ROMANIAN JOURNAL OF INFORMATION SCIENCE AND TECHNOLOGY
Volume **16**, Number 4, 2013, 365–372

A Note on the Reversibility Of Elementary Cellular Automaton 150 With Periodic Boundary Conditions

Angel Martín DEL REY

Department of Applied Mathematics
Institute of Fundamental Physics and Mathematics
Universidad de Salamanca, Spain

E-mail: delrey@usal.es

Abstract. In this work, the reversibility problem for the elementary cellular automaton with rule number 150 is tackled. Although this problem was solved before, we will introduce in this work an alternative construction of the inverse cellular automaton by means of the transition matrices instead of transition dipolynomials. This new approach allows one to obtain a more efficient and effective algorithm to compute the inverse cellular automaton.

Keywords: Reversibility, Elementary cellular automata, circulant matrix.

1. Introduction

A cellular automaton is a simple model of computation which is used to simulate complex phenomena ([11]). It is defined by a discrete spatial lattice of memory units called cells which are endowed with a state at every step of time. The state of each cell is updated synchronously according to a local transition function which depends on the states of the cells in some neighborhood around it. The most important type of cellular automaton is elementary cellular automaton: the state of each cell depends on the states of the cell itself and its two nearest cells and the state set is $\mathbb{F}_2$. One of the most important elementary cellular automaton is that one whose local transition function is defined the XOR sum of the three states; it is called elementary cellular automaton with rule number 150 and its importance is due to its several applications to cryptography (see, for example, [6]).

The reversibility is one of the most important properties of cellular automata. It implies that information can be neither created or destroyed: A cellular automaton is reversible when there exists another cellular automaton which makes possible the evolution backwards ([11]). The reversibility property has been extensively studied (see, for example, [4, 9]). Although the reversibility problem for elementary cellular automata with rule number 150 was solved using transition dipolynomials (see, for example, [3, 7]), the main goal of this work is to introduce an alternative construction of its inverse cellular automaton by means of the transition matrices instead of transition dipolynomials. The main advantage of this new approach is that it provides us a more efficient algorithm to compute the inverse cellular automaton using circulant matrices.

The rest of the paper is organized as follows: In section 2 the basic theory of elementary cellular automata is introduced, and the problem of the reversibility of the elementary cellular automaton with rule number 150 is solved in section 3. Finally, the conclusions are shown in section 4.

2. Elementary cellular automata

An elementary cellular automaton (ECA for short) is a discrete dynamical system formed by n identical objects called cells that are arranged linearly. Each cell assume at every step of time a state from $\mathbb{F}_2 = \{0, 1\}$, such that the ith cell at time t is denoted by $x_i^t \in \mathbb{F}_2$. The states change synchronously in discrete steps of time according to a local transition rule defined by a boolean function f whose variables are the previous states of the two nearest neighbor cells, and the cell itself:

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

for every $1 \leq i \leq n$. Consequently, 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:

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

where the truth table of the boolean function f is:

$$\begin{array}{rcl} f\,(0,0,0) & = & \alpha_0 \\ f\,(0,0,1) & = & \alpha_1 \\ f\,(0,1,0) & = & \alpha_2 \\ f\,(0,1,1) & = & \alpha_3 \\ f\,(1,0,0) & = & \alpha_4 \\ f\,(1,0,1) & = & \alpha_5 \\ f\,(1,1,0) & = & \alpha_6 \\ f\,(1,1,1) & = & \alpha_7 \end{array} \tag{3}$$

Consequently we denote by ECA(w) the elementary cellular automaton with rule number w.

As the number of cells is finite, periodic boundary conditions can be considered in order to preserve the well-defined evolution of the ECA: the cells are handled with a toroidal arrangement, that is: $x_i^t = x_j^t$ if $i \equiv j \pmod{n}$ for every t.

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

$$\begin{array}{rcl} \Phi\colon \mathbb{F}_2^n & \to & \mathbb{F}_2^n \\ X^t & \mapsto & \Phi\left(X^t\right) = X^{t+1} \end{array} \tag{4}$$

An ECA is called reversible if there exists another cellular automaton (called inverse cellular automaton) that makes possible the evolution backwards in time ([8]); In this sense, this inverse cellular automaton is not an elementary one since, in the majority of the cases, its local transition function depends on several neighborhood states and such function could be different depending on the cell considered (hybrid cellular automaton). The global transition function, Φ, of a reversible cellular automaton is bijective ([10]); as a consequence Φ^{-1} is the global transition function of the inverse cellular automaton.

The ECA with rule number 150 is a linear elementary cellular automaton since its local transition function is linear:

$$x_i^{t+1} = f\left(x_{i-1}^t, x_i^t, x_{i+1}^t\right) = x_{i-1}^t \oplus x_i^t \oplus x_{i+1}^t, \tag{5}$$

where $\oplus$ stands for the XOR operation (the sum modulo 2). As a consequence, the global transition function of ECA(150) can be easily defined in terms of matrix theory:

$$X^{t+1} = \Phi\left(X^t\right) = M_n \cdot X^t \,(\mathrm{mod}\, 2)\,, \tag{6}$$

where M_n is the following local transition matrix:

$$M_n = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 1 & \ddots & & 0 \\ 0 & 1 & 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & & \ddots & \ddots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix} \tag{7}$$

In the case of linear ECA 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 (see [3]).

3. The reversibility problem

As is well known (see [7]), the reversibility of ECA(150) depends on the number of cells of its cellular space. More precisely:

Proposition 1. *The ECA*(150) *is reversible if and only if* $n \not\equiv 0 \pmod 3$.

When the ECA(150) is reversible there exists a procedure to compute the inverse cellular automata in terms of the transition dipolynomial (see [7]). Specifically, it states the following:

Theorem 2. *Set* $D_m(y) = 1 + \sum_{j=1}^{m} \left(y^{-j} + y^j\right)$ *and let* $T(y) = y^{-1} + 1 + y$ *be the transition dipolynomial of ECA*(150). *Then, the transition dipolynomial* $\bar{T}(y)$ *of the inverse cellular automaton is defined as follows:*

(1) *If* $n \equiv 1 \pmod 3$, *then*

$$\bar{T}(y) = D_{\lfloor \frac{n-1}{2} \rfloor}(x) + \sum_{i=1}^{\lfloor \frac{n-1}{6} \rfloor} \left(y^{-(3i-1)} + y^{3i-1}\right). \tag{8}$$

(2) *If* $n \equiv 2 \pmod 3$, *then*

$$\bar{T}(y) = D_{\lfloor \frac{n-1}{2} \rfloor}(y) + \sum_{i=1}^{\lfloor \frac{n+2}{6} \rfloor} \left(y^{-(3i-2)} + y^{3i-2}\right). \tag{9}$$

Unfortunately, this is not an efficient procedure to compute the inverse cellular automaton; the following and novel result provides us an efficient algorithm to compute such inverse cellular automaton:

Theorem 3. *The inverse cellular automaton of ECA*(150) *when* $n \not\equiv 0 \pmod 3$ *is defined by the following transition matrix:*

(1) *If* $n \equiv 1 \pmod 3$, *then*

$$Q_n = \begin{pmatrix} 1 & A & A & \overset{(k)}{\cdots} & A \\ A^T & B & C & \overset{(k-1)}{\cdots} & C \\ A^T & C^T & B & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & C \\ A^T & C^T & \overset{(k-1)}{\cdots} & C^T & B \end{pmatrix} \tag{10}$$

with

$$A = \begin{pmatrix} 1 & 0 & 1 \end{pmatrix}, \tag{11}$$

$$B = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \tag{12}$$

$$C = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}. \tag{13}$$

(2) *If* $n \equiv 2 \pmod 3$, *then*

$$Q_n = \begin{pmatrix} Id_2 & D & D & \overset{(k)}{\cdots} & B \\ D^T & E & F & \overset{(k-1)}{\cdots} & F \\ D^T & F^T & E & \cdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & F \\ D^T & F^T & \overset{(k-1)}{\cdots} & F^T & E \end{pmatrix}, \tag{14}$$

where

$$D = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \tag{15}$$

$$E = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \tag{16}$$

$$F = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}, \tag{17}$$

and Id_2 *is de identity matrix of order* 2.

Proof. (1) Suppose that $n \equiv 1 \pmod 3$, then $n = 3k + 1$ with $k \in \mathbb{Z}^+$. It is easy to check that the matrix given in equation (10) is a circulant matrix whose first row is $F = \begin{pmatrix} f_1 & f_2 & \cdots & f_n \end{pmatrix}$, where:

$$f_i = \begin{cases} 0, & \text{if } i = 3m, m \in \mathbb{Z}^+ \\ 1, & \text{if } i \neq 3m, m \in \mathbb{Z}^+ \end{cases} \tag{18}$$

We have to prove that $Q \cdot M_n = M_n \cdot Q = Id_n$ using the arithmetic modulo 2. As M_n and Q are circulant matrices then $Q \cdot M_n$ and $M_n \cdot Q$ are also circulant matrices (see [5]). Consequently, we finish if we prove that the first row of $Q \cdot M_n$ and $M_n \cdot Q$ are:

$$\begin{pmatrix} 1 & 0 & \overset{(n-1)}{\cdots} & 0 \end{pmatrix}. \tag{19}$$

In the first case (when $Q \cdot M_n$ is computed) we distinguish the following cases:

- The first coefficient of the first row of $M_n \cdot Q$ is $F \cdot C_1$, where C_1 is the first column of M_n; then:

$$F \cdot C_1 = \left(\underbrace{1\,1\,0}\overset{(k)}{\cdots}\underbrace{1\,1\,0}\,1\right) \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = 1 + 1 + 1 = 1 \,(\mathrm{mod}\, 2)\,. \tag{20}$$

- The i-th coefficient ($2 \leq i \leq n-1$) of the first row of $M_n \cdot Q$ is given by $F \cdot C_i$, where C_i is the i-th column of M_n:

$$\begin{aligned} F \cdot C_i &= \left(\underbrace{1\,1\,0}\overset{(k)}{\cdots}\underbrace{1\,1\,0}\,1\right) \cdot \begin{pmatrix} 0 & \overset{(i-2)}{\cdots} & 0 & 1 & 1 & 1 & 0 & \overset{(n-i-1)}{\cdots} & 0 \end{pmatrix}^T \\ &= 1 + 1 = 0 \,(\mathrm{mod}\, 2)\,. \end{aligned} \tag{21}$$

- The last coefficient of the first row of $M_n \cdot Q$ is $F \cdot C_n$, where C_i is the last column of M_n:

$$F \cdot C_1 = \left(\underbrace{1\,1\,0}\overset{(k)}{\cdots}\underbrace{1\,1\,0}\,1\right) \cdot \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 1 \\ 1 \end{pmatrix} = 1 + 1 = 0 \,(\mathrm{mod}\, 2)\,. \tag{22}$$

  As a consequence, the first row of the circulant matrix $Q \cdot M_n$ is the first row of the identity matrix, thus finishing.
  The second case, that is, $M_n \cdot Q = Id_n$, is proven in a similar way.

(2) If $n \equiv 2 \pmod 3$, the matrix given in equation (14) is a circulant matrix whose first row is $F = \begin{pmatrix} f_1 & f_2 & \cdots & f_n \end{pmatrix}$, where:

$$f_i = \begin{cases} 0, & \text{if } i = 3k-1, k \in \mathbb{Z}^+ \\ 1, & \text{if } i \neq 3k-1, k \in \mathbb{Z}^+ \end{cases} \tag{23}$$

and the proof is similar to case (1).

□

As a consequence of this theorem, the following result holds:

Corollary 4. *The inverse cellular automaton of ECA*(150) *when* $n \not\equiv 0 \pmod 3$ *is defined by a circulant matrix* Q_n*, where:*

1. *If* $n \equiv 1 \pmod 3$ *with* $n = 3k+1$, $k \in \mathbb{Z}^+$*, the first row of* Q_n *is:*

$$\left(\underbrace{1\,1\,0}\overset{(k)}{\cdots}\underbrace{1\,1\,0}\,1\right). \tag{24}$$

2. If $n \equiv 2 \pmod 3$ *with* $n = 3k + 2$, $k \in \mathbb{Z}^+$, *the first row of* Q_n *is:*

$$\left(\underbrace{1\,0\,1}\overset{(k)}{\cdots}\underbrace{1\,0\,1}\,1\,0\right). \tag{25}$$

Note that this result provides a more efficient method to compute the inverse cellular automaton. If we want to compute the configuration X^{t+1} of such automata from X^t using the corresponding transition dipolynomial, the following computation must be done:

$$P^{t+1}(y) = \bar{T}(y) \cdot P^t(y) \bmod (x^n - 1), \tag{26}$$

where $P^t(y) = \sum_{i=0}^{n-1} x_i^t y^i$ is the characteristic polynomial at time t representing the configuration X^t.

The cost of this polynomial multiplication is $O(n \log n + n \log n \log\log n)$ (see, for example, [2]). On the other hand, the computation of the configuration X^{t+1} using the circulant matrix Q_n takes $O(n \log n)$ bit operations (see [1]).

4. Conclusions

In this paper the reversibility problem for elementary cellular automaton with rule number 150 has been considered. Although this problem was solved before using transition dipolynomials, we have introduced a new proof of the reversibility in this work. It is based on the use circulant transition matrices. This novel approach allows us to obtain a more efficient procedure to compute the inverse cellular automaton.

Acknowledgements. This work has been supported by Consejería de Educación (Junta de Castilla y León, Spain).

References

[1] Bai Z., Demmel J., Dongarra J., Ruhe A., van der Vorst H., *Templates for the solution of Algebraic Eigenvalue Problems: A Practical Guide*, SIAM, 2000.

[2] Bini D., Pan V.Y., *Polynomial and Matrix Computations, Volume 1: Fundamental Algorithms*. Birkhäuser, 1994.

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

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

[5] Davies P. J., *Circulant Matrices*. Wiley-Intersicence, NY, 1979.

[6] Fúster A., Caballero P., *On the Use of Cellular Automata in Symmetric Cryptography*, Acta Appl. Math., **93**(2):215–236, 2006.

[7] Hernández Encinas L., del Rey A. M., *Inverse rules of ECA with rule number* 150, Appl. Math. Comput., **189**:1782–1786, 2007.

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

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

[10] Toffoli M., Margolus N., *Invertible cellular automata: a review*, Physica D, **45**:229–253, 1990.

[11] Wolfram S., *A New Kind of Science*, Wolfram Media Inc., Champaing, IL, 2002.