REVISTA DE LA
UNIÓN MATEMÁTICA ARGENTINA
Vol. 56, No. 1, 2015, Pages 107–125
Published online: May 4, 2015

A NOTE ON THE REVERSIBILITY OF THE ELEMENTARY CELLULAR AUTOMATON WITH RULE NUMBER 90

A. MARTÍN DEL REY

Abstract. The reversibility properties of the elementary cellular automaton with rule number 90 are studied. It is shown that the cellular automaton considered is not reversible when periodic boundary conditions are considered, whereas when null boundary conditions are stated, the reversibility appears when the number of cells of the cellular space is even. The DETGTRI algorithm is used to prove these statements. Moreover, the explicit expressions of inverse cellular automata of reversible ones are computed.

1. Introduction

Cellular automata are simple models of computation capable to simulate physical, biological or environmental complex phenomena (see, for example, [19, 30]). This concept was introduced by J. von Neumann and S. Ulam in the late 1940s (see [17]), their motivation being to obtain a better formal understanding of biological systems that are composed of many identical objects that are relatively simple. The local interactions of these objects yield the pattern evolution of the cellular automata. Cellular automata have been studied from a dynamical system perspective, from a logic, automata and language theoretic perspective, and through ergodic theory.

Roughly speaking, a cellular automaton consists of a discrete spatial lattice of sites called cells, each one endowed at each time with a state belonging to a finite state set. The state of each cell is updated in discrete time steps according to a local transition function which depends on the states of the cells in some neighborhood around it. As the lattice is finite some type of boundary conditions must be imposed: usually null and periodic boundary conditions are considered.

Of special interest are those cellular automata for which the state set is $\mathbb{F}_2$ and the local transition function is a 3-variable boolean function whose variables are the states of the main cell and its two nearest neighbors (see, for example, [29]). They are called *elementary cellular automata*, and consequently there exist $2^{2^3} = 256$ of

2010 *Mathematics Subject Classification.* Primary 68Q80.

Key words and phrases. Reversibility, elementary cellular automata, transition rule number 90, matrix theory, DETGTRI algorithm.

This work was supported by Junta de Castilla y León (Spain) and by MINECO under grant TIN2014-55325-C2-2-R.

them. This type of cellular automata is very interesting since over the last decades several works related to their applications to cryptography have appeared (see, for example, [1, 12, 16, 22, 24, 26, 27, 28]).

Reversibility is an important property of cellular automata which implies that information can be neither created nor destroyed. A cellular automaton is said to be reversible when the evolution backwards is possible by means of the inverse cellular automata (see [25]). This property has been extensively studied in several works (see, for example, [2, 4, 5, 15, 18, 20, 23]). The majority of these works deal with the reversibility properties and their characterizations, and, unfortunately, there are few papers dedicated to the explicit computation of the inverse rules of reversible cellular automata ([11, 14, 21]).

The goal of this paper is to study the reversibility properties of one of the most important elementary cellular automata due to its applications to cryptography: the elementary cellular automata with rule number 90 (see [8]). It is well-known that the reversibility of this cellular automaton depends on the number of the cells ([3]), but the explicit computation of the inverse cellular automaton has not been done. In this paper, we introduce an alternative proof of the conditions for reversibility using the DETGTRI algorithm, and the novel explicit calculation of the inverse cellular automata is also shown.

The rest of the paper is organized as follows: In section 2 the basic theory of elementary cellular automata is introduced; in section 3 the problem of the reversibility of elementary cellular automaton with rule number 90 is shown, and finally some considerations about the reversibility of linear elementary cellular automata are presented in section 4.

2. Elementary cellular automata

2.1. **Basic theory.** *Elementary cellular automata* (ECA for short) are finite state machines formed by n memory units called cells that are arranged linearly, in such a way that each cell assumes a state from the finite state set $\mathbb{F}_2$ at every time step. The state of the ith cell at time t is denoted by $x_i^t \in \mathbb{F}_2$, and it changes synchronously in discrete time steps according to a *local transition function* f. This function is a 3-variable boolean function whose variables are the previous states of the three nearest neighbor cells, that is:

$$f\colon \mathbb{F}_2^3 \to \mathbb{F}_2$$
$$\left(x_{i-1}^t, x_i^t, x_{i+1}^t\right) \mapsto x_i^{t+1} = f\left(x_{i-1}^t, x_i^t, x_{i+1}^t\right)$$

for every $1 \leq i \leq n$. As a consequence, there exist $2^{2^3} = 256$ possible elementary cellular automata, each of which can be indexed by a rule number w which is computed as follows (see, for example, [30]):

$$0 \leq w = \sum_{i=0}^{7} \alpha_i \cdot 2^i \leq 255,$$

where the truth table of the boolean function f is:

s_{i-1}^t	s_i^t	s_{i+1}^t	$\mapsto$	s_i^{t+1}
0	0	0	$\mapsto$	α_0
0	0	1	$\mapsto$	α_1
0	1	0	$\mapsto$	α_2
0	1	1	$\mapsto$	α_3
1	0	0	$\mapsto$	α_4
1	0	1	$\mapsto$	α_5
1	1	0	$\mapsto$	α_6
1	1	1	$\mapsto$	α_7

As the number of cells is finite, some boundary conditions must be stated in order to preserve the well-defined evolution of the cellular automata. Periodic boundary conditions and null boundary conditions are usually considered. They are defined as follows:

- With periodic boundary conditions the cells are handled with a toroidal arrangement (when one goes off the left, one comes in on the right), that is: $x_i^t = x_j^t$ if $i \equiv j \pmod{n}$ for every t.
- If null boundary conditions are used the cells beyond each end are modified to maintain state 0 at every step of time: $x_i^t = 0$ for every t if $i < 1$ or $i > n$.

The n-dimensional vector $X^t = (x_1^t, \ldots, x_n^t) \in \mathbb{F}_2^n$ is called a *configuration* of the elementary cellular automaton at time t. The whole evolution of a particular cellular automaton can be comprised in its *global transition function*:

$$\begin{aligned} \Phi\colon \mathbb{F}_2^n &\to \mathbb{F}_2^n \\ X^t &\mapsto \Phi\left(X^t\right) = X^{t+1}. \end{aligned}$$

When the local transition function is a linear function:

$$x_i^{t+1} = f\left(x_{i-1}^t, x_i^t, x_{i+1}^t\right) = b \cdot x_{i-1}^t \oplus d \cdot x_i^t \oplus a \cdot x_{i+1}^t, \quad b, d, a \in \mathbb{F}_2,$$

the cellular automaton is called a *linear* cellular automaton (note that "$\oplus$" stands for the XOR operation, that is, the addition in $\mathbb{F}_2$). In this case, the evolution given by the global transition function can be interpreted in terms of matrix theory:

$$X^{t+1} = \Phi\left(X^t\right) = M_n \cdot (X^t)^T,$$

where

$$M_n = \begin{pmatrix} d & a & 0 & \cdots & 0 & \beta \\ b & d & a & \ddots & & 0 \\ 0 & b & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & a & 0 \\ 0 & & \ddots & b & d & a \\ \alpha & 0 & \cdots & 0 & b & d \end{pmatrix},$$

is the local transition matrix of the cellular automaton and the arithmetic is performed modulo 2, where:

$$\beta = \begin{cases} b, & \text{if periodic boundary conditions are stated,} \\ 0, & \text{if null boundary conditions are considered,} \end{cases}$$

$$\alpha = \begin{cases} a, & \text{if periodic boundary conditions are stated,} \\ 0, & \text{if null boundary conditions are considered.} \end{cases}$$

The graphic representation of the evolution of an elementary cellular automata, provided by its global transition function, is done by means of both the state transition diagram and the space-time diagram. The state transition diagram is a digraph with each configuration of the CA as a vertex and directed edges showing their progression under the global function, i.e. there is an edge between vertex u and vertex v if $\Phi(X) = Y$, where X stands for the configuration associated with u and Y is the configuration associated with v. The space-time diagram is a graphic diagram where the configurations are drawn as horizontal rows of states and the values 0 and 1 are depicted by white and black pixels respectively; the topmost row stands for the initial configuration and the time increases downwards.

A local transition function is called *reversible* if there exists another rule (called the inverse rule) that makes the automaton retrace its computation steps backwards in time. A cellular automaton is said to be reversible if it is defined by means of a reversible transition rule. The global transition function of a reversible cellular automata is bijective; consequently, if Φ is such a global transition function, then Φ^{-1} is the global transition function of the inverse cellular automata. Moreover, the following result holds ([3]):

Lemma 2.1. *In the case of linear cellular automata the study of the reversibility can be reduced to the study of the local transition matrix: a linear cellular automaton is reversible iff its local transition matrix is non-singular.*

The reversibility of a cellular automaton determines the state transition diagram: there are no trees in the state transition diagrams of a reversible cellular automaton; in particular, an elementary cellular automaton exhibits reversibility when every configuration (node) has exactly one predecessor.

The standard paradigm for cellular automata states that the evolution of all cells is governed by the same local transition function. Nevertheless, when different local transition rules are considered for different cells, hybrid cellular automata are given:

$$f_i : \mathbb{F}_2^3 \to \mathbb{F}_2$$
$$\left(x_{i-1}^t, x_i^t, x_{i+1}^t\right) \mapsto x_i^{t+1} = f_i\left(x_{i-1}^t, x_i^t, x_{i+1}^t\right)$$

for $1 \leq i \leq n$. The hybrid cellular automata obtained from an ECA rule is denoted by $\{w_1, w_2, \ldots, w_n\}$, where w_i stands for the rule number associated with the ECA with transition rule function f_i.

2.2. **The ECA with rule number 90.** The ECA with rule number 90 is the one defined by the following local transition function:

$$x_i^{t+1} = f\left(x_{i-1}^t, x_i^t, x_{i+1}^t\right) = x_{i-1}^t \oplus x_{i+1}^t.$$

Note that this is a linear cellular automaton and its global transition function can be defined in terms of matrices (where, as was mentioned in the last section, the arithmetic is performed modulo 2):

$$X^{t+1} = \Phi\left(X^t\right) = M_n \cdot \left(X^t\right)^T,$$

and M_n is the local transition matrix:

$$M_n = \begin{pmatrix} 0 & 1 & 0 & \cdots & \cdots & 0 \\ 1 & 0 & 1 & \ddots & & \vdots \\ 0 & 1 & 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 0 & 1 \\ 0 & \cdots & \cdots & 0 & 1 & 0 \end{pmatrix}, \tag{2.1}$$

for null boundary conditions, and

$$M_n = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 1 & \ddots & & 0 \\ 0 & 1 & 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & & \ddots & \ddots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix} \tag{2.2}$$

when periodic boundary conditions are stated.

All elementary cellular automata are categorized into four classes (see [30]) taking into account the behavior: the cellular automata of Class I exhibit trivial behavior, the cellular automata of Class II demonstrate behavior that quickly becomes stable or oscillatory, Class III comprises those elementary cellular automata that exhibit chaotic behavior, and finally the behavior of elementary cellular automata belonging to Class IV may eventually become stable but contains nested structures that interact in complex ways. The rule number 90 defines a Class IV cellular automata. This behavior can be viewed in Figure 1 and Figure 2, where the space-time diagrams are shown with different initial and boundary conditions.

As is mentioned in Section 1, elementary cellular automata can be applied to the design of cryptographic protocols. Particularly, the elementary cellular automaton with rule number 90 is usually used with the elementary cellular automata with rule number 150 in order to produce hybrid cellular automata that have good pseudorandom properties (see, for example, [9, 10]).

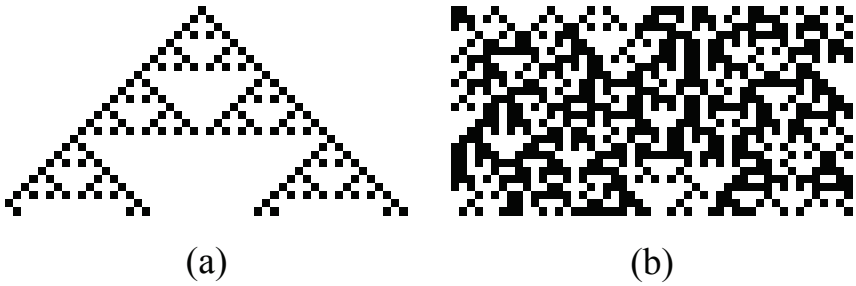

FIGURE 1. Space-time diagrams of elementary cellular automata with rule number 90, null boundary conditions and $n = 50$. (a) The initial configuration is given by only one cell endowed with state 1. (b) The initial configuration is defined at random. Both diagrams have been computed using the computer algebra system Mathematica (version 9.0).

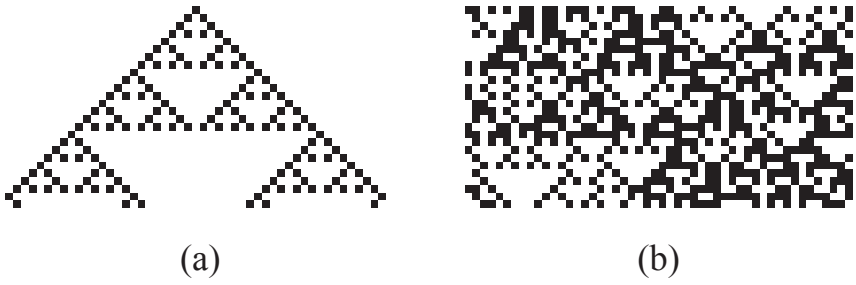

FIGURE 2. Space-time diagrams of elementary cellular automata with rule number 90, periodic boundary conditions and $n = 50$. (a) The initial configuration is given by only one cell endowed with state 1. (b) The initial configuration is defined at random. Both diagrams have been computed using the computer algebra system Mathematica (version 9.0).

3. The reversibility

3.1. **The influence of the cellular space.** In what follows it is shown that the reversibility depends on the boundary conditions stated and the number of cells of the cellular space (see Figure 3 and Figure 4). Note that for $n = 4$ (Figure 3) the ECA with rule number 90 is reversible since each node has exactly one predecessor. This fact does not occur when $n = 7$ (Figure 4-(a)): the transition diagram of the ECA with rule number 90 exhibits trees and, consequently, is not reversible.

The main result about the reversibility of this ECA is based on the DETGTRI algorithm proposed by El-Mikkawy in [6, 7], and devoted to compute the determinant of an n-th order tri-diagonal matrix:

$$T = \begin{pmatrix} d_1 & a_1 & 0 & \cdots & \cdots & 0 \\ b_2 & d_2 & a_2 & \ddots & & \vdots \\ 0 & b_3 & d_3 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & d_{n-1} & a_{n-1} \\ 0 & \cdots & \cdots & 0 & b_n & d_n \end{pmatrix},$$

This algorithm is as follows: set

$$c_i = \begin{cases} d_1, & \text{if } i = 1 \\ d_i - \frac{a_{i-1}b_i}{c_{i-1}}, & \text{if } 2 \leq i \leq n \end{cases}$$

for $1 \leq i \leq n$, then:

(1) Compute the parameters $c_1, \ldots, c_n$ taking into account the following condition: If $c_i = 0$ for any i, set $c_i = x$ and continue to compute $c_{i+1}, c_{i+2}, \ldots$ in terms of the variable x.
(2) Compute the following polynomial in the variable x:

$$P(x) = \prod_{i=1}^{n} c_i,$$

and evaluate $P(0)$; the result is the determinant of the tri-diagonal matrix, that is, $\det(T) = P(0)$.

Taking into account this previous result, the following holds:

Proposition 3.1. *The elementary cellular automaton with rule number 90 satisfies the following:*

(a) *If null boundary conditions are considered, it is reversible if and only if the number of cells of the cellular space is even.*
(b) *If periodic boundary conditions are taken into account, it is irreversible.*

Proof. (a) A simple calculus based on the DETGTRI algorithm shows that:

$$c_i = \begin{cases} x, & \text{if } i \text{ is odd} \\ -\frac{1}{x}, & \text{if } i \text{ is even} \end{cases}$$

for $1 \leq i \leq n$. Then

$$P(x) = \prod_{i=1}^{n} c_i = \begin{cases} (-1)^{\frac{n}{2}}, & \text{if } n \text{ is even} \\ (-1)^{\frac{n-1}{2}} x, & \text{if } n \text{ is odd} \end{cases}$$

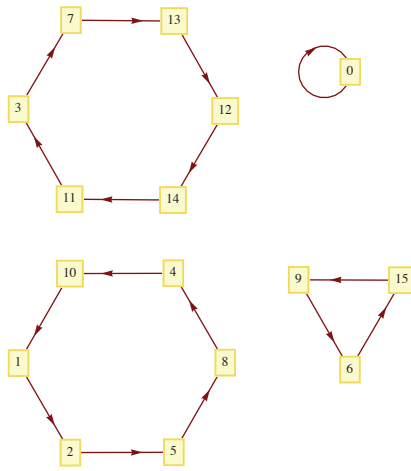

FIGURE 3. State transition diagram of elementary cellular automaton with rule number 90, null boundary conditions and $n = 4$. Each configuration of the ECA stands for a node of the transition diagram an each of them is labelled by the number whose binary code is given by the configuration

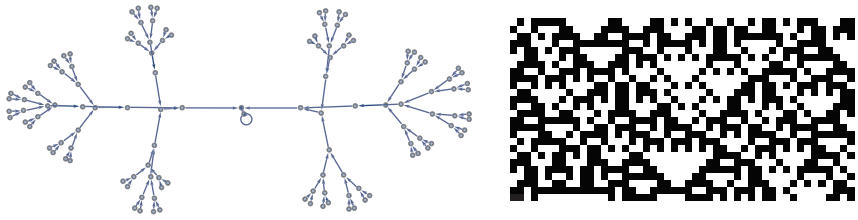

FIGURE 4. Irreversible elementary cellular automaton with rule number 90 and null boundary conditions. (a) State transition diagram for $n = 7$. (b) Space-time diagram for $n = 49$.

and consequently using the arithmetic modulus 2, we get:

$$\det(M_n) = P(0) = \begin{cases} 1, & \text{if } n \text{ is even} \\ 0, & \text{if } n \text{ is odd} \end{cases}$$

thus finishing.

(b) The local transition matrix of the ECA with rule number 90 and periodic boundary conditions is given in equation (2.2), and it is a singular matrix (taking into account the arithmetic modulo 2) since the first row is equal to the XOR sum of the rest of $n-1$ rows. Consequently, $\det(M_n) = 0$ for every n and the elementary cellular automaton is not reversible. □

3.2. **Computation of the inverse cellular automata.** In this section the inverse cellular automata of reversible elementary cellular automata are explicitly defined in terms of their local transition matrices. In this sense, the following result holds:

Theorem 3.2. *The inverse cellular automaton of the elementary cellular automaton with rule number 90 (and endowed with null boundary conditions) is defined by the following local transition matrix:*

$$Q = \begin{pmatrix} A & B & B & \overset{\left(\frac{n-4}{2}\right)}{\cdots} & B \\ B^T & A & B & \ddots & \vdots \\ B^T & B^T & A & \ddots & B \\ \vdots & \ddots & \ddots & \ddots & B \\ B^T & \overset{\left(\frac{n-4}{2}\right)}{\cdots} & B^T & B^T & A \end{pmatrix},$$

where

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

Proof. The local transition matrix of the ECA with rule number 90 and null boundary conditions is given in equation (2.1) and it can be expressed as the following block matrix:

$$M = \begin{pmatrix} A & B^T & O & \overset{(m-2)}{\cdots} & O \\ B & A & B^T & \ddots & \vdots \\ O & B & A & \ddots & O \\ \vdots & \ddots & \ddots & \ddots & B^T \\ O & \overset{(m-2)}{\cdots} & O & B & A \end{pmatrix},$$

where $m = \frac{n}{2}$, and the following relations holds:

$$A^2 = \mathrm{Id}, \quad B^2 = 0,$$

$$A \cdot B = B^T \cdot A = B^T \cdot B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

$$A \cdot B^T = B \cdot A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Then,

$$M \cdot Q = \begin{pmatrix} R_{11} & R_{12} & \cdots & R_{1m} \\ R_{21} & R_{22} & \cdots & R_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ R_{m1} & R_{m2} & \cdots & R_{mm} \end{pmatrix},$$

with

$$R_{ij} = \bigoplus_{k=1}^{m} M_{ik} \cdot Q_{kj},$$

where M_{ik} is the (i,k) block-coefficient of the matrix M, and Q_{kj} is the (k,j) block-coefficient of the matrix Q. Now, we compute the coefficients R_{ij} considering some cases:

(1) The diagonal coefficients are all equal to the identity matrix:

$$\begin{aligned} R_{ii} &= \bigoplus_{k=1}^{m} M_{ik} \cdot Q_{ki} \\ &= 0 \cdot B \oplus \overset{(i-2)}{\cdots} \oplus 0 \cdot B \oplus B^2 \oplus A^2 \oplus \left(B^T\right)^2 \oplus 0 \cdot B^T \oplus \overset{(m-i-1)}{\cdots} \oplus 0 \cdot B^T \\ &= B^2 \oplus A^2 \oplus \left(B^T\right)^2 = 0 \oplus \mathrm{Id} \oplus 0 = \mathrm{Id}, \end{aligned}$$

for $1 \leq i \leq m$.

(2) In order to compute the coefficients R_{ij}, with $1 \leq i < j \leq m$, we distinguish the following cases:

i. Set $i = 1$ and $2 \leq j \leq m-1$. Then:

$$R_{1j} = A \cdot B \oplus \begin{cases} B^T \cdot A \oplus \bigoplus_{k=1}^{m-2} 0 \cdot B^T, & \text{if } j = i+1, \\ B^T \cdot B \oplus 0 \cdot A \oplus \bigoplus_{k=1}^{m-3} 0 \cdot B^T, & \text{if } j = i+2, \\ B^T \cdot B \oplus \bigoplus_{k=1}^{j-3} 0 \cdot B \oplus 0 \cdot A \oplus \bigoplus_{k=1}^{m-j} 0 \cdot B^T, & \text{if } j > i+2. \end{cases}$$

A simple computation shows that $R_{1j} = 0$ for $2 \leq j \leq m-1$.

ii. Set $i = 1$ and $j = n/2$. Then:

$$R_{1m} = A \cdot B \oplus B^T \cdot B \oplus \bigoplus_{k=1}^{m-3} 0 \cdot B \oplus 0 \cdot A = 0.$$

iii. Set $i = 2$ and $2 \leq j \leq m-1$ with $i < j$. Then:

$$\begin{aligned} R_{2j} &= B \cdot B \oplus A \cdot B \\ &\quad \oplus \begin{cases} B^T \cdot A \oplus \bigoplus_{k=1}^{m-3} 0 \cdot B^T, & \text{if } j = 3 \\ B^T \cdot B \oplus 0 \cdot A \oplus \bigoplus_{k=1}^{m-4} 0 \cdot B^T, & \text{if } j = 4 \\ B^T \cdot B \oplus \bigoplus_{k=1}^{j-4} 0 \cdot B \oplus 0 \cdot A \oplus \bigoplus_{k=1}^{m-j} 0 \cdot B^T, & \text{if } j > 4 \end{cases} \\ &= 0. \end{aligned}$$

iv. Set $i = 2$ and $j = m$. Then:

$$R_{2m} = B \cdot B \oplus A \cdot B \oplus B^T \cdot B \oplus \bigoplus_{k=1}^{m-4} 0 \cdot B \oplus 0 \cdot A = 0.$$

v. Suppose that $3 \leq i \leq m-2$ and $2 \leq j \leq m-1$. Then:

$$\begin{aligned} R_{ij} &= \bigoplus_{k=1}^{i-2} 0 \cdot B \oplus B \cdot B \oplus A \cdot B \\ &\quad \oplus \begin{cases} B^T \cdot A \oplus \bigoplus_{k=1}^{m-i-1} 0 \cdot B^T, & \text{if } j = i+1 \\ B^T \cdot B \oplus 0 \cdot A \oplus \bigoplus_{k=1}^{m-i-2} 0 \cdot B^T, & \text{if } j = i+2 \\ B^T \cdot B \oplus \bigoplus_{k=1}^{j-i-2} 0 \cdot B \oplus 0 \cdot A \oplus \bigoplus_{k=1}^{m-j} 0 \cdot B^T, & \text{if } j > i+2 \end{cases} \\ &= 0. \end{aligned}$$

vi. Set $i = m-1$, and $j = m$. Then:

$$R_{n/2-1,n/2} = \bigoplus_{k=1}^{m-3} 0 \cdot B \oplus B \cdot B \oplus A \cdot B \oplus B^T \cdot A = 0.$$

(3) The computation of the coefficients R_{ij} with $i > j$ is similar to the previous one and for the sake of simplicity we will avoid these calculations.

As a consequence

$$M \cdot Q = \begin{pmatrix} \mathrm{Id} & O & \cdots & O \\ O & \mathrm{Id} & \ddots & \vdots \\ \vdots & \ddots & \ddots & O \\ O & \cdots & O & \mathrm{Id} \end{pmatrix} = \mathrm{Id}.$$

In a similar way it is proved that $Q \cdot M = \mathrm{Id}$, thus finishing. □

3.3. **An example.** As is shown in the last subsections, the elementary cellular automaton with rule number 90, null boundary conditions, and $n = 10$ cells is reversible. Its local transition matrix is

$$M = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

and the local transition matrix of its inverse cellular automata is given by:

$$Q = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

The inverse cellular automaton is a hybrid cellular automaton defined by the following local transition rules:

$$\begin{aligned} f_1(x_1,\ldots,x_{10}) &= x_2 \oplus x_4 \oplus x_6 \oplus x_8 \oplus x_{10}, \\ f_2(x_1,\ldots,x_{10}) &= x_1, \\ f_3(x_1,\ldots,x_{10}) &= x_4 \oplus x_6 \oplus x_8 \oplus x_{10}, \\ f_4(x_1,\ldots,x_{10}) &= x_1 \oplus x_3, \\ f_5(x_1,\ldots,x_{10}) &= x_6 \oplus x_8 \oplus x_{10}, \\ f_6(x_1,\ldots,x_{10}) &= x_1 \oplus x_3 \oplus x_5, \\ f_7(x_1,\ldots,x_{10}) &= x_8 \oplus x_{10}, \\ f_8(x_1,\ldots,x_{10}) &= x_1 \oplus x_3 \oplus x_5 \oplus x_7, \\ f_9(x_1,\ldots,x_{10}) &= x_{10}, \\ f_{10}(x_1,\ldots,x_{10}) &= x_1 \oplus x_3 \oplus x_5 \oplus x_7 \oplus x_9. \end{aligned}$$

3.4. **Experimental deduction of the matrix Q.** The explicit expression of the matrix Q (the local transition matrix of the inverse cellular automaton of ECA with rule number 90) was initially obtained by an experimental study using the computer algebra system Mathematica (version 9.0). The computational simulations obtained provide a pattern for the matrix structure that leads to the theoretical result stated in Theorem 3.2. The Mathematica code is the following:

```
end = 10;
Do[
M= SparseArray[
Band[{1, 1}] $->$ 0, Band[{2, 1}] $->$ 1,
Band[{1, 2}] $->$ 1}, {n, n}];
Print[StringForm["n=’’,Q=’’ ", n, Mod[Inverse[M], 2] // MatrixForm]],
{n, 4, end, 2}];
```

The results obtained for $n = 4, 6, 8, 10$ and the pattern generated are shown in Figure 5.

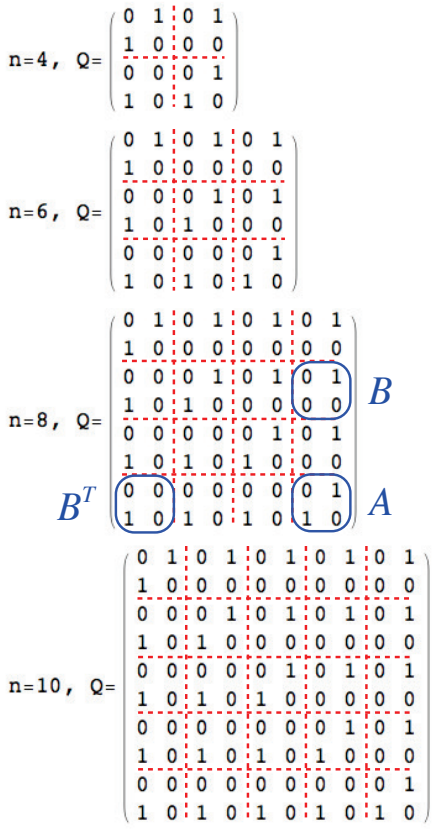

FIGURE 5. Computer simulations of the matrix Q using Mathematica (version 9.0). The pattern obtained involves the 2×2 matrices A, B and B^T.

Note that once the pattern was experimentally obtained, the theoretical proof given in section 3.2 was constructed.

4. The reversibility of linear elementary cellular automata

As was previously mentioned, the dynamic of linear elementary cellular automata can be characterized in terms of matrices. As a consequence, the linear ECA with local transition function $x_i^{t+1} = b \cdot x_{i-1}^t \oplus d \cdot x_i^t \oplus a \cdot x_{i+1}^t$, $b, d, a \in \mathbb{F}_2$, is

TABLE 1. Linear elementary cellular automata

Rule number	Local transition function	Parameters
0	$s_i^{t+1} = 0$	$b = d = a = 0$
60	$s_i^{t+1} = s_{i-1}^t \oplus s_i^t$	$b = d = 1$, $a = 0$
90	$s_i^{t+1} = s_{i-1}^t \oplus s_{i+1}^t$	$b = a = 1$, $d = 0$
102	$s_i^{t+1} = s_i^t \oplus s_{i+1}^t$	$b = 0$, $d = a = 1$
150	$s_i^{t+1} = s_{i-1}^t \oplus s_i^t \oplus s_{i+1}^t$	$b = d = a = 1$
170	$s_i^{t+1} = s_{i+1}^t$	$b = d = 0$, $a = 1$
204	$s_i^{t+1} = s_i^t$	$b = a = 0$, $d = 1$
240	$s_i^{t+1} = s_{i-1}^t$	$b = 1$, $d = a = 0$

reversible if its local transition matrix

$$M_n = \begin{pmatrix} d & a & 0 & \cdots & 0 & \beta \\ b & d & a & \ddots & & 0 \\ 0 & b & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & a & 0 \\ 0 & & \ddots & b & d & a \\ \alpha & 0 & \cdots & 0 & b & d \end{pmatrix}$$

in non-singular. Then, taking into account the explicit expressions of linear elementary cellular automata given in Table 1, the additional following results follow.

Reversibility of ECA 0. The ECA 0 is not reversible since its local transition matrix is $M_n = O$ for both null and periodic boundary conditions.

Reversibility of ECA 60. The evolution of the ECA 60 with null boundary conditions is ruled by the following local transition matrix:

$$M_n = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 0 & \ddots & & 0 \\ 0 & 1 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 & 0 \\ 0 & & \ddots & 1 & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 1 \end{pmatrix}.$$

Then, it is easy to see that $\det(M_n) = 1$ since M_n is a triangular matrix whose diagonal coefficients are all equal to 1. As a consequence, the ECA 60 with null boundary conditions is reversible such that the local transition matrix of the inverse

cellular automaton is:

$$M_n^{-1} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 1 & 0 & \ddots & & 0 \\ 1 & 1 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 & 0 \\ 1 & & \ddots & 1 & 1 & 0 \\ 1 & 1 & \cdots & 1 & 1 & 1 \end{pmatrix}.$$

If periodic boundary conditions are stated, this ECA is non-reversible since in this case:

$$\det(M_n) = \det(W) + (-1)^n \det\left(W^T\right),$$

where W is the local transition matrix of the ECA 60 with $n-1$ cells and null boundary conditions. Consequently, $\det(M_n) = 1 + (-1)^n \equiv 0 \mod 2$ and the ECA 60 with periodic boundary conditions is non-reversible.

Reversibility of ECA 102. Arguments similar to those used for ECA 60 show that the ECA 102 is reversible for null boundary conditions and non-reversible for periodic boundary conditions. Furthermore, the local transition matrix of the inverse cellular automaton when null boundary conditions are considered is:

$$M_n^{-1} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & 1 & 1 & \ddots & & 1 \\ 0 & 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 1 & 1 \\ 0 & & \ddots & 0 & 1 & 1 \\ 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix}.$$

Reversibility of ECA 150. The reversibility of ECA 150 depends on the number of cells of the cellular space n and the boundary conditions stated. Specifically, for null boundary conditions, the ECA 150 is reversible if $n \equiv 0, 1 \mod 3$ and the following result holds (see [14]):

Proposition 4.1. *The inverse cellular automaton of ECA* 150 *with null boundary conditions is defined by the following local transition matrix:*

(1) *If* $n \equiv 0 \mod 3$, *where* $n = 3k$, $k \in \mathbb{Z}^+$, *then*

$$P = \begin{pmatrix} A & B & \overset{(k-1)}{\cdots} & B \\ B^T & A & \ddots & \vdots \\ \vdots & \ddots & \ddots & B \\ B^T & \overset{(k-1)}{\cdots} & B^T & A \end{pmatrix},$$

where

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

(2) *If* $n \equiv 1 \mod 3$, *where* $n = 3k+1$, $k \in \mathbb{Z}^+$, *then:*

$$P = \begin{pmatrix} 1 & F & F & \overset{(k)}{\cdots} & F \\ F^T & C & D & \overset{(k)}{\cdots} & D \\ F^T & D^T & C & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & D \\ F^T & D^T & \overset{(k)}{\cdots} & D^T & C \end{pmatrix}$$

with

$$F = \begin{pmatrix} 0 & 1 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \quad D = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}.$$

On the other hand, when periodic boundary conditions are considered, it is reversible when $n \equiv 1, 2 \mod 3$ (see [11]). In this case, the following result holds ([13]):

Proposition 4.2. *The local transition matrix of the inverse cellular automaton of the ECA* 150 *when* $n \not\equiv 0 \mod 3$ *is a circulant matrix defined as follows:*

(1) *If* $n \equiv 1 \mod 3$ *where* $n = 3k+1$, $k \in \mathbb{Z}^+$, *the first row of the circulant matrix is:*

$$\left(\underbrace{1\,1\,0}\overset{(k)}{\cdots}\underbrace{1\,1\,0}\,1\right).$$

(2) *If* $n \equiv 2 \mod 3$ *where* $n = 3k+2$, $k \in \mathbb{Z}^+$, *the first row of the circulant matrix is:*

$$\left(\underbrace{1\,0\,1}\overset{(k)}{\cdots}\underbrace{1\,0\,1}\,1\,0\right).$$

Reversibility of ECA 170. If null boundary conditions are considered then $\det(M_n) = 0$ since

$$M_n = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \ddots & & 0 \\ 0 & 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 1 & 0 \\ 0 & & \ddots & 0 & 0 & 1 \\ 0 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}.$$

Consequently, the ECA 170 with null boundary conditions is not reversible. Nevertheless, when periodic boundary conditions are stated, its local transition matrix

is

$$M_n = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \ddots & & 0 \\ 0 & 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 1 & 0 \\ 0 & & \ddots & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix},$$

and

$$\det(M_n) = (-1)^n \det(\mathrm{Id}) = (-1)^n \neq 0.$$

Then, the ECA 170 with periodic boundary conditions is reversible for every n. Moreover, the inverse cellular automaton is defined by means of the following local transition matrix:

$$M_n^{-1} = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \ddots & & 0 \\ 0 & 1 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 & 0 \\ 0 & & \ddots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix},$$

that is, the inverse cellular automaton of ECA 170 with periodic boundary conditions is the ECA 240 with periodic boundary conditions.

Reversibility of ECA 204. This ECA is reversible for every n since the local transition matrix is $M_n = \mathrm{Id}$ for both null and periodic boundary conditions. Obviously, the inverse cellular automaton is the ECA 204 itself.

Reversibility of ECA 240. An argument similar to the one used for ECA 170 shows that the ECA 240 is reversible for every n when periodic boundary conditions are stated (and the inverse cellular automaton is the ECA 170 endowed with periodic boundary conditions), and it is non-reversible when null boundary conditions are used.

References

[1] A.A. Abdo, S. Lian, I.A. Ismail, H. Diab, *A cryptosystem based on elementary cellular automata.* Commun. Nonlinear Sci. Numer. Simulat. **18** (2013), 136–147. MR 2974369.

[2] T. Boykett, *Efficient exhaustive listings of reversible one dimensional cellular automata.* Theor. Comput. Sci. **325** (2004), 215–247. MR 2086738.

[3] P. Chaudhuri, D. Chowdhury, S. Nandi, S. Chattopadhyay, *Additive Cellular Automata, Theory and Applications, vol. 1.* IEEE Computer Society Press, Los Alamitos, CA, 1997.

[4] Z. Çinkir, H. Akin, I. Şiap, *Reversibility of 1D cellular automata with periodic boundary over finite fields.* J. Stat. Phys. **143** (2011), 807–823. MR 2800666.

[5] E. Czeizler, *On the size of inverse neighborhoods for one-dimensional reversible cellular automata*. Theor. Comput. Sci. **325** (2004), 273–284. MR 2086740.

[6] M.E.A. El-Mikkawy, *On the inverse of a general tridiagonal matrix*. Appl. Math. Comput. **150** (2004), 669–679. MR 2039666.

[7] M.E.A. El-Mikkawy, *A fast algorithm for evaluating nth order tridiagonal determinants*. J. Comput. Appl. Math. **166** (2004), 581–584. MR 2041200.

[8] A. Fúster-Sabater, P. Caballero-Gil, *On the use of cellular automata in symmetric cryptography*. Acta. Appl. Math. **93** (2006), 215–236. MR 2267990.

[9] A. Fúster-Sabater, P. Caballero-Gil, *Synthesis of cryptographic interleaved sequences by means of linear cellular automata*. Appl. Math. Lett. **22** (2009), 1518–1524. MR 2561728.

[10] A. Fúster-Sabater, P. Caballero-Gil, *Chaotic modelling of the generalized self-shrinking generator*. Appl. Soft. Comput. **11** (2011), 1876–1880.

[11] L. Hernández Encinas, A. Martín del Rey, *Inverse rules of ECA with rule number* 150. Appl. Math. Comput. **189** (2007), 1782–1786. MR 2332130.

[12] J. Jin, *An image encryption based on elementary cellular automata*. Opt. Laser. Eng. **50** (2012), 1836–1843.

[13] A. Martín del Rey, *A note on the reversibility of elementary cellular automata 150 with periodic boundary conditions*. Rom. J. Inf. Sci. Technol. **16** (2013), 365–372.

[14] A. Martín del Rey, G. Rodríguez Sánchez, *On the reversibility of* 150 *Wolfram cellular automata*. Internat. J. Mod. Phys. C **17** (2006), 975–984.

[15] K. Morita, *Reversible cellular automata*. J. Inform. Process. Soc. Jpn. **35** (1994), 315–321.

[16] S. Nandi, B.K. Kar, P. Pal Chaudhuri, *Theory and applications of cellular automata in cryptography*. IEEE Trans. Comput. **43** (1994), 1346–1357. MR 1306115.

[17] J. von Neumann, The general and logical theory of automata. In: Cerebral mechanisms in behavior, The Hixon Symposium, pp. 1–31, John Wiley & Sons, New York, 1951. MR 0045446.

[18] A. Nobe, F. Yura, *On reversibility of cellular automata with periodic boundary conditions*. J. Phys. A: Math. Gen. **37** (2004), 5789–5804. MR 2066630.

[19] P. Sarkar, *A brief history of cellular automata*. ACM Comput. Surv. **32** (2000), 80–107.

[20] J.C. Seck Tuoh Mora, *Matrix methods and local properties of reversible one-dimensional cellular automata*. J. Phys. A: Math. Gen. **35** (2002), 5563–5573. MR 1917250.

[21] J.C. Seck Tuoh Mora, S.V. Chapa Vergara, G. Juarez, H.V. McIntosh, *Procedures for calculating reversible one-dimensional cellular automata*. Physica D **202** (2005), 134–141. MR 2131890.

[22] M. Seredynski, P. Bouvry, *Block encryption using reversible cellular automata*. Proc. of ACRI 2004, Lect. Notes Comput. Sci. **3305** (2004), 785–792.

[23] I. Şiap, H. Akin, F. Şah, *Characterization of two dimensional cellular automata over ternary fields*. J. Franklin Inst. **348** (2011), 1258–1275. MR 2826041.

[24] S.K. Tan, S.U. Guan, *Evolving cellular automata to generate nonlinear sequences with desirable properties*. Appl. Soft. Comput. **7** (2007), 1131–1134.

[25] M. Toffoli, N. Margolus, *Invertible cellular automata: a review*. Physica D **45** (1990), 229–253. MR 1094877.

[26] M. Tomassini, M. Perrenoud, *Cryptography with cellular automata*. Appl. Soft. Comput. **1** (2001), 151–160.

[27] S. Wolfram, *Random sequence generation by cellular automata*. Adv. Appl. Math. **7** (1986), 123–169. MR 0845373.

[28] S. Wolfram, *Cryptography with cellular automata*. In: Advances in Cryptology, CRYPTO '85 proceedings, Lecture Notes in Computer Science **218** (1986), 429–432.

[29] S. Wolfram, *Cellular automata and complexity: collected papers*. Addison-Wesley, Reading, MA, 1994.

[30] S. Wolfram, *A new kind of science*. Wolfram Media, Champaign, IL, 2002. MR 1920418.

A. Martín del Rey
Department of Applied Mathematics, Institute of Fundamental Physics and Mathematics, University of Salamanca, Spain
delrey@usal.es

Received: December 16, 2013
Accepted: July 14, 2014