Applied Mathematics and Computation 357 (2019) 23–34

Contents lists available at ScienceDirect

Applied Mathematics and Computation

journal homepage: www.elsevier.com/locate/amc

A closed formula for the inverse of a reversible cellular automaton with $(2R+1)$-cyclic rule

D. Hernández Serrano[a], A. Martín del Rey[b,*]

[a] Institute of Fundamental Physics and Mathematics, Department of Mathematics, University of Salamanca, Plaza de la Merced 1, Salamanca 37008, Spain

[b] Institute of Fundamental Physics and Mathematics, Department of Applied Mathematics, University of Salamanca, Calle del Parque 2, Salamanca 37008, Spain

ARTICLE INFO

MSC:
68Q80
94A60

Keywords:
Elementary cellular automata
Reversibility
Rule 150
Periodic boundary conditions
Cyclic cellular automata
Transition dipolynomial

ABSTRACT

Reversibility of cellular automata (CA) has been an extensively studied problem from both a theoretical and a practical point of view. It is known when a $(2R+1)$-cyclic cellular automaton with periodic boundary conditions (p.b.c.) is reversible (see Siap et al., 2013) but, as far as we know, no explicit expression is given for its inverse cellular automaton apart from the case $R=1$ (see Encinas and del Rey, 2007). In this paper we give a closed formula for the inverse rule of a reversible $(2R+1)$-cyclic cellular automaton with p.b.c. over the finite field $\mathbb{F}_2$ for any value of the neighbourhood radius R. It turns out that the inverse of a reversible $(2R+1)$-cyclic CA with p.b.c. is again a cyclic CA with p.b.c., but with a different neighbourhood radius, and this radius depends on certain numbers which need to be computed by a new algorithm we introduce. Finally, we apply our results to the case $R=1$ (which is the ECA with Wolfram rule number 150) to introduce an alternative and improved expression for the inverse transition dipolynomial formulated in Encinas and del Rey (2007). We also illustrate these results by giving explicit computations for the inverse transition dipolynomial of a reversible cellular automaton with penta-cyclic rule.

1. Introduction

A cellular automaton is a simple model of computation capable to simulate complex phenomena. It can be defined as a finite state machine constituted by a finite number of cells (cellular space) that are endowed with a state belonging to a –finite– state set; these states change in discrete steps of time according to a local transition rule whose variables are the states of a fixed collection of cells at the previous steps of time [34]. The vector formed by the states of all cells of the cellular automaton at a particular step of time t is called its configuration at t, and the evolution process is governed by means of the global transition function (the function that maps configurations into configurations).

Reversibility is a very important characteristic of the dynamics of cellular automata. It is intimately related to the physical notion of "reversibility", which is one of the fundamental microscopic physical laws of Nature. A cellular automaton is said to be reversible when every configuration has only one previous configuration and, consequently, the evolution backwards is possible by means of the invertible cellular automaton associated. In a more precise way, a cellular automaton is invertible if and only if its global transition function is injective [10,24]. Fundamental results in the study of the reversibility

* Corresponding author.
E-mail addresses: dani@usal.es (D. Hernández Serrano), delrey@usal.es (A. Martín del Rey).

https://doi.org/10.1016/j.amc.2019.03.060
0096-3003/

of cellular automata are related with the existence of an algorithm to decide the injectivity and surjectivity of cellular automata. In this sense, it is shown that such algorithm exists for the case of uni-dimensional cellular automata [1], whereas this question is undecidable for two-dimensional cellular automata [12]. Since these earlier studies there have been a number of works dealing with the study of reversibility properties of cellular automata; in fact it remains a very topical issue (see, for example, [2,4,9,14,26,27]). For a more detailed explanation of reversible cellular automata we refer the reader to [13,20,21] and references therein.

Elementary cellular automata (ECA for short) are, probably, the most studied class of cellular automata. Their cells are linearly arranged, and the state set is given by $\mathbb{Z}_2$. The state of each cell is ruled by a three-variable boolean function whose variables are the states of the main cell and its two nearest cells on each side. Due to the nature of the local transition function there are 256 possible ECA, and they have been extensively studied from a theoretical and practical point of view [33]. Furthermore, its reversibility problem has been also tackled in several papers (see, for example, [3,16–18,23,25,27]). The reversibility problem consists of both determining the length of the cellular space for reversible elementary cellular automata, and computing the inverse cellular automata. The second one is the most important issue due to the potential applications it could have, in fact, treated in terms of circulant matrices it has a wide range of applications in signal and image processing, linear forecast or error correcting code theory (see [5,8,28,32,35]).

In this paper we deal with $(2R+1)$-cyclic cellular automata with periodic boundary conditions over the finite field $\mathbb{F}_2$, $(2R+1)$-CCA with p.b.c. for short, which are cellular automata with a cyclic structure and neighborhood radius R. In [29] it is shown that if the number n of cells of the automaton and $2R+1$ are coprime, then the $(2R+1)$-CCA with p.b.c. is reversible, but no explicit formula is given for its inverse, what they propose is to use the Euclides algorithm over the polynomial ring $\mathbb{F}_2[x]$ (modulo x^n-1) if one would like to compute the inverse transition dipolynomial.

As far as we know, a closed formula for the inverse transition polynomial of a reversible $(2R+1)$-CCA with p.b.c is only given for the case $R=1$ in [11], which corresponds to the ECA with Wolfram rule number 150, which is an automata used in several and different applications (see for instance [6,7,15,22,31]). The problem of explicit computation of the inverse transition dipolynomial for $R>1$ has not been solved.

We give in these notes an explicit and closed formula for the inverse transition dipolynomial of a reversible $(2R+1)$-CCA with p.b.c. over the finite field $\mathbb{F}_2$ valid for any value of the neighbourhood radius R and any number of cells n (subject to the reversibility condition $(n, 2R+1)=1$). This also shows that the inverse of a reversible $(2R+1)$-CCA with p.b.c. is also a CCA but with a different neighbourhood radius in general. Whereas the original reversible $(2R+1)$-CCA depends on n and R, its inverse (and thus its neighbourhood radius) also depends on two other parameters which are computed by a new algorithm we introduce here, and this is what allow us to efficiently implement the novel closed formula we propose. What we present is, instead of using the Euclides algorithm over the polynomial ring $\mathbb{F}_2[x]$ (modulo x^n-1) to compute the inverse transition dipolynomial of a reversible $(2R+1)$-CCA with p.b.c., we give a closed and explicit formula which depends on an algorithm making only use of the Euclides algorithm over $\mathbb{F}_2$. In particular, applying our results to the case $R=1$ we give an alternative and improved expression for the inverse transition dipolynomial of the 150 ECA formulated in [11]. The case $R=2$ (which corresponds to the penta-cyclic rule of [30]) is also dealt in detail. It should be interesting to apply these ideas over the finite field $\mathbb{F}_p$ as a states set (see [18,19] for the 150 ECA over this field).

The rest of the paper is organized as follows: in Section 2 the mathematical background related to elementary cellular automata with neighbourhood radius R is given; Section 3 is devoted to state useful results on dipolynomials and to introduce a new formal dipolynomial which extends the notion of an standard transition dipolynomial for rational numbers, and which we shall use to prove that the closed formula we propose in the next section is correct; we present in Section 4 the main results of these notes: an explicit formula for the transition dipolynomial of a reversible $(2R+1)$-CCA with p.b.c. is given and the algorithm to compute the numbers on which this formula depends on is introduced. We finish the section by presenting an implementation of the whole process which might help in both understanding and programming the results here contained. Finally, in Section 5, by restricting our results to the case $R=1$ and $R=2$, we end up with an improved expression to the one formulated in [11] for the inverse of the 150 ECA (case $R=1$), and we give an explicit formula for the inverse transition dipolynomial of a reversible cellular automaton with a penta-cyclic rule (case $R=2$).

2. The basic theory of elementary cellular automata

Elementary cellular automata with neighborhood radius R are characterized by the following features:

(1) The n cells constituting the cellular space are uniformly arranged in a one-dimensional grid.
(2) The state set is $\mathbb{F}_2=\{0,1\}$, such that s_i^t stands for the state of the ith cell at the step of time t.
(3) The state of each cell at time $t+1$ depends on the states of R left and right neighbour cells and the cell itself at the previous step of time. Consequently, the local transition function is as follows:

$$s_i^{t+1}=f\left(s_{i-R}^t,\ldots,s_{i-1}^t,s_i^t,s_{i+1}^t,\ldots,s_{i+R}^t\right).$$

(4) As the number of cells is finite, boundary conditions must be taken into account. Usually periodic boundary conditions are assumed, that is, if $i\equiv j\ (\mathrm{mod} n)$ then $s_i^t=s_j^t$.

We are interested in the $(2R+1)$-cyclic cellular automata with p.b.c, which are defined by the local transition function:

$$s_i^{t+1} = s_{i-R}^t \oplus \cdots s_{i-1}^t \oplus s_i^t \oplus s_{i+1}^t \oplus \cdots s_{i+R}^t, \quad 1 \le i \le n, \tag{1}$$

where $\oplus$ denotes the sum in $\mathbb{F}_2$. If $P^t(x) = \sum_{i=1}^n s_i^t x^i$ is the configuration polynomial at step of time t, its global dynamics can be represented in $\mathbb{F}_2[x]/(x^n-1)$ as follows:

$$P^{t+1}(x) \equiv T_n(x) \cdot P^t(x) \mod x^n - 1, \tag{2}$$

where

$$T_n(x) \equiv D_R(x) = 1 + \sum_{j=1}^{R} (x^j + x^{-j})$$

is the transition dipolynomial (of neighbourhood radius R).

Remark 1. Notice that it is invariant under the transformation $x \mapsto x^{-1}$ modulo $x^n - 1$, that is: $T_n(x) \equiv T_n(x^{-1})$ modulo $x^n - 1$.

The dynamics of the $(2R+1)$-CCA with p.b.c. can be also interpreted in terms of matrix theory as follows:

$$C^{t+1,T} = M \cdot C^{t,T}, \tag{3}$$

where $C^t = \left(s_1^t, s_2^t, \ldots, s_n^t\right) \in \mathbb{F}_2^n$ is the configuration at step of time t, $C^{t+1,T}$ and $C^{t,T}$ denotes their transpose vectors respectively, and M is a particular nth order circulant matrix (with $n \ge 2R+1$): is a $n \times n$ symmetric circulant matrix with only a $(2R+1)$-diagonal band as non zero entries. For example, in the case $R=1$ (that is, for the 150 ECA) is given by:

$$M = \operatorname{circ}(1,1,0,\ldots,0,1) = \begin{pmatrix} 1 & 1 & 0 & 0 & \cdots & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & \cdots & 0 & 1 & 1 \end{pmatrix}. \tag{4}$$

3. The transition dipolynomial with rational neighborhood radius

Let us start by showing the following properties of dipolynomials, which we will use to prove the main results.

Lemma 1. *Over $\mathbb{F}_2$ we have the following formulae:*

(a) $D_m(x) = \frac{x^{-m}(1+x^{1+2m})}{1+x}$. *In particular* $D_R(x) = \frac{x^{-R}(1+x^N)}{1+x}$.
(b) $D_{n+i}(x) \equiv D_i(x) \pmod{x^n-1}$. *In particular* $D_n(x) \equiv 1 \pmod{x^n-1}$.
(c) $D_{n-i}(x) \equiv D_{i-1}(x) \pmod{x^n-1}$. *In particular* $D_{n-1}(x) \equiv 1 \pmod{x^n-1}$.
(d) $(x^{-i} + x^i) D_b(x) = D_{b-i}(x) + D_{b+i}(x)$.
(e) $D_a(x) D_b(x) = \sum_{i=-a}^{a} D_{b+i}(x)$.

Proof.

(a) It follows from the expressions $\sum_{j=0}^{m} x^j = \frac{1+x^{m+1}}{1+x}$ and $\sum_{j=1}^{m} x^j = \frac{x(1+x^m)}{1+x}$.
(b) Using (a) we have:

$$D_{n+i}(x) = \frac{x^{-n}x^{-i}(1+x^{2n}x^{1+2i})}{1+x} \equiv \frac{x^{-i}(1+x^{1+2i})}{1+x} = D_i(x) \pmod{x^n-1}.$$

(c) Again using (a) we have:

$$D_{n-i}(x) = \frac{x^{-n}x^{i}(1+x^{2n}x^{1-2i})}{1+x} \equiv \frac{x^{i}(1+x^{1-2i})}{1+x} = \frac{x^i x^{-2i}(x^{2i}+x)}{1+x} = D_{i-1}(x) \pmod{x^n-1}.$$

(d) A simple calculus shows:

$$\begin{aligned} D_{b-i}(x) + D_{b+i}(x) &= \frac{x^{-(b-i)}(1+x^{1+2(b-i)})}{1+x} + \frac{x^{-(b-i)}(1+x^{1+2(b-i)})}{1+x} \\ &= \frac{x^i x^{-b} + x^{1+b-i} + x^{-i}x^{-b} + x^{1+b+i}}{1+x} = \frac{x^{-i}x^{-b} + x^{1+b-i}}{1+x} + \frac{x^i x^{-b} + x^{1+b+i}}{1+x} \\ &= \frac{x^{-i}x^{-b}(1+x^{1+2b})}{1+x} + \frac{x^i x^{-b}(1+x^{1+2b})}{1+x} = (x^{-i}+x^i) D_b(x) \end{aligned}$$

(e) It follows from (d).

□

Notice that, even the dipolynomial $D_m(x) = 1 + \sum_{j=1}^{m}(x^j + x^{-j})$ is not defined when m is rational number, we can formally write:

$$D_{\frac{b}{c}}(x^c) = \frac{x^{-b}(1 + x^{c(1+2\frac{b}{c})})}{1 + x^c} = \frac{x^{-b}(1 + x^{c+2b})}{1 + x^c}\,. \tag{5}$$

Remark 2. We will see that, at least for certain values of b, this is a particular dipolynomial with neighbourhood radius b, but where some neighbours might be zero (in the sense that some of the coefficients of its dipolynomial expression might be zero).

We have the following result for the dipolynomial $D_{\frac{b}{c}}(x^c)$ when $c = 2a + 1$, which we will be using in the proof of the main results.

Proposition 1. *We have:*

$$D_a(x)D_{\frac{b}{2a+1}}(x^{2a+1}) = D_{a+b}(x)\,.$$

Proof. Indeed, using (a) of Lemma 1 and Eq. (5) we have:

$$\begin{aligned} D_a(x)D_{\frac{b}{2a+1}}(x^{2a+1}) &= \frac{x^{-a}(1 + x^{1+2a})}{1 + x}\,\frac{x^{-b}(1 + x^{(2a+1)(1+2\frac{b}{2a+1})})}{1 + x^{2a+1}} \\ &= \frac{x^{-a-b}(1 + x^{1+2a+2b})}{1 + x} = D_{a+b}(x) \end{aligned}$$

□

4. The inverse of a reversible $(2R + 1)$-cyclic ECA

This section is devoted to present the main results of the work: a closed formula for the transition dipolynomial of a reversible $(2R + 1)$-CCA with p.b.c. over $\mathbb{F}_2$ and an algorithm which computes certain numbers on which this formula depends on.

Let $N = 2R + 1$ and $n = Nk + r$ where k is a natural number and $r \in \{1, 2, \ldots, N - 1\}$ is the remainder of n modulo N. We shall prove that, given a reversible $(2R + 1)$-CCA with p.b.c. and n cells, the transition dipolynomial of its inverse is given by the formal expression:

$$D_{\frac{b}{N}}(x^N) \equiv \frac{x^{rr'-tN} + x^{(t+1)N-rr'}}{1 + x^N}\,, \quad \text{where } b = n + tN - rr'\,. \tag{6}$$

This expression is no yet formulated as a dipolynomial and it depends on the additional numbers r' and t. Firstly, we will show how to compute the numbers r' and t by introducing a new algorithm which determines a "correct" (in a sense which we shall specify later) sequence of couples (r', t) for all the remainder values $\{1, 2, \ldots, N - 1\}$. Once the algorithm is applied, we can introduce a particular $n = Nk + r$ and look for its unique pair (r', t). Then, we will exhibit the formula above as a dipolynomial expression and prove that indeed it represents the transition dipolynomial of the inverse of a reversible $(2R + 1)$-CCA with p.b.c. with n cells. Moreover, this will reveal the inverse also as a cyclic CA with, possibly, different neighbourhood radius.

Remark 3. In the literature (see [29] for instance), if we denote by $T_n(x)$ the transition dipolynomial of a reversible $(2R + 1)$-CCA with p.b.c. with n cells, the inverse transition dipolynomial could be computed as the polynomial $\widetilde{T}_n(x)$ verifying that $T_n(x)\widetilde{T}_n(x) \equiv 1$ modulo $x^n - 1$, that is, it could be computed by using the Euclides algorithm in the polynomial ring $\mathbb{F}_2[x]$ modulo $x^n - 1$, but no explicit expression is given for it (apart from the case $R = 1$ in [11]). Instead, we state a closed formula for the inverse which depends on an algorithm making only use of the Euclides algorithm in $\mathbb{F}_2$, which is also a more effective process computationally.

Remark 4. Recall that if N and n are coprime then the $(2R + 1)$-CCA is reversible (see [29]) and notice that, if $N = \prod_{i=1}^{m} p_i^{n_i}$ is the prime factorization of $N = 2R + 1$, we need $(r, p_i) = 1$ for all $i = 1, \ldots, m$ to achieve reversibility.

4.1. The CES algorithm

Recall that $N = 2R + 1$ and $n = Nk + r$ where $0 \le r < N = 2R + 1$. The algorithm will be given for the the case on which $0 \le r \le R$, we shall show later on how to deal with the remaining values until $N - 1 = 2R$ by using $N - r$.

The algorithm will finally end up with a sequence of ceiling function expressions for remainder entries in $\{1, 2, \ldots, R\}$, so that we shall refer to it as the "*ceiling expression sequence algorithm*" (CES algorithm). Before stating the algorithm, let us prove the following result:

Lemma 2. *Let s be a positive number and write $r' = \lceil \frac{sR}{r} \rceil$ for the ceiling function of $\frac{sR}{r}$. Then $r = \lceil \frac{sR}{r'} \rceil$.*

Proof. Let us write $r' = \lceil \frac{sR}{r} \rceil$, then we have that $sR = Qr + h$ where $0 \leq h < r$ and:

$$r' = \begin{cases} Q+1 & \text{if} \quad h \neq 0 \\ Q & \text{if} \quad h = 0 \end{cases}$$

If $h = 0$ the statement is trivial, so let us assume that $h \neq 0$. Then, $sR = (r'-1)r + h$ where $0 \leq h < r$ and we can write:

$$sR = r'r - r + h = r'r - r + h - r' + r' = (r-1)r' + h - r + r' .$$

Since $h - r < 0$, we have $h' \overset{not}{=} h - r + r' < r'$ and thus $sR = (r-1)r' + h'$ with $h' < r'$, that is: $r = \lceil \frac{sR}{r'} \rceil$. □

Definition 1. The CES algorithm is the following:

1. Start by computing in order the following sequence:
$$R = \frac{R}{1}, \left\lceil \frac{R}{2} \right\rceil, \left\lceil \frac{R}{3} \right\rceil, \ldots, \left\lceil \frac{R}{R-1} \right\rceil, \frac{R}{R} = 1$$
and store 1 and R.
2. In order, and for each $j \in \{2, \ldots, R-1\}$ such that $(j, p_i) = 1$, write $R = qj + h$.
   - If $j - h = 1$ we store $j' = \lceil \frac{R}{j} \rceil$ and $j = \lceil \frac{R}{j'} \rceil$ (this last one only if $j \neq j'$). For the remainder j' we set $(r', s, t) = (j, 1, 0)$; for the remainder j we set $(r', s, t) = (j', 1, 0)$. Continue not allowing already stored numbers.
   - If $j - h \neq 1$, remove $\lceil \frac{R}{j} \rceil$ and continue in order with the sequence.
3. If $j \in \{2, \ldots, R-1\}$ (with $(j, p_i) = 1$) is the first number such that $\lceil \frac{R}{j-1} \rceil = \lceil \frac{R}{j} \rceil$, then compute $\lceil \frac{sR}{j} \rceil$ where $s = 2t + 1$ is the smallest odd integer number which is smaller or equal that j and such that $\lceil \frac{sR}{j} \rceil \neq \lceil \frac{R}{i} \rceil$ for all $i = 2, \ldots, j-1$.
4. For each $2 \leq j \leq R-1$, let $j' = \lceil \frac{sR}{j} \rceil$ be the result of the previous step and let h be such that $sR = Qj + h$ (where $h < j$).
   - If $j - h - t = 0, 1$ then we store $j' = \lceil \frac{sR}{j} \rceil$ and $j = \lceil \frac{sR}{j'} \rceil$ (this last one only if $j \neq j'$). For the remainder j' we set $(r', s, t) = (j, s, \frac{s-1}{2})$; for the remainder j we set $(r', s, t) = (j', s, \frac{s-1}{2})$.
   - If $j - h - t \neq 0, 1$, remove such an j' and go back to step 3 starting from that j' and not allowing the already stored numbers.

The following result is included only because it might simplify the computational implementation of the algorithm.

Lemma 3. *Write $r' = \lceil \frac{sR}{r} \rceil$ and $sR = Qr + h$. If $h = 0$ then $s = 1$ (and thus $t = 0$). That is, the only exact fractions $\frac{sR}{r} \in \mathbb{Z}_+$ produced by the algorithm are those having $s = 1$.*

Proof. If $h = 0$ then $r' = \frac{sR}{r}$ is a natural number. Let us write $R = \frac{rr'}{s}$ and let us assume that $s > 1$ in order to get a contradiction. The following cases might occur:

1. s divides r. Then $r = s\bar{r}$ with $\bar{r} < r$ and thus $r' = \frac{R}{\bar{r}}$ is a natural number where $\bar{r} < r$. Therefore by applying the algorithm we get a contradiction.
2. s divides r'. Similar argument works as before by applying the algorithm to $r = \frac{sR}{r'}$.
3. $s = aa'$ where a divides r, a' divides r' and $1 < a$, $a' < s$. Then $r = ac$, $r' = a'c'$ where $c < r$ and $c' < r'$. Thus, $r' = \frac{a'R}{c}$ where $a' < s$ and $c < r$ and we have simplified the expression for r'. By iterating this process we arrive to one of the above cases.

Therefore we have proved that $s = 2t + 1 = 1$. □

Remark 5. Notice that the number $r' = \lceil \frac{sR}{r} \rceil$ can not be repeated in the algorithm sequence, or that the Lemma above shows that some value $r' = \lceil \frac{sR}{r} \rceil$ could not be in the sequence if, following the order of computation in the algorithm, we have that $r' = \lceil \frac{\tilde{s}R}{\tilde{r}} \rceil$ for a smaller $\tilde{r}$. The case on which r or r' are a multiple of some factor p_i in the prime decomposition $N = \prod_{i=1}^{m} p_i^{n_i}$ need to be removed from the sequence since then the ECA will not be reversible (as mention in the introduction of this section). These are the reasons why we are including the restriction $r - h - t = 0, 1$ in the algorithm. The CES algorithm finally ends up with all possible, non repeated and possibly not ordered numbers r' such that $1 \leq r' \leq R$ and $(r', p_i) = 1$ (which represents the valid remainders modulo N for a given n) and gives a unique ceiling sequence $r = \lceil \frac{sR}{r'} \rceil$ for entries in $\{1, 2, \ldots, R\}$.

Let us show now how to work with entries in $\{R+1, \ldots, 2R = N-1\}$. If the rest $\bar{r}$ (that is $n = Nk + \bar{r}$) verifies that $R + 1 \leq \bar{r} \leq 2R$, then there exists $r \leq R$ such that $\bar{r} = N - r$, and we have the following result:

Lemma 4. *If $r = \lceil \frac{sR}{r'} \rceil$ then:*

$$\bar{r} = N - r = \begin{cases} \left\lceil \dfrac{(2r' - s)R}{r'} \right\rceil & \text{if} \quad h' \neq 0 \\ \dfrac{(2r' - 1)R}{r'} + 1 & \text{if} \quad h' = 0 \end{cases}$$

where $h' = h - r + r'$.

Proof. If $r = \lceil \frac{sR}{r'} \rceil$ then $sR = (r-1)r' + h'$ where $0 \leq h' < r$.

- If $h' = 0$ then Lemma 2 implies $h = 0$ and by Lemma 3 then $s = 1$. Thus $r = \frac{R}{r'}$ and therefore:

$$N - r = \frac{Nr' - R}{r'} = \frac{(2R+1)r' - R}{r'} = \frac{(2r'-1)R}{r'} + 1\,.$$

- If $h' \neq 0$ then $sR = rr' - r' + h'$ and $r = \frac{sR + r' - h'}{r'}$. Then $N - r = \frac{(2r'-s)R + h'}{r'}$ and then

$$(2r' - s)R = (N-r)r' - h' + r' - r' = (N - r - 1)r' + r' - h'\,,$$

where $r' - h' < r'$ and therefore $N - r = \lceil \frac{(2r'-s)R}{r'} \rceil$. □

Corollary 1. *In particular if we write* $N - r = (N - r - 1)r' + \bar{h}'$ *where* $0 \leq \bar{h}' < r'$ *then* $\bar{h}' = r' - h' = r - h < r'$.

Let us write $\bar{s} = 2r' - s$ and define $\bar{s} = 2\bar{t} + 1$. Once we apply the CES algorithm for the entries in $\{1, 2, \ldots, R\}$, we can compute the associated r' and $\bar{t}$ for the entries $\bar{r}$ in $\{R+1, \ldots, 2R\}$ as follows:

- Do $r = N - \bar{r}$ (which belongs to $\{1, 2, \ldots, R\}$) and look for its associated r' and $s = 2t + 1$ given by the CES algorithm of Definition 1.
- Use $\bar{s} = 2r' - s = 2\bar{t} + 1$ and apply Lemma 4 to compute its associated $\bar{t}$.

Example 1. Consider the case $R = 5$ so that $N = 2R + 1 = 11$. The possible remainders for an $n = Nk + r$ are in $\{1, 2, \ldots 5, 6, \ldots, 10\}$. Let us apply the CES algorithm for the entries in {1, 2, 3, 4, 5} (notice that since 11 is prime, coprime conditions in the algorithm are always satisfied):

- For the entry 1: we do $\lceil \frac{5}{1} \rceil = \frac{5}{1} = 5$ so that $j = 1$ and $j' = 5$ and $R = qj + h$ implies that $j - h = 0$. We then store $j' = \frac{5}{1} = \boxed{5}$ and $j = \frac{5}{5} = \boxed{1}$. That is, for the remainder $j' = 5$ we set $(r', s, t) = (1, 1, 0)$ and for the remainder $j = 1$ we set $(r', s, t) = (5, 1, 0)$.
- For the entry 2: we have $\lceil \frac{5}{2} \rceil = 3$ so that $R = q2 + h$ and thus $j - h = 1$. We store $j' = \lceil \frac{5}{2} \rceil = \boxed{3}$ and $j = \lceil \frac{5}{3} \rceil = \boxed{2}$ since $j \neq j'$ and they are not already stored. That is, for the remainder $j' = 3$ we set $(r', s, t) = (2, 1, 0)$ and for the remainder $j = 2$ we set $(r', s, t) = (3, 1, 0)$.
- The entry 3 is already stored.
- For the entry 4: we have that $\lceil \frac{R}{4} \rceil = 2$ is repeated, so we do $\lceil \frac{3 \cdot 5}{4} \rceil = 4$ which is no repeated. Its $j = j' = 4$, $s = 3$ (so that $t = 1$) and $h = 3$. Thus $j - h - t = 0$ and then we can store $j' = \lceil \frac{3 \cdot 5}{4} \rceil = \boxed{4}$. For the remainder $j' = 4$ we ser $(r', s, t) = (4, 3, 1)$.
- The entry 5 is already stored.

Now we use Lemma 4 to compute r' and $\bar{t}$ for the entries in {6, 7, 8, 9, 10}:

- If $\bar{r} = 6$ then $r = N - \bar{r} = 5 = \frac{5}{1}$ so that $(r', s, t) = (1, 1, 0)$. Then by Lemma 4 we have $\boxed{6} = \bar{r} = N - r = \frac{5}{1} + 1$ and therefore $r' = 1$ and $\bar{s} = 1 \Rightarrow t = 0$. For the remainder 6 we set $(r', \bar{s}, \bar{t}) = (1, 1, 0)$.
- If $\bar{r} = 7$ then $r = N - \bar{r} = 4 = \lceil \frac{3 \cdot 5}{4} \rceil$ so that $(r', s, t) = (4, 3, 1)$. Then by Lemma 4 we have $\boxed{7} = \bar{r} = N - r = \lceil \frac{5 \cdot 5}{4} \rceil$ (since $s + \bar{s} = 2r'$). For the remainder 7 we set $(r', \bar{s}, \bar{t}) = (4, 5, 2)$.
- If $\bar{r} = 8$ then $r = N - \bar{r} = 3 = \lceil \frac{5}{2} \rceil$ so that $(r', s, t) = (2, 1, 0)$. Then by Lemma 4 we have $\boxed{8} = \bar{r} = N - r = \lceil \frac{3 \cdot 5}{2} \rceil$ (since $s + \bar{s} = 2r'$). For the remainder 8 we set $(r', \bar{s}, \bar{t}) = (2, 3, 1)$.
- If $\bar{r} = 9$ then $r = N - \bar{r} = 2 = \lceil \frac{5}{3} \rceil$ so that $(r', s, t) = (3, 1, 0)$. Then by Lemma 4 we have $\boxed{9} = \bar{r} = N - r = \lceil \frac{5 \cdot 5}{3} \rceil$ (since $s + \bar{s} = 2r'$). For the remainder 9 we set $(r', \bar{s}, \bar{t}) = (3, 5, 2)$.
- If $\bar{r} = 10$ then $r = N - \bar{r} = 1 = \frac{5}{5}$ so that $(r', s, t) = (5, 1, 0)$. Then by Lemma 4 we have $\boxed{10} = \bar{r} = N - r = \frac{9 \cdot 5}{5} + 1$ (since $s + \bar{s} = 2r'$). For the remainder 10 we set $(r', \bar{s}, \bar{t}) = (5, 9, 4)$.

Finally we end up with the following Table 1:

Table 1
Applying the CES algorithm for $R = 5$.

r	1	2	3	4	5	6	7	8	9	10
ceilings	$\frac{5}{5}$	$\lceil \frac{5}{3} \rceil$	$\lceil \frac{5}{2} \rceil$	$\lceil \frac{3 \cdot 5}{4} \rceil$	$\frac{5}{1}$	$\frac{5}{1} + 1$	$\lceil \frac{5 \cdot 5}{4} \rceil$	$\lceil \frac{3 \cdot 5}{2} \rceil$	$\lceil \frac{5 \cdot 5}{3} \rceil$	$\frac{9 \cdot 5}{5} + 1$
r′	5	3	2	4	1	1	4	2	3	5
s or $\bar{\mathbf{s}}$	1	1	1	3	1	$\bar{1}$	$\bar{5}$	$\bar{3}$	$\bar{5}$	$\bar{9}$
t or $\bar{\mathbf{t}}$	0	0	0	1	0	$\bar{0}$	$\bar{2}$	$\bar{1}$	$\bar{2}$	$\bar{4}$

4.2. The inverse transition dipolynomial

Once the CES algorithm is given, we are in condition of stating the main results of the work: a closed formulae for the transition dipolynomial of a reversible $(2R+1)$-CCA with p.b.c., and explicit expressions for the inverse local transition rules.

Theorem 1. *Let $N = 2R+1$ and $n = Nk + r$, where $r \leq R$ and $(N, n) = 1$. The transition dipolynomial corresponding to the inverse of a reversible cellular automaton with $(2R+1)$-cyclic rule and periodic boundary conditions is given by:*

$$\widetilde{T}_n(x) \equiv D_{\frac{b}{N}}(x^N) \mod x^n - 1,$$

where $b = n + Nt - rr'$ and the numbers t and r' are computed by the algorithm of Section 4.1.

Proof. We have to show that $T_n(x)\widetilde{T}_n(x) \equiv 1 \mod x^n - 1$. Indeed, since $T_n(x) \equiv D_R(x)$ and $N = 2R+1$, using Proposition 1 for $a = R$ we have:

$$T_n(x)\widetilde{T}_n(x) \equiv D_R(x) D_{\frac{b}{N}}(x^N) = D_{R+b}(x) \mod x^n - 1.$$

Since $b = n + Nt - rr'$, where $r' = \lceil \frac{sR}{r} \rceil$ (and thus $sR = rr' - r + h$), it is $R + b = n - (r - h - t)$. Since the algorithm (see Section 4.1) only allows $r - h - t = 0, 1$ then:

$$D_{R+b}(x) = \begin{cases} D_n(x) & \text{if } r - h - t = 0 \\ D_{n-1}(x) & \text{if } r - h - t = 1 \end{cases}$$

Thus, using (b) and (c) of Lemma 1 we have that $D_n(x) \equiv 1$ and $D_{n-1}(x) \equiv 1 \mod x^n - 1$, and therefore we conclude that $T_n(x)\widetilde{T}_n(x) \equiv 1 \mod x^n - 1$. □

Theorem 2. *Let $N = 2R+1$ and $n = Nk + r$, where $r \leq R$ and $(N, n) = 1$. The transition dipolynomial corresponding to the inverse of a reversible cellular automaton with $(2R+1)$-cyclic rule and periodic boundary conditions is given by:*

$$\widetilde{T}_n(x) = 1 + \sum_{\substack{l=1,\dots,k \\ j=0,1,\dots,r'-1}} \left(x^{(lN-rj)} + x^{-(lN-rj)} \right) + \sum_{l'=1,\dots,t} \left(x^{((k+l')N-r(r'-1))} + x^{-((k+l')N-r(r'-1))} \right).$$

Which we can symbolically write as follows:

$$\widetilde{T}_n(x) = 1 + \sum_{i \in I^{vir}} \left(x^i + x^{-i} \right), \quad \text{where } i = (l+l')N - rj$$

$$\text{and } I^{vir} = \begin{cases} l = 1, \dots, k \text{ and } j = 0, 1, \dots, r'-1 & \text{if} \quad l' = 0 \\ l = k \text{ and } j = r'-1 & \text{if} \quad l' = 1, \dots, t \end{cases}$$

Proof. Indeed, since $n = Nk + r$ and we are working over $\mathbb{F}_2$, using (a) of Lemma 1 and the equivalence $\equiv$ modulo $x^n - 1$ (which implies $x^{Nk} \equiv x^{-r}$), we have:

$$\begin{aligned}
\widetilde{T}_n(x) &= 1 + \sum_{l=1}^{k} (x^{lN} + x^{-lN}) + \sum_{\substack{l=1,\dots,k \\ j=1,\dots,r'-1}} x^{(lN-rj)} + \sum_{\substack{l=1,\dots,k \\ j=1,\dots,r'-1}} x^{-(lN-rj)} \\
&\quad + \sum_{l'=1,\dots,t} x^{((k+l')N-r(r'-1))} + \sum_{l'=1,\dots,t} x^{-((k+l')N-r(r'-1))} \\
&= \frac{x^{-Nk}(1+x^{N(1+2k)})}{1+x^N} + \sum_{l=1}^{k} \frac{x^{lN-r} + x^{lN-r'r}}{1+x^{-r}} + \sum_{l=1}^{k} \frac{x^{-(lN-r)} + x^{-(lN-r'r)}}{1+x^r} \\
&\quad + \frac{x^{(k+1)N-r(r'-1)} + x^{(k+t+1)N-r(r'-1)}}{1+x^N} + \frac{x^{-((k+1)N-r(r'-1))} + x^{-((k+t+1)N-r(r'-1))}}{1+x^{-N}} \\
&= \frac{x^{-Nk}(1+x^{N(1+2k)})}{1+x^N} + \frac{\sum_{l=1}^{k} x^{lN}(1+x^{-r(r'-1)}) + \sum_{l=1}^{k} x^{-lN}(x^r + x^{rr'})}{1+x^r} \\
&\quad + \frac{x^{(k+1)N-r(r'-1)}(1+x^{tN}) + x^{-N}x^{-((k+1)N-r(r'-1))}(1+x^{-tN})}{1+x^N} \\
&\equiv \frac{x^{-Nk}(1+x^{N(1+2k)})}{1+x^N} + \frac{x^N(1+x^{Nk})(1+x^{-r(r'-1)}) + (1+x^{Nk})x^{-Nk}(x^r + x^{rr'})}{(1+x^r)(1+x^N)} \\
&\quad + \frac{x^{N-rr'}(1+x^{tN}) + x^N x^{-(N-rr')}(1+x^{-tN})}{1+x^N} \\
&= \frac{x^{-Nk} + x^{N+Nk}}{1+x^N} + \frac{x^N x^{-r}(1+x^r)(1+x^{-rr'+r}) + (1+x^{-r})x^r(x^r + x^{rr'})}{(1+x^r)(1+x^N)}
\end{aligned}$$

$$
\begin{aligned}
&+\frac{x^{N-rr'}+x^{(t+1)N-rr'}+x^{rr'}+x^{rr'-tN}}{1+x^N}\\
&\equiv \frac{x^r+x^{N-r}+x^{N-r}+x^{N-rr'}+x^r+x^{rr'}+x^{N-rr'}+x^{(t+1)N-rr'}+x^{rr'}+x^{rr'-tN}}{1+x^N}\\
&= \frac{x^{(t+1)N-rr'}+x^{rr'-tN}}{1+x^N}\,.
\end{aligned}
$$

Now, taking $b=n+Nt-rr'$ it is:

$$rr'-tN=n-b \quad \text{and} \quad (t+1)N-rr'=N+b-n\,,$$

and we have that:

$$\frac{x^{(t+1)N-rr'}+x^{rr'-tN}}{1+x^N}\equiv\frac{x^{N+b}+x^{-b}}{1+x^N}=\frac{x^{-b}(1+x^{N+2b})}{1+x^N}=D_{\frac{b}{N}}(x^N)\pmod{x^n-1}\,.$$

That is to say, we have proved that

$$\widetilde{T}_n(x)\equiv D_{\frac{b}{N}}(x^N)\mod x^n-1\,,$$

where $b=n+Nt-rr'$, and thus we have concluded by Theorem 1. □

Corollary 2. *Let $N=2R+1$ and $n=Nk+r$, where $r\le R$ and $(N,n)=1$. The local transition rule corresponding to the inverse of a reversible cellular automaton with $(2R+1)$-cyclic rule and periodic boundary conditions is given for $1\le i\le n$ by:*

$$s_i^{t+1}=\sum_{l'=1,\dots,t} s^t_{i-((k+l')N-r(r'-1))}\oplus\sum_{\substack{l=1,\dots,k\\ j=0,1,\dots,r'-1}} s^t_{i-(lN-rj)}\oplus s_i^t\oplus\sum_{\substack{l=1,\dots,k\\ j=0,1,\dots,r'-1}} s^t_{i+(lN-rj)}\oplus\sum_{l'=1,\dots,t} s^t_{i+(k+l')N-r(r'-1)}\,,$$

where the summation symbol also denotes summation in $\mathbb{F}_2$.

Remark 6. The upper script t denotes time evolution of the automata and the subscript stands for the number computed by the algorithm.

As a direct consequence we have the following:

Proposition 2. *Let $N=2R+1$ and $n=Nk+r$, where $r\le R$ and $(N,n)=1$. The inverse of a reversible $(2R+1)$-CCA with p.b.c. is a $(2b+1)$-CCA with p.b.c. where $b=(k+t)N-r(r'-1)$. It has $kr'+t$ non zero entries fitted in a neighborhood radius of b.*

Let us study now the case on which $n=Nk+\bar{r}$ and $R+1\le\bar{r}\le 2R$. We have that there exists $r\le R$ such that $\bar{r}=N-r$, and then Lemma 4 says that $\bar{r}=N-r=\lceil\frac{\bar{s}R}{r'}\rceil$ where $\bar{s}=2\bar{t}+1$ and $s+\bar{s}=2r'$ (so that $\bar{t}=r'-1-t$). Thus, similar computations to those of Theorems 1 and 2 shows that:

Theorem 3. *Let $n=Nk+\bar{r}$ where $R\le\bar{r}<N$. The transition dipolynomial corresponding to the inverse of a reversible cellular automaton with $(2R+1)$-cyclic rule and periodic boundary conditions is given by:*

$$
\begin{aligned}
\widetilde{T}_n(x)=D_{\frac{\bar{b}}{N}}(x^N)&=1+\sum_{\substack{l=1,\dots,k\\ j=0,1,\dots,r'-1}}(x^{(lN-\bar{r}j)}+x^{-(lN-\bar{r}j)})+\sum_{\bar{l}'=1,\dots,\bar{t}}(x^{((k+\bar{l}')N-\bar{r}(r'-1))}+x^{-((k+\bar{l}')N-\bar{r}(r'-1))})\\
&\equiv 1+\sum_{\substack{l=1,\dots,k\\ j=0,1,\dots,r'-1}}(x^{(l+kj)N}+x^{-(l+kj)N})+\sum_{\bar{l}'=1,\dots,\bar{t}}(x^{(l'+kr')N}+x^{-(l'+kr')N})\,,
\end{aligned}
$$

where $\bar{b}=n+\bar{t}N-\bar{r}r'$.

We can symbolically write it as follows:

$$\widetilde{T}_n(x)=1+\sum_{\bar{i}\in\bar{I}^{vir}}(x^{\bar{i}}+x^{-\bar{i}})\,,\quad \text{where } \bar{i}=(l+\bar{l}')N-\bar{r}j\equiv(l+\bar{l}'+kj)N$$

and $\bar{I}^{vir}=\begin{cases} l=1,\dots,k \text{ and } j=0,1,\dots,r'-1 & \text{if} \quad \bar{l}'=0\\ l=k \text{ and } j=r'-1 & \text{if} \quad \bar{l}'=1,\dots,t\,.\end{cases}$

Corollary 3. *Let $n=Nk+\bar{r}$ where $R\le\bar{r}<N$ and $(N,n)=1$. The local transition rule corresponding to the inverse of a reversible cellular automaton with $(2R+1)$-cyclic rule and periodic boundary conditions is given for $1\le i\le n$ by:*

$$s_i^{t+1}=\sum_{l'=1,\dots,\bar{t}} s^t_{i-((k+\bar{l}')N-\bar{r}(r'-1))}\oplus\sum_{\substack{l=1,\dots,k\\ j=0,1,\dots,r'-1}} s^t_{i-(lN-\bar{r}j)}\oplus s_i^t\oplus\sum_{\substack{l=1,\dots,k\\ j=0,1,\dots,r'-1}} s^t_{i+(lN-\bar{r}j)}\oplus\sum_{\bar{l}'=1,\dots,\bar{t}} s^t_{i+(k+\bar{l}')N-\bar{r}(r'-1)}\,,$$

where the summation symbol also denotes summation in $\mathbb{F}_2$.

Proposition 3. *For $n = Nk + \bar{r}$ and $R \leq \bar{r} < N$, the inverse of a reversible $(2R+1)$-CCA with p.b.c. is a $(2\bar{b}+1)$-CCA with p.b.c. where $\bar{b} = (k+\bar{t})N - \bar{r}(r'-1)$. It has $kr' + \bar{t}$ non zero entries fitted in a neighborhood radius of $\bar{b}$.*

Corollary 4. *For $r = R, R+1$ the transition dipolynomial corresponding to the inverse of a reversible cellular automaton is given by the dipolynomial:*

$$\widetilde{T}_n(x) = 1 + \sum_{l=1}^{k} (x^{Nl} + x^{-Nl}) = D_k(x^N)\,,$$

and thus, the inverse cyclic CA has $2k$ symmetric neighbours fitted in a radius of $b = Nk$ and each of them separated by N slots. That is, the inverse is a $(2Nk+1)$-cyclic CA. The local transition rule is given by:

$$s_i^{t+1} = \sum_{l=1}^{k} s_{i-Nl}^t \oplus s_i^t \oplus \sum_{l=1}^{k} s_{i+Nl}^t\,.$$

Corollary 5. *The inverse of a reversible $(2R+1)$-CCA has the same reciprocity as for the original one: its inverse dipolynomial is also invariant under the change $x \mapsto x^{-1}$, that is, $\widetilde{T}_n(x) = \widetilde{T}_n(x^{-1})$.*

Remark 7. These results can be translated into the language of circulant matrices: the inverse of an invertible circulant matrix given by a reversible $(2R+1)$-CCA will not be a full diagonal band circulant matrix, but a semi-full diagonal band block matrix, in the sense that in might contain diagonal rows of zeros. This allows to reduce the time of computation in the coding theory applications treated in [29]. It should be interesting to generalice our results the case on which the set of states were the finite field $\mathbb{F}_p$.

4.3. The implementation process

Finally, and to summarize, the procedure goes as follows:

1. Introduce R and n. Define $N := 2R+1$ and compute $N = \prod_{i=1}^{m} p_i^{n_i}$ the prime factorization of N.
   - 1.1 If $(n, p_i) = 1$ for all $i = 1, \ldots, m$ continue to next step.
   - 1.2 If $(n, p_i) \neq 1$ for some $i = 1, \ldots, m$ stop. The $(2R+1)$-CCA is not reversible.
2. Apply the algorithm of Section 4.1 to correctly compute the numbers r' and t for the values in $\{1, 2, \ldots, R\}$.
3. In order, and for each entry $\bar{r}$ in $\{R+1, \ldots 2R\}$:
   - 3.1 Do $r = N - \bar{r}$ (which belongs to $\{1, 2, \ldots, R\}$) and look for its associated r' and $s = 2t+1$ given by step 2.
   - 3.2 Apply Lemma 4 to compute its associated $\bar{t}$.
4. Divide n by N so that $n = Nk + r$, where $1 \leq r < N$
   - 4.1 If $1 \leq r \leq R$, localice its associated r' and t from step 2 and use the Theorem 2 to give the dipolynomial associated with the inverse CA.
   - 4.2 If $R+1 \leq \bar{r} \leq 2R$, localice its associated r' and $\bar{t}$ from step 3 and use the Theorem 3 to give the dipolynomial associated with the inverse CA.

5. The reversibility problem for the ECA 150 and the ECA with penta cyclic rule

We apply in this section our results to the cases $R = 1$ and $R = 2$. In the first case, we find out an improved and simplified expression to that of [11] for the inverse of the transition dipolynomial of a reversible CA with rule number 150; in the second case we explicitly compute the closed formula for the inverse of a reversible CA with penta-cyclic rule.

5.1. Case $R = 1$. The reversibility problem for the 150 ECA

As mentioned in the introduction, special interest deserves the ECA with rule number 150 (ECA150) due to its many applications (and in particular the ones in Cryptography, see for instance [7,15,22,31]). This cellular automaton is defined by the local transition function:

$$s_i^{t+1} = s_{i-1}^t \oplus s_i^t \oplus s_{i+1}^t\,, \quad 1 \leq i \leq n\,,$$

so that it corresponds to the $(2R+1)$-CCA with p.b.c for $R = 1$. Its transition dipolynomial for a given $n = 3k + r$ is

$$T_n(x) \equiv x^{-1} + 1 + x = D_1(x)\,.$$

The reversibility problem for ECA 150 endowed with periodic boundary conditions and n cells was solved in [11], it is reversible if and only if $n \not\equiv 0$ (modulo 3). Moreover, they show that local transition function of the inverse cellular automaton is given by:

Table 2
Expressions of $\widetilde{T}_n(x)$ for different values of n.

n	$\widetilde{T}_n(x)$
4,5	$x^{-3}+1+x^3$
7,8	$x^{-6}+x^{-3}+1+x^3+x^6$
10,11	$x^{-9}+x^{-6}+x^{-3}+1+x^3+x^6+x^9$
16,17	$x^{-15}+x^{-12}+x^{-9}+x^{-6}+x^{-3}+1+x^3+x^6+x^9+x^{12}+x^{15}$

(i) For $n \equiv 1 (\mathrm{mod} 3)$, where $n = 3k+1$ with $k \in \mathbb{Z}^+$,

$$s_i^{t+1} = \bigoplus_{j \in I} s_{i+j}^t, \quad 1 \leq i \leq n, \tag{7}$$

where the set of indices is $I = \{0, \pm \lfloor \frac{3i}{2} \rfloor\}_{1 \leq i \leq k}$.

(ii) For $n \equiv 2 (\mathrm{mod} 3)$, where $n = 3k+2$ with $k \in \mathbb{Z}^+$,

$$s_i^{t+1} = \bigoplus_{j \in I} s_{i+j}^t, \quad 1 \leq i \leq n, \tag{8}$$

where the set of indices is $I = \left\{0, \pm \left\lfloor \frac{3i+1}{2} \right\rfloor\right\}_{1 \leq i \leq k}$.

Explicit expressions for the transition dipolynomials corresponding to the inverse cellular automata were also computed: if $n \equiv 1 (\mathrm{mod} 3)$

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

and for $n \equiv 2 (\mathrm{mod} 3)$ it is:

$$\widetilde{T}(x) = D_{\lfloor \frac{n-1}{2} \rfloor}(x) + \sum_{i=1}^{\lfloor \frac{n+2}{6} \rfloor} \left(x^{-(3i-2)} + x^{3i-2} \right), \tag{10}$$

where, as before, $D_m(x) = 1 + \sum_{j=1}^{m} \left(x^{-j} + x^j \right)$.

We can drastically simplify these expressions to a single and closed one. Since $n = 3k+r$ and $r = 1, 2 = R, R+1$, we only have to apply Corollary 4 in order to obtain the following formula for the inverse transition dipolynomial:

Theorem 4. *When $(n, 3) = 1$, the transition dipolynomial corresponding to the inverse of a reversible cellular automaton with Rule 150 and periodic boundary conditions is given, mod $x^n - 1$, by:*

$$\widetilde{T}_n(x) \equiv D_{\frac{n-r}{3}}(x^3) = D_k(x^3) = 1 + \sum_{i=1}^{k} (x^{3i} + x^{-3i}) .$$

And thus, the local transition function of the inverse cellular automaton of the 150 ECA is given by:

$$s_i^{(t+1)} = \sum_{l=-k}^{k} s_{i+3l}^{(t)} \text{ for } 1 \leq i \leq n ,$$

where $n = 3k+r$ and the last summation symbol is the XOR summation, that is, summation over $\mathbb{F}_2$.

In Table 2 some transition dipolynomials of the inverse cellular automaton for different values of n are shown.

Notice that the numbers $3j$ in the second formula of theorem above could be computed modulo n so that they give equivalent expressions for the local transition function of the inverse cellular automata. These equivalent expressions are precisely the ones given in [11, Theorem 1]. Let us illustrate this fact with the following example.

Example 2. Let us consider the ECA 150 for $n = 10 \equiv 1 \pmod 3$. We have that $k = 3$ and thus the transition dipolynomial of the inverse cellular automata is given by:

$$\widetilde{T}_{10}(x) = 1 + \sum_{i=1}^{3} (x^{3i} + x^{-3i}) = x^{-9} + x^{-6} + x^{-3} + 1 + x^3 + x^6 + x^9$$

which is equivalent $(\mathrm{mod}\ x^{10} - 1)$ to:

$$\widetilde{T}_{10}(x) = x^{-4} + x^{-3} + x^{-1} + 1 + x + x^3 + x^4 .$$

The local transition function of the inverse cellular automata is:

$$s_i^{(t+1)} = \sum_{j=-k}^{k} s_{i+3j}^{(t)} = s_{i-9}^{(t)} + s_{i-6}^{(t)} + s_{i-3}^{(t)} + s_i^{(t)} + s_{i+3}^{(t)} + s_{i+6}^{(t)} + s_{i+9}^{(t)},$$

which is equivalent to:

$$s_i^{(t+1)} = \sum_{j=-k}^{k} s_{i+3j}^{(t)} = s_{i-4}^{(t)} + s_{i-3}^{(t)} + s_{i-1}^{(t)} + s_i^{(t)} + s_{i+1}^{(t)} + s_{i+3}^{(t)} + s_{i+4}^{(t)}.$$

This last expression is the one given by equation (1) in [11, Theorem 1].

5.2. Case $R = 2$. The reversibility problem for the penta-cyclic ECA

The cellular automaton with penta cyclic rule is defined by the local transition function:

$$s_i^{t+1} = s_{i-2}^t \oplus s_{i-1}^t \oplus s_i^t \oplus s_{i+1}^t \oplus s_{i+2}^t, \quad 1 \le i \le n = 5k + r$$

where $r < 5$, so that it corresponds to the $(2R+1)$-CCA with p.b.c for $R = 2$ (that is, $5 = 2R + 1$). It is reversible if $(5, n) = 1$ and its transition dipolynomial is:

$$T_n(x) \equiv D_2(x) = x^{-2} + x^{-1} + 1 + x + x^2 \pmod{x^n - 1}.$$

The CES algorithm of Section 4.1 has an immediate application:

- If $r = 1$ we have $r = 1 = \frac{R}{2}$ so that $r' = 2$ and $t = 0$ (since $s = 2t + 1 = 1$).
- If $r = 2$, we have $r = 2 = \frac{R}{1}$ so that $r' = 1$ and $t = 0$ (we can also directly apply Lemma 2).
- Denoting the remainder $\bar{r} = 3$ then $r = N - \bar{r} = 2 = \frac{R}{1}$ so that $r' = 1$. By Lemma 4 it is $\bar{r} = N - r = \frac{R}{1} + 1$ and thus, $\bar{s} = 1$ and $\bar{t} = 0$.
- Denoting the remainder $\bar{r} = 4$ then $r = N - \bar{r} = 1 = \frac{R}{2}$ so that $r' = 2$. By Lemma 4 it is $\bar{r} = N - r = \lceil \frac{3R}{2} \rceil$ and thus, $\bar{s} = 3$ and $\bar{t} = 1$.

Using now Theorems 2 and 3 we have:

Theorem 5. *The transition dipolynomial corresponding to the inverse of a reversible cellular automaton with penta-cyclic rule and periodic boundary conditions is given modulo $x^n - 1$ by:*

- *For $r = 1$:*

$$\widetilde{T}_n(x) = 1 + \sum_{l=0}^{k} (x^{5l} + x^{-5l}) + \sum_{l=0}^{k} (x^{5l-1} + x^{-(5l-1)}).$$

- *For $r = 2$ and $\bar{r} = 3$:*

$$\widetilde{T}_n(x) = 1 + \sum_{i=1}^{k} (x^{5i} + x^{-5i}).$$

- *For $\bar{r} = 4$:*

$$\widetilde{T}_n(x) = 1 + \sum_{l=0}^{k} (x^{5l} + x^{-5l}) + \sum_{l=0}^{k} (x^{5l-4} + x^{-(5l-4)}) + x^{5k+1} + x^{-(5k+1)}.$$

Acknowledgment

This work has been supported by Ministerio de Economía y Competitividad (Spain) and the European Union through FEDER funds under grants TIN2017-84844-C2-1-R and MTM2017-86042-P.

References

[1] S. Amoroso, Y.N. Patt, Decision procedures for surjectivity and injectivity of parallel maps for tessellations structures, J. Comput. Syst. Sci. 6 (1972) 525–532.
[2] C.H. Chang, H. Chang, On the bernoulli automorphism of reversible linear cellular automata, Inf. Sci. 345 (2016) 217–225.
[3] P. Chaudhuri, D. Chowdhury, S. Nandi, S. Chattopadhyay, Additive Cellular Automata. Theory and Applications, vol. 1, IEEE Computer Society Press, Los Alamitos, 1997.
[4] Z. Cinkir, H. Akin, I. Siap, Reversibility of 1d cellular automat with periodic boundary over finite fields $\mathbb{Z}_p$, J. Stat. Phys. 143 (2011) 807–823.
[5] I.B. Collings, I. Vaughan, L. Clarkson, A low-complexity lattice-based low-PAR transmission scheme for DSL channels, IEEE Trans. Commun. 52 (2004) 755–764.
[6] A. Fúster-Sabater, P. Caballero-Gil, On the use of cellular automata in symmetric cryptography, Acta Appl. Math. 93 (1) (2006) 215–236.
[7] A. Fúster-Sabater, P. Caballero-Gil, Chaotic modelling of the generalized self-shinking generator, Appl. Soft Comput. 11 (2) (2011) 1876–1880.

[8] L. Fuyong, The inverse of circulant matrix, Appl. Math. Comput. 217 (2011) 8495–8503. N21
[9] A. Gajardo, J. Kari, A. Moreira, On time-symmetry in cellular automata, J. Comput. Syst. Sci. 78 (2012) 1115–1126.
[10] G.A. Hedlund, Endomorphisms and automorphisms of the shift dynamical systems, Math. Syst. Theory 3 (1968) 320–375.
[11] L.H. Encinas, A.M. del Rey, Inverse rules of ECA with rule number 150, Appl. Math. Comput. 189 (2007) 1782–1786.
[12] J. Kari, Reversibility and surjectivity problems of cellular automata, J. Comput. Syst. Sci. 48 (1994) 149–182.
[13] J. Kari, Reversible cellular automata, in: C. de Felice, A. Restivo (Eds.), Proceedings of the DLT, Lecture Notes in Computer Science, vol. 3572, Springer, 2005, pp. 57–68.
[14] P.D. Lena, L. Margara, Nondeterministic cellular automata, Inf. Sci. 287 (2014) 13–25.
[15] X. Li, C. Li, I.K. Lee, Chaotic image encryption using pseudo-random masks ad pixel mapping, Signal Process 125 (2016) 48–63.
[16] A.M. del Rey, A note on the reversibility of the elementary cellular automaton with rule number 90, Rev. Union Mat. Argent. 56 (1) (2015) 107–125.
[17] A.M. del Rey, G.R. Sánchez, On the reversibility of 150 wolfram cellular automata, Int. J. Mod. Phys. C 17 (2006) 975–984.
[18] A.M. del Rey, G.R. Sánchez, On the invertible cellular automata 150 over $\mathbb{F}_p$, Appl. Math. Comput. 219 (10) (2013) 5427–5432.
[19] A.M. del Rey, G.R. Sánchez, Reversible cellular automaton with rule number 150 and periodic boundary conditions over $\mathbb{F}_p$, Int. J. Mod. Phys. C 26 (11) (2015) 1550120.
[20] K. Morita, Reversible computing and cellular automata—a survey, Theor. Comput. Sci. 396 (2008) 101–131.
[21] K. Morita, Reversible cellular automata, in: G. Rozenberg, et al. (Eds.), Handbook of Natural Computing, Springer-Verlag, Berlin Heidelberg, 2012, pp. 231–257.
[22] A.Y. Niyat, M.H. Moattar, M.N. Torshi, Color image encryption based on hybrid hyper-chaotic system and cellular automata, Opt. Lasers Eng. 90 (2017) 225–237.
[23] A. Nobe, F. Yura, On reversibility of cellular automata with periodic boundary conditions, J. Phys. A Math. Gen. 37 (2004) 5789–5804.
[24] D. Richardson, Tessellations with local transformations, J. Comput. Syst. Sci. 6 (1972) 373–388.
[25] J.C. Seck-Tuoh-Mora, G.J. Martínez, R. Alonso-Sanz, N. Hernández-Romero, Invertible behavior in elementary cellular automata with memory, Inf. Sci. 199 (2012) 125–132.
[26] J.C. Seck-Tuoh-Mora, J. Medina-Marín, N. Hernández-Romero, G.J. Martínez, I. Barragán-Vite, Welch sets for random generation and representation of reversible one-dimensional cellular automata, Inf. Sci. 382–383 (2017) 81–95.
[27] B. Sethi, N. Fatès, S. Das, Reversibility of elementary cellular automata under fully asynchronous update, in: T.V. Gopal, M. Agrawal, A. Li, S.B. Cooper (Eds.), Proceedings of the International Conference on Theory and Applications of Models of Computation, Lecture Notes in Computer Science, vol. 8402, Springer International Publishing, 2014, pp. 39–49.
[28] S.Q. Shen, J.M. Cen, Y. Hao, On the determinants and inverses of circulant matrices with fibonacci and Lucas numbers, App. Math. Comput. 217 (23) (2011) 9790–9797.
[29] I. Siap, H. Akin, M.E. Koroglu, The reversibility of $(2r+1)$-cyclic rule cellular automata, TWMS J. Pure Appl. Math. 4 (2013) 215–225.
[30] I. Siap, H. Akin, M.E. Koroglu, E. Mehmet, Reversible cellular automata with penta-cyclic rule and ECCs, Int. J. Mod. Phys. Comput. 23 (13) (2012) 1250066.
[31] M. Tomassini, M. Perrenoud, Cryptography with cellular automata, Appl. Soft Comput. 1 (2) (2001) 151–160.
[32] J. Wang, C. Dong, Inverse matrix of symmetric circulant matrix on skew field, Int. J. Algebra 1 (2007) 541–546.
[33] S. Wolfram, Cellular Automata and Complexity, Collected Papers, Westview Press, 1994.
[34] S. Wolfram, A New Kind of Science, Wolfram Media Inc., 2002.
[35] Y. Yazlik, N. Taskara, On the inverse of circulant matrix via generalized k-Horadam numbers, App. Math. Comput. 223 (2013) 191–196.