nd edition*. Cambridge University Press.

[10] H. Meyn. (1990). On the construction of irreducible self-reciprocal polynomials over finite fields. *Appl. Alg. in Eng., Comm., and Comp.*, 1:43–53.

[11] J.V. Neumann. (1966). *The theory of self-reproducing automata, Burks, A.W. (Ed.)*. University of Illinois Press.

[12] V. Pless. (1998). *Introduction to the theory of error-correcting codes, 3rd edition*. Wiley-Interscience.

[13] S. Roy, S. Nandi, J. Dansana, and P.K. Pattnaik. (2014). Application of cellular automata in symmetric key cryptography. *IEEE International Conference on Communication and Signal Processing*, 114:572–576.

[14] S. Wolfram. (1983). Statistical mechanics of cellular automata. *Rev. Modern Physics*, 66:601–644.