TWMS J. Pure Appl. Math. V.4, N.2, 2013, pp.215-225

THE REVERSIBILITY OF $(2r+1)-$CYCLIC RULE CELLULAR AUTOMATA*

I. SIAP[1], H. AKIN[2], M.E. KOROGLU[1]

Abstract. In this paper, we introduce a family of one dimensional finite linear cellular automata with periodic boundary condition over primitive finite fields with p elements ($\mathbb{Z}_p$) which leads to a generalization in two directions: the radius and the field that states take values. This family of cellular automata is called $(2r+1)$-cyclic cellular automata since it has a cyclic structure and its radius is r. Here, we establish a connection between the generator matrices of cyclic codes and the rule matrix of $(2r+1)$-cyclic cellular automata. Thus this enables the determination of the reversibility problem of this cellular automaton by means of the algebraic coding theory. Further, we explicitly determine the reverse CA of this family and prove that the reverse CA of this family again falls into this family.

Keywords: cellular automata, $(2r+1)$-cyclic cellular automata, reversibility, error correcting codes.

AMS Subject Classification: Primary 28D20; Secondary 37A35, 37B40.

1. Introduction

Since first introduced by Ulam and von Neumann [16], cellular automaton (CA) has found many interesting applications in science. This fact is based on the nature of cellular automata which basically consists of cells lined up in one dimensional array and have interaction among themselves. In many applications of dynamical systems, especially modeled by discrete cells, CA offers a way to express the behavior of such systems. In many discrete models the neighbors that are close to each other play an important role on evolution. Thus, the definition of CA is based on the neighboring relations assumed among cells which determines the CA. Though the evolution of a CA in real life is very complicated, it is observed that with a simple neighboring rule and a initial condition cellular automata generate very complicated and sophisticated structures after a reasonable evolution time. This observation has led scientists to study and do a more detailed research on cellular automata. Some of recent application areas of CA surely not all can be seen in physics, computer science, chemistry, image processing, fast computations, cryptography etc. [1, 2, 3, 4, 7, 8, 11, 14].

A CA that can be traced back to any desirable evolution time is called a reversible CA (RCA). Reversible Cellular Automata are deterministic in both directions of time [12]. In many applications the feature of being able to trace the evolution process backwards plays a crucial role. So studying the reversibility problem of CA is one of the most important problems.

*This work is presented in the 1^{st} International Eurasian Conference on Mathematical Sciences and Applications (IECMSA-2012)

[1] Department of Mathematics, Yildiz Technical University, Istanbul, Turkey, e-mail: isiap@yildiz.edu.tr

[2] Department of Mathematics, Zirve University, Gaziantep, Turkey, e-mail: hasanakin69@gmail.com, sadecesad@gmail.com

Manuscript received August 2012.

Another subject that we relate to answering the question of the reversibility property of a CA is error correcting codes. Due to the digital era that we are in, this subject has also found many applications. The idea of algebraic error correcting codes is to construct schemes that can be easily implemented in detection and correction of digital data while storing or transferring [10].

The idea of studying a special family of one dimensional CA comes from the fact that a very special case of CA over binary fields is studied first in [12], then over primitive fields by Cinkir et al. in [6] and again over primitive fields by Siap et al. in [15] with a special rule that is called penta cyclic rule. Here, these three very recent studies are generalized to primitive fields where with this generalization all primitive fields are covered together with their generalizations on rules. This one dimensional CA family that generalizes all previous studies is called $(2r+1)$-cyclic cellular automaton (or shortly $(2r+1)-$CCA) over primitive fields. In this paper, first, we state the definition of $(2r+1)-$CCA, next we determine their rule matrix. After presenting some necessary definitions and theorems from the theory of error correcting codes we establish the connection between the generator matrices of cyclic codes and the rule matrix of $(2r+1)-$CCA. One of the important feature of CA is their reversibility problem [2, 7, 8, 11, 12, 14]. Hence this relation leads to an easy determination of the reversibility problem of $(2r+1)-$CCA. We also determine the reverse CA explicitly and prove that the reverse CA of this family falls into this family. At the end, we present an application of reversible $(2r+1)-$CCA to error correcting codes by extending the method originally introduced by Chowdhury et al. [5] for binary cases. We conclude by presenting a table that points out the advantage of $(2r+1)-$CCA if used in error detection-correction. Finally, some conclusions and future studies are presented.

2. Preliminaries

In this section, we define one dimensional (1D) finite $(2r+1)$ $-$cyclic CA with periodic boundary conditions (shortly PBC) over primitive fields with p elements $\mathbb{Z}_p = \{0, 1, \cdots, p-1\}$ where p is prime and clearly $p \geq 2$. This definition is a natural generalization of particular 1D null boundary CA. As a special case with $p = 2$ the structure and reversibility problem over binary fields ($\mathbb{Z}_2 = \{0, 1\}$) is studied by del Rey et al. in [12] and primitive fields is studied by Cinkir et al. in [6] and Siap et al. in [15] respectively. Here, we generalize the approach first presented in [15] to studying the algebraic structure and the reversibility of this new family of CA.

The elements of the set $\mathbb{Z}_p^{\mathbb{Z}}$ are doubly-infinite sequences denoted as $x = (x_n)_{n=-\infty}^{\infty}$ where the entries are from $\mathbb{Z}_p$. Let $T_f : \mathbb{Z}_p^{\mathbb{Z}} \to \mathbb{Z}_p^{\mathbb{Z}}$ be a map that acts locally on the set of doubly-infinite sequences by means of a local map $f : \mathbb{Z}_p^{2r+1} \to \mathbb{Z}_p$ of radius r. This map is called a cellular automaton (CA).

$$x_i^{t+1} = \begin{cases} a_{-r}x_{n-r+1}^t + ... + a_{-1}x_n^t + a_0x_1^t + a_1x_2^t + ... + a_rx_{r+1}^t, & i = 1; \\ a_{-r}x_{n-r+2}^t + ... + a_{-1}x_1^t + a_0x_2^t + a_1x_3^t + ... + a_rx_{r+2}^t, & i = 2; \\ \vdots & \\ a_{-r}x_0^t + ... + a_{-1}x_{r-1}^t + a_0x_r^t + a_1x_{r+1}^t + ... + a_rx_{2r}^t, & i = r; \\ a_{-r}x_{i-r}^t + ... + a_{-1}x_{i-1}^t + a_0x_i^t + a_1x_{i+1}^t + ... + a_rx_{i+r}^t, & r+1 \leq i \leq n-r-1; \\ a_{-r}x_{n-2r}^t + ... + a_{-1}x_{n-r-1}^t + a_0x_{n-r}^t + ... + a_rx_n^t, & i = n-r; \\ \vdots & \\ a_{-r}x_{n-1-r}^t + ... + a_{-1}x_{n-2}^t + a_0x_{n-1}^t + ... + a_rx_{n+r-1}^t, & i = n-1; \\ a_{-r}x_{n-r}^t + ... + a_{-1}x_{n-1}^t + a_0x_n^t + a_1x_1^t + ... + a_rx_r^t, & i = n. \end{cases} \quad (1)$$

If a local rule f is a linear map, then a CA can be presented by a local rule linear function $f(x_{-r}, \cdots, x_r) = \sum_{i=-r}^{r} \lambda_i x_i \pmod p$, where at least one of $\lambda_{-r}, \cdots, \lambda_r$ is nonzero mod p [13]. The local rule of a $(2r+1)$ $-$cyclic

CA is defined by (1), where $a_i \in \mathbb{Z}_p$ $(i=-r,-r+1,...,-1,0,1,...,r)$, and x_i^t is a symbol of the state of the i^{th} cell at time t. Since the number of cells is finite, PBC can be stated as follows:

If $i \equiv j \pmod n$, then $x_i^t = x_j^t$ [8]. Let us define the 1D finite CA $\mathcal{A}_n$ $(n \geq 2r+1)$ with PBC:

$$\begin{aligned} & x_{n-r}^t,...,x_{n-1}^t,x_n^t[x_1^t,x_2^t,\cdots,x_{n-1}^t,x_n^t]x_1^t,x_2^t,...,x_r^t \\ \overset{\mathcal{A}_n}{\rightarrow} \quad & x_{n-r}^{t+1},...,x_{n-1}^{t+1},x_n^{t+1}[x_1^{t+1},x_2^{t+1},\cdots,x_{n-1}^{t+1},x_n^{t+1}]x_1^{t+1},x_2^{t+1},...,x_r^{t+1}. \end{aligned} \tag{2}$$

In this study, we will only consider the 1D finite LCA defined by local rule (1) under modulo-p addition where $p \geq 2$ is a prime number. $(2r+1)-$cyclic CAs are defined by a special local rule; next state cell is determined by all neighboring cells within radius r such that the first and last cell are assumed to be next to each other in a cyclic manner. A configuration at time t is a vector $C^t = (x_1^t, x_2^t, x_3^t, \cdots, x_{n-1}^t, x_n^t) \in \mathbb{Z}_p^n$ and therefore C^0 stands for the initial configuration. The configuration length of a vector will be assumed to be n in this paper. Hence, $2r+1 \leq n$.

A common approach for defining a CA which merely depends on its local rule is to introduce a numbering label. We introduce the following ordering for the rule number:

$$x_i^{t+1} = \sum_{j=-r}^{r} a_j x_{i+j}^t \Rightarrow RN = \sum_{k=-r}^{r} a_k p^{r+k} = (a_r...a_1a_0a_{-1}...a_{-r})_p\,. \tag{3}$$

For instance, if $r=2$, $p=3$,and $(a_{-2},a_{-1},a_0,a_1,a_2)=(2,2,1,1,1)$ then this rule will be named as rule number (RN) $3^4+3^3+3^2+2\cdot 3^1+2\cdot 3^0=(11122)_3=125$ or if $r=1$, $p=5$, and $(a_{-1},a_0,a_1)=(2,1,1)$ then this rule will be named as rule number (RN) $5^2+5^1+2\cdot 5^0=$ $=(112)_5=32$. In this presentation, the cells are assumed to effect the next state configuration, so we take $a_i \in \mathbb{Z}\backslash\{0\}$.

By studying the image of the basis vectors on $\mathbb{Z}_p^n$, it can be easily proven that the representation (rule) matrix M_n of an $(2r+1)$-CCA with PBC is

$$M_n = \begin{pmatrix} a_0 & a_1 & ... & a_r & 0 & 0 & \cdots & 0 & a_{-r} & \cdots & a_{-2} & a_{-1} \\ a_{-1} & a_0 & a_1 & ... & a_r & 0 & 0 & \cdots & 0 & a_{-r} & \cdots & a_{-2} \\ ... & a_{-1} & a_0 & a_1 & ... & a_r & 0 & 0 & \cdots & 0 & a_{-r} & \cdots \\ a_{-r} & ... & a_{-1} & a_0 & a_1 & ... & a_r & 0 & 0 & \cdots & 0 & a_{-r} \\ 0 & a_{-r} & ... & a_{-1} & a_0 & a_1 & ... & a_r & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & ... & \ddots & \ddots & \ddots & ... & \ddots & \vdots & \vdots & \cdots \\ a_r & 0 & \cdots & 0 & 0 & a_{-r} & ... & a_{-1} & a_0 & a_1 & ... & 0 \\ ... & a_r & 0 & \cdots & 0 & 0 & a_{-r} & ... & a_{-1} & a_0 & a_1 & ... \\ a_2 & ... & a_r & 0 & \cdots & 0 & 0 & a_{-r} & ... & a_{-1} & a_0 & a_1 \\ a_1 & a_2 & ... & a_r & 0 & \cdots & 0 & 0 & a_{-r} & ... & a_{-1} & a_0 \end{pmatrix}. \tag{4}$$

These type of matrices are called circulant matrices. This observation leads to some relations that will be very helpful on studying these matrices in the sequel.

3. Some algebraic coding theory

Algebraic coding theory has been a very active research area after its application in error detection and correction in digital information storage and transferring process. Though there are several schemes for encoding a digital data, the ones that have found applications are the schemes that are obtained from algebraic structures. This is important because encoding and decoding processes are easier and practical for implementation. In this paper, our focus will be mainly on cyclic codes which is a special family of linear codes. We are going to present the

basic and the most important results that we are going to use for our purpose. The readers are welcome to refer to this subject if necessary for further details which can be found in [10].

$V = \mathbb{Z}_p^n = \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$ is a $\mathbb{Z}_p$-vector space.

Definition 3.1. [10] *A linear code of length n is a $\mathbb{Z}_p$-subspace C of V. The elements of C are called codewords and the elements of V are called words.*

If a set of p^k information messages are to be encoded, then a linear map from $\mathbb{Z}_p^k$ to $V = \mathbb{Z}_p^n$ can be used. So, the image of this map is called a linear code and the n tuples that fall into this image are called codewords. After the transmission process due to its algebraic structure, if a linear code can detect and correct t errors then the code is called a t error correcting code.

The number of nonzero entries of an element $v \in V$ is called the Hamming weight of v. The smallest nonzero weight among all codewords of a linear code C is called the minimum Hamming weight of C. Since a linear code C is a vector subspace of V, it has a dimension k, and if it has minimum Hamming weight d, then C is called a linear code of length n, dimension k and minimum distance d and shortly it is denoted by $[n, k, d]$. All these three parameters determine the quality of the code, among these the minimum Hamming weight of a code plays an important role which is evident by the following theorem:

Theorem 3.1. [10] *If C is a linear code with minimum Hamming weight $d = 2t+1$ or $d = 2t+2$, then C can correct up to t errors and detect $d-1$ errors.*

Definition 3.2. *If C is a linear code of length n with the property that for each codeword $(c_0, c_1, \ldots, c_{n-1})$ in C, its right cyclic shift $(c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ also falls in C, then C is called a cyclic code.*

This cyclic property leads to a richer algebraic structure. First, the vectors are identified with polynomials in the following way:

$$\Phi : (c_0, c_1, \ldots, c_{n-1}) \to c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}. \tag{5}$$

Next by definition $\Phi(C)$ is $\mathbb{Z}_p$-vector subspace of $\mathbb{Z}_p[x]$ and since $x(c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}) \in \in \Phi(C)$ modulo $x^n - 1$, it is clear that $\Phi(C)$ is an ideal in the quotient ring $\mathbb{Z}_p[x]/(x^n - 1)$. Since the ring $\mathbb{Z}_p[x]/(x^n - 1)$ is a principal ideal ring so is $\Phi(C)$ is a principal ideal. The following theorem gives the structure of a cyclic code.

Theorem 3.2. [10] *If C is a cyclic code of length n, then C is an ideal generated by a polynomial $g(x)$ where $g(x)|x^n - 1$, i.e. $C = \langle g(x) \rangle$.*

A cyclic code C is a sub vector space and it has a basis $\{g(x), xg(x), \ldots, x^{n-k-1}g(x)\}$ and further the dimension of C is equal to $n - k$ where the degree of $g(x)$ is k.

Example: Let $\Phi(C) = \langle (1 + x + x^2)^2 \rangle$ be an ideal in $\mathbb{Z}_2[x]/(x^6 - 1)$. $\dim(C) = 6 - 4 = 2$. Then the code is $\Phi(C) = \{0, 1 + x^2 + x^4, x + x^3 + x^5, 1 + x + x^2 + x^3 + x^4 + x^5\}$. Hence, $C = \{000000, 101010, 010101, 111111\}$. Since there is a vector isomorphism between $\Phi(C)$ and C we do not distinguish between polynomial and vector representation of codewords.

4. The rank of a $(2r+1)-$cyclic CA over $\mathbb{Z}_p$ with PBC

The main purpose of this section which is at the same time of the paper is to determine when a $(2r+1)$-cyclic CA with periodic boundary condition (PBC) is reversible. In order to accomplish this task, we need to study the rank of the rule matrix M_n given in (4). Since the rule matrix has a special form that has a special meaning in error correcting theory, we are

going to establish this relation in the sequel by relating these two topics. First we recall the rule matrix M_n in (4) and associate a polynomial for each row by applying the map (5).

Let $p(x) = \sum_{j=-r}^{r} a_j x^{j+r}$. After reordering the rows of M_n we can easily observe that the rows are exactly the elements of $\{p(x), xp(x), \ldots, x^{n-1}p(x)\}$ in different row ordering. So the row space of M_n is actually an ideal generated by $p(x)$ in $\mathbb{Z}_p[x]/(x^n-1)$. In other words, the row space of M_n is a cyclic code C generated by $p(x)$.

Further it is well known that if $C = \langle p(x) \rangle$, then there exists a monic polynomial $g(x)$ such that $C = \langle g(x) \rangle$ where $g(x) | x^n - 1$ and $g(x) = (p(x), x^n - 1)$.

Theorem 4.1. *Let M_n be the transition matrix of a $(2r+1)$-Cyclic CA with PBC and rule number $(a_r \cdots a_0 \cdots a_{-r})_p$. Then, $rank(M_n) = n - \deg(g(x))$, where $g(x) = (p(x), x^n - 1)$ in $\mathbb{Z}_p[x]$ and $p(x) = \sum_{j=-r}^{r} a_j x^{j+r}$.*

Example: Let $r = 1$ and M_9 be a rule matrix of a 3-Cyclic CA with PBC and $(a_{-1}, a_0, a_1) = = (1,1,1)$. Then, $g(x) = (1+x+x^2, x^9-1) = 1+x+x^2 \mod 3$. So, $rank(M_9) = 9-\deg(g(x)) = = 9-2 = 7$. Then, this CA is not reversible.

Lemma 1. [10] *If $(f(x), x^n - 1) = 1$, then $f(x)$ is invertible (unit) in the quotient ring $\mathbb{Z}_p[x]/(x^n-1)$.*

The following corollary is a natural consequence of the discussions presented above:

Corollary 4.1. *If $f(x)$ represents the polynomial counterpart of a rule number of a $(2r+ + 1)-$cyclic CA with PBC and configuration length n, then this CA is reversible if and only if $(f(x), x^n - 1) = 1$.*

Theorem 4.2. *For any given p, either both $rank(M_n)$ and $rank(M_{np^k})$ are full or not. If they are not full, then $\det(M_n) = \det(M_{np^k}) = 0$.*

Proof. By Theorem 4.1, $rank(M_n) = n - \deg(g(x))$ where $g(x) = (p(x), x^n - 1)$ in $\mathbb{Z}_p[x]$. $x^{np^k} - 1 = (x^n - 1)^{p^k}$ in $\mathbb{Z}_p[x]$. So, if $(p(x), x^n - 1) = 1$, then $(p(x), x^{np^k} - 1) = 1$. Hence, $rank(M_n) = n$ and $rank(M_{np^k}) = np^k$. So, they are both of full rank hence the 1D $(2r+1)-$ Cyclic CA is reversible. Otherwise, they are both irreversible. □

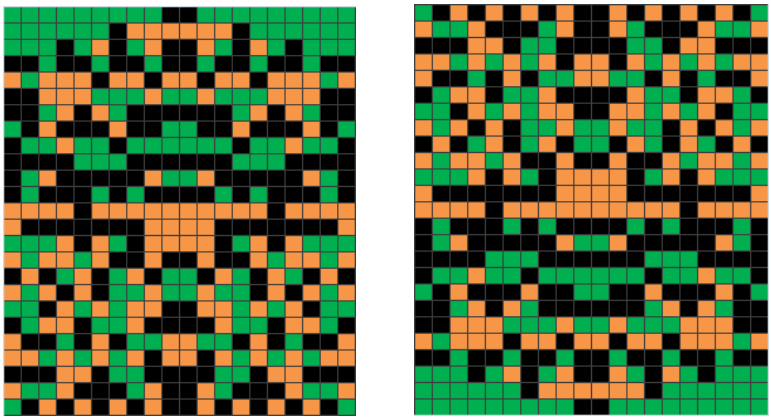

Figure 1. (Color online) Space time diagram of the 7-CCA $\mathcal{A}_{20}$ (left) and its inverse (right) with $n = 20$ and $0 \le t \le 25$, $p = 3$.

Example: Let us consider a 7-CCA with the following parameters: $n = 20, r = 3$ and $p = 3$, $a_{-3} = a_{-2} = a_{-1} = a_0 = a_1 = a_2 = a_3 = 1$. Then, $p(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6$ and $gcd(p(x), x^{20} - 1) = 1$. By the Theorem 4.1 $rank(M_n) = n - \deg(g(x))$. Hence, $rank(M_{20}) = 20 - 0 = 20$. Thus, this rule matrix is invertible, therefore the 7-CCA is reversible.

Now, we illustrate the space time diagram of a particular CCA that is reversible. We choose the initial configuration as follows: $C^0 = [00000000011000000000]$. Now, we give the space time diagram of 1D finite $(2r + 1)-$cyclic CA defined in (1) and its inverse with $r = 3$, $n = 20$ and $0 \leq t \leq 25$. In the Figure 4 the space time diagrams of the 1D finite CA T_{20} and its inverse are presented, with a random initial configuration C^0, we calculate the last configuration C^{25} by means of the rule matrix T_{20}. Thus, we obtain the backward evolution of the 1D finite the 7-CCA T_{20}. On the left T_{20} is shown and its inverse is displayed on its right. Hence, we obtain the configuration of T_{20} at times $0 \leq t \leq 25$. Green pixels are used for 0, black pixels are used for 1, and orange pixels are used for 2.

Next by making use of algebra we can present some families of $(2r+1)-$cyclic CA with PBC that are reversible or irreversible.

Theorem 4.3. *For a given prime p and rule number $(p^{2r+1} - 1)/(p - 1)$, if $(2r + 1, n) \neq 1$ or $(2r+1, p) \neq 1$ with configuration length n, then the $(2r+1)-$cyclic CA with PBC is irreversible.*

Proof. The rule number $k(p^{2r+1} - 1)/(p-1)$ with $r \in \mathbb{Z}^+$ and $k \in \{1, 2, \ldots p-1\}$ corresponds to the polynomial $f(x) = k(\sum_{j=0}^{2r} x^j)$. We observe that $f(x) = k(x^{2r+1}-1)/(x-1)$. If $(2r+1, n) \neq 1$, then there exists $d \in \mathbb{Z}^+$ with $d \leq 2$ such that $(2r + 1, n) = d$, then $d|2r + 1$ and $d|n$ which implies that $x^d - 1|x^{2r+1} - 1$ and $x^d - 1|x^n - 1$ and hence $x^d - 1|gcd(x^{2r+1} - 1, x^n - 1)$ and $d \leq 2$. Therefore, $gcd(f(x), x^n - 1) > 1$ which implies that $f(x)$ does not have an inverse in the quotient ring, by Theorem 4.4 thus the corresponding CA is not reversible. If $(2r + 1, p) \neq 1$, then $p|2r + 1$ since p is prime. Then, $x^p - 1|x^{2r+1} - 1$. Since $x^p - 1 = (x - 1)^p \mod p$, we have $(x - 1)^p|x^{2r+1} - 1$, and hence $x - 1|gcd(f(x), x^p - 1)$. This gives $x - 1|gcd(f(x), x^n - 1)$, which implies that $f(x)$ does not have an inverse thus the corresponding CA is not reversible. □

Example: Let $p = 3$, $n = 15$ and $r = 1$ be given for a 3-cyclic CA with PBC. Since, $gcd(3, 15) = 3$ and the rule number $RN := (3^3 - 1)/(3 - 1) = 26 = 2.3^2 + 2.3^1 + 2.3^0$ by Theorem 4.3 we can conclude that this CA is irreversible. Indeed, since $f(x) = 2 + 2x + 2x^2$, and $gcd(2 + 2x + 2x^2, x^{15} - 1) = 1 + x + x^2 = g(x)$, then $rank(M_{15}) = 15 - \deg(g(x)) = 15 - 2 = 13$ which is immediate by the Theorem 4.1. Hence, this rule is not reversible. Carrying out similar discussions as in the previous theorem, we also have the following:

Theorem 4.4. *For any given prime p and rule number $(p^{2r+1} - 1)/(p - 1)$ if $(2r + 1, n, p) = 1$ with configuration length n, then the $(2r + 1)-$cyclic CA with PBC is reversible.*

Example: Let $p = 3$, $n = 9$ and $r = 2$ be given for a 3-cyclic CA with PBC. Since, $gcd(5, 3, 9) = 1$ and the rule number $RN := (3^5 - 1)/(3 - 1) = 121 = 3^4 + 3^3 + 3^2 + 3^1 + 3^0$ by Theorem 4.4 we can conclude that this CA is irreversible. Indeed, $f(x) = 1 + x + x^2 + x^3 + x^4$, and $gcd(1 + x + x^2 + x^3 + x^4, x^3 - 1, x^9 - 1) = 1 = g(x)$, then $rank(M_9) = 9 - \deg(g(x)) = 9 - 0 = 9$. Thus, this rule is reversible.

4.1. **The structure of reversible $(2r+1)-$ circulant CA with PBC.** The rule matrix (4) of a $(2r + 1)-$circulant CA with PBC consists of the shifts of the row $(a_{-r}, \ldots, a_{-1}, a_0, a_1, \ldots, a_r)$ and such matrices are known as circulant matrices [10]. If we define a square circulant matrix $U = (U(i, j))$ where $U(i, j)$ denotes the $(i, j)^{th}$ entry of the matrix U of size n such that $U(i, j) = 1$ if $j - i \equiv 0 \mod n$ and otherwise zero, then each circulant matrix A can be written in terms of

the powers of matrix U i.e. a polynomial U as $A = \sum_{i=0}^{n-1} a_i U^i i$ with $a_i \in \mathbb{Z}_p$. Hence by associating a polynomial $a(x) = \sum_{i=0}^{n-1} a_i x^i$ in the quotient ring $\mathbb{Z}_p[x]/(x^n-1)$ to a circulant matrix, the set of ring of circulant matrices and the quotient ring are isomorphic. Due to this fact, we have the following theorem:

Theorem 4.5. [10] *Let $f(x) \in \mathbb{Z}_p[x]/(x^n-1)$ such that $(f(x), x^n-1) = 1$. Then, there exists a $g(x) \in \mathbb{Z}_p[x]/(x^n-1)$ such that $f(x)g(x) \equiv 1 \mod x^n - 1$.*

This theorem can now easily interpreted in terms of circulant matrices as follows:

Corollary 4.2. *Let $f(x) \in \mathbb{Z}_p[x]/(x^n-1)$ such that $(f(x), x^n-1) = 1$ and $f(x)$ be associated with a circulant matrix F. Then, there exists a circulant matrix G associated to a polynomial $g(x) \in \mathbb{Z}_p[x]/(x^n-1)$ such that $FG = I$ (where I is identity matrix) with entries in $\mathbb{Z}_p$.*

Now, if we again consider the circulant matrix that appears as a rule matrix of this special family of CA, we can associate a polynomial $p(x) = \sum_{i=-r}^{r} a_i x^{i+r}$ to this circulant matrix. Then we have the following theorem whose proof follows by considering the arguments presented above:

Theorem 4.6. *Let $p(x) = \sum_{i=-r}^{r} a_i x^{i+r}$ be a polynomial associated to a rule matrix of a $(2r+1)-$cyclic CA with PBC. If $(p(x), x^n-1) = 1$, then there exists a $q(x) \in \mathbb{Z}_p[x]/(x^n-1)$ such that $p(x)q(x) \equiv 1 \mod x^n - 1$. Hence, the associated matrix Q to the polynomial $q(x)$ is also circulant and $PQ = I$ with entries in $\mathbb{Z}_p$. Thus, the reverse rule of a $(2r+1)-$cyclic CA with PBC exists and its rule matrix is Q which represents a $(2r+1)-$cyclic CA with PBC.*

Below we give a moderate example that illustrates Theorem 4.6.
Example: Suppose that for $n = 7$, $p = 3$, the matrix

$$M_7 = \begin{pmatrix} 1 & 2 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 2 \\ 2 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix} \tag{6}$$

is the rule matrix of a $3-$cyclic CA with PBC. The associated polynomial to this rule matrix is $p(x) = 1 + 2x + x^6 \in \mathbb{Z}_3[x]/(x^7-1)$. Since $(p(x), x^7-1) = 1$, then there exists the inverse of $p(x)$ which is the polynomial $q(x) = 2 + 2x^2 + x^3 + x^4 + x^6$, i.e. $p(x)q(x) \equiv 1 \mod x^7 - 1$. Hence the reverse rule of this CA is given by

$$Q = \begin{pmatrix} 2 & 0 & 2 & 1 & 1 & 0 & 1 \\ 1 & 2 & 0 & 2 & 1 & 1 & 0 \\ 0 & 1 & 2 & 0 & 2 & 1 & 1 \\ 1 & 0 & 1 & 2 & 0 & 2 & 1 \\ 1 & 1 & 0 & 1 & 2 & 0 & 2 \\ 2 & 1 & 1 & 0 & 1 & 2 & 0 \\ 0 & 2 & 1 & 1 & 0 & 1 & 2 \end{pmatrix}, \tag{7}$$

which is the associate matrix of the polynomial $q(x)$.

5. Error correcting codes based $(2r+1)-$ cyclic CA with PBC

One dimensional cellular automata based bit error correcting binary codes (CA-ECC) were first proposed by Chowdhury et al. in [5] in 1994. This method recently has been generalized to error correcting codes over non binary fields [9]. It is also known that CA based error correcting codes have some advantages compared to the classical ones [9, 5]. In this section, we present an application of CA based bit error correcting codes by applying reversible CA which fall into $(2r+1)-$cyclic CA family. First we present the encoding and decoding process that is given in [9]:

We assume that T is nonsingular rule matrix of $(2r+1)-$cyclic CAs of order n. Further, assume that there exists $1 \leq k \leq n$, $k \in \mathbb{Z}^+$ such that $G = \left[I_n | T^k\right]$ (I_n, $n \times n$ identity matrix) generates a linear code that can correct up to t errors.

The Encoding Process: Let $I = (i_1, i_2, \cdots, i_n) \in \mathbb{Z}_3^n$ denote the information part, where n is the rank of the nonsingular transition matrix of a $(2r+1)-$CCA. Then, the encoded codeword is $CW = \left(I, T^k[I]\right) = (i_1, i_2, ..., i_n, c_{n+1}, c_{n+2}, \ldots, c_{2n})$, i.e. $C = T^k[I] = (c_{n+1}, c_{n+2}, \ldots, c_{2n})$ is the check vector.

The Decoding Process: Suppose that the codeword $CW = (I, T^k[I])$ is sent and $CW' = = \left(I', T^k[I]\right) = \left(i'_1, i'_2, ..., i'_n, c'_{n+1}, c'_{n+2}, \ldots, c'_{2n}\right) = (I \oplus I_e, T^k[I] \oplus C_e)$ (where the operator $\oplus$ represents modulo 3 addition) is the received word. I_e and C_e represent the errors that have occurred in information and check vectors respectively. We assume that the sum of the Hamming weight of I_e and C_e are less or equal to t i.e. if $w_H(I_e) \leq i$ and $w_H(C_e) \leq t - i$ $(i = 1, 2, ..., t)$, then $w_H(I_e) + w_H(C_e) \leq t$. Hence, the syndrome vector is defined by:

$$S = 2T^k\left[I'\right] \oplus C' = 2T^k[I_e] \oplus C_e. \tag{8}$$

The syndrome of both the information and check vectors is defined by

$$S_n = 2T^k[I'] \oplus C' \tag{9}$$

and

$$S_c = T^k[I'] \oplus 2C' \tag{10}$$

respectively. In Table 1 the decoding scheme is shown, and where $CW' = (I', C')$ is the received word, I_e is the error vector of the information part, and C_e is the error vector of the check part respectively. The uniqueness of the error vector I_e is guarantied by the minimum distance of the code.

Table 1. Decoding scheme.

Case	CW'	I_e	C_e
I	(I', C')	$2T^{-k}(S_n)$	0
II	(I', C')	0	S_c
III	(I', C')	$2T^{-k}(S \oplus C_e)$	Try all possible $C_e \oplus C' = T^k[I]$

Now we give an example:

Example: Let the matrix $M_7 = T$ be given as in *Example 4.5.* Then the matrix T is of full rank and for $k = 2$ the matrix $G = \left[I_7 | T^2\right]$ generates a $[14, 7, 5]_3 -$ linear code with minimum distance $d(C) = 5$. Thus, this code can correct up to two errors. For instance, let us take the codeword is $CW = 11111111111111$ where the information and check parts of this codeword are $I = 1111111$, and $C = T^2[I] = 1111111$ respectively.

Case I. Suppose that two errors occur in the information part. For example assume that the received word is $CW' = \widehat{22}111111111111 = (I'|C')$. Now, we compute the syndrome as

$S = 2T^2[I'] \oplus C' = 2121210 \oplus 1111111 = 0202021$. The syndrome of the check part is $S_c = 0000000$. Hence, $S_7 = S \oplus S_c = 0202021$ which implies $\Rightarrow I_e = T^{-2}[S_7] = 2200000$. $I = I' \oplus I_e = 2211111 \oplus 2200000 = 1111111$. $C = C' = 1111111$. Therefore, the error vector is $E = 22000000000000$.

Case II. Now, assume that two errors occur in the check part. Let the received word be $CW' = 11111111111\widehat{00} = (I'|C')$. We compute the syndrome of the check part, which is $S = T^2[I'] \oplus 2C' = 1111111 \oplus 2222200 = 0000011$. Therefore, the syndromes of both the information and the check parts are $S_7 = 0000000$ and $S_c = 0000011$ respectively. Next, $I_e = T^{-2}[S_7] = 0000000$ and $C_e = S_c = 0000011$. Hence, $C = C' \oplus C_e = 1111100 \oplus 0000011 = 1111111$. Thus, the error vector is $E = 00000000000011$.

Case III. Now suppose that both information and check parts are in error. Let the received word be $CW' = \widehat{0}1111111111110\widehat{}$. Then, $S = 2T^2[I'] \oplus C' = 1102200 \oplus 1111110 = 2210010$. Hence both syndromes are nonzero, so the errors are in both parts. Now, we compute the syndrome S_c as in the classical error correction. By checking the syndrome of the check part and all possible errors of weight less than or equal to two beginning form the lowest weight we see that $S_c = 0000001$. $S_7 = S \oplus S_c = 2210011 \Rightarrow I_e = T^{-2}[S_7] = 1000000$. $I = I' \oplus I_e = 0111111 \oplus 1000000 = 1111111$. $C = C' \oplus C_e = 1111110 \oplus 0000001 = 1111111$. Hence, the error vector is $E = 10000000000001$.

In Case-III, where errors occur in the both information and check part, firstly the check part is corrected by classical syndrome decoding which require in total $\sum_{i=0}^{1} \binom{7}{i} 2^i = 15$ operations. Secondly the information part is corrected by applying Case-1 which required only one matrix operation. On the other hand if the classical decoding method is used, $\sum_{i=0}^{2} \binom{14}{i} 2^i = 393$ operations are required. So as n, q, and $d\,(= 2t+1)$ are larger the advantage of using CA becomes more evident. Table 2 clarifies this observation.

In Table 2 classical decoding and CA based decoding are compared in terms of complexity. In Table 2, q is the characteristic of finite fields, n is the number of information bits, and t is the number of correctable errors.

Table 2. CA based and the classical decoding are compared in terms of their complexity.

q	n	t	CA based decoding	Classical decoding
3	5	2	11	201
3	10	2	21	801
3	20	3	801	82241
3	20	4	9921	1544481

6. Conclusion

In this paper we relate the reversibility problem of the family of 1D $(2r+1)-$cyclic CA with the theory of error correcting codes. By means of this relation, solving the reversibility problem computationally becomes very feasible, since instead of computing the rank of the matrix one needs to compute the greatest common divisor of two polynomials over polynomial prime fields. Some other interesting features related to this family of CA and further connections on this direction wait to be explored.

7. Acknowledgement

This work is partially supported by The Scientific and Technological Research Council of Turkey (TÜBİTAK) (Project Number: 110T713).

References

[1] Akın, H., (2008), The topological entropy of invertible cellular automata, J. Comput. Appl. Math., 213(2), pp.501-508.
[2] Akın, H., Sah, F., Siap, I., (2012), On 1D reversible cellular automata with reflective boundary over the prime field of order p, Int. J. Mod. Phys. C, 23(1), pp.1-13.
[3] Akın, H., Siap, I., (2007), On cellular automata over Galois rings, Information Processing Letters, 103(1), pp.24-27.
[4] Chaudhuri, P. P., Chowdhury, D.R., Nandi, S., Chattopadhyay, S., (1997), Additive Cellular Automata. Theory and Applications, IEEE Computer Society Press, California.
[5] Chowdhury, D.R., Basu, S., Gupta, I.S., Chaudhuri, P.P., (1994), Design of CAECC-Cellular Automata Based Error Correcting Code, IEEE Trans. Computers, 43, pp.759-764.
[6] Cinkir, Z., Akın, H., Siap, I., (2011), Reversibility of 1D Cellular automata with periodic boundary over finite fields $\mathbb{Z}_p$, Journal of Statistical Physics, 143(4), pp.807-823.
[7] Czeizler, E., (2004), On the size of inverse neighborhoods for one-dimensional reversible cellular automata, Theor. Comput. Sci., 325, pp.273-284.
[8] Hernández Encinas, L., Martín del Rey, A., (2007), Inverse rules of ECA with rule number 150, Appl. Math. Comput., 189, pp.1782-1786.
[9] Koroglu, M.E., Siap, I., Akın, H., (2012), Error correcting codes via reversible cellular automata over finite fields, The Arabian Journal for Science and Engineering, (accepted) DOI : 10.1007/s13369-013-0757-0.
[10] MacWilliams, F.J., Sloane, N.J.A., (1977), The Theory of Error-Correcting Codes, North-Holland: New York.
[11] Manzini, G., Margara, L., (1998), Invertible linear cellular automata over: Algoritheoremic and dynamical aspects, J. Comput. Syst. Sci., 56, pp.60-67.
[12] Martín del Rey, A., Rodríguez Sánchez, G., (2011), Reversibility of linear cellular automata, Applied Mathematics and Computation, 217(21), pp.8360-8366.
[13] Martin, O., Odlyzko, A.M., Wolfram, S., (1984), Algebraic properties of cellular automata, Comm. Math. Phys., 93, pp.219-258.
[14] Seck-Tuoh-Mora, J.C., Martínez, G.J., McIntosh, H.V., (2006), The inverse behaviour of a reversible one-dimensional cellular automaton obtained by a single Welch diagram, J. Cell. Automata, 1, pp.25-39.
[15] Siap, I., Akın, H., Koroglu, M.E., (2012), Reversible cellular automata with Penta-Cyclic Rule and ECCs, Int. J. Mod. Phys. C, 23(10), 13p.
[16] von Neumann, J., (1996), Theory and organization of complicated automata, in: A.W. Burks (Ed.), The Theory of Self-Reproducting Automata, University of Illinois Press, Urbana.

Irfan Siap received his B.Sc. degree from Istanbul University in 1992 in mathematics. He received both his M.Sc. and Ph.D. degrees from The Ohio State University in 1996 and 1999 respectively in mathematics. He is currently with the Department of Mathematics, Yildiz Technical University, where he is the chair of the department. His research is mainly on algebraic coding theory, cellular automata, discrete structures and cryptography. He has published over 50 papers in distinguished international journals and presented research studies in international conferences. He is one of the associate Editors of The Journal of Franklin Institute besides other editorial services.

Hasan Akin is an associate professor in the Department of Mathematics at Zirve University, Turkey. He got M.D. in Mathematics in 1995 and Ph.D. in Mathematics in 1998 at Yuzuncu Yil University. His research interests are ergodic theory, dynamical systems, quadratic stochastic operators and processes-ergodic properties, topological and metric entropies, cellular automata and lattice (ising and potts etc.) models. Current research interests of H. Akin are centered on entropies (measure-theoretical, topological and directional etc.) of cellular automata. Also, he is intensively working the phase diagrams of lattice mo dels. He is author of more than 35 articles published in international ISI journals.

Mehmet Emin Koroglu received his B.Sc. degree in Mathematics in 2009 from Ataturk University and M.Sc. degree in Mathematics in 2012 from Yildiz Technical University respectively. He is currently a Ph.D. student in mathematics and research assistant in Yildiz Technical University, Istanbul, Turkey. His research interests are algebraic coding theory and cellular automata.