

Computing the transition dipolynomials of certain reversible cellular automata

A. Martín del Rey
Department of Applied Mathematics,
E.P.S., University of Salamanca
C/ Santo Tomás s/n, 05003-Ávila, Spain
E-mail: delrey@usal.es

Abstract

It is a well-known fact that the reversibility problem for elementary cellular automaton with Wolfram rule number 150 and null boundary conditions, depends on the number of cells of its cellular space, n ([1]). In fact, it is reversible when $n \equiv 0 \pmod{3}$ or $n \equiv 1 \pmod{3}$. Nevertheless, no explicit expression for the inverse cellular automaton is known.

In this work, the reversibility problem for 150-Wolfram cellular automaton with periodic boundary conditions is tackled. It is proved that the reversibility depends on the number of cells, n . Moreover, the explicit expressions of the inverse cellular automaton in terms of its transition dipolynomial are calculated.

Computational experiments using MATLAB and MATHEMATICA allows one to state the following conjecture: *The 150-Wolfram cellular automata with periodic boundary conditions and n cells is reversible if and only if $n \not\equiv 0 \pmod{3}$.* In these cases, one can compute the inverse cellular automata by simply inverting certain n th-order tridiagonal matrix, which yields the evolution of the cellular automata. Any computer algebra system (such as MATLAB and MATHEMATICA) can be used to compute them, but the calculus turn infeasible when n is too high. In this way, an efficient computational algorithm is needed in order to obtain the inverse cellular automata. It is led from Theorem 3.

One-dimensional cellular automata (CA) are discrete dynamical systems formed by a finite set of identical objects called cells, arranged linearly in one dimension. Each cell can assume a state in \mathbb{F}_2 . It evolves deterministically in discrete time steps, changing the states of all cells according to the previous states of a set of cells (its neighborhood) and a local transition function. As the number of cells of the CA is finite, boundary conditions must be considered in order to ensure a well-defined dynamics. If we suppose $a_i^{(t)} = 0$ for $i < 0$ and $i > n - 1$, then the CA is endowed with *null boundary conditions*, on the other

hand, if $a_i^{(t)} = a_j^{(t)}$ when $i \equiv j \pmod{n}$, then the CA is said to be endowed with *periodic boundary conditions*.

The global function of a CA is a linear transformation, $\Phi: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$, that yields the configuration at the next time step during the evolution of the CA. Its dynamical properties are essentially related to the properties of such global function, such as surjectivity, injectivity, and bijectivity. Another important property is the reversibility. In this sense, if Φ is bijective, there exists another CA, called its *inverse*, with global function Φ^{-1} . When such inverse cellular automaton exists, then the CA is called *reversible* and the evolution backward is possible.

An important type of CAs are *elementary CA (ECA)*, whose local function is a three variable boolean function of the form

$$a_i^{(t+1)} = f\left(a_{i-1}^{(t)}, a_i^{(t)}, a_{i+1}^{(t)}\right), \quad 0 \leq i \leq n-1,$$

where $a_i^{(t)}$ stands for the state of the i -th cell at time t . The vector $C^{(t)} = \left(a_0^{(t)}, \dots, a_{n-1}^{(t)}\right) \in \mathbb{F}_2^n$ is called the *configuration at time t* .

There are eight possible configurations for ECA's neighborhood, hence there exists 256 local functions, every one of which is conveniently specified by a decimal integer called Wolfram rule number ([2]): $w = \sum_{i=0}^7 f_i \cdot 2^i$, where $f_0 = f(0, 0, 0)$, $f_1 = f(0, 0, 1)$, $f_2 = f(0, 1, 0)$, $f_3 = f(0, 1, 1)$, $f_4 = f(1, 0, 0)$, $f_5 = f(1, 0, 1)$, $f_6 = f(1, 1, 0)$, $f_7 = f(1, 1, 1)$.

The ECA with $w = 150$ —ECA(150)— is particularly interesting due to its algebraic properties (see [1]). Its local transition function is a boolean linear function of the form:

$$a_i^{(t+1)} = a_{i-1}^{(t)} + a_i^{(t)} + a_{i+1}^{(t)} \pmod{2}, \quad 0 \leq i \leq n-1.$$

If periodic boundary conditions are considered, its evolution is given by the following matrix expression: $C^{(t+1),T} = M_n \cdot C^{(t),T}$ where $C^{(t),T}$ stands for the transpose of $C^{(t)}$, and the (i, j) -coefficient of the transition matrix, M_n , is given by

$$m_{ij} = \begin{cases} 1, & \text{if } (i, j) \in \{(1, n), (n, 1)\} \text{ or } |i - j| < 2 \\ 0, & \text{otherwise} \end{cases}$$

Furthermore, we can model the evolution of such ECA in terms of polynomials. In this way, the configuration of an ECA (150) with n cells at time t , $C^{(t)}$, can be represented by the *characteristic polynomial at time t* :

$$P^{(t)}(x) = \sum_{i=0}^{n-1} a_i^{(t)} x^i.$$

Periodic boundary conditions are implemented by reducing $P^{(t)}(x)$ modulo the fixed polynomial $x^n - 1$ at every step. Moreover, time evolution can be represented by multiplication of the characteristic polynomial by a fixed dipolynomial, $T(x) = x^{-1} + 1 + x$, called the *transition dipolynomial*. Thus,

$$Ch^{(t+1)}(x) = T(x) \cdot Ch^{(t)}(x) \pmod{x^n - 1},$$

where the arithmetic is performed in \mathbb{F}_2 .

The notion of reversibility for ECA(150) leads to the study of its transition matrix. In this way, if the transition matrix is non-singular, then the CA is reversible. Also, the reversibility property can be expressed in terms of dipolynomials:

Proposition 1 *The n -cell ECA (150) is reversible if and only if there exists another CA with transition dipolynomial $\tilde{T}(x)$, such that $T(x) \cdot \tilde{T}(x) = 1 \pmod{(x^n - 1)}$.*

As a consequence, in our case, the following results are obtained:

Theorem 2 *The n -cell ECA(150) with $n \geq 3$ and periodic boundary conditions is reversible if and only if $n \not\equiv 0 \pmod{3}$.*

Theorem 3 *The transition dipolynomial of the inverse CA of the n -cell ECA(150) with $n \not\equiv 0 \pmod{3}$, is $R(x) = \sum_{j \in I} x^j$, where I is the following set of indices:*

1. For $n \equiv 1 \pmod{3}$, with $n = 3k + 1$, $k \in \mathbb{Z}^+$, then

$$I = \left\{ 0, \pm \left\lfloor \frac{3}{2} \right\rfloor, \pm \left\lfloor \frac{6}{2} \right\rfloor, \dots, \pm \left\lfloor \frac{3(k-1)}{2} \right\rfloor, \pm \left\lfloor \frac{3k}{2} \right\rfloor \right\}.$$

2. For $n \equiv 2 \pmod{3}$, with $n = 3k + 2$, $k \in \mathbb{Z}^+$, then

$$I = \left\{ 0, \pm \left\lfloor \frac{4}{2} \right\rfloor, \pm \left\lfloor \frac{7}{2} \right\rfloor, \dots, \pm \left\lfloor \frac{3(k-1)+1}{2} \right\rfloor, \pm \left\lfloor \frac{3k+1}{2} \right\rfloor \right\}.$$

References

- [1] P. Chaudhuri, D. Chowdhury, S. Nandi and S. Chattopadhyay, *Additive cellular automata. Theory and Applications. Volume 1*. IEEE Computer Society Press, Los Alamitos, 1997.
- [2] O. Martin, A. M. Odlyzko and S. Wolfram, Algebraic properties of cellular automata, *Comm. Math. Phys.* **93** (1984) 219–258.