TÜBİTAK

Turkish Journal of Mathematics

http://journals.tubitak.gov.tr/math/

Research Article

Turk J Math
(2016) 40: 665 – 678
© TÜBİTAK
doi:10.3906/mat-1503-18

The reversibility problem for a family of two-dimensional cellular automata

Mehmet Emin KÖROĞLU[1,*], **İrfan ŞİAP**[1], **Hasan AKIN**[2]
[1]Department of Mathematics, Faculty of Arts and Sciences, Yıldız Technical University, İstanbul, Turkey
[2]Department of Mathematics, Faculty of Education, Zirve University, Gaziantep, Turkey

Received: 06.03.2015 • **Accepted/Published Online:** 13.10.2015 • **Final Version:** 08.04.2016

Abstract: In this paper the reversibility problem of a family of two-dimensional cellular automata is completely resolved. It is well known that the reversibility problem is a very difficult one in general. In order to determine whether a cellular automaton is reversible or not the reversibility of its rule matrix is studied via linear algebraic tools. However, in this particular study the authors consider a novel approach. By observing the algebraic structures of rule matrices that represent these families and associating them with polynomials in two variables in a quotient ring, the solution to the reversibility problem is simplified greatly. Hence, this approach not only drastically decreases the computational time for determining the reversibility of these families but also provides an explicit construction of reverse cellular automata in the case of the existence of their inverses. The paper concludes with a consideration of the rule matrices of these families in obtaining linear codes over group rings, which are referred to as zero-divisor codes.

Key words: Cellular automata, reversibility, linear codes, group rings

1. Introduction

Complex structures are generally divided into small pieces that are called cells and are studied accordingly. Observations have shown that the evolution of dynamical systems depends on the interactions among their neighboring cells. Due to this reason, dynamic structures are studied by cellular automata (CAs) that are composed of cells that interact with each other with respect to some local rules. Cellular automata have proven to be one of the best tools to model such dynamical systems. The first and successful attempt on modeling dynamical systems by cellular automata was presented by Ulam and von Neumann [26]. In this particular study, it is shown that even by assuming simple local rules among the neighboring cells one obtains very complicated dynamical systems after a reasonable number of steps. On the other hand, having represented a dynamical system by a CA, it is also important to be able to trace the configuration back to a particular stage. Such CAs that enjoy this property are called reversible or shortly RCAs. RCAs are deterministic in both directions of time [16]. RCAs have found applications in many diverse areas such as physics, cryptography (generating pseudo-random numbers), computer science, chemistry, image processing ([25]), analysis of universal model of computations ([19]), and coding theory, which is a partial but not an exhaustive list [1, 5, 9, 14, 15, 22, 20].

The reversibility problem of CA and Garden of Eden (for short GOE) configurations are closely related and both are important concepts. In [18], Moore showed that the existence of mutually erasable configurations in a two-dimensional (2D) tessellation space is sufficient for the existence of GOE configurations. In [3], Amoroso

*Correspondence: mkoroglu@yildiz.edu.tr
2010 *AMS Mathematics Subject Classification:* Primary 28D20; Secondary 37A35, 37B40.

et al. established a necessary and sufficient condition for the existence of GOE configurations with finitely many configurations. In [8], Hartman and Heule demonstrated how quantified Boolean formula (QBF) and satisfiability (SAT) techniques can be used to find GOE in Conway's Game of Life.

In [2], the authors studied the reversibility of 2D CAs defined by a local rule, which they called the nearest neighborhoods and prolonged next nearest neighborhoods (briefly, $NPNN$), over the field $\mathbb{Z}_p$ with null boundary, and further they characterized these CAs with some of their important characteristics. Recently, studies on the reversibility problem of some families of CAs are also presented in [21, 22, 24]. Some further and related studies on this direction can be found in [4, 7, 12, 13].

In the present paper, we restudy the reversibility problem of 2D CAs with respect to the rule $NPNN$ ([23]) with periodic boundary condition (PBC) via a novel algebraic approach. In [23], originally the problem was studied for a subfamily and it was solved by using classical algorithmic rank computations. Here, we construct a one to one correspondence between the rule matrices of $NPNN$ and the elements of a quotient ring of polynomials with two indeterminates. By means of this correspondence, we are able to relate the reversibility of CA with the inverse problem of two variable polynomials in the quotient ring.

The rest of the paper is organized as follows: in Section 2, we present some related basic definitions and concepts. In Section 3, we present the rule matrix that represents a 2-D finite CA with PBC generated by the local rule $NPNN$ over the field $\mathbb{Z}_p$. In Section 4, the reversibility problem is presented and solved by transforming the problem into a quotient ring of two variables. Here the problem becomes equivalent to determining the units of this ring and further by finding the inverses of the elements in the ring we are able to give explicitly the inverse matrix of the rule matrix. In Section 5, we present an example of zero-divisor codes by using this family of CAs and then finally we conclude the paper.

2. Preliminaries

2.1. Cellular automata basics

In this section, we introduce a family of 2D CAs over the finite field with p (prime) elements $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ by using some local rules. First, we recall the definition of a 2D CA. We consider the 2-dimensional integer lattice $\mathbb{Z}^2$ and the configuration space $\Omega = \mathbb{Z}_p^{\mathbb{Z}^2}$ with elements

$$\sigma : \mathbb{Z}^2 \to \mathbb{Z}_p.$$

σ_v as usual denotes the value of σ at a point $v \in \mathbb{Z}^2$. Let $u_1, \ldots, u_s \in \mathbb{Z}^2$ be a finite set of distinct elements in the lattice and $F : \mathbb{Z}_p^s \to \mathbb{Z}_p$ be a function. A CA with the local rule F is defined as a pair (Ω, T_F), where the global transition map $U_F : \Omega \to \Omega$ is given by

$$(U_F\sigma)_v = F(\sigma_{v+u_1}, \ldots, \sigma_{v+u_s}), v \in \mathbb{Z}^2.$$

2D CAs can be viewed locally as matrices of size $m \times n$ over $\mathbb{Z}_p$. The entries of these matrices, called cells, are assigned values referred to as configurations. As time evolves, the configurations change. If the transition is linear as in our case, then this is called the local rule matrix of CA. The local rule matrix determines the transition of the states from time t to next time $(t+1)$ modulo p. In a 2D CA (see Figure) the closest cells to the center cell, excluding itself, of radius one and two are the four and the eight neighbors (see [4, 6, 7] for further details). 2D CAs are defined and studied with respect to their active neighbors, i.e. the neighbors that are assumed to affect the cell in the center. In general, it is well known that the closest cells to the center are

more effective. There are some classical types of neighborhoods, but in this work we only restrict ourselves to the nearest neighborhood and prolonged next nearest neighborhood (briefly, $NPNN$), which consists of cells with radius two or less. These cells are located at the main directions North, South, East, and West (see Figure). As mentioned above, the relation among the cells is assumed to be linear and hence one can define the $(t+1)^{st}$ state of the $(i,j)^{st}$ cell as follows:

$$x_{(i,j)}^{(t+1)} = ax_{(i-1,j)}^{(t)} + bx_{(i,j+1)}^{(t)} + cx_{(i+1,j)}^{(t)} + dx_{(i,j-1)}^{(t)} + ex_{(i-2,j)}^{(t)} + fx_{(i,j+2)}^{(t)} + gx_{(i+2,j)}^{(t)} + hx_{(i,j-2)}^{(t)} (\text{mod } p), \qquad (1)$$

where $a, b, c, d, e, f, g, h \in \mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$.

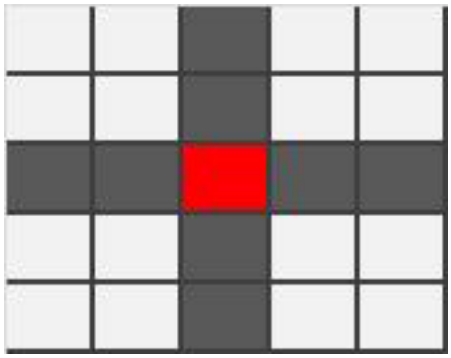


Figure. The neighborhood $NPNN$, i.e. the plus symbol, where the red cell is called the center cell and the gray ones are the active neighbors of the center cell.

In order to define a CA according to the neighboring relations, which is referred to as the local rule function (see Eq. (1)), the following ordering and hence the numbering of the rules is introduced:

$$RN = ap^0 + bp^1 + cp^2 + dp^3 + ep^4 + fp^5 + gp^6 + hp^7 = (hgfedcba)_p . \qquad (2)$$

Since the lattice of cells is infinite dimensional, in order to study CAs considered locally finite, the interactions on the boundary cells are considered under two assumptions that are commonly made:

- A periodic boundary CA is one where the boundary cells are assumed to be neighbored by its own copies periodically.
- A null boundary CA is one where the boundary cells are assumed to be neighbored by zero states only.

Now we give the mathematical definition of a 2D CA generated by the local rule $NPNN$ with PBC (briefly $NPNNP$). In the sequel, for convenience we will use notation for $NPNNP$.

A 2-D CA with the local rule R_N and PBC is a function $U_{R_N} : \Omega \to \Omega$ defined by

$$\begin{aligned} (U_{R_N} x)_{(i,j)}^{(t)} &= ax_{(i-1,j)}^{(t)} + bx_{(i,j+1)}^{(t)} + cx_{(i+1,j)}^{(t)} + dx_{(i,j-1)}^{(t)} + ex_{(i-2,j)}^{(t)} + fx_{(i,j+2)}^{(t)} + gx_{(i+2,j)}^{(t)} + hx_{(i,j-2)}^{(t)} \\ &= x_{(i,j)}^{(t+1)} (\text{mod } p). \end{aligned} \qquad (3)$$

In this paper, we consider 2D finite CAs generated by the rule $NPNN$ with PBC. It is well known that these CAs are discrete dynamical systems formed by a finite 2D array $m \times n$ and composed of identical objects called cells.

Let $\Phi : M_{m\times n}(\mathbb{Z}_p) \to \mathbb{Z}_p^{mn}$. Φ takes the t^{th} state $[X_t]$ given by

$$\begin{pmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{pmatrix} \longrightarrow (x_{11}, x_{12}, \ldots, x_{1n}, \ldots, x_{m1}, \ldots, x_{mn})^T,$$

where T stands for the transpose of a matrix. Therefore, the local rules will be assumed to act on $\mathbb{Z}_p^{mn}$ rather than $M_{m\times n}(\mathbb{Z}_p)$.
Let $[X_t]_{m\times n}$ be a matrix of size $m \times n$ with entries from $\mathbb{Z}_p$

$$[X_t]_{m\times n} = \begin{pmatrix} x_{11}^{(t)} & \cdots & x_{1n}^{(t)} \\ \vdots & \ddots & \vdots \\ x_{m1}^{(t)} & \cdots & x_{mn}^{(t)} \end{pmatrix}.$$

This matrix is called either the information matrix or the configuration of a 2D finite CA at time t.
By using (3), we can define the evolution of a configuration as a matrix multiplication by

$$(T_{R_N})_{mn\times mn} \begin{pmatrix} x_{11}^{(t)} \\ \vdots \\ x_{1n}^{(t)} \\ \vdots \\ x_{m1}^{(t)} \\ \vdots \\ x_{mn}^{(t)} \end{pmatrix} = \begin{pmatrix} x_{11}^{(t+1)} \\ \vdots \\ x_{1n}^{(t+1)} \\ \vdots \\ x_{m1}^{(t+1)} \\ \vdots \\ x_{mn}^{(t+1)} \end{pmatrix}$$

where $x_{i,j}^{(t+1)}$ is defined in Eq. (1). The rule matrix $(T_{R_N})_{mn\times mn}$ is the representation matrix of a 2D finite CA$_{m\times n}$ with rule R_N (for further details please see [4]). In a more concise form, we have

$$[T_{R_N}]_{mn\times mn} \begin{pmatrix} X_1^T \\ X_2^T \\ X_3^T \\ \vdots \\ X_m^T \end{pmatrix}_{mn\times 1} = \begin{pmatrix} Y_1^T \\ Y_2^T \\ Y_3^T \\ \vdots \\ Y_m^T \end{pmatrix}_{mn\times 1}.$$

For example, if $i = j = 3$, then we have

$$x_{33}^{(t+1)} = ax_{23}^{(t)} + bx_{34}^{(t)} + cx_{43}^{(t)} + dx_{32}^{(t)} + ex_{13}^{(t)} + fx_{35}^{(t)} + gx_{53}^{(t)} + hx_{31}^{(t)} (\text{mod } p).$$

3. Rule matrix of 2D finite CA with rule R_N

In this section, we present the rule matrix that represents a 2D CA with PBC generated by the local rule R_N over the field $\mathbb{Z}_p$, which are given in [23] in more detail.

Table 1. An information (or configuration) matrix of order 5×5 with PBC.

x_{44}	x_{45}	x_{41}	x_{42}	x_{43}	x_{44}	x_{45}	x_{41}	x_{42}
x_{54}	x_{55}	x_{51}	x_{52}	x_{53}	x_{54}	x_{55}	x_{51}	x_{52}
x_{14}	x_{15}	x_{11}	x_{12}	x_{13}	x_{14}	x_{15}	x_{11}	x_{12}
x_{24}	x_{25}	x_{21}	x_{22}	x_{23}	x_{24}	x_{25}	x_{21}	x_{22}
x_{34}	x_{35}	x_{31}	x_{32}	x_{33}	x_{34}	x_{35}	x_{31}	x_{32}
x_{44}	x_{45}	x_{41}	x_{42}	x_{43}	x_{44}	x_{45}	x_{41}	x_{42}
x_{54}	x_{55}	x_{51}	x_{52}	x_{53}	x_{54}	x_{55}	x_{51}	x_{52}
x_{14}	x_{15}	x_{11}	x_{12}	x_{13}	x_{14}	x_{15}	x_{11}	x_{12}
x_{24}	x_{25}	x_{21}	x_{22}	x_{23}	x_{24}	x_{25}	x_{21}	x_{22}

Theorem 1 *Let $a, b, c, d, e, f, g, h \in \mathbb{Z}_p^*$, $m \geq 5$ and $n \geq 5$. Then the rule matrix of T_{R_N} from $\mathbb{Z}_p^{mn}$ to $\mathbb{Z}_p^{mn}$, which takes the t^{th} state $[X_t]$ (as identified in (3)) to the $(t+1)^{st}$ state $[X_{t+1}] = [Y]$, is given by*

$$[23](T_{R_N})_{mn\times mn} = \begin{pmatrix} S & cI & gI & 0 & \cdots & \cdots & eI & aI \\ aI & S & cI & gI & \cdots & \cdots & 0 & eI \\ eI & aI & S & cI & gI & \cdots & 0 & 0 \\ 0 & eI & aI & S & \cdots & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & eI & aI & S & cI & gI \\ gI & \cdots & \cdots & 0 & eI & aI & S & cI \\ cI & gI & \cdots & \cdots & 0 & eI & aI & S \end{pmatrix}_{mn\times mn} \tag{4}$$

where each submatrix is of order $n \times n$, and

$$S_{n\times n} = \begin{pmatrix} 0 & b & f & 0 & 0 & 0 & \cdots & h & d \\ d & 0 & b & f & 0 & 0 & \cdots & 0 & h \\ h & d & 0 & b & f & 0 & \cdots & 0 & 0 \\ 0 & h & d & 0 & b & f & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ f & \cdots & \cdots & \cdots & 0 & h & d & 0 & b \\ b & f & \cdots & \cdots & \cdots & 0 & h & d & 0 \end{pmatrix}_{n\times n}. \tag{5}$$

For example, if we take $m = 5$ and $n = 5$, then the representation matrix T_{R_N} is of order 25×25 and it acts on configurations of sizes 5×5 with PBC.

Since the action of the linear transformation on the basis leads to the unique determination of itself, one needs only to check the values on the basis. To see this, if the local rule in Eq. (1) is applied to all cells of the first row of information matrix 5×5, then the first block row of the rule matrix T_{R_N} is determined. Next by reapplying the rule R_N to the second row of information matrix 5×5, the second block row of the rule matrix T_{R_N} is also determined. Similarly, the rest of the block rows of rule matrix T_{R_N} are determined.

More explicitly, by considering the neighborhood presented in Table 1 and Theorem 1, one obtains the matrix for $m = 5$ and $n = 5$ as follows:

$$(T_{R_N})_{25\times 25} = \begin{pmatrix} S & cI_5 & gI_5 & eI_5 & aI_5 \\ aI_5 & S & cI_5 & gI_5 & eI_5 \\ eI_5 & aI_5 & S & Ic_5 & gI_5 \\ gI_5 & eI_5 & aI_5 & S & cI_5 \\ cI_5 & gI_5 & eI_5 & aI_5 & S \end{pmatrix},$$

where each submatrix is of order 5×5, and $S_{5\times 5}=\begin{pmatrix} 0 & b & f & h & d\\ d & 0 & b & f & h\\ h & d & 0 & b & f\\ f & h & d & 0 & b\\ b & f & h & d & 0 \end{pmatrix}_{5\times 5}$.

4. The Reversibility of R_N

In the previous section, we showed that the rule matrix consists of block circulant matrices and further it is itself a circulant matrix of block matrices. In this section, these structural rule matrices are going to be represented by elements of a special quotient ring and hence the reversibility problem of these CAs will be answered by means of this approach.

Let $R=\mathbb{Z}_p[x,y]/\langle x^n-1,y^m-1\rangle$ be the quotient ring of two indeterminates x and y. We can represent each polynomial of R by a circulant matrix whose entries are also circulant matrices in the $\mathbb{Z}_p$. In order to accomplish this correspondence, we let $f(x,y)=\sum_{i=1}^{n}a_{1i}^{1}x^{i-1}+\left(\sum_{i=1}^{n}a_{1i}^{2}x^{i-1}\right)y+\ldots+\left(\sum_{i=1}^{n}a_{1i}^{m}x^{i-1}\right)y^{m-1}$ be a polynomial in the quotient ring R and define the matrix representation from R onto $M_{nm}(\mathbb{Z}p)$ as

$$\begin{aligned}\Phi &: R\to M_{nm}(\mathbb{Z}_p)\\ \Phi(f(x,y)) &= \begin{pmatrix} A_1 & A_2 & \ldots & A_{m-1} & A_m\\ A_m & A_1 & A_2 & \ldots & A_{m-1}\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ A_2 & \ldots & A_{m-1} & A_m & A_1 \end{pmatrix}, \end{aligned}\tag{6}$$

where

$$A_j=\begin{pmatrix} a_{11}^{j} & a_{12}^{j} & \ldots & a_{1n}^{j}\\ a_{1n}^{j} & a_{11}^{j} & \ldots & a_{1n-1}^{j}\\ \vdots & \vdots & \vdots & \vdots\\ a_{12}^{j} & a_{13}^{j} & \ldots & a_{11}^{j} \end{pmatrix}_{n\times n} \quad (1\le j\le m).$$

Φ is an injective ring homomorphism.

Now we give an example of this representation.

Example 1 *Let $f(x,y)=2x+2x^2+x^3+x^4+y+2y^2+y^3+2y^4$ be a polynomial in the quotient ring $R=\mathbb{Z}_3[x,y]/\langle x^5-1,y^5-1\rangle$. Then the corresponding matrix of $f(x,y)$ is*

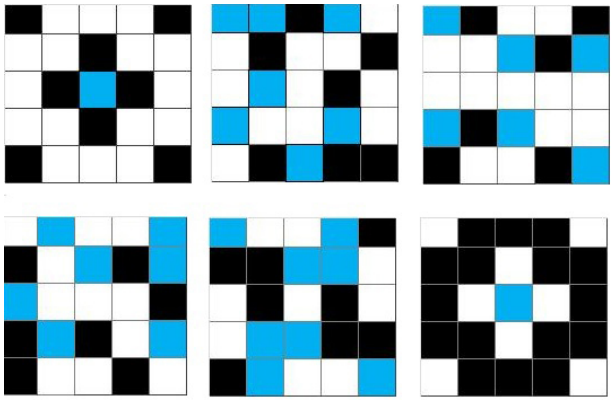
$$\Phi(f(x,y))=\begin{pmatrix} A_1 & A_2 & A_3 & A_4 & A_5\\ A_5 & A_1 & A_2 & A_3 & A_4\\ A_4 & A_5 & A_1 & A_2 & A_3\\ A_3 & A_4 & A_5 & A_1 & A_2\\ A_2 & A_3 & A_4 & A_5 & A_1 \end{pmatrix},$$

where

$$A_1=\begin{pmatrix} 0 & 2 & 2 & 1 & 1\\ 1 & 0 & 2 & 2 & 1\\ 1 & 1 & 0 & 2 & 2\\ 2 & 1 & 1 & 0 & 2\\ 2 & 2 & 1 & 1 & 0 \end{pmatrix}, \qquad A_2=A_4=I_5,\ \text{and } A_3=A_5=2I_5.$$

$\Phi(f(x,y))$ is also the rule matrix of a CA with $n=5$, $m=5$ and $a=2,b=2,c=1,d=1,e=1,f=2,g=2,h=1$. Some specific configurations with respect to this rule are presented in Table 2. Further, by Eq. (2) this rule can be labeled with the rule number $(12211122)_3 = 3^7+2.3^6+2.3^5+3^4+3^3+3^2+2.3+2.1=4256$.

Table 2. Some configurations of the rule 4256



Some configurations of the rule 4256 given in Example 1, where the first one is the initial configuration and the sequent from left to right are configurations at time $t=1,2,3,4$, and 8. The white cells have 0-states, the black cells have 1-states, and the blue cells have 2-states.

Theorem 2 *Let $R=\mathbb{Z}_p[x,y]/\langle x^n-1,y^m-1\rangle$ be the quotient ring of two indeterminates and let $f(x,y)\in R$. The matrix $\Phi(f(x,y))$ is nonsingular if and only if $f(x,y)$ is a unit in the quotient ring R.*

Proof Assume that $f(x,y)\in R$ is a unit. Then there exists a unique $g(x,y)\in R$ such that $f(x,y)\,g(x,y)=1$. By applying Φ to both sides of the last equality we get $\Phi(f(x,y))\,\Phi(g(x,y))=\Phi(1)$. Equivalently, $AB=I_{mn}$ implies $A^{-1}=B$. Therefore, the matrix $\Phi(f(x,y))=A$ is nonsingular. Conversely, suppose that $\Phi(f(x,y))=A$ is nonsingular. Then there exists a unique matrix B such that $AB=I_{mn}$ and $\Phi(g(x,y))=B$. By taking a preimage of A and B we get $\Phi^{-1}(A)\,\Phi^{-1}(B)=f(x,y)\,g(x,y)=\Phi^{-1}(I)=1$. Hence, $f(x,y)$ is a unit in the ring R and has an inverse $g(x,y)$. □

Theorem 3 *Let $R=\mathbb{Z}_p[x,y]/\langle x^n-1,y^m-1\rangle$ be the quotient ring of two indeterminates and let $f(x,y)\in R$. The matrix $\Phi(f(x,y))$ is singular if and only if $f(x,y)$ is a zero-divisor in the quotient ring R.*

Proof The proof is analogous to the previous proof and so we skip it. □

Now we give a decomposition of the ring R. Let $x^n-1=f_1(x)\dots f_r(x)$, $y^m-1=g_1(y)\dots g_s(y)$ be factorizations of x^n-1 and y^m-1 in irreducible polynomials, respectively. Then by applying the Chinese remainder theorem we get the following decomposition:

$$\begin{aligned} R &\cong \mathbb{Z}_p[x,y]/\langle f_1(x),g_1(y)\rangle \oplus \mathbb{Z}_p[x,y]/\langle f_1(x),g_2(y)\rangle \\ &\quad \oplus\dots\oplus \mathbb{Z}_p[x,y]/\langle f_r(x),g_s(y)\rangle \end{aligned} \tag{7}$$

$$\begin{aligned} \psi &: R\to S \\ \psi(f(x,y)) &= (f(x,y)\,(mod\ f_1(x),g_1(y)),\dots,f(x,y)\,(mod\ f_r(x),g_s(y))). \end{aligned} \tag{8}$$

This decomposition gives us an easy way to determine the zero-divisors and the units of the quotient ring R.

Corollary 1 *Let $R=\mathbb{Z}_p[x,y]/\langle x^n-1,y^m-1\rangle$ be the quotient ring of two indeterminates and let $f(x,y)\in R$. $f(x,y)$ is a zero-divisor of R if at least one of the components of (8) is zero or a zero-divisor.*

Corollary 2 *Let $R=\mathbb{Z}_p[x,y]/\langle x^n-1,y^m-1\rangle$ be the quotient ring of two indeterminates and let $f(x,y)\in R$. $f(x,y)$ is a unit of R if all components of (8) are units.*

Example 2 *Let $R=\mathbb{Z}_2[x,y]/\langle x^3-1,y^3-1\rangle$. Then $x^3-1=(x-1)\left(x^2+x+1\right)=f_1(x)f_2(x)$ and $y^3-1=(y-1)\left(y^2+y+1\right)=g_1(y)g_2(y)$.*

$$\begin{aligned} R &\cong \mathbb{Z}_2[x,y]/\langle f_1(x),g_1(y)\rangle \oplus \mathbb{Z}_2[x,y]/\langle f_1(x),g_2(y)\rangle \\ &\quad \oplus \mathbb{Z}_2[x,y]/\langle f_2(x),g_1(y)\rangle \oplus \mathbb{Z}_2[x,y]/\langle f_2(x),g_2(y)\rangle . \end{aligned}$$

Consider the polynomial $f(x,y)=1+x+x^2+y+xy+xy^2+x^2y^2\in\mathbb{Z}_2[x,y]/\langle x^3-1,y^3-1\rangle$. Then $\psi(f(x,y))=(1,1,x,1+xy)$. The element $1+xy\in\mathbb{Z}_2[x,y]/\langle f_2(x),g_2(y)\rangle$ is a zero divisor and so is $f(x,y)=1+x+x^2+y+xy+xy^2+x^2y^2\in\mathbb{Z}_2[x,y]/\langle x^3-1,y^3-1\rangle$. The corresponding matrix of $f(x,y)$ is

$$\Phi(f(x,y))=\begin{pmatrix} 1&1&1&1&1&0&0&1&1\\ 1&1&1&0&1&1&1&0&1\\ 1&1&1&1&0&1&1&1&0\\ 0&1&1&1&1&1&1&1&0\\ 1&0&1&1&1&1&0&1&1\\ 1&1&0&1&1&1&1&0&1\\ 1&1&0&0&1&1&1&1&1\\ 0&1&1&1&0&1&1&1&1\\ 1&0&1&1&1&0&1&1&1 \end{pmatrix}$$

and $det(\Phi(f(x,y)))=0 \mod 2$.

Similarly, consider the polynomial $f(x,y)=1+x^2+y+xy+x^2y^2\in\mathbb{Z}_2[x,y]/\langle x^3-1,y^3-1\rangle$, where $\psi(f(x,y))=(1,1+y,x,1)$. All components of $\psi(f(x,y))$ are units and so

$$f(x,y)\in\mathbb{Z}_2[x,y]/\langle x^3-1,y^3-1\rangle$$

is a unit. Thus the matrix corresponding to $f(x,y)$ given below is invertible.

$$\Phi(f(x,y))=\begin{pmatrix} 1&0&1&1&1&0&0&0&1\\ 1&1&0&0&1&1&1&0&0\\ 0&1&1&1&0&1&0&1&0\\ 0&0&1&1&0&1&1&1&0\\ 1&0&0&1&1&0&0&1&1\\ 0&1&0&0&1&1&1&0&1\\ 1&1&0&0&0&1&1&0&1\\ 0&1&1&1&0&0&1&1&0\\ 1&0&1&0&1&0&0&1&1 \end{pmatrix}.$$

Note that $\det(\Phi(f(x,y)))=1 \mod 2$.

Theorem 4 *Let $R=\mathbb{Z}_p[x,y]/\langle x^n-1,y^m-1\rangle$ be the quotient ring of two indeterminates and let $R_1\oplus R_2\oplus\ldots\oplus R_t$ be a minimal decomposition of R. Then $rank(\Phi(f(x,y)))=rank(\Phi(f_1(x,y)))+\ldots+rank(\Phi(f_t(x,y)))$.*

Proof. Since the decomposition stated in the theorem is minimal every component can be considered as a field extension of order $\alpha_i,\ i=1,2,\ldots,t$. The image of $f(x,y)$ in each component is either a unit or the zero element. Moreover, we can consider each element as a circulant matrix of order $\alpha_i,\ i=1,2,\ldots,t$. Then we get the following diagonal matrix:

$$\Phi(f(x,y))=\begin{pmatrix}\Phi(f_1(x,y)) & 0 & 0 & 0\\ 0 & \Phi(f_2(x,y)) & 0 & 0\\ & & \ddots & \\ 0 & 0 & & 0\\ 0 & 0 & 0 & \Phi(f_t(x,y))\end{pmatrix}.$$

All matrices located on the diagonal of $\Phi(f(x,y))$ are either unitary matrices or all zero matrices. From linear algebra we know that unitary matrices have full rank and the rank of an all zero matrix is zero. Therefore, the rank of $\Phi(f(x,y))$ is the sum of order of diagonal matrices. Thus, we have $rank(\Phi(f(x,y))) = rank(\Phi(f_1(x,y))) + \ldots + rank(\Phi(f_t(x,y)))$.

Example 3 *Let* $f(x,y)=1+x+x^2+y+xy+xy^2+x^2y^2\in\mathbb{Z}_2[x,y]/\langle x^3-1,y^3-1\rangle$. *By Example 2 we know that* $\Phi(f(x,y))$ *is irreversible. The decomposition*

$$\begin{aligned}&\mathbb{Z}_2[x,y]/\langle f_1(x),g_1(y)\rangle\oplus\mathbb{Z}_2[x,y]/\langle f_1(x),g_2(y)\rangle\\ &\oplus\mathbb{Z}_2[x,y]/\langle f_2(x),g_1(y)\rangle\oplus\mathbb{Z}_2[x,y]/\langle f_2(x),g_2(y)\rangle\end{aligned}$$

is not minimal, since the last part can be decomposed further as

$$(\mathbb{Z}_2[x,y]/\langle f_2(x),g_2(y)\rangle)(x+y)\oplus(\mathbb{Z}_2[x,y]/\langle f_2(x),g_2(y)\rangle)(1+x+y),$$

where $x+y$ *is an idempotent of the* $\mathbb{Z}_2[x,y]/\langle f_2(x),g_2(y)\rangle$. *This can be also viewed as*

$$\mathbb{F}_2\oplus\mathbb{F}_4\oplus\mathbb{F}_4\oplus\mathbb{F}_4\oplus\mathbb{F}_4.$$

Then we have $\psi(f(x,y))=(1,1,x,0,1+xy)$, *where* $1+xy$ *is a unit in*

$$(\mathbb{Z}_2[x,y]/\langle f_2(x),g_2(y)\rangle)(1+x+y).$$

Then the rank of $\Phi(f(x,y))$ *is the sum of the rank of the components, i.e.* $rank(\Phi(f(x,y)))=1+2+2+0+2=7$.

Theorem 5 *Let* $R=\mathbb{Z}_p[x,y]/\langle x^n-1,y^m-1\rangle$ *be the quotient ring of two indeterminates where* $(m,n)=1$. *Then* $R\cong\mathbb{Z}_p[z]/\langle z^{nm}-1\rangle$.

Proof. Define $\varphi: R\to\mathbb{Z}_p[z]/\langle z^{nm}-1\rangle$ as $x\mapsto z^m$ and $y\mapsto z^n$. Then $\varphi(x+y)=z^n+z^m$ and $\varphi(xy)=z^{n+m}=z^nz^m=\varphi(x)\varphi(y)$. It is easy to see the injectivity of φ. Since the range and the domain of the map are finite φ is also surjective. Consequently φ is a ring isomorphism.

Corollary 3 *Let* $R=\mathbb{Z}_p[x,y]/\langle x^n-1,y^m-1\rangle$ *be the quotient ring of two indeterminates where* $(m,n)=1$ *and let* $f(x,y)\in R$. $f(x,y)$ *is a unit in* R *if and only if* $(\varphi(f(x,y)),z^{nm}-1)=1$.

Corollary 4 *Let* $R=\mathbb{Z}_p[x,y]/\langle x^n-1,y^m-1\rangle$ *be the quotient ring of two indeterminates,* $(m,n)=1$ *and let* $f(x,y)\in R$. $f(x,y)$ *is a zero-divisor in* R *if and only if* $\varphi(f(x,y))\,|\,z^{nm}-1$.

Example 4 *Let* $f(x,y) = 2x+2x^2+x^4+y+y^2+2y^3$ *be a polynomial in the quotient ring* $R = \mathbb{Z}_3[x,y]/\langle x^5-1, y^4-1\rangle$. *Then the corresponding matrix of* $f(x,y)$ *is*

$$\Phi(f(x,y)) = \begin{pmatrix} A_1 & A_2 & A_3 & A_4 \\ A_4 & A_1 & A_2 & A_3 \\ A_3 & A_4 & A_1 & A_2 \\ A_2 & A_3 & A_4 & A_1 \end{pmatrix},$$

and

$$A_1 = \begin{pmatrix} 0 & 2 & 2 & 0 & 1 \\ 1 & 0 & 2 & 2 & 0 \\ 1 & 1 & 0 & 2 & 2 \\ 0 & 1 & 1 & 0 & 2 \\ 2 & 0 & 1 & 1 & 0 \end{pmatrix}, \qquad A_2 = A_3 = I_5, \text{ and } A_4 = 2I_5$$

and $det(\Phi(f(x,y))) = 0 \mod 3$. *Algebraically,* $\varphi(f(x,y)) = 2z^4 + z^5 + 2z^8 + z^{10} + 2z^{15} + z^{16}$ *and* $\left(\varphi(f(x,y)), z^{20}-1\right) = 2+z^2$, *and so* $f(x,y)$ *is a zero-divisor of* R.

5. Group rings and zero-divisor codes

In this section we present an application to zero-divisor codes obtained from rule matrix of R_N. Error correcting codes are used in applications such as storing or transferring digital data. Due to some recently established relations and potential good examples, the study of codes over fields has been extended to study of codes over rings. Such an extension for codes over group rings is presented by Hurley and Hurley in [10]. They have introduced the concept of zero-divisor codes. Here, we summarize the basic theory of zero-divisor codes and present some applications of such codes obtained through the representation matrices of CAs studied in the previous sections.

5.1. Group ring basics

Let R be a ring and G be a group and define the group ring RG to be the set of all R-linear combinations $u = \sum_{g\in G} \alpha_g g$, where $\alpha_g \in R$ and where only finitely many of the α_g's are nonzero. The sum and the product of two group ring elements are defined respectively as

$$u+v = \sum_{g\in G} \alpha_g g + \sum_{g\in G} \beta_g g = \sum_{g\in G} (\alpha_g + \beta_g) g$$

and

$$uv = \left(\sum_{g\in G} \alpha_g g\right)\left(\sum_{h\in G} \beta_h h\right) = \sum_{g,h\in G} \alpha_g \beta_h gh.$$

Since G is a group the product can be rewritten as

$$uv = \sum_{g\in G} \left(\sum_{h\in G} \alpha_h \beta_{h^{-1}g} h\right) g.$$

Example 5 *Let* $R = \mathbb{Z}_2 = \{0,1\}$ *and* $G = C_3 = \left\{1, g, g^2\right\}$. *Then*

$$\mathbb{Z}_2 C_3 = \left\{0, 1, g, g^2, 1+g, 1+g^2, g+g^2, 1+g+g^2\right\}.$$

For further and detailed information on group rings the authors may refer to [17].

Definition 1 *Let* R *be a ring.*

- *A nonzero element* $z \in R$ *is said to be a zero-divisor if and only if there exists a nonzero* $r \in R$ *such that* $zr = 0$.
- *An element* $u \in R$ *is said to be a unit if and only if there exists an element* $v \in R$ *such that* $uv = 1 = vu$. *If such a* v *exists, then it is generally written as* u^{-1}.

Let $\{g_1, g_2, \ldots, g_n\}$ be a fixed listing of the elements of G. The RG matrix $M(RG, w) \in R_{n\times n}$ (the ring of $n \times n$ matrices) associated with the group ring element $w = \sum_{i=1}^{n} \alpha_{g_i} g_i \in RG$ is defined as

$$M(RG, w) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \ldots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \ldots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \ldots & \alpha_{g_n^{-1}g_n} \end{pmatrix}.$$

A group ring RG is isomorphic to a ring of RG matrices over R, which is a subring of $R_{n\times n}$ [11].

Example 6 *The associated* RG *matrix of the element* $w = 1 + g \in \mathbb{Z}_2 C_3$ *is*

$$M(\mathbb{Z}_2 C_3, w) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}.$$

5.2. Zero-divisor codes from rule matrix R_N

Zero divisor codes are introduced by [10]. Following the method introduced in [10], here we consider and use the rule matrices and hence their corresponding representations in the quotient ring to devise zero divisor codes. We present examples that illustrate the relations.

Definition 2 *[10] Let* W *be a submodule of* RG *and* $u \in RG$, $x \in W$. *A group ring encoding is a mapping* $f : W \to RG$, *such that* $f(x) = xu$ *or* $f(x) = ux$. *In the latter case,* f *is a left group ring encoding. In the former, it is a right group ring encoding.*

$$C = \{ux \,|\, x \in W\} \text{ or } C = \{xu \,|\, x \in W\}.$$

Definition 3 *[10] Let* u *be a zero-divisor in* RG, *i.e.* $uv = 0$ *for some nonzero* $v \in RG$. *Let* W *be a submodule of* RG *with basis consisting of group elements* $S \subseteq G$. *A zero-divisor code* C *is defined as* $C = \{ux \,|\, x \in W\} = uW$ *or* $C = \{xu \,|\, x \in W\} = Wu$. *A zero-divisor code is constructed from a zero-divisor* u, *and a submodule* W. u *is said to be a generator element of the code* $C = Wu$ *relative to the submodule* W.

Definition 4 *[10] A set of group ring elements $T \subset RG$ is linearly independent if, for $\alpha_x \in R$, $\sum_{x \in T} \alpha_x x = 0$ only when α_x for all $x \in T$. Otherwise T is linearly dependent.*

- We define the rank (T) to be the maximum number of linearly independent elements of T. Thus rank $(T) = |T|$ if and only if T is linearly independent.
- Note that a zero-divisor code $C = Wu$, where W generated by S, is the submodule of RG consisting of all elements of the form $\sum_{g \in S} \alpha_g gu$. The dimension of this submodule is the rank (Su).

Example 7 *Let $RG = \mathbb{Z}_2 C_3 = \left\{1, g, g^2, 1+g, 1+g^2, g+g^2, 1+g+g^2\right\}$, $u = 1+g$ and $v = 1+g+g^2$. Furthermore, let W be the submodule of $\mathbb{Z}_2 C_3$ generated by $S = \{1, g\}$, i.e. $W = \langle S \rangle = \{0, 1, g, 1+g\}$. $(Su) = \{1, g\}(1+g) = \left\{1+g, g+g^2\right\}$, and so rank $(Su) = 2$. Moreover, the zero-divisor code is then $C = Wu = \left\{0, 1+g, g+g^2, 1+g^2\right\}$.*

Definition 5 *[10] For a zero-divisor u with rank $U = r$, u is said to be a principal zero-divisor if and only if there exists a $v \in RG$ such that $uv = 0$ and further rank $V = n - r$.*

Example 8 *The elements $u = 1+g$ and $v = 1+g+g^2$ in $\mathbb{Z}_2 C_3$ are principal zero-divisors.*

$$M(\mathbb{Z}_2 C_3, u) = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix},$$

$$M(\mathbb{Z}_2 C_3, v) = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}.$$

Theorem 6 *[10] Let $C = \{xu \mid x \in W\}$, where W is generated by S such that Su is linearly independent and $|S| = rankU = r$. Suppose further that $uv = 0$ in the group ring RG so that $rankV = n - r$. Then y is a codeword if and only if $yv = 0$.*

- The element $v \in RG$ is called the check element of the code C.

Example 9 *The element $v = 1+g+g^2$ in Example 7 is the check element of the given code C.*

Example 10 *Consider the polynomial $f(x,y) = 2x + 2x^2 + x^4 + y + y^2 + 2y^3 \in R = \mathbb{Z}_3[x,y]\left\langle x^5 - 1, y^4 - 1\right\rangle$. By Example 4 we know that $f(x,y)$ is a zero divisor and $\varphi(f(x,y)) = 2z^4 + z^5 + 2z^8 + z^{10} + 2z^{15} + z^{16}$. By using $\varphi^{-1}(f(x,y))$ we get the principal zero-divisor of $f(x,y)$ as $g(x,y) = 1+x+x^2+x^3+x^4+(1+x+x^2+x^3+x^4)y^2$. Moreover, $R \cong \mathbb{Z}_3(C_5 \times C_4) \cong \mathbb{Z}_3(C_{20})$. By using the method given above we obtain a $[20, 18, 2]$ cyclic linear code with check element $g(x,y)$.*

6. Conclusion

In this work, we relate the reversibility problem of a special family of 2D CAs with polynomial algebra. We present a map between these two structures and hence due to this relation we can then answer the reversibility question in polynomial algebra. Moreover, we can also compute the corresponding reverse rule if it exists in polynomial algebra and carry it back to CA. Similar to this approach, researchers may look for families of CAs

that can be represented by algebraic structures and try to address the reversibility problem and some other structural properties. Further, in this paper we present some examples of zero-divisor codes obtained through these CA rule matrices. Here, we present an illustrative example but this research direction is very new and group ring codes that are obtained by CA families need to be explored further.

Acknowledgment

This research was supported by the project 110T713 TÜBİTAK-TBAG. The authors wish to express their thanks to the anonymous reviewers, whose suggestions and remarks helped to improve the paper.

References

[1] Akın H, Siap I. On cellular automata over Galois rings. Inform Process Lett 2007; 103: 24-27.

[2] Akın H, Siap I, Uguz S. Two dimensional cellular automata with nearest and prolonged next nearest neighborhoods. Global Journal on Technology 2012; 1: 804-808.

[3] Amoroso S, Cooper G. The Garden of Eden theorem for finite configurations. P Am Math Soc 1970; 26: 158-164.

[4] Chattopdhyay P, Choudhury PP, Dihidar K. Characterisation of a particular hybrid transformation of two dimensional cellular automata. Comput Math Applic 1999; 38: 207-216.

[5] Czeizler E. On the size of inverse neighborhoods for one dimensional reversible cellular automata. Theor Comput Sci 2004; 325: 273-284.

[6] Das AK. Additive cellular automata: theory and application as a built-in self-test structure. PhD, I.I.T. Kharagpur, India, 1990.

[7] Dihidar K, Choudhury PP. Matrix algebraic formulae concerning some exceptional rules of two dimensional cellular automata. Inf Sci 2004; 165: 91-101.

[8] Hartman C, Heule MJH, Kwekkeboom K, Alain N. Symmetry in Gardens of Eden. The Electronic Journal of Combinatorics 2013; 20: 1-19.

[9] Hernández Encinas L, Martín del Rey A. Inverse rules of ECA with rule number 150, Appl Math Comput 2007; 189: 1782-1786.

[10] Hurley P, Hurley T. Codes from zero-divisors and units in group rings. International Journal of Information and Coding Theory 2009; 1: 57-87.

[11] Hurley T. Group rings and rings of matrices. Int J Pure Appl Math 2006; 31: 319-335.

[12] Khan AR, Choudhury PP, Dihidar K, Mitra S, Sarkar P. VLSI architecture of a cellular automata. Comput Math Applic 1997; 33: 79-94.

[13] Khan AR, Choudhury PP, Dihidar K, Verma R. Text compression using two dimensional cellular automata. Comput Math Applic 1999; 37: 115-127.

[14] Koroglu ME, Siap I, Akın H. Error correcting codes via reversible cellular automata over finite fields. Arab J Sci Eng 2014; 39: 1881-1887.

[15] Manzini G, Margara L. Invertible linear cellular automata over $\mathbb{Z}_m$: algorithmic and dynamical aspects. J Comput Syst Sci 1998; 56: 60-67.

[16] Martín del Rey A, Rodríguez Sánchez G. Reversibility of linear cellular automata. Appl Math Comput 2011; 217: 8360-8366.

[17] Milies CP, Sehgal SK. An Introduction to Group Rings. Dordrecht, The Netherlands: Kluwer Academic Publishing, 2002.

[18] Moore EF. Machine models of self reproduction. Proc Symp Appl Math 1962; 14: 17-33.

[19] Sahin U, Uguz S, Akın H, Siap I. Three-state von Neumann cellular automata and pattern generation. Appl Math Model 2015; 39: 2003-2024.

[20] Seck-Tuoh-Mora JC, Martínez GJ, McIntosh HV. The inverse behaviour of a reversible one-dimensional cellular automaton obtained by a single Welch diagram. J Cell Automata 2006; 1: 25-39.

[21] Siap I, Akın H, Uguz S. Structure and reversibility of 2-dimensional hexagonal cellular automata. Comp and Math Appl 2011; 62: 4161-4169.

[22] Siap I, Akın H, Koroglu ME. Reversible cellular automata with penta cyclic rule and ECCs. Int J Mod Phys C 2012; 23: 1-13.

[23] Siap I, Akın H, Uguz S. 2-D Reversible cellular automata with nearest and prolonged next nearest neighborhoods under periodic boundary. European Journal of Pure and Applied Mathematics 2013; 6: 315-334.

[24] Uguz S, Akın H, Siap I. Reversibility algorithms for 3-state hexagonal cellular automata with periodic boundaries. Int J Bifurcat Chaos 2013; 23: 1-15.

[25] Uguz S, Sahin U, Akın H, Siap I. 2D cellular automata with an image processing application. Acta Phys Polon A 2014; 125: 435-438.

[26] Von Neumann J. The Theory of Self Reproducing Automata. Burks AW, editor. Urbana, IL, USA: Univ. of Illinois Press, 1966.