On irreversibility of von Neumann additive cellular automata on grids

N.Y. Soma*, J.P. Melo

Instituto Tecnológico de Aeronáutica, CTA/ITA/IEC, São José dos Campos, Brazil

Received 9 December 2002; received in revised form 19 September 2003; accepted 31 May 2005
Available online 2 December 2005

Abstract

The von Neumann cellular automaton appears in many different settings in Operations Research varying from applications in Formal Languages to Biology. One of the major questions related to it is to find a general condition for irreversibility of a class of two-dimensional cellular automata on square grids (\(\sigma^+\)-automata). This question is partially answered here with the proposal of a sufficient condition for the irreversibility of \(\sigma^+\)-automata.

© 2005 Elsevier B.V. All rights reserved.

Keywords: Cellular automata; Chebyshev polynomials over GF(2); Von Neumann automata

1. Introduction

A two-dimensional cellular automaton (CA) is defined as an array of \(n \times n\) of cells over GF(2). Time is introduced as a synchronous and discrete evolution of those cells. The neighbourhood of a cell \(c\) is a pre-defined set of cells which influences the state of \(c\) in the next instant of time. The von Neumann two-dimensional CA, from now on referred as \(\sigma^+(2)\) is

\[
c_{i,j}^{t+1} = c_{i-1,j}^t + c_{i,j-1}^t + c_{i,j}^t + c_{i+1,j}^t + c_{i,j+1}^t \pmod{2},
\]

where \(c_{i,j}^t\) is the state of cell \(i, j\) at time \(t\) and \(i, j \in \{1, \ldots, n\}\), \(c_{i,j}^t = 0\) or \(1\). The states of the cells \(c_{0,i}, c_{i,0}, c_{i,n+1}\) and \(c_{i,n+1}\) are always 0 for any non-negative integer \(t\). Any configuration of a CA can be represented by a system of linear equations over GF(2) of the form \(Bx^t = x^{t+1}\), where \(x^t\) and \(x^{t+1}\) are elements amidst a finite set with \(2^n\) different configurations, related to instants \(t\) and \(t + 1\); and \(B\) is the adjacency matrix associated to the \(n \times n\) grid graph.

Some authors consider the \(\sigma^+\) as the hardest one to find inverse configurations amidst CAs with maximum neighbourhood distance 1, cf. [2] and stronger results to support this hypothesis were given recently in [10] and [14], where the roots of such a difficulty were tracked down, i.e. the reversibility of \(\sigma^+(2)\) is related to irreducible polynomials, more specifically, with Chebyshev polynomials of second kind over finite fields. These results were established by
It is worth of mentioning that given a configuration of $\sigma^+(2)$ (values of the cells $c_{i,j}^{t+1}$'s) its previous configuration ($c_{i,j}^t$) can be determined by the inverse $n^2 \times n^2$ adjacency matrix ($B^{-1}$) over GF(2), if such an inverse matrix exists. The main idea of this work is to avoid the whole computation of such large matrices.

It is presented here a new and more general condition for the irreversibility cases of $\sigma^+(2)$ (Theorem 2), answering, in part, a question concerning reversibility of $\sigma^+(2)$ on squares, cf. [10].

Additionally, elementary proofs (arithmetic) of some results from [2,5,9] are also given, e.g. the Chebyshev polynomials generates the Sierpiński Gasket.

2. Canonical enumeration of polynomials

To derive the relation between the two-dimensional von Neumann cellular automata ($\sigma^+(2)$-automata) and the Chebyshev polynomials, the line of attack chosen is different from those presented in [2] and [14], i.e., it is chosen here to consider the matrices ($B$) associated to $\sigma^+(1)$ (uni-dimensional) and $\sigma^+(2)$ to derive Sarkar and Barua’s [10] canonical enumeration ($\pi_n$) via a new recurrent procedure. Notice that the uni-dimensional ($n \times 1, n \geq 3$) von Neumann cellular automata ($\sigma^+(1)$), still over GF(2), is

\[
\begin{align*}
\sigma_0^{t+1} = &\; \sigma_0^t - \sigma_1^t + \sigma_2^t + \sigma_3^t, \\
\sigma_0^0 = &\; \sigma_{n+1}^0 = 0 \quad \text{at any time } t.
\end{align*}
\]

Moreover, the adjacency matrices for the uni ($\left( B_n^1 \right)_{n \times n}$) and two-dimensional ($\left( B_n^2 \right)_{n^2 \times n^2}$) cases are given respectively by

\[
B_n^1 = \begin{pmatrix}
1 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\
1 & 1 & 1 & 0 & \cdots & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & \cdots & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & 0 & \cdots & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & \cdots & 1 & 1 & 1 \\
0 & 0 & 0 & 0 & \cdots & 0 & 1 & 1 
\end{pmatrix}; \\
B_n^2 = \begin{pmatrix}
B_n^1 & I_n & O_n & \cdots & O_n & O_n & O_n \\
I_n & B_n^1 & I_n & \cdots & O_n & O_n & O_n \\
O_n & I_n & B_n^1 & \cdots & O_n & O_n & O_n \\
O_n & O_n & I_n & \cdots & O_n & O_n & O_n \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
O_n & O_n & O_n & \cdots & I_n & O_n & O_n \\
O_n & O_n & O_n & \cdots & B_n^1 & I_n & O_n \\
O_n & O_n & O_n & \cdots & I_n & B_n^1 & O_n \\
O_n & O_n & O_n & \cdots & I_n & B_n^1 & O_n
\end{pmatrix},
\]

where $B_n^2$ is given as a block matrix, $I_n$ and $O_n$ are, respectively, the identity and zero $n \times n$ matrices. A derivation of the $B_n^2$ is given in [10] via Kronecker product.

The reversibility of those automata can be detected by examining the rank of the above matrices, or what is the same, their determinants. For the one-dimensional case ($n \times 1$), it is well known that $\sigma^+(1)$ has not inverse configurations iff $n \equiv 2 \pmod{3}$, cf. [8].

The determinant of $B_n^2$ with $n^2 \times n^2$ elements can be reduced to an $n \times n$ by the following recurrent procedure:

**Step 1:** (Block permutation).

Multiply $B_n^2$ (to the left) by the matrix $\tilde{P}_n^2$, given by

\[
\tilde{P}_n^2 = \begin{pmatrix}
O_n & I_n & O_n & O_n & \cdots & O_n & O_n & O_n \\
O_n & O_n & I_n & O_n & \cdots & O_n & O_n & O_n \\
O_n & O_n & O_n & I_n & \cdots & O_n & O_n & O_n \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
O_n & O_n & O_n & O_n & \cdots & I_n & O_n & O_n \\
O_n & O_n & O_n & O_n & \cdots & I_n & O_n & O_n \\
I_n & O_n & O_n & O_n & \cdots & I_n & O_n & O_n
\end{pmatrix},
\]
Step 2: [Determinant of transformed $\bar{P}_n^{[2]} \cdot B_n^{[2]}$].

Find recursively Schur’s complements of matrix $P_n^{[2]}[1] = \bar{P}_n^{[2]}[1] \cdot B_n^{[2]}$, starting from the first identity $I_n$, $n \times n$ block, i.e.:

$$P_n^{[2]}[1] = \begin{pmatrix}
I_n & B_n^{[1]} & O_n & \cdots & O_n & O_n \\
O_n & I_n & B_n^{[1]} & \cdots & O_n & O_n \\
O_n & O_n & I_n & B_n^{[1]} & \cdots & O_n \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
O_n & O_n & O_n & \cdots & I_n & B_n^{[1]} \\
B_n^{[1]} & I_n & O_n & \cdots & O_n & O_n
\end{pmatrix}.$$

and the determinant of $P_n^{[2]}[1]$ can be expressed as

$$\det(P_n^{[2]}[1]) = \det(M_{(n^2-n),(n^2-n)} + L(1)R(1)).$$

Notice that $M_{(n^2-n),(n^2-n)} + L(1)R(1)$ is also expressed in terms of Schur’s complement (in GF(2)), so $P_n^{[2]}[j]$ can be defined recursively as

$$P_n^{[2]}[j] = M_{(n^2-(j-1)n),(n^2-(j-1)n)} + L(j)R(j), \quad j = 1, \ldots, n$$

and clearly, $\det(B_n^{[2]}) = \det(P_n^{[2]}[1]) = \cdots = \det(P_n^{[2]}[n])$. These polynomials matrices, formed from the recurrent procedure, do not possess the same order, i.e. there is a decrease of $n$ in the order of the matrices for an increase of a degree in the polynomial. The correctness of the procedure is immediate and will not be shown.

The last iteration of the recurrent procedure, i.e. the $n$th gives a polynomial matrix of the form $P_n^{[2]}[n] = \sum_{j=0}^{n} a_j (B_n^{[1]})^j$, $a_i = 0$ or 1, $n \in N$. Moreover, Sarkar and Barua’s $\pi$’s polynomials can be derived directly from the relation between the matrix polynomials $P_n^{[2]}$ for each value of $n \in N$ and the given recurrent relation, but before, and for the sake of clarity, let it be assumed that $\pi_n = P_n^{[2]}[n]$, $x = B_n$, $0 = O_n$ and $1 = I_n$.

The Fibonacci (or Sarkar and Barua’s) $\pi_n$’s polynomials are given by

$$\pi_0 = 1; \quad \pi_1 = x; \quad \pi_j = x\pi_{j-1} + \pi_{j-2}, \quad 2 \leq j \leq n. \quad (1)$$

The proof that Steps 1 and 2, in GF(2) verifies the $\pi$’s polynomials (or $P_n^{[2]}[n]$) is trivially proved by induction wherefore it is not carried out here.

It is worth mentioning that the $\pi_n$’s polynomials derived here differ from [14] (the polynomials there begin with $\pi_0 = 0$) and they are equal to [2] and [12]. The reason to adopt the current numbering comes from the fact that the line of
attack adopted here is different from that presented in those works i.e. there, the properties of division of polynomials over finite fields are explored.

Here, Steps 1 and 2 are carried out in $\mathcal{R}$ instead of GF(2) and the $n$’s polynomials, from now on are referred as $P$’s to indicate the change of field. Moreover, these matrix polynomials recurrence in $\mathcal{R}$ can be readily shown to be

$$\Pi_0(x) = 1; \quad \Pi_1(x) = x; \quad \Pi_n(x) = x\Pi_{n-1} - \Pi_{n-2}(x), \quad 2 \leq j \leq n. \quad (2)$$

3. Chebyshev and the $P$ polynomials

It is shown now a different proof from that presented in [14] relating the Chebyshev second order polynomials (cf. e.g. [16]) with the $P(n)$ polynomials. Notice that here $x$ is treated as a real number instead of the $P_n^{[2]}$ matrix in GF(2).

**Theorem 1.** The $P(n)$ polynomials can be expressed as Chebyshev second order polynomials.

**Proof.** The recurrent definition of $P_n(x)$ can be rewritten as

$$P_n(x) = \sum_{p=0}^{q} (-1)^p \left( \frac{n-p}{p} \right) x^{n-2p}, \quad \text{where} \quad q = \left\lceil \frac{n}{2} \right\rceil. \quad (3)$$

This relation is easy to be verified by induction, since for $n = 1$, $P_0(x) = 1$ and for $n := n + 1$ and (2) it follows that

$$P_{n+1}(x) = x \sum_{p=0}^{\lfloor n/2 \rfloor} (-1)^p \left( \frac{n-1}{p} \right) x^{n-2p} - \sum_{p=0}^{\lfloor (n-1)/2 \rfloor} (-1)^p \left( \frac{n-2}{p} \right) x^{n-2p-1}$$

$$= x^{n+1} - \left( \frac{n}{1} \right) x^{n-1} + \left( \frac{n-1}{2} \right) x^{n-3} - \left( \frac{n-2}{3} \right) x^{n-5} + \ldots$$

$$= \sum_{p=0}^{q} (-1)^p \left( \frac{n-p+1}{p} \right) x^{n-2p}, \quad \text{where} \quad q = \lfloor (n + 1)/2 \rfloor.$$

By doing the following change of variables $x := 2 \cos \phi$ along with the well known identity, (cf. [3]),

$$\frac{\sin(m+1)\phi}{\sin \phi} = 2 \cos \phi \frac{\sin m\phi}{\sin \phi} - \frac{\sin(m-1)\phi}{\sin \phi}, \quad m \in N, \quad \phi \neq h\pi, \quad h \in Z, \quad (4)$$

it is immediate to conclude that

$$P_n(\cos \phi) = \frac{\sin(n+1)\phi}{\sin \phi},$$

which are the second order Chebyshev polynomials. \hfill $\square$

The next result gives a new irreversibility condition for the two-dimensional von Neumann CA.

**Theorem 2.** If the relation

$$\cos \left( \frac{(k_1 + k_2)\pi}{2(n+1)} \right) \cos \left( \frac{(k_1 - k_2)\pi}{2(n+1)} \right) = \frac{1}{4}, \quad 1 \leq k_1, \quad k_2 \leq n, \quad k_1 \neq k_2, \quad (5)$$

is satisfied by some integers $k_1$ and $k_2$, then the $\sigma^+(2)$ is irreversible in GF(2).

**Proof.** The determinants of matrices $B_n^{[2]}$ (with $n^2 \times n^2$ elements) and the associated polynomial $P_n(B_n^{[1]})$ (with $n \times n$ elements) as given in (3) have the same value. Additionally, the eigenvalues of $B_n^{[1]}$ can be easily shown to be of the form $\lambda_k = 1 - 2 \cos k\pi/(n+1)$, $k = 1, \ldots, n$ and also it is well known that the determinant of a polynomial matrix can
be given by the product of the same polynomial evaluated at the eigenvalues associated to that given matrix, cf. [6]. It is easy to see that the given condition is equivalent to \( \lambda_{k_1} + \lambda_{k_2} = 1 \). Since

\[
\pi(\lambda_{k_2}) = \pi(1 - \lambda_{k_1}) = \pi(2 \cos k_1 \pi/(n + 1)) = \frac{\sin k_1 \pi}{\sin k_1 \pi/(n + 1)} = 0,
\]

the result follows. \( \square \)

For example, \( \sigma^+(2) \) and \( n = 4 \) is irreversible (cf. Proposition 3.1 of [9]), since for \( k_1 = 3 \) and \( k_2 = 1 \) in (5) implies:

\[
\cos \frac{4 \cdot \pi}{2 \cdot 5} \cos \frac{2 \cdot \pi}{2 \cdot 5} = \frac{1}{16} (-1 + \sqrt{5}) \cdot (1 + \sqrt{5}) = \frac{1}{4}.
\]

Also, to inspect the result, notice that in GF(2) the determinant of \( B_4^{[2]} \) has the same value of \( (B_4^{[1]})^4 + (B_4^{[1]})^2 + I_4 \), by the recurrent procedure (Steps 1 and 2), but \( (B_4^{[1]})^4 + (B_4^{[1]})^2 + I_4 = O_n \), hence \( \det B_4^{[2]} = 0 \).

Condition (5) is sufficient, but not necessary, since in \( \Re \), \( \det B_n^{[2]} \) can be an even positive integer; e.g. \( \det B_{16}^{[2]} \) is a non-zero even number and there are no \( k_1 \) and \( k_2 \) satisfying (5).

The following results are known from the literature, cf. e.g. [5] and [12], but the proofs given here are essentially arithmetical ones. Before stating the results consider the two identities (cf. [3]):

\[
x^{2m} - 1 = (x^2 - 1) \prod_{k=1}^{m-1} \left( x^2 - 2x \cos \frac{k \pi}{m} + 1 \right),
\]

\[
x^{2m+1} - 1 = (x - 1) \prod_{k=1}^{m} \left( x^2 - 2x \cos \frac{2k \pi}{2m+1} + 1 \right).
\]

**Proposition 3.** For every nonzero rational \( r \) it holds that \( \cos(r \pi) \neq \frac{1}{4} \).

**Proof.** For every positive integer \( n \geq 1 \) the polynomial \( x^{2n} - 1 \) is not divisible by \( x^2 - x/2 + 1 \) since the roots of this latter polynomial do not satisfy the two previous identities on \( x^{2m} - 1 \) and \( x^{2m+1} - 1 \), a fortiori, \( r \) cannot be rational. \( \square \)

**Proposition 4.** The coefficients of \( \Pi_n(x) \) in GF(2) generate the Sierpiński gasket.

**Proof.** A famous result of Lucas (cf. [5] and [7]) shows that the well known Sierpiński gasket [11] can be generated by taking \( \left( \binom{n}{p} \right) \mod 2 \), for \( n \geq p \geq 0 \), \( n \) and \( p \) integer numbers. To show that the coefficients of \( \Pi_n(x) \) in GF(2) gives the same result it is necessary to show that

\[
\left( \binom{n}{p} \right) \equiv \left( p - n - 1 + 2^{m+1} \right) \mod 2
\]

and by using the binomial identity, cf. [4],

\[
\left( \binom{n}{p} \right) \equiv \left( p - n - 1 \right) \mod 2,
\]

it is immediate to conclude that

\[
\left( p - n - 1 + 2^{m} \right) \equiv \left( p - n - 1 \right) \mod 2 \iff \left( p - n - 1 + 2^{m} \right) \equiv \left( \binom{n}{p} \right) \mod 2,
\]

by the Lucas theorem and the fact that \( 2^m > n + 1 - p \). \( \square \)
Acknowledgements

The authors express gratitude to Profs. Celso de Renna e Souza, Antônio Marmo de Oliveira, Horacio Hideki Yanasse, Yoshiko Wakabayashi and Salah-Eddine Rebiai for useful discussions.

References