*Publicaciones en Ciencias y Tecnología.* Vol 4, 2010 N$^0$ 1, pp.17–23, ISSN:1856-8890,Dep.Legal pp200702LA2730

# Surjective multiband linear cellular automata and Smith's normal form

[*]Ignacia Arcaya [†]Neptalí Romero

Recibido: 21 de Marzo 2009, Aceptado:10 de Julio 2009

**Abstract**

In this paper the Smith normal form of certain matrices is used to provide another characterization for the surjectivity of one-dimensional linear cellular automata with multiple local rules over the ring $\mathbb{Z}_N$ of integers modulo $N \geq 2$. We reached this goal through an adaptation of a well known result of G. A. Hedlund which characterize the surjectivity of general one-dimensional cellular automata.

**Keywords**: Smith normal form multiband cellular automata.

**Autómatas celulares sobreyectivos multibanda y la forma normal de Smith**
**Resumen**

En este artículo es empleada la forma normal de Smith de ciertas matrices para ofrecer otra caracterización de la sobreyectividad de autómatas celulares lineales unidimensionales con múltiples reglas local sobre el anillo $\mathbb{Z}_N$ de los enteros módulo $N \geq 2$. El objetivo es logrado mediante la adaptación de un conocido resultado de G. A. Hedlund que caracteriza la sobreyectividad de autómatas celulares unidimensionales en general.

**Palabras clave**: Forma normal de Smith, autómatas celulares multibandas.

## Introduction

Cellular Automata are dynamical systems which are the simplest idealization of space-time physical and biological systems, also are considered in computer sciences to study several aspects related to parallel computer devices, image processing, cryptography and analysis of universal model of computations.

The notion of cellular automaton was introduced by John von Newmann and Stanislaw Ulam in the 1940's at Los Alamos National Laboratory. The configuration space where these dynamical systems act consists of a discrete lattice $\mathcal{L}$ such that each cell of $\mathcal{L}$ holds a state taking on a value from a finite set $\mathcal{A}$ called alphabet; thus a configuration is an element of the product space $\mathcal{A}^{\mathcal{L}} = \{x : \mathcal{L} \to \mathcal{A}\}$. Usually the lattice $\mathcal{L}$ is the set of $d$-dimensional integers $\mathbb{Z}^d$ ($d \geq 1$); but finitely generated Abelian groups have been considered. The temporary evolution of a cellular automaton $F$ is given by its action on $\mathcal{A}^{\mathcal{L}}$, updating synchronously the states of the cells according to a *local rule* (the same for each cell and configuration), which takes into account the states of a finite neighborhood of each cell on the previous time step, this neighborhood is the shift, to the corresponding cell, of a fixed nonempty and finite subset of $\mathcal{L}$. More precisely, for any finite and nonempty subset $U$ of $\mathcal{L}$, a local rule is any function $\phi : \mathcal{A}^U \to \mathcal{A}$, where $\mathcal{A}^U$ denotes the set of all function from $U$ to $\mathcal{A}$. So, the cellular automaton induced by $U$ and $\phi$ is the operator $F : \mathcal{A}^{\mathcal{L}} \to \mathcal{A}^{\mathcal{L}}$ defined, for each $x \in \mathcal{A}^{\mathcal{L}}$ and $\ell \in \mathcal{L}$, by

$$F(x)(\ell) = \phi\left(x|_{U+\ell}\right), \tag{1}$$

[*] *Departamento de Matemática, Universidad Central de Venezuela , Ciudad Universitaria, Caracas, Venezuela*
[†] *Departamento de Matemática Universidad Centroccidental Lisandro Alvarado, Barquisimeto, Lara, Apdo 3001, Venezuela, nromero@ucla.edu.ve*

where $U+\ell=\{u+\ell : u\in U\}$ and $x|_{U+\ell} : U\to\mathcal{A}$ is given by $x|_{U+\ell}(u)=x(u+\ell)$, for every $u\in U$.

Classical examples of cellular automata are given by the shifts: for a fixed $\ell\in\mathcal{L}$, let $\sigma_\ell$ be the selfmapping of $\mathcal{A}^{\mathcal{L}}$ given, for every $x\in\mathcal{A}^{\mathcal{L}}$ and $u\in\mathcal{L}$, by $\sigma_\ell(x)(u)=x(u+\ell)$. Clearly each $\sigma_\ell$ is a cellular automaton; the neighborhood in this case is $U=\{\ell\}$ and the local rule $\phi$ is the identity map of $\mathcal{A}$, notice that $\mathcal{A}^{\{\ell\}}$ is identified with the alphabet $\mathcal{A}$. Observe that $\sigma_{\mathcal{L}}=\{\sigma_\ell : \ell\in\mathcal{L}\}$ is an Abelian group under composition of maps, and the cellular automaton (1) can be written as

$$F(x)(\ell)=\phi\left(\sigma_\ell(x)|_U\right), \tag{2}$$

where $\sigma_\ell(x)|_U$ denotes the restriction of $\sigma_\ell(x)$ to $U$.

G. A. Hedlund in [7] developed, in the context of symbolic dynamics, the theoretical formalism for cellular automata on $\mathcal{A}^{\mathbb{Z}}$, $\mathcal{A}$ any finite alphabet, as homeomorphisms of the shift dynamical system. In that seminal Hedlund's paper the product topology is considered on $\mathcal{A}^{\mathbb{Z}}$ to prove:

**Theorem 0.1 (Hedlund)** *[7] A continuous transformation $F:\mathcal{A}^{\mathbb{Z}}\to\mathcal{A}^{\mathbb{Z}}$ is a cellular automaton if, and only if, it commutes with the shift map $\sigma:\mathcal{A}^{\mathbb{Z}}\to\mathcal{A}^{\mathbb{Z}}$ given by $\sigma(x)(n)=x(n+1)$, for all $x\in\mathcal{A}^{\mathbb{Z}}$ and all $n\in\mathbb{Z}$.*

The proof of this theorem in [7] contains the following fact: $F:\mathcal{A}^{\mathbb{Z}}\to\mathcal{A}^{\mathbb{Z}}$ is a cellular automaton if, and only if, there are an integer $r\geq 0$ (*radius* of $F$) and a function $\phi:\mathcal{A}^{2r+1}\to\mathcal{A}$, such that for all $x\in\mathcal{A}^{\mathbb{Z}}$ and $n\in\mathbb{Z}$:

$$F(x)(n)=\phi(x(n-r)\cdots x(n+r)). \tag{3}$$

In this notation the cartesian product $\mathcal{A}^{2r+1}$, of all ordered $(2r+1)$-blocks $a_{-r}\cdots a_r$ over $\mathcal{A}$, is identified with $\mathcal{A}^{[-r,r]}=\{\varphi:[-r,r]\to\mathcal{A}\}$, where $[-r,r]$ denotes the interval over $\mathbb{Z}$ between $-r$ and $r$.

Motivated by theorem 0.1 several extensions of the concept of cellular automata have been established. One of them preserves the finite alphabet $\mathcal{A}$ and the lattice $\mathbb{Z}$; but configurations states are updated by means of a finite number of local rules. Actually, E. Lange et al. [9], see also [1] and [8], introduced the following concept.

**Definition 0.1** *Given an integer $m\geq 2$ and a finite alphabet $\mathcal{A}$. A continuous transformation $F:\mathcal{A}^{\mathbb{Z}}\to\mathcal{A}^{\mathbb{Z}}$ is called* $m$-cellular automaton *(also* place-dependent cellular automaton *or* multiband cellular automaton*) if it commutes with $\sigma^m$, where $\sigma^m$ is the m-th iteration of the shift map $\sigma$.*

It can be showed that $F:\mathcal{A}^{\mathbb{Z}}\to\mathcal{A}^{\mathbb{Z}}$ is a $m$-cellular automaton if, and only if, $F$ is a continuous transformation and there are an integer $r\geq$ and $m$ local rules $\phi_j:\mathcal{A}^{2r+1}\to\mathcal{A}$ $(0\leq j<m)$ such that, for every $x\in\mathcal{A}^{\mathbb{Z}}$ and $n\in\mathbb{Z}$:

$$F(x)(n)=\phi_{n_m}(x|_{[n-r,n+r]}), \tag{4}$$

where $x|_{[n-r,n+r]}$ is the ordered $(2r+1)$-block appearing in $x$ between the cells $n-r$ and $n+r$, and $n_m$ is the integer $n$ taken modulo $m$. Notice that the preceding statement is analogous to the Hedlund's characterization for cellular automata. It is not difficult to prove that any $m$-cellular automaton over $\mathcal{A}$ is topologically conjugated to a cellular automaton over $\mathcal{A}^m$; obviously this property does not detract the study of $m$-cellular automata over particular alphabets. Another kind of extensions are known. In [2] and [10] are proved analogous versions of theorem 0.1 where the alphabet is any infinite discrete topological space. On the other hand, Baas and Helvik [3] introduced the notion of higher order cellular automata, which constitutes a generalization of the classical concept of cellular automata in a more general setting; in this context there is no similar result to Hedlund's theorem characterizing these mathematical objects in terms of the shift dynamical systems.

In this paper we deal with $m$-cellular automata where the alphabet $\mathcal{A}$ is the ring $\mathbb{Z}_N$ (integers modulo $N\geq 2$) and the local rules are additives; that is, for every $0\leq j<m$ there exist constants $\lambda^j_{-r},\cdots,\lambda^j_r\in\mathbb{Z}_N$ such that the local rule $\phi_j:\mathbb{Z}_N^{2r+1}\to\mathbb{Z}_N$ is given by:

$$\phi_j(a_{-r}\cdots a_r)=\sum_{|i|\leq r}\lambda^j_i a_i \pmod{N}. \tag{5}$$

Clearly if one considers on $\mathbb{Z}_N^{\mathbb{Z}}$ the algebraic structure of $\mathbb{Z}_N$-module, it follows from (4) and (5) that the $m$-cellular automaton induced by these additive local rules is linear; this means: for all $x, y \in \mathbb{Z}_N^{\mathbb{Z}}$ and all $\lambda \in \mathbb{Z}_N$ it holds

$$F(x + \lambda y) = F(x) + \lambda F(y);$$

consequently $F$ is called a linear $m$-cellular automaton.

## Surjectivity and Smith's normal form

In his remarkable article Hedlund [7] proved several necessary and sufficient conditions for the surjectivity of cellular automata. For our purpose we make an adaptation of one of these equivalences. Assume that $F : \mathcal{A}^{\mathbb{Z}} \to \mathcal{A}^{\mathbb{Z}}$ is the $m$-cellular automaton of radius $r$ induced by the local rules $\phi_0, \cdots, \phi_{m-1}$. Whatever the integers $0 \le j < m$ and $s \ge 0$, the function $\phi_{j,s} : \mathcal{A}^{2r+s+1} \to \mathcal{A}^{s+1}$ is defined, for all $a_0 \cdots a_{2r+s} \in \mathcal{A}^{2r+s+1}$, as

$$\begin{aligned}&\phi_{j,s}(a_0 \cdots a_{2r+s}) = \\ &\qquad \phi_j(a_0 \cdots a_{2r})\phi_{(j+1)_m}(a_1 \cdots a_{2r+1}) \cdots \phi_{(j+s)_m}(a_s \cdots a_{2r+s}),\end{aligned} \tag{6}$$

where $(j+1)_m, \cdots, (j+s)_m$ are, respectively, the integers $j+1, \cdots, j+m$ module $N$. The proof of the next theorem is a slight modification of the Hedlund's proof of theorem 5.1 in [7]; despite its simplicity we include it.

**Theorem 0.2** *The $m$-cellular automaton $F$ is surjective if, and only if, for all intergers $0 \le j < m$ and $s \ge 0$ the function $\phi_{j,s}$ is also surjective.*

**Proof 0.1** *Take $0 \le j < m$, $s \ge 0$, $w = w_0 \cdots w_s \in \mathcal{A}^{s+1}$ and $z \in \mathcal{A}^{\mathbb{Z}}$ such that $z|_{[j,j+s]} = w$: $z(j+\ell) = w_\ell$ for all $0 \le \ell \le s$. Assume $F$ surjective. Let $x$ be a preimage of $z$ under $F$; consequently, for all $0 \le j < m$ and $0 \le \ell \le s$:*

$$F(x)(j+\ell) = \phi_{(j+\ell)_m}(x(j+\ell-r) \cdots x(j+\ell+r)) = w_\ell;$$

*thus, $b = x(j-r) \cdots x(j+\ell+r)$ satisfies $\phi_{j,s}(b) = w$ and $\phi_{j,s}$ is surjective.*

*On the other hand, assume that for all $0 \le j < m$ and $s \ge 0$ the function $\phi_{j,s}$ is surjective. Take $z \in \mathcal{A}^{\mathbb{Z}}$ and any integer $\ell \ge 1$; let $b^\ell = b_0^\ell \cdots b_{2(r+\ell)}^\ell$ in $\mathcal{A}^{2(r+\ell)+1}$ such that $\phi_{(-\ell)_m, 2\ell}(b^\ell) = z|_{[-\ell,\ell]} = z(-\ell) \cdots z(\ell)$. Taking, for example, $x^\ell \in \mathcal{A}^{\mathbb{Z}}$ in such a way that $x^\ell|_{[-\ell-r,\ell+r]} = b^\ell$ and $x(k) = 0$ for all $k \notin [-\ell-r, \ell+r]$, then $F(x^\ell)|_{[-\ell,\ell]} = z|_{[-\ell,\ell]}$. From this fact it follows that $F(\mathcal{A}^{\mathbb{Z}})$ is dense in $\mathcal{A}^{\mathbb{Z}}$. Finally the continuity of $F$ and the compactness of $\mathcal{A}^{\mathbb{Z}}$ implies $F(\mathcal{A}^{\mathbb{Z}}) = \mathcal{A}^{\mathbb{Z}}$.*

From now on we will consider linear $m$-cellular automata with local rules as in (5) to analyze the surjectivity problem for this kind of dynamical systems. After Hedlund's characterization for surjective cellular automata, several contributions to the surjective problem for cellular automata are known in different contexts. In the particular case of linear cellular automata, contributions of Itô et. al. [4] are pioneers. In this paper the authors make use of a Laurent polynomial representation of the local rule and Laurent formal series representation of the configuration space to study linear cellular automata over $\mathbb{Z}_m$. In fact, with these tools they showed, among other facts, the following result.

**Theorem 0.3 (Itô et al., [4])** *The linear cellular automaton of radius $r$ over $\mathbb{Z}_N$ whose local rule is given by the coefficients $\lambda_{-r}, \cdots, \lambda_r$ is surjective if, and only if, $gcd(\lambda_{-r}, \cdots, \lambda_r, N) = 1$.*

Kari in [8] slightly modifies both polynomial and series representations in [4] to provide a characterization of surjective linear $m$-cellular automata over any commutative ring with identity, see Section 3 in [8] for details. Instead these tools we will use Smith's normal form to obtain another characterization of linear $m$-cellular automata over $\mathbb{Z}_N$; actually, it works over any commutative ring with identity.

The criterion of Itô et al. is not a sufficient condition for the surjectivity of linear $m$-cellular automata. The following example shows this claim.

**Example 0.1** *Take $\mathcal{A} = \mathbb{Z}_4$ and consider local rules $\phi_0, \phi_1 : \mathcal{A}^3 \to \mathcal{A}$ given by*

$$\phi_0(a_{-1}, a_0, a_1) = 3a_1 \text{ (mod 4) and } \phi_1(a_{-1}, a_0, a_1) = 3a_0 \text{ (mod 4)}.$$

*Clearly $gcd(\lambda^i_{-1}, \lambda^i_0, \lambda^i_1, 4) = 1$ for $i = 0, 1$; however, the 2-cellular automaton $F$ induced by these rules is not surjective. Observe that for all $x \in \mathcal{A}^{\mathbb{Z}}$ and $n \in \mathbb{Z}$, $F(x)(n) = \begin{cases} 3x(n+1) \text{ (mod 4)}, & \text{if } n \text{ is even} \\ 3x(n) \text{ (mod 4)}, & \text{if } n \text{ is odd} \end{cases}$; thus, it is easy to verify that any configuration $y = (y(n))_{n\in\mathbb{Z}} \in \mathbb{Z}_4^{\mathbb{Z}}$ with $y(0) = 3$ and $y(1) = 1$ has no preimages.*

Let $F$ be a linear $m$-cellular automaton over $\mathbb{Z}_N$ with local rules $\phi_0, \cdots, \phi_{m-1}$ as in (5). It follows from theorem 0.2 and (6) that $F$ is surjective if, and only if, for all integers $0 \le j < m$ and $s \ge 0$ and every column vector $b \in \mathbb{Z}_N^{s+1}$, the system of linear equations modulo $N$

$$A_{j,s}x = b \text{ (mod } N), \tag{7}$$

has solutions in $\mathbb{Z}_N^{2r+s+1}$, where $A_{j,s}$ is the $(s+1) \times (2r+s+1)$ matrix

$$A_{j,s} = \begin{pmatrix} \lambda^j_{-r} & \lambda^j_{1-r} & \cdots & \lambda^j_r & 0 & 0 & \cdots & 0 \\ 0 & \lambda^{(j+1)_m}_{-r} & \cdots & \lambda^{(j+1)_m}_{r-1} & \lambda^{(j+1)_m}_r & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & \lambda^{(j+s)_m}_{-r} & \lambda^{(j+s)_m}_{1-r} & \cdots & \lambda^{(j+s)_m}_r \end{pmatrix}.$$

The main result of this paper is the following.

**Theorem 0.4** *The linear $m$-cellular automaton $F$ is surjective if, and only if, for all the Smith normal form of each matrix $A_{j,s}$ has full rank and its non-zero coefficients are coprimes to $N$.*

In order to prove this theorem we recall some facts dealing with Smith's normal form, which will all be found, for example, in [5], [6] and [11]. First of all some notations. For any pair of positive integers $p$ and $q$, $p \mid q$ indicates that $p$ is a divisor of $q$, $M_{p\times q}(\mathbb{Z})$ and $M_{p\times q}(\mathbb{Z}_N)$ denote the sets of all $p \times q$ matrices with coefficients in $\mathbb{Z}$ and $\mathbb{Z}_N$, respectively. Let $A$ be a matrix in $M_{p\times q}(\mathbb{Z})$ with $p \le q$. Given $1 \le k \le p$, $A(k)$ is the set of all $k \times k$ submatrices of $A$, $d_k(A)$ is the $k$th determinantal divisor of $A$, that is $d_k(A) = gcd\{det(B) : B \in A(k)\}$, where *gcd* means greatest common divisor and $det(B)$ denotes the determinant of $B$; if $k = rank(A)$, rank of $A$, then $d_k(A)$ is denoted by $d(A)$. It is well known that $d_{k-1}(A) \mid d_k(A)$ for all $2 \le k \le rank(A)$, and $rank(A) = \ell$ if, and only if, $d_k(A) \ne 0$ for each $1 \le k \le \ell$ and $det(B) = 0$ if $B \in A(k)$ and $k > \ell$. Use also use the column notation, that is, if $a_1, \cdots, a_q$ are the columns of $A$, and $b_1, \cdots, b_r$ are the columns of $B \in M_{p\times r}(\mathbb{Z})$, then $[A, B]$ is the matriz with columns $a_1, \cdots, a_q, b_1, \cdots, b_r$; finally, if $J \subset \{1, \cdots, p\}$, $A(J)$ is the matrix made up of the rows of $A$ indicated by $J$.

A matrix $U \in M_{p\times p}(\mathbb{Z})$ is called *unimodular* whenever $det(U) = \pm 1$, and $B \in M_{p\times q}(\mathbb{Z})$ is *equivalent* to $A \in M_{p\times q}(\mathbb{Z})$ if there exist unimodular matrices $L \in M_{p\times p}(\mathbb{Z})$ and $R \in M_{q\times q}(\mathbb{Z})$ such that $B = LAR$. Unimodularity induces a partition on $M_{p\times q}(\mathbb{Z})$ where determinantal divisors are invariants.

**Theorem 0.5 (Smith's normal form)** *Let $A$ be an $p \times q$ integer matrix. If $1 \le ran(A) = \ell \le p$, then there exist unimoldular matrices $L \in M_{p\times p}(\mathbb{Z})$ and $R \in M_{q\times q}(\mathbb{Z})$ such that*

$$S = LAR = \begin{pmatrix} a_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & a_\ell & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}, \tag{8}$$

*where $a_1 \geq 1$, $a_1 \mid a_2 \mid \cdots \mid a_\ell$, and $d_k(A) = \prod_{i=1}^{\ell} a_i$, for all $1 \leq k \leq \ell$. The matrix $S$ is called the* Smith normal form *of $A$.*

The next statement establishes a criterion for the existence of solutions with coefficients in $\mathbb{Z}$ for any system of linear equations over $\mathbb{Z}$.

**Theorem 0.6** *Given $A \in M_{p\times q}(\mathbb{Z})$ and $b \in \mathbb{Z}^p$, the equation $Ax = b$ has integers solutions if, and only if, the following conditions hold:*

*(i) $rank(A) = rank([A, b])$.*

*(ii) There exists $J \subset \{1, \cdots, p\}$ with cardinal equal to $rank(A)$ in such a way that $rank(A) = rank(A(J))$ and $d(A(J)) = d([A, b](J))$.*

Observe that the rank is invariant for equivalent matrices, and if $L$ and $R$ are unimodular matrices and $S = LAR$ is the Smith normal form of $A \in M_{p\times q}(\mathbb{Z})$, then $x_0 \in \mathbb{Z}^q$ is a solution of $Ax = b$ if, and only if, $y_0 = R^{-1}x_0$ is a solution of $Sy = c$, where $c = Lb$. In particular, this fact implies that $Ax = b$ has integer solutions for all $b \in \mathbb{Z}^p$ if, and only if, $A$ has full rank and $d(A) = 1$. It is also important to note that from the criterion in theorem 0.6 it follows that if $A \in M_{p\times q}(\mathbb{Z}_N)$ and $b \in \mathbb{Z}_N^p$, then the system of linear equations $Ax = b$ has solutions with coefficients in $\mathbb{Z}_N$ if, and only if, $[A, NI_p]x = b$ has solutions in $\mathbb{Z}$; here $NI_p$ is the $p \times p$ scalar matrix with $N$ in the diagonal; therefore, as $[A, NI_p]$ has full rank, then $Ax = b$ has solutions with coefficients in $\mathbb{Z}_N$ for all $b \in \mathbb{Z}_N^p$ if, and only if, $d([A, NI_p]) = 1$.

**Proof of Theorem 1** *Let $F$ be the linear $m$-cellular automaton whose local rules are given by (5). According to the previous comments, if $F$ is surjective, then $d([A_{j,s}, NI_{s+1}]) = 1$ for all integers $0 \leq j < m$ and $s \geq 0$. In this case the Smith normal form of $[A_{j,s}, NI_{s+1}]$ is* $\widetilde{S}_{j,s} = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & \cdots & 0 \end{pmatrix}$. *Let us see that the Smith normal form $S_{j,s}$ of $A_{j,s}$ has full rank and its non-zero coefficients are coprimes to $N$. First we suppose that the rank of $S_{j,s}$ is not full, i.e. $0 < \ell = rank(S_{j,s}) < s+1$. Then there exist unimodular matrices $L$ and $R$ such that $S_{j,s} = LA_{j,s}R$ is as in (8). Consider the unimodular matrix $\widetilde{R} = \begin{pmatrix} R & 0 \\ 0 & L^{-1} \end{pmatrix}$; it is easy to check that*

$$L[A_{j,s}, NI_{s+1}]\widetilde{R} = \begin{pmatrix} a_1 & \cdots & 0 & 0 & \cdots & 0 & N & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \cdots & \vdots & \vdots & \ddots & \vdots & \vdots & \cdots & \vdots \\ 0 & \cdots & a_\ell & 0 & \cdots & 0 & 0 & \cdots & N & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & N & \cdots & 0 \\ \vdots & \cdots & \vdots & \vdots & \cdots & \vdots & \vdots & \cdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & N \end{pmatrix}.$$

*After a finite number of elementary column operations (interchanging columns) the matrix $L[A_{j,s}, NI_{s+1}]\widetilde{R}$ can be reduced to the form*

$$\begin{pmatrix} a_1 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 & N & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \cdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & a_\ell & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & N \\ 0 & \cdots & 0 & N & \cdots & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \cdots & \vdots & \vdots & \ddots & \vdots & \vdots & \cdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & N & 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix},$$

*which is not equivalent to $\widetilde{S}_{j,s}$ because $N \geq 2$ has no multiplicative inverse in $\mathbb{Z}$, in this way we conclude that $rank(S_{j,s}) = rank(A_{j,s}) = s+1$. Now we will prove that $gcd(a_\ell, N) = 1$ for all $1 \leq \ell \leq s+1$. It is clear that*

$$[A_{j,s}, NI_{s+1}](s+1) = \bigcup_{\ell=1}^{s} A^{\ell}_{j,s} \cup A_{j,s}(s+1) \cup \{NI_{s+1}\},$$

*where $A^{\ell}_{j,s}$ is the set of all $(s+1)\times(s+1)$ submatrices of $[A_{j,s}, NI_{s+1}]$ with $s+1-\ell$ columns of $A_{j,s}$ and $\ell$ columns of $NI_{s+1}$. Thus*

$$\begin{aligned} 1 &= d([A_{j,s}, NI_{s+1}]) = gcd\{det(B) : B \in [A_{j,s}, NI_{s+1}](s+1)\} \\ &= gcd(d(A_{j,s}), N^{s+1}, N^s d_1(A_{j,s}), \cdots, Nd_s(A_{j,s})) \\ &= gcd(d(A_{j,s}), Ngcd(N^s, N^{s-1}d_1(A_{j,s}), \cdots, Nd_{s-1}(A_{j,s}), d_s(A_{j,s}))), \end{aligned}$$

*which implies that $gcd(d(A_{j,s}), N) = 1$. But $d(A_{j,s}) = \prod_{\ell=1}^{s+1} a_\ell$, consequently it holds $gcd(a_\ell, N) = 1$ for all $1 \leq \ell < s+1$.*

*Suppose on the other hand that the Smith normal form of $A_{j,s}$,*

$$S_{j,s} = LA_{j,s}R = \begin{pmatrix} a_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & a_\ell & 0 & \cdots & 0 \end{pmatrix},$$

*satisfies $a_\ell \geq 1$ and $gcd(a_\ell, N) = 1$ for all $1 \leq \ell \leq s+1$. Let $\widetilde{R} = \begin{pmatrix} R & 0 \\ 0 & L^{-1} \end{pmatrix}$ be as above, then*

$$L[A_{j,s}, NI_{s+1}]\widetilde{R} = \begin{pmatrix} a_1 & \cdots & 0 & 0 & \cdots & 0 & N & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \cdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & a_{s+1} & 0 & \cdots & 0 & 0 & \cdots & N \end{pmatrix}.$$

*Take $\alpha_\ell, \beta_\ell \in \mathbb{Z}$ ($1 \leq \ell \leq s+1$) such that $\alpha_\ell a_\ell + \beta_\ell N = 1$ (recall that $gcd(a_\ell, N) = 1$). Now consider the matrix $\widehat{R} = \begin{pmatrix} A & 0 & NI_{s+1} \\ 0 & I_{2r} & 0 \\ B & 0 & -D \end{pmatrix}$, where $I_{2r}$ is the $2r \times 2r$ identity matrix, and $A$, $B$ and $C$ are the diagonal matrices:*

$$A = diag(\alpha_1, \cdots, \alpha_{s+1}), B = diag(\beta_1, \cdots, \beta_{s+1}) \text{ and } D = diag(a_1, \cdots, a_{s+1}).$$

*It is no difficult to show that $\widehat{R}$ is equivalent to $\begin{pmatrix} R_1 & 0 & 0 & \cdots & 0 \\ 0 & R_2 & 0 & \cdots & 0 \\ \vdots & \cdots & \ddots & \cdots & \vdots \\ 0 & \cdots & 0 & R_{s+1} & 0 \\ 0 & \cdots & 0 & 0 & I_k \end{pmatrix}$, where $R_\ell = \begin{pmatrix} \alpha_\ell & N \\ \beta_\ell & -a_\ell \end{pmatrix}$ for all $1 \leq \ell \leq s+1$. As $detR_\ell = -1$ for each value of $\ell$, it follows that $\widehat{R}$ is unimodular. Finally, a straightforward computation shows that $L[A_{j,s}, NI_{s+1}]\widetilde{R}\widehat{R} = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & \cdots & 0 \end{pmatrix}$, establishing the surjectivity of $F$ because $d([A_{j,s}, NI_{s+1}]) = 1$.*

# References

[1] J.P. Allouche and G. Skordev. *Remarks on permutive cellular automata. J. Comput. Syst. Sci.* **67**, (2003) 174–182.

[2] I. Arcaya and N. Romero. *On a Hedlund's theorem and place-dependent cellular automata. Divulg. Mat.* **15(2)** 81–92 (2007).

[3] N. A. Baas and T. Helvik. *Higher order Cellular Automata. Adv. Complex Syst.* **8**. (2005) 169–192.

[4] M. Itô, N. Ôsato and M. Nasu. *Linear Cellular Automata over* $\mathbb{Z}_m$*. Journal of Computer and System Sciences*, **27** (1983) 125–140.

[5] R. Q. Jia. *Multivariate Discrete Splines and Linear Diophantine Equations. Trans. Amer. Math. Soc.* **340** (1993) 179–198.

[6] F. Lazebnik. *On Systems of Linear Diophantine Equations. Math. Mag.* **69** (1996) 261–266.

[7] G. A. Hedlund. *Endomorphisms and Automorphisms of the shift dynamical systems. Math. Sys. Th.* **3**, (1969) 320–375.

[8] J. Kari. *Linear cellular automata with multiple state variables. Lecture Notes in Computer Science* Vol. **1770**, (2000) 110–121. Springer, New York.

[9] E. Lange, H.O. Peitgen and G. Skordev. *Fractal patterns in Gaussian and Stirling number tables. Ars Combin.* **48**, (1998) 3–26.

[10] N. Romero, A. Rovella and F. Vilamajó. *Remark on Cellular Automata and Shift Preserving Maps. Appl. Math. Lett.* **19**, (2006) 576–580.

[11] B.L. van der Waerden. Algebra. Springer-Verlag. Berlin, Heidelberg, New York (1967).