Multidimensional σ-automata, π-polynomials and generalised S-matrices

Palash Sarkar[a,*], Rana Barua[b]

[a] *Computer Science Unit, Indian Statistical Institute, 203, B.T. Road, Calcutta 700035, India.*
[b] *Stat-Math Unit, Indian Statistical Institute, 203, B.T. Road, Calcutta 700035, India*

Received January 1996
Communicated by M. Nivat

Abstract

In this article we study σ (σ^{-1})-automata on finite multidimensional grids with different boundary conditions. We obtain a natural representation of the global linear map of such automata in terms of Kronecker products of matrices having a simple structure. Using this representation and properties of binary Chebyshev polynomials, we obtain necessary and sufficient condition for the invertibility of this map. Also in certain cases, we relate this condition to the number theoretic properties of the number of dimensions and the lengths of the dimensions. We generalise the notion of nearest neighbourhood to many dimensions and characterise invertibility of σ-automata with such neighbourhoods.

1. Introduction

Recently, there has been a tremendous amount of interest in the study of cellular automata (CA) (see [16, 17] for bibliographies). This stemmed mainly due to the seminal work done by Wolfram [16]. In [16], an extensive (empirical) study and analysis of the dynamics of CA was done revealing several interesting phenomena. The book by Wolfram [17] shows applications of CA in several areas. Martin et al. [7] obtained the basic results of a class of CA known as linear CA, using purely algebraic means.

A special class of binary cellular automata is the σ-automata where the next state of any cell is the sum (modulo two) of the previous states of all its neighbouring cells. Such automata over arbitrary graphs have been studied in literature and were first studied by Lindenmayer [6]. Study of σ-automata is related to the study of σ-game, which is a combinatorial game first introduced by Sutner in [13] and is based on the battery-operated toy MERLIN [9]. In [13], Sutner reduces the study of σ-game

to that of a suitably constructed σ-automaton. Combinatorial techniques are then used to obtain expressions for the dimension of the kernel of σ-automata on product graphs of the form $G_1 \times G_2$ (see also [10]). For the special case of product graphs of the form $P_m \times P_n$, where P_i is a path graph on i vertices, it was shown that the automaton is invertible iff $m+1$ and $n+1$ are relatively prime.

Barua and Ramakrishna in [3] consider the product graph $P_m \times P_n$ as a two-dimensional grid and reduce the σ-game to the study of invertibility of cellular automata on two-dimensional array. The global CA rule is considered to be a linear transformation of the form $AX + XB$, where X is a two-dimensional CA configuration, regarded as a 0–1 matrix, and A and B are special kinds of tridiagonal matrices, which we call S-matrices (see Section 2). Analysis of this equation provides an algebraic proof for the dimension of the kernel of the linear map.

The matrix equation representation provides a necessary and sufficient condition for invertibility in terms of the characteristic polynomials of A and B. In special cases the invertibility is related to the lengths in both the dimensions. The characteristic polynomial for an S-matrix satisfies a nice recurrence, and has many interesting properties (see [3, 14]). In [15] these polynomials are called binary Chebyshev polynomials and following [14] we will call them π-polynomials.

A natural consequence is to consider σ-games (and hence σ-automata) on multi-dimensional grids. Sutner in [10, 13] introduced combinatorial techniques to tackle the multidimensional case. For product graphs of the form $G = H \times P_n$ (where P_n is a path graph on n-vertices) there is an expression relating the coranks (dimension of kernel) of G and H, viz.,

$$cork\ \sigma(G) = cork\ \pi_{n+1}(\sigma(H)).$$

where $\sigma(G)$ denotes the global rule for σ-automaton on graph G and $\pi_{n+1}(x)$ is the characteristic polynomial for the global rule of the σ-automaton on P_n. However, analysis of $\pi_{n+1}(\sigma(H))$ seems to be complicated. Though this is a general result, for the special case where G is a multidimensional grid, we use a suitable transformation to obtain a much more elegant representation of the global rule in terms of Kronecker products. Using this representation we attack the question of invertibility of σ-automata.

Invertibility is an important question since this means that the State Transition Diagram consist entirely of cycles with no tree configurations. In other words, starting from any configuration it is possible to evolve the automaton over a finite number of steps and get back to the original configuration. Here we note that even if a finite cellular automaton is invertible, its inverse need neither be uniform nor nearest neighbourhood. Finite linear cellular automata on multidimensional grids have been considered before [7]. Martin et al. [7] used polynomials of several variables to tackle multidimensional configuration. It is a difficult technique and known results on finite multidimensional cellular automata are few. However, our approach yields interesting results on the invertibility of finite multidimensional linear cellular automata. Using the

Kronecker product representation of the global rule, we obtain the characteristic roots of the global rule in terms of the roots of π-polynomials. In special cases this is then related to the number theoretic properties of the number of dimensions and the lengths in each dimension.

The article is organised as follows. We first present some new results on the global map of one-dimensional σ-automata. Next we go on to study σ, σ^{-1} automata on finite orthogonal multidimensional grids with different boundary conditions. We use algebraic methods akin to that in [3] and obtain a general representation of the corresponding linear transformation. Using this representation we obtain necessary and sufficient conditions for the invertibility of such automata. We use several properties of the π-polynomials from [14] to relate the invertibility to the number theoretic properties of the number of dimensions and the lengths of the dimensions. Both symmetric (equal lengths) and asymmetric grids with null, periodic and mixed boundary conditions are considered. Lastly, we tackle more general cases of multidimensional nearest-neighbourhood σ-automata.

2. Preliminaries

In this section we make precise certain terms and also present some basic results required in later sections. We will denote the field of two elements by $GF(2)$ and by $GF(2^l)$ we will denote the extension field of dimension l over $GF(2)$. The set $V_l = \{(i_1,\ldots,i_l) : i_j \in GF(2), 1 \leqslant j \leqslant l\}$ with the usual $+$ operator is a vector space of dimension l over $GF(2)$. Under suitably defined multiplication V_l is isomorphic to $GF(2^l)$. Hence, we will drop the distinction between the two and use the notation $GF(2^l)$ throughout. The exact meaning will be clear from the context. Throughout the paper, the base field is $GF(2)$ and we will denote the identity matrix of order n by I_n. Also $\phi(n)$ is the Euler totient whose value is the number of positive integers less than n and coprime to n.

Definition 2.1. (1) A k dimensional grid is a multidimensional array $G[0..l_1 - 1][0..l_2 - 1]\ldots[0..l_k - 1]$, with length l_i in the ith dimension. It will be denoted by $G(l_1,\ldots,l_k)$. Any cell of the array is uniquely identified by a tuple $(i_1,\ldots,i_k)$, with $0 \leqslant i_j < l_j$ and $1 \leqslant j \leqslant k$ and has a finite set of neighbours as defined below.

(2) The neighbours of any cell $(i_1,\ldots,i_k)$ are given by $(i_1,\ldots,i_j \pm 1,\ldots,i_k)$ with $1 \leqslant j \leqslant k$. If the jth component has a periodic boundary condition, then $i_j \mp 1$ is evaluated modulo l_j. If the jth component has a null boundary condition, then there are no neighbours corresponding to -1 and l_j in the jth component.

(3) If all dimensions have null boundary condition then the grid is a null boundary grid. If all dimensions have periodic boundary condition then the grid is a folded grid. If some dimensions have null boundary condition and some have periodic boundary condition then we will call the grid a mixed grid.

(4) The grid is symmetric if the lengths of all dimensions are equal. Else it is an asymmetric grid. A k-dimensional symmetric grid of length l will be denoted by $G_k(l)$.

A k-dimensional grid $G(l_1,\ldots,l_k)$ has $\prod_{i=1}^{k} l_i$ cells. It is also possible to define a k-dimensional grid (folded, null or mixed) as a finite product of path or cycle graphs (see [10]).

Definition 2.2. (1) A σ-automaton on a multidimensional grid is a cellular automaton where

- a > the state of each cell belongs to $GF(2)$.
- b > the next state for any cell is the sum (modulo 2) of the current states of its neighbours (this specifies the local rule for the σ-automaton).

(2) A σ^{-}-automaton is defined similarly, the only difference being the fact that in this case the cell itself is also considered to be its neighbour.

An assignment of values 0 or 1 to the cells of a k-dimensional grid is called a *configuration*. We define $\mathscr{C}$ to be the set of all configurations. The *global transition rule* for a σ-automaton is a map $T : \mathscr{C} \to \mathscr{C}$, where $T(c)$ is the configuration obtained from configuration c by applying the local rule to each cell. The global dynamics of a σ-automaton is determined by T and is best expressed in terms of the *state transition diagram* (STD), which is a directed graph $D = (V,A)$ where $V = \mathscr{C}$ and $(c_1,c_2) \in A$ iff $T(c_1) = c_2$. It is easy to see that the STD for a σ-automaton consists of disjoint components, where each component has a cycle with trees of height $\geqslant 0$ rooted on each cycle vertex [7]. The σ-automaton is said to be *invertible* iff T is a bijection. Also we can consider $\mathscr{C}$ to be a vector space over $GF(2)$ and then T is a linear transformation from $\mathscr{C}$ to $\mathscr{C}$. So T is invertible iff $\dim \ker T = 0$. With respect to the standard basis, T is uniquely determined by a matrix M. Then T is invertible iff M is invertible. This M is called the *transition matrix* for the σ-automaton. In this paper we will be concerned with the representation and invertibility of M.

For basic algebraic properties of CA see [7].

Definition 2.3. (1) An S-matrix of order l, S_l, is a square tridiagonal matrix of order l, defined as

$$[s_{ij}] = \begin{cases} 1 & \text{if } |i-j| = 1, \\ 0 & \text{elsewhere.} \end{cases}$$

(2) A C-matrix is a square matrix of order l, denoted by C_l, and is defined as

$$[c_{ij}] = \begin{cases} 1 & \text{if } |i-j| = 1, \\ 1 & \text{if } (i = 1 \text{ and } j = l) \text{ or } (i = l \text{ and } j = 1), \\ 0 & \text{elsewhere.} \end{cases}$$

Thus, the forms of S-matrix and C-matrix are

$$S_l = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 1 & 0 & 1 & \dots & 0 & 0 \\ . & . & . & \dots & . & 0 \\ . & . & . & \dots & . & 1 \\ 0 & . & . & \dots & 1 & 0 \end{bmatrix},$$

$$C_l = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 1 \\ 1 & 0 & 1 & \dots & 0 & 0 \\ . & . & . & \dots & . & 0 \\ . & . & . & \dots & . & 1 \\ 1 & . & . & \dots & 1 & 0 \end{bmatrix}.$$

It is easy to see that a C-matrix is circulant.

Definition 2.4. The π-polynomials are a sequence of polynomials over $GF(2)$ defined as

$$\pi_0(x) = 0,$$
$$\pi_1(x) = 1,$$
$$\pi_i(x) = x\pi_{i-1}(x) + \pi_{i-2}(x) \quad \text{for } i \geq 2.$$

This definition of π-polynomials was introduced in [14], and in [15] they are called binary Chebyshev polynomials. Similar polynomials were studied in [3].

The global rule for a σ-automaton on a one-dimensional array of length l, is given by S_l for null boundary condition and by C_l for periodic boundary condition. For the σ^{-}-automaton the corresponding maps are given by $S_l^{-1} = S_l + I_l$ and $C_l^{-1} = C_l + I_l$. The characteristic polynomial for S_l is $\pi_{l+1}(x)$ and for C_l it is $x\pi_l(x)$ (see [3]). Also in [14] it is shown that the minimal polynomial for S_l is $\pi_{l+1}(x)$ and the minimal polynomial for C_l is $x\pi_{l/2}(x)$ for even l and is $x\sqrt{\pi_l(x)}$ for odd l. The minimal polynomial for S_l was also obtained in [12] in the context of hybrid 90/150 CA. We shall use these facts in later sections.

Definition 2.5. The exponent of an invertible $n \times n$ matrix A is defined to be the least positive integer e such that

$$A^e = I_n.$$

Since we are considering matrices over finite fields, the existence of such an e is guaranteed. Next we have the following result from [7].

Lemma 2.1. *For odd l, there exists an integer $p > 0$, such that for any $\underset{\sim}{x} \in GF(2^l)$,*

$$C_l^{p+1}\underset{\sim}{x} = C_l\underset{\sim}{x}$$

and the least such integer p divides $2^{ord_l(2)} - 1$, where $ord_l(2)$ is the least integer j, such that $2^j = \pm 1 \bmod l$. Consequently, $C_l^{p-1} = C_l$.

In what follows, we will use certain properties of π-polynomials, all of which can be found in [14]. We will denote the Kronecker (or direct) product of two matrices A and B by $A \otimes B$ and the resultant of two polynomials $p(x)$ and $q(x)$ by $Res_x(p(x), q(x))$. The reader is referred to [2] for a discussion on Kronecker products and to [8] for a discussion on resultants.

3. S-matrix

The C-matrix operator corresponds to the global rule for an uniform one-dimensional periodic boundary condition CA with rule 90 [15]. Basic properties of this transformation have been studied in [7]. The S-matrix, on the other hand, corresponds to an uniform null boundary condition CA with rule 90. In [15] it is noted that the global dynamics of null boundary CA is similar to that of periodic boundary CA. The null boundary CA is of special importance in VLSI applications, since it maintains local connection. Hence, the null boundary CA have been studied for VLSI applications [4].

In this section, we present some new results on the inverse and exponent of the S-matrix operator. First, we note that S_n is invertible iff n is even and S_n^+ is invertible iff $n \not\equiv 2 \bmod 3$ (see [3]). Next, we have

Theorem 3.1. *For even n, the inverse of S_n satisfies the recurrence*

$$S_n^{-1} = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & \dots & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & & & & & & & \\ 1 & 0 & & & & & & & \\ \vdots & \vdots & & & & & & & \\ \vdots & \vdots & & & S_{n-2}^{-1} & & & & \\ \vdots & \vdots & & & & & & & \\ 0 & 0 & & & & & & & \\ 1 & 0 & & & & & & & \end{bmatrix},$$

$$S_2^{-1} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Proof. By induction one can show that

$$S_n^{-1} S_n = \begin{bmatrix} 0 & 1 & 0 & 1 & \dots & 0 & 1 \\ 1 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & & & & & \\ 1 & 0 & & & & & \\ \cdot & \cdot & & & & & \\ \cdot & \cdot & & & S_{n-2}^{-1} & & \\ \cdot & \cdot & & & & & \\ 0 & 0 & & & & & \\ 1 & 0 & & & & & \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & & & & & \\ 0 & 0 & & & & & \\ \cdot & \cdot & & & & & \\ \cdot & \cdot & & & S_{n-2} & & \\ \cdot & \cdot & & & & & \\ 0 & 0 & & & & & \\ 0 & 0 & & & & & \end{bmatrix}$$

$$= \begin{bmatrix} I_2 & O \\ O & I_{n-2} \end{bmatrix}$$

$$= I_n. \qquad \square$$

Remark 3.1. The above theorem not only gives an algorithm for finding the inverse of S_l but also an algorithm for finding the predecessor of a given configuration.

Next we obtain a similar result for generalised inverse of S-matrix when n is odd.

Theorem 3.2. *For odd n, the matrices obtained by the following recurrence are generalised inverses of the corresponding S-matrices:*

$$S_n^- = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 & \dots & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & & & & & & & \\ 1 & 0 & & & & & & & \\ \cdot & \cdot & & & & & & & \\ \cdot & \cdot & & & & S_{n-2}^- & & & \\ \cdot & \cdot & & & & & & & \\ 0 & 0 & & & & & & & \\ 1 & 0 & & & & & & & \\ 1 & 0 & & & & & & & \end{bmatrix},$$

$$S_3^- = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}.$$

Proof. By induction one can verify that

$$S_n S_n^- S_n = S_n. \qquad \square$$

Theorem 3.3. *For even n, S_n satisfies*

$$S_n^{2^{1+ord_{n+1}(2)}-2} = I_n.$$

Thus, the exponent of S_n divides $2^{1+ord_{n+1}(2)}-2$, where the suborder function is as in Lemma 2.1.

Proof. The minimal polynomial for S_n is

$$\pi_{n-1} = \prod_{d|n} \rho_d^2 \quad \text{where } \rho_d \text{ is as in [14]}$$

$$= \rho^2.$$

The minimal polynomial for C_{n-1} is $m(x) = x\rho$ (see [14]). Also we know from Lemma 2.1,

$$C_{n-1}^{2^{ord_{n+1}(2)}} = C_{n+1}. \qquad (*)$$

Let $e = 2^{ord_{n+1}(2)}$. Then $(*)$ yields

$$\begin{aligned}
&m(x) \mid x^e - x \\
&\Rightarrow x\rho \mid x(x^{e-1} - 1) \\
&\Rightarrow \rho \mid (x^{e-1} - 1) \\
&\Rightarrow \rho^2 \mid (x^{e-1} - 1)^2 = x^{2e-2} - 1 \\
&\Rightarrow \pi_{n-1}(x) \mid (x^{2e-2} - 1) \\
&\Rightarrow S_n^{2e-2} = I_n \\
&\Rightarrow S_n^{2^{1+ord_{n+1}(2)}-2} = I_n. \qquad \square
\end{aligned}$$

Corollary 3.1. *For even n, S_n^+ satisfies*

$$(S_n^+)^{2^{1+ord_{n+1}(2)}} = (S_n^+)^2.$$

If also $n \not\equiv 2 \bmod 3$, then

$$(S_n^+)^{2^{1+ord_{n+1}(2)}-2} = I_n.$$

In fact, we can prove a stronger result.

Theorem 3.4. *For even n, the exponent e of S_n equals $2e-2$, where e is the smallest integer such that $C_{n+1}^e = C_{n+1}$.*

To prove the theorem we require the following lemma, which can easily be proved by induction.

Lemma 3.1. *Let $\underline{r}_j^i$, $j = 1,\ldots,n$ be the row vectors for S_n^i, where S_n^i is the ith power of S_n. Then if i is odd we have*

$$\underline{r}_j^i = \begin{cases} c_{j1}\underline{r}_1^1 + c_{j3}\underline{r}_3^1 + \cdots + c_{j,n-1}\underline{r}_n^1, & \text{for odd } j, \\ c_{j2}\underline{r}_2^1 + c_{j4}\underline{r}_4^1 + \cdots + c_{jn}\underline{r}_n^1 & \text{for even } j, \end{cases}$$

and if i is even,

$$\underline{r}_j^i = \begin{cases} c_{j2}\underline{r}_2^1 + c_{j4}\underline{r}_4^1 + \cdots + c_{jn}\underline{r}_n^1 & \text{for odd } j, \\ c_{j1}\underline{r}_1^1 + c_{j3}\underline{r}_3^1 + \cdots + c_{j,n-1}\underline{r}_n^1, & \text{for even } j, \end{cases}$$

where $c_{jk} \in \{0,1\}$, $1 \leqslant j \leqslant n$ and $1 \leqslant k \leqslant n$.

Proof of Theorem 3.4. From the proof of the above theorem it is clear that $\varepsilon \geqslant 2e-2$. This implies $e/2+1 \leqslant e$.

Using the above lemma, we can say that for even i, $S_n^i \neq S_n$. This is so since for even i, the first row is a linear combination of $\underline{r}_k^1$ for even k. But for all even k, the second entry of $\underline{r}_k^1$ is 0 and hence the second entry in the first row of S_n^i cannot be 1.

Thus it follows that the exponent ε of S_n must be even. For if ε is odd, then $S_n^{\varepsilon} = I_n$ implies $S_n^{\varepsilon-1} = S_n$ and $\varepsilon-1$ is even which is a contradiction to the above.

Now we can complete the proof:

$$\begin{aligned} & S_n^{\varepsilon} = I_n \\ & \Rightarrow \pi_{n+1}(x) \mid x^{\varepsilon} - 1 \\ & \Rightarrow \rho^2 \mid x^{\varepsilon} - 1 = (x^{\frac{\varepsilon}{2}} - 1)^2 \quad \text{where } \rho \text{ is as in the proof of Theorem 3.3} \\ & \Rightarrow \rho \mid x^{\frac{\varepsilon}{2}} - 1 \\ & \Rightarrow x\rho \mid x^{\frac{\varepsilon}{2}+1} - x \\ & \Rightarrow C_{n-1}^{\frac{\varepsilon}{2}+1} = C_{n-1} \quad \text{since } x\rho \text{ is the minimal polynomial of } C_{n+1} \\ & \Rightarrow e \leqslant \frac{e}{2} + 1. \end{aligned}$$

Then it follows that $e = e/2 + 1$ and so $\varepsilon = 2e - 2$. $\square$

The fact that ε is even can also be proved using a nice trick introduced in [7]. Let $(a_1,\ldots,a_N)$ be any configuration of an N cell null boundary CA A_1. Then the evolution from this configuration will be equivalent to the evolution from a $2N+2$ cell periodic boundary CA A_2, which starts from the initial configuration $(0,a_1,\ldots,a_N,0,a_N,a_{N-1},\ldots,a_1)$ (we are assuming σ-automaton evolution which is rule 90 of [7]). Let L_N' be the length of the largest cycle in an N cell null boundary CA and let L_N be the length of the largest cycle in a N cell periodic boundary CA. Then by the above embedding we have $L_N' = L_{2N+2}$. Again, from [7], we have $L_{2N-2} = 2L_{N+1}$ and this implies that L_N'

and hence e must be even. However, the lemma that we have used is interesting in its own right.

Let $K_{n+1} = 2^{ord_{n-1}(2)} - 1$. In [7] it is noted that for almost all even n ($n+1$ is odd), $e = K_{n+1} + 1$. By the above theorem, the exponent of S_n is $2^{1+ord_{n-1}(2)} - 2$, exceptions occurring exactly at values for which exceptions occur for K_{n-1}.

4. Generalised S-matrix and higher-dimensional σ-automata

In this section we obtain a representation for the linear transformation defined by the global rule of a σ-automaton on a *null boundary multidimensional grid*. For the one-dimensional case this is given by an S-matrix of order n. For the two-dimensional case, a representation was obtained in [3] as $AX + XB$, where A and B are S-matrices of proper order. We will show that for a k-dimensional grid, the global rule can be represented as a sum of Kronecker product of matrices. We will use this representation in later sections to perform an algebraic analysis of the linear map.

In the following discussion, we will consider a multidimensional configuration as a vector in a suitable vector space. To do this we will need to map a multidimensional configuration to a one-dimensional vector. For this we use the standard one-to-one correspondence used by compilers [1]. Consider a k-dimensional grid $G(l_1,\ldots,l_k)$. Then the coordinate $(i_1,\ldots,i_k)$ $0 \leqslant i_r \leqslant l_r - 1$ becomes the jth component of a vector where

$$\begin{aligned} j &= (\ldots((i_1 l_2 + i_2) l_3 + i_3)\ldots) l_k + i_k \\ &= i_1 l_2 l_3 \ldots l_k + i_2 l_3 \ldots l_k + \cdots + i_{k-1} l_k + i_k. \end{aligned} \tag{1}$$

In other words, j is the position of $(i_1,\ldots,i_k)$ in the lexicographic ordering of the k-tuples. Thus, each such k-dimensional configuration is identified with a vector in a vector space of dimension $L = \prod_{i=1}^{i=k} l_i$. Hence, we can consider the global rule of a σ-automaton to be represented by a square binary matrix of order L. We characterise this matrix as a sum of Kronecker products and refer to as a *generalised S-matrix*. The name is justified as it turns out that the matrix is block tridiagonal. We obtain the matrix as follows. For each cell $(i_1,\ldots,i_k)$ of the array, we have the jth row in the matrix, where j is given by (1). The L entries in the row correspond to the L cells in the array and the cth column in the jth row is 1 iff the cth cell is a neighbour of the jth cell. It is easy to see that a generalised S-matrix is sparse, symmetric and has all entries on the main diagonal to be zero.

Next we prove a technical lemma, which will be used in this and later sections to express a generalised S-matrix as a sum of Kronecker products. We denote the entry in the rth row and cth column of a matrix A by $A(r,c)$.

Lemma 4.1. *Consider a k-dimensional grid $G(l_1,\ldots,l_k)$ and let d be the map from k dimension to one dimension, i.e.*

$$d : \{(i_1,\ldots,i_k) : 0 \leqslant i_j < l_j, 1 \leqslant j \leqslant k\} \longrightarrow \{J : 0 \leqslant J < L\}$$

given by

$$d(i_1,\ldots,i_k) = (\ldots((i_1l_2+i_2)l_3+i_3)\ldots)l_k+i_k. \tag{II}$$

Consider the matrix $T = A_1 \otimes \cdots \otimes A_k$, *where* A_i *is a square matrix of order* l_i.

Let $\{(x_i,y_i): 1\leqslant i\leqslant k, 0\leqslant x_i,y_i < l_i\}$ *be a set of ordered pairs and let*

$$X = d(x_1,\ldots,x_k), \qquad Y = d(y_1,\ldots,y_k).$$

Then $T(X,Y) = 1$ *iff* $A_i(x_i,y_i) = 1$ *for all* i.

Proof. The proof is by induction on r, with $1\leqslant r\leqslant k$. For $r = 1$, the result is trivial. Assume that the result holds for $r-1$. Then we have to show that the result holds for

$$T_r = A_1 \otimes \cdots \otimes A_r = A_1 \otimes \cdots \otimes A_{r-1} \otimes A_r$$
$$= T_{r-1} \otimes A_r,$$

where T_{r-1} is a square matrix of order $L_r = l_1\ldots l_{r-1}$. Given r pairs $(x_1,y_1),\ldots,(x_r,y_r)$ with $0\leqslant x_i,y_i < l_i$, let $X_{r-1} = d(x_1,\ldots,x_{r-1})$ and $Y_{r-1} = d(y_1,\ldots,y_{r-1})$. Then, $X_r = d(x_1,\ldots,x_r) = l_rX_{r-1} + x_r$ and $Y_r = d(y_1,\ldots,y_r) = l_rY_{r-1} + y_r$. So,

$$T_r = T_{r-1} \otimes A_r = \begin{bmatrix} t_{11}A_r & t_{12}A_r & \cdots & t_{1Y_{r-1}}A_r & \cdots & t_{1L_{r-1}}A_r \\ t_{21}A_r & t_{22}A_r & \cdots & t_{2Y_{r-1}}A_r & \cdots & t_{2L_{r-1}}A_r \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ t_{X_{r-1}1}A_r & t_{X_{r-1}2}A_r & \cdots & t_{X_{r-1}Y_{r-1}}A_r & \cdots & t_{X_{r-1}L_{r-1}}A_r \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ t_{L_{r-1}1}A_r & t_{L_{r-1}2}A_r & \cdots & t_{L_{r-1}Y_{r-1}}A_r & \cdots & t_{L_{r-1}L_{r-1}}A_r \end{bmatrix},$$

where $t_{ij} = T_{r-1}(i,j)$. From this we get that $T_r(X,Y) = 1$ iff $t_{X_{r-1},Y_{r-1}} = 1$ and $A_r(x_r,y_r) = 1$. This is so iff $T_{r-1}(X_{r-1},Y_{r-1}) = 1$ and $A_r(x_r,y_r) = 1$ iff $A_i(x_i,y_i) = 1$, $\forall 1\leqslant i\leqslant r-1$ (by induction hypothesis) and $A_r(x_r,y_r) = 1$ iff $A_i(x_i,y_i) = 1, \forall 1\leqslant i\leqslant r$. □

Now we can present the main result of this section.

Theorem 4.1. *For the* σ*-automaton on* $G(l_1,\ldots,l_k)$ *with null boundary condition, the transition matrix is a generalised S-matrix* T, *defined by*

$$T = I_{l_1} \otimes I_{l_2} \otimes \cdots \otimes S_{l_i} + I_{l_1} \otimes I_{l_2} \otimes \cdots \otimes S_{l_i} \otimes I_{l_i}$$
$$+ \cdots + S_{l_1} \otimes I_{l_2} \otimes \cdots \otimes I_{l_i}. \tag{III}$$

Proof. Let $I = (i_1,\ldots,i_k)$ be any cell of the underlying k-dimensional grid. Then its neighbours are given by $(i_1,\ldots,i_j \pm 1,\ldots,i_k), 1\leqslant j\leqslant k$.

Let T_j be the global transformation corresponding to the local rule where we consider neighbours in the jth dimension only. Then by linearity we can write

$$T = \sum_{j=1}^{k} T_j = T_1 + \cdots + T_k.$$

If we can show that $T_j = I_{l_1} \otimes \cdots \otimes S_{l_j} \otimes \cdots \otimes I_{l_k}$ then we are done.

Let $X = d(i_1, \ldots, i_j, \ldots, i_k)$ where d is as in (II) above. Let

$$X_1 = d(i_1, \ldots, i_j - 1, \ldots, i_k),$$

$$X_2 = d(i_1, \ldots, i_j + 1, \ldots, i_k).$$

Here we assume that both $i_j - 1$ and $i_j + 1$ lie between 0 and $l_j - 1$. The other cases are similar. Hence, we have

$$T_j(X, Y) = 1 \quad \text{iff} \quad Y = X_1 \text{ or } Y = X_2.$$

Let the entry (X, C) in $P_j = I_{l_1} \otimes \cdots \otimes S_{l_j} \otimes \cdots \otimes I_{l_k}$ be 1. Then $C = d(x_1, \ldots, x_k)$ for some $x_1, \ldots, x_k$ with $0 \leqslant x_i < l_i$. By the above lemma $P_j(X, C) = 1$ iff $I_{l_t}(i_t, x_t) = 1$ for $t \neq j, 1 \leqslant t \leqslant k$ and $S_{l_j}(i_j, x_j) = 1$. But this happens iff $x_t = i_t$ for $t \neq j, 1 \leqslant t \leqslant k$ and $x_j = i_j \pm 1$.

Thus, $P_j(X, C) = 1$ iff $C = X_1$ or $C = X_2$. But this means that each row of P_j and T_j are equal. Therefore, $T_j = I_{l_1} \otimes \cdots \otimes S_{l_j} \otimes \cdots \otimes I_{l_k}$ and hence the result follows. □

The proof actually provides a recurrence for the generalised S-matrix. This recurrence become particularly interesting when the lengths are equal (a symmetric grid). In this case,

$$T^{(k)} = I_l \otimes I_l \otimes \cdots \otimes S_l + \cdots + S_l \otimes I_l \otimes \cdots \otimes I_l.$$

From now on we will follow the convention of dropping the subscript l when the lengths are equal. Also we will denote by $I^{(k)}$ the identity matrix $I_l \otimes \cdots \otimes I_l = I_{l^k}$. Then we can neatly write the recurrence as

$$T^{(k)} = I \otimes T^{(k-1)} + S \otimes I^{(k-1)}. \tag{IV}$$

Thus, our investigation of the invertibility of a symmetric σ-automaton is reduced to the study of non-singularity of $T^{(k)}$ as given by (IV).

In [3], the global transformation of a two-dimensional CA is represented in the following way. For an $m \times n$ grid the global map T is given by $T(X) = S_m X + X S_n$ where X is an $m \times n$ matrix representing a particular configuration of the CA. This matrix equation is completely equivalent to the map $T\underset{\sim}{x} = (S_m \otimes I_n + I_m \otimes S_n)\underset{\sim}{x}$, where $\underset{\sim}{x}$ is a vector formed from X using the map given in (1). This result can be found in any standard book on matrix algebra [2]. Thus, our representation for the multidimensional case is a natural generalisation of the two dimensional case as used in [3].

Next we note several basic properties of generalised S-matrix on symmetric grids.

Proposition 4.1. *a>* $(T^{(k)})^{2^r} = I \otimes (T^{(k-1)})^{2^r} + S^{2^r} \otimes I^{(k-1)}$,

b> $T^{(2k)} = I^{(k)} \otimes T^{(k)} + T^{(k)} \otimes I^{(k)}$,

c> $T^{(2k+1)} = I^{(k)} \otimes T^{(k+1)} + T^{(k)} \otimes I^{(k+1)}$.

Proof. (a) For square matrices A,B,C,D we have $(A \otimes B)(C \otimes D) = (AC \otimes BD)$. The proof follows from this and the fact that we are working over a field of characteristic 2.

(b) and (c) follow from (IV) by induction on k. □

Proposition 4.2. *Let $p(x)$ be an annihilating polynomial for S_l, such that the powers of x are of the form 2^i. Then $p(x)$ annihilates $T^{(k)}$ as given by (IV), unless k is even and $p(x)$ has a constant term, in which case $p(x)-1$ annihilates $T^{(k)}$.*

Proof.

$$T^{(k)} = I \otimes I \otimes \cdots \otimes S + I \otimes I \otimes \cdots \otimes S \otimes I - \cdots - S \otimes I \otimes \cdots \otimes I$$

which is a sum of k terms. Then,

$$(T^{(k)})^{2^i} = I \otimes I \otimes \cdots \otimes S^{2^i} + I \otimes I \otimes \cdots \otimes S^{2^i} \otimes I - \cdots - S^{2^i} \otimes I \otimes \cdots \otimes I.$$

Using this the result follows. To see the special case, just note that when k is odd, $I^{(k)}$ added k times in just $I^{(k)}$. This however is not possible when k is even. □

Using the above proposition it can be shown that for $l = 2,4,6$, a σ-automaton on a k-dimensional null boundary grid is invertible iff k is odd. For the case $l = 2$, there is a nice geometric argument. In this case, any cell is identified by a k-tuple $(a_1,\ldots,a_k)$ where each a_i is 0 or 1. Since we are considering null boundary condition any cell has exactly k neighbours. Moreover, two cells $v_1 = (x_1,\ldots,x_k)$ and $v_2 = (y_1,\ldots,y_k)$ can either share two neighbours or no neighbours. To see this note that if the Hamming distance between v_1 and v_2 is greater then two, then they share no neighbours and if it is one then they are adjacent cells and hence also do not share any neighbour. Thus, v_1 and v_2 share neighbours iff their Hamming distance is two and in this case they share exactly two neighbours. Now if T be the matrix representing the global transformation of the σ-automaton, then T^2 is I or 0 according as k is odd or even. This is because to find T^2, we have to consider the inner product of the ith row r_i and the jth column c_j, and by the above discussion and symmetry, this product is k mod 2 if $i = j$ else it is 0. So if k is odd the STD consists of disjoint cycles each of length one or two and if k is even then the STD consists of a single tree rooted on the null configuration having height 1. Also the structure of the STD in this case is independent of the number of dimensions.

The above can also be proved using the following result from [10]. For product graphs $G = H \times P_n$, the coranks of rule σ on G and H are related by

$$cork\, \sigma(G) = cork\, \pi_{n+1}(\sigma(H)).$$

Then by induction it can be shown that for a k-dimensional structure the corank is 0 or k according as k is odd or even.

Let $T^{(k)}$ be invertible. Then, as we will prove in the next section, it necessarily follows that l is even and k is odd. Since l is even we know from Theorem 3.3 that the exponent of S_l divides $2^{l-\mathrm{ord}_{\pi_l}(2)}-2$ and S_l satisfies

$$p(x)=x^{2^{l-\mathrm{ord}_{\pi_l}(2)}-2}+1.$$

Thus, $x^2p(x)$ is a polynomial where the powers of x are of the form 2^i (such polynomials are called linearised polynomials [5]). Hence, $T^{(k)}$ satisfy $x^2p(x)$ and since it is invertible it also satisfies $p(x)$. Thus, in this case the exponent of $T^{(k)}$ also divide $2^{l-\mathrm{ord}_{\pi_l}(2)}-2$. Note that if l is even, then $T^{(k)}$ satisfies $x^2p(x)$ whether k is odd or even.

Remark 4.1. The matrices $T^{(k)}$ have another interesting feature. The above discussion implies that if l is fixed then for infinitely many k, $T^{(k)}$ will have the same minimal polynomial.

5. Symmetric grids

In this section we consider $\sigma(\sigma^{-1})$-automata on *symmetric null boundary grids*.

5.1. Invertibility of σ-automata

We obtain necessary and sufficient condition for the invertibility of σ-automata on symmetric, null boundary grids and relate this condition to the number theoretic properties of k, the number of dimensions and l, the length in any dimension.

Theorem 5.1. *For the σ-automaton on $G_k(l)$, the following hold:*

- *a> If l is odd, then the automaton is non-invertible.*
- *b> If k is even, then the automaton is non-invertible.*

Proof. (a) By induction on k. When $k=1$, l is odd implies $T^{(k)}=S_l$ is singular. So assume $k>1$. By (IV) we have

$$T^{(k)}=I_l\otimes T^{(k-1)}+S_l\otimes I^{(k-1)}.$$

By induction hypothesis, $T^{(k-1)}$ is singular and so x divides the characteristic polynomial $p(x)$ for $T^{(k-1)}$. Also, since l is odd $x\mid\pi_{l-1}$. Therefore, $p(x)$ and π_{l-1} share a common root and hence $T^{(k)}$ is non-invertible (see [2]).

(b) Suppose $k=2r$. Then,

$$T^{(k)}=T^{(2r)}=I^{(r)}\otimes T^{(r)}+T^{(r)}\otimes I^{(r)}.$$

Hence, it easily follows that 0 is a characteristic root and hence $T^{(k)}$ is non-invertible.

The case when l is even and k is odd, shows more interesting behaviour. *It is the only case under which $T^{(k)}$ can be invertible.* To analyse the behaviour of $T^{(k)}$ we need the following result.

Theorem 5.2. *Let*

$$T^{(k)} = I_l \otimes I_l \otimes \cdots \otimes S_l + I_l \otimes \cdots \otimes S_l \otimes I_l + \cdots + S_l \otimes I_l \otimes \cdots \otimes I_l.$$

Then α is a root of its characteristic polynomial $p(x)$ iff α is of the form

$$\alpha_1 + \cdots + \alpha_k,$$

where α_i's are the roots of π_{l-1} over the splitting field of π_{l-1}.

Proof. By induction on k. For $k = 2$ this is a standard result [2]. Assume it to be true for $k-1$ dimensions. Then,

$$T^{(k)} = I_l \otimes T^{(k-1)} + S_l \otimes I^{(k-1)}.$$

So α is a root of $p(x)$ iff it is of the form $\beta+\alpha_k$, where β is any root of the characteristic polynomial for $T^{(k-1)}$ and α_k is any root of π_{l-1} (see [2]). But by induction hypothesis β is of the form $\alpha_1 + \cdots + \alpha_{k-1}$. Hence, α is a root of $p(x)$ iff it is of the form $\alpha_1 + \cdots + \alpha_k$. □

Corollary 5.1. *$T^{(k)}$ given by (IV) is non-invertible iff for some choice of $\alpha_1, \ldots, \alpha_k$ of the roots of π_{l-1}, we have $\alpha_1 + \cdots + \alpha_k = 0$.*

Proof. $T^{(k)}$ is non-invertible iff 0 is a root of the characteristic polynomial for $T^{(k)}$ iff $\alpha_1 + \cdots + \alpha_k = 0$ for some choice of α_i's. □

This corollary provides a necessary and sufficient condition for $T^{(k)}$ to be invertible in terms of the roots of π_{l-1}. We know that invertibility can occur only when l is even and k is odd. Note that the other cases can also be derived by examining the sum $\alpha_1 + \cdots + \alpha_k$. This constitutes an alternative proof to the approach in Theorem 5.1.

The following can easily be proved by induction.

Lemma 5.1. *When l is even, π_{l-1} contains both the terms x^l and x^{l-2}.*

Remark 5.1. Hence for $l = 2r$, $p(x) = \sqrt{\pi_{2r-1}(x)}$ contains both the terms x^r and x^{r-1} and so the sum of the roots of $p(x)$ is 1.

Theorem 5.3. *Consider the σ-automaton on $G_k(l)$. If the following conditions hold, then the σ-automaton is invertible.*

1. *k is odd,*
2. *$l+1$ is an odd prime,*
3. *$2 \text{ord}_{l+1}(2) = \phi(l+1) = l$. In this case, $\pi_{l+1} = \rho^2$ with ρ irreducible.*

Proof. For the last observation see [14]. To see the first, note that the roots of the characteristic polynomial $p(x)$ for $T^{(k)}$ are of the form $\alpha_1 + \cdots + \alpha_k$, where α_i's are roots of π_{l+1}. To show that $T^{(k)}$ is invertible we have to show that the sum $\alpha_1 + \cdots + \alpha_k$ cannot be 0 for any choice of α_i and for any odd k. Now,

$$\pi_{l+1} = \rho^2 \quad \text{where } \rho \text{ is an irreducible polynomial.}$$

Suppose $l = 2r$. Then by the above lemma, ρ has both the terms x^r and x^{r-1}. Also all the distinct roots of π_{l+1} are given by all the distinct roots of ρ. Since degree of ρ is r, and ρ is irreducible, it has r distinct roots $\alpha_1 \ldots \alpha_r$ and the sum

$$\alpha_1 + \cdots + \alpha_r = 1 \quad \text{since } \rho \text{ has the term } x^{r-1},$$

When analysing the sum $\alpha_1 + \cdots + \alpha_k$, we can consider all of them to be distinct. Since, in a field of characteristic 2 equal roots cancel in pairs, without disturbing the oddity of k.

Thus, we have to show that $\alpha_1 + \cdots + \alpha_k$ cannot be 0 for odd $k \leqslant r$ and for distinct α_i's.

Since ρ is irreducible all its roots are of the form $\beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^{r-1}}$, where β is any root of ρ. Then it follows that ρ is the minimal polynomial for β.

If possible let for some odd $k \leqslant r$, $\alpha_1 + \cdots + \alpha_k = 0$. Then, $\beta^{2^1} + \cdots + \beta^{2^k} = 0$.

Hence, β satisfies $q(x) = x^{2^1} + \cdots + x^{2^k}$ and therefore $\rho \mid q(x)$. So all roots of ρ are roots of $q(x)$ and we get the following r relations:

$$\beta^{2^1} + \cdots + \beta^{2^k} = 0,$$

$$\beta^{2^{1+1}} + \cdots + \beta^{2^{k+1}} = 0,$$

$$\vdots$$

$$\beta^{2^{1+r-1}} + \cdots + \beta^{2^{k+r-1}} = 0.$$

Summing up left- and right-hand side we get

$$1 + 1 + \cdots + 1 = 0.$$

Here we use $\beta^{2^i} + \beta^{2^i} = 1$.

But there are k (odd) 1's on the left-hand side and so the sum is 1. This gives us the required contradiction. ⊓

Note that there exist primes n, such that $\phi(n) \geqslant 2\,ord_n(2)$. In fact, this will hold for any prime of the form $2^i + 1$.

Lemma 5.2. *If for some even length l, odd dimension k, a σ-automaton is non-invertible, then it is non-invertible for all odd dimensions $\geqslant k$.*

Proof. It is non-invertible for k implies that there exists roots $\alpha_1, \ldots, \alpha_k$ of π_{l+1}, such that $\alpha_1 + \cdots + \alpha_k = 0$.

But then for any odd dimension d greater than k, we know that $d - k$ is even and we can form the sum $\alpha_1 + \cdots + \alpha_k + \alpha_1 + \cdots + \alpha_1 = 0$ where α_1 is repeated $d - k$ times. But this shows that the σ-automaton on d dimensions is also non-invertible. □

Theorem 5.4. *If for some even length l, $l+1$ has two factors congruent to* 1 mod 4 *and* 3 mod 4, *then there exists an odd integer k, such that the σ-automaton on k dimensions is non-invertible.*

Proof. Let $l+1$ have at least two factors p_1 and p_2, with

$$p_1 \equiv 1 \bmod 4 \quad \text{and} \quad p_2 \equiv 3 \bmod 4.$$

Then corresponding to these factors p_1 and p_2, $\pi_{l+1}(x)$ has two factors $\pi_{p_1}(x)$ and $\pi_{p_2}(x)$ with $\pi_{p_1} = \rho_1^2$ and $\pi_{p_2} = \rho_2^2$ for some polynomials $\rho_1(x)$ and $\rho_2(x)$ [14]. Since $p_1 \equiv 1 \bmod 4$, degree of $\rho_1(x)$ is even (say $2r_1$) and since $p_2 \equiv 3 \bmod 4$, degree of $\rho_2(x)$ is odd (say $2r_2+1$). Also since p_1 and p_2 are both odd, by Remark 5.1, we get

$$\alpha_1 + \cdots + \alpha_{2r_1} = 1,$$

$$\beta_1 + \cdots + \beta_{2r_2+1} = 1,$$

where α_i's are roots of ρ_1 and β_j's are roots of ρ_2. Let $k = 2r_1 + 2r_2 + 1$. Then,

$$\alpha_1 + \cdots + \alpha_{2r_1} + \beta_1 + \cdots + \beta_{2r_2+1} = 0,$$

and hence the σ-automaton on k dimensions is non-invertible. □

Theorem 5.5. *If for some even length l, $l+1$ has two relatively prime factors both congruent to* 3 mod 4, *then there exists an odd integer k, such that the σ-automaton on k dimensions is non-invertible.*

Proof. Let $p_1 \mid l+1$ and $p_2 \mid l+1$, with p_1 and p_2 both congruent to 3 mod 4. Let $n = p_1 p_2 \equiv 1 \bmod 4$. Since $\gcd(p_1, p_2) = 1$, we can write, $\pi_n(x) = \pi_{p_1}(x)\pi_{p_2}(x)(p(x))^2$ for some polynomial $p(x)$ (cf. [14]).

Now degrees of both $\sqrt{\pi_{p_1}}$ and $\sqrt{\pi_{p_2}}$ are odd, so $p(x)$ must be an even degree polynomial. (Since $\sqrt{\pi_n}$ is of even degree).

Let the degrees of $\sqrt{\pi_{p_1}}$, $\sqrt{\pi_{p_2}}$ and $p(x)$ be r_1, r_2, r_3, respectively, with $r_1 = (p_1 - 1)/2$, $r_2 = (p_2 - 1)/2$ and $r_1 + r_2 + r_3 = (n - 1)/2$. By Lemma 5.1 $\sqrt{\pi_{p_1}}, \sqrt{\pi_{p_2}}$ and $\sqrt{\pi_n}$ contain the terms $x^{r_1}, x^{r_2}, x^{(n-3)/2}$, respectively. But this implies that $p(x)$ has the term x^{r_3}.

Let $\alpha_1, \ldots, \alpha_{r_1}$ be the roots of $\sqrt{\pi_{p_1}}$ and $\beta_1, \ldots, \beta_{r_3}$ be the roots of $p(x)$.

Then for $k = r_1 + r_3$,

$$\sum \alpha + \sum \beta = 1 + 1 = 0$$

and k is odd. □

Remark 5.2. By Lemma 5.2 it follows that such σ-automata are also non-invertible for all odd dimension $\geqslant k$ and hence for all dimension $\geqslant k$ (since if k is even it is in any case non-invertible). This however does not preclude the fact that it may be invertible for some lower odd dimension. Thus, in these cases, invertibility has to be checked only for finitely many dimensions.

This method does not work if all prime factors of $l+1$ are congruent to 1 mod 4.

Examples

(1) l odd, k even, $l=3$ $k=4$, σ-automata non-invertible.

(2) l odd, k odd, $l=3$ $k=5$, σ-automata non-invertible.

(3) l even, k even, $l=4$ $k=8$, σ-automata non-invertible.

(4) l even, k odd.

(a) $l=10$, $l+1=11$, $\phi(11)=10=2\times 5=2\,ord_{11}(2)$. Hence, σ-automata invertible for all odd dimensions.

(b) $l=34$, $l+1=35=5\times 7$. $5\equiv 1 \bmod 4$ and $7\equiv 3 \bmod 4$. Then for $k=2\cdot 3=5$ dimensions σ-automata is non-invertible.

(c) $l=76$, $l+1=77=7\times 11$. $7\equiv 3 \bmod 4$ and $11\equiv 3 \bmod 4$. Then for $k=3+30=33$ dimensions σ-automata is non-invertible.

5.2. *Invertibility of σ^--automata*

In this subsection we will consider σ^+-automaton on a k-dimensional symmetric orthogonal grid $G_k(l)$. The analysis is similar to that in the case of σ automaton. We start with the following

Theorem 5.6. *The global transformation of a σ^--automaton on $G(l_1,\ldots,l_k)$, is given by a generalised S^+-matrix written as*

$$T^+ = T - I_{l_1}\otimes I_{l_2}\otimes\cdots\otimes I_{l_k}.$$

For the special case of symmetric σ^--automaton, this reduces to

$$\begin{aligned} T^{(k)-} &= T^{(k)} + I^{(k)} \\ &= I\otimes T^{(k-1)} + S^-\otimes I^{(k-1)}. \end{aligned} \tag{V}$$

From this we get a result similar to that in Theorem 5.2. However, in this case the recurrence itself is difficult to analyse because of the asymmetry in the expression.

Theorem 5.7. *The symmetric (length l) σ^--automaton on $G_k(l)$ is non-invertible iff*

$$\alpha_1+\cdots+\alpha_k=1$$

for some choice of $\alpha_1,\ldots\alpha_k$, where α_i's are roots of π_{l+1} over its splitting field.

Proof. The proof is similar to that of Theorem 5.2. The right-hand side is 1 because of S^{-1} in Eq. (V). Since the characteristic polynomial for S^{-1} is $\pi_{l+1}(x+1)$, its roots are of the form $\alpha-1$ where α is any root of $\pi_{l-1}(x)$. □

Remark 5.3. Analogous to Lemma 5.2 we can deduce for the σ^+-automaton that if it is non-invertible for k dimensions, it is also non-invertible for $k+2i$ dimensions ($i=1,2,\ldots$).

Lemma 5.3. *If $l-1$ has a divisor congruent to* $3 \bmod 4$, *then there exists an odd k such that the σ^--automaton on k dimensions is non-invertible.*

Proof. Let $a \mid l+1$ and $a = 3 \bmod 4$. Then $\pi_a \mid \pi_{l+1}$ and so the roots of π_a are the roots of π_{l+1}. Also $\pi_a = p^2(x)$, where $p(x)$ has odd degree $d = (a-1)/2$ and sum of roots of $p(x)$ is 1 (by Remark 5.2). Then the σ^--automaton on d dimensions is non-invertible. □

Arguing similarly, we have

Lemma 5.4. *If $l+1$ has a divisor congruent to* $1 \bmod 4$, *then there exists an even k such that σ^+-automaton on k dimensions is non-invertible.*

The above two lemmas and the remark yield

Lemma 5.5. *If $l+1$ has two divisors a and b with $a \equiv 1 \bmod 4$ and $b \equiv 3 \bmod 4$, then there exists an integer k such that σ^--automaton on i dimensions is non-invertible for all $i \geqslant k$.*

Remark 5.4. Thus, invertibility has to be checked only for finitely many dimensions.

Lemma 5.6. *If l is of the form 2^n-1 for some n, then the σ^--automaton is invertible for all dimensions.*

Proof. In this case, $\pi_{l+1} = x^{2^n-1}$ and hence the only root of π_{l+1} is 0, so it is impossible to have a subset sum of roots to be 1. □

The following is an analogue of Theorem 5.3.

Theorem 5.8. *Let $l+1$ be a prime such that $\pi_{l+1}(x)$ has only one irreducible factor (i.e., $\phi(l+1) = 2\,\mathrm{ord}_{l+1}(2)$).*

- *If $l+1 \equiv 3 \bmod 4$, then σ^+-automaton is invertible for all even dimensions.*
- *If $l-1 \equiv 1 \bmod 4$, then σ^+-automaton is invertible for all odd dimensions.*

Proof. Let $\pi_{l-1} = \rho^2$ with ρ irreducible and of degree $r = l/2$.

Then there are r distinct roots $\alpha_1,\ldots,\alpha_r$ of π_{l-1}, and by Remark 5.2,

$$\alpha_1 + \cdots + \alpha_r = 1.$$

Since ρ is irreducible its roots are $\beta, \beta^2, \ldots, \beta^{2^{l-1}}$ and so

$$\beta + \beta^2 + \cdots + \beta^{2^{l-1}} = 1.$$

Let if possible for some $k < r$ such that $k \bmod 2 \neq r \bmod 2$,

$$\alpha_1 + \cdots + \alpha_k = 1.$$

Then for some $i_1,\ldots,i_k$,

$$\beta^{2^{i_1}} + \cdots + \beta^{2^{i_k}} = 1 \tag{VI}$$

and by an argument similar to the one in the proof of Theorem 5.3, (VI) will be satisfied by all roots of ρ and hence we will get the r equations.

$$\begin{aligned}
\beta^{2^{i_1}} + \cdots + \beta^{2^{i_k}} &= 1,\\
\beta^{2^{i_1+1}} + \cdots + \beta^{2^{i_k+1}} &= 1,\\
&\vdots\\
\beta^{2^{i_1+r-1}} + \cdots + \beta^{2^{i_k+r-1}} &= 1.
\end{aligned}$$

Summing up we get $k \bmod 2 = r \bmod 2$ which is a contradiction. Hence, for dimension k such that, $k \bmod 2 \neq r \bmod 2$, it is not possible to obtain $\alpha_1,\ldots,\alpha_k$ (which are roots of ρ and hence of π_{l-1}) such that $\alpha_1 + \cdots + \alpha_k = 1$. But this means that the σ^+-automaton on $G_k(l)$ is invertible. Now $k \bmod 2 \neq r \bmod 2$ means that if $l+1 = 3 \bmod 4$, then r is odd and k must be even. And if $l+1 = 1 \bmod 4$, then r is even and k must be odd. Hence the result. □

Examples

(1) If $l = 6$, $l+1 = 7 = 3 \bmod 4$. Then for $k = 3+2i$ dimensions σ^+-automata is non-invertible.

(2) If $l = 8$, $l+1 = 9 = 1 \bmod 4$. Then for $k = 4+2i$ dimensions σ^+-automata is non-invertible.

(3) If $l = 134$, $l+1 = 135 = 9 \times 15$ with $9 = 1 \bmod 4$ $15 = 3 \bmod 4$. Then for $k \geqslant 7$ dimensions σ^+-automata is non-invertible.

(4) $l = 7 = 2^3 - 1$, $\pi_8 = x^7$ and σ -automata is invertible for all dimensions k.

(5) (a) $l = 6$, $l+1 = 7 \equiv 3 \bmod 4$, $\phi(l+1) = 2\,sord_{l+1}(2)$. So σ^1-automata is invertible for all even dimensions.

(b) $l = 4$, $l+1 = 5 = 1 \bmod 4$, $\phi(l+1) = 2\,sord_{l+1}(2)$. So σ^1-automata is invertible for all odd dimensions.

Some more results on σ^+-automata are obtained in the next subsection.

5.3. Characteristic polynomial of generalised S-matrix

We now derive an expression for the characteristic polynomial of a generalised S-matrix in terms of resultant of two polynomials. First we need the following which can easily be proved using the identity 3.6(c) of [8] for the resultant of two polynomials.

Lemma 5.7. *If $P(x)$ and $Q(x)$ are two non-constant polynomials with coefficients in a field K and with roots $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$, respectively, then the roots of the polynomial*

$$R(y) = Res_x(P(x+y), Q(-x))$$

are the elements $\alpha_i + \beta_j$, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$.

Theorem 5.9. *For a fixed length l, define a sequence of polynomials by the following recurrence:*

$$Q_1(x) = \pi_{l-1}(x),$$

$$Q_k(x) = Res_y(Q_1(x+y), Q_{k-1}(y)), \quad k > 1.$$

Then $Q_k(x)$ is the characteristic polynomial for the transition matrix $T^{(k)}$ of the σ-automaton on $G_k(l)$.

Proof. By induction on k we prove that α is a root of $Q_k(x)$ iff α is of the form $\alpha_1 + \cdots + \alpha_k$, where α_i's are roots of $\pi_{l-1}(x)$. Then using Theorem 5.2 we are done.

For $k = 1$ the result is easy.

So assume the result to be true for $k-1$.

Then $Q_k(x) = Res_y(Q_1(x+y), Q_{k-1}(x))$, and α is a root of $Q_k(x)$ iff it is of the form $\beta + \alpha_i$, where β is any root of $Q_{k-1}(x)$ and α_i is any root of $Q_1(x)$. But by induction hypothesis β is of the form $\alpha_1 + \cdots + \alpha_{k-1}$. Hence the result follows. □

Corollary 5.2. *$Q_k(1+x)$ is the characteristic polynomial for $T^{(k)} + I^{(k)}$, the matrix for σ^--automaton on $G_k(l)$.*

We will write $T^{(k)+}$ for $T^{(k)} + I^{(k)}$ and $Q_k^+(x)$ for $Q_k(1+x)$. The characteristic polynomial can be used to settle a few more cases for the non-invertibility of σ^--automata.

Theorem 5.10. *If $l \equiv 2 \bmod 3$ and σ-automaton on $(k-1)$ dimensions is non-invertible then so is σ^--automaton on k dimensions.*

Proof. Since $l \equiv 2 \bmod 3$, $l+1 \equiv 0 \bmod 3$ and so $3 \mid l+1$. Hence, noting that $\pi_3(x) = 1 + x^2$ we get, $(x+1)^2 \mid \pi_{l+1}(x)$ and we can write $\pi_{l+1}(x) = (x+1)^2 \pi'_{l-1}(x)$. So,

$$\begin{aligned} Q_k(y) &= Res_x((x+y+1)^2 \pi'_{l+1}(x+y), Q_{k-1}(x)) \\ &= Q_{k-1}^2(1+y) Res_x(\pi'_{l-1}(x+y), Q_{k-1}(x)) \quad \text{(see [8])}. \end{aligned}$$

But this shows $Q_{k-1}(y) \mid Q_k(1-y)$. Thus, if $T^{(k-1)}$ is non-invertible then $y \mid Q_{k-1}(y)$. Hence $y \mid Q_k(1+y)$ and so $T^{(k)^+}$ is non-invertible. □

Corollary 5.3. *If $l = 2 \bmod 3$, then σ^+-automaton is non-invertible for all odd dimensions k.*

Proof. Follows from the above theorem and the fact that σ-automaton is non-invertible for $k = 1$ (since $k-1$ is even). □

Theorem 5.11. *If $l = 1 \bmod 2$ and if σ^--automaton on k dimensions is non-invertible then so is σ^+-automaton on $k+1$ dimensions.*

Proof. Since $l = 1 \bmod 2$ we have $\pi_{l+1}(x) = x\,\pi'_{l-1}(x)$. Hence,

$$\begin{aligned} Q_{k+1}(y) &= Res_x((x-y)\,\pi'_{l+1}(x+y), Q_k(x)) \\ &= Q_k(y)\,Res_x(\pi'_{l-1}(x+y), Q_k(x)) \quad (cf.[8]). \end{aligned}$$

But then $Q_k(1+y) \mid Q_{k-1}(1-y)$. Hence, if $T^{(k)^-}$ is non-invertible then so is $T^{(k+1)^+}$. □

Corollary 5.4. *If $l+1 \equiv 0 \bmod 6$, then σ^--automaton is non-invertible for all dimensions.*

Proof. Since $l-1 = 0 \bmod 6$, it follows that l is odd and hence by the above theorem it is sufficient to prove that $x \mid \pi_{l+1}(1+x)$. But this happens iff $(1+x) \mid \pi_{l+1}(x)$. Again since $l+1 = 0 \bmod 6$ we have $3 \mid l+1$, so $(1+x)^2 \mid \pi_{l+1}(x)$. This proves the result. □

6. Generalisations

6.1. Asymmetric grids

In this subsection we extend the results of previous sections to cover σ-automata on *null boundary asymmetric grids*. Most of the proofs are plain generalisations and will be omitted.

Theorem 6.1. *A σ-automaton (resp. σ^+-automaton) on $G(l_1, \ldots, l_k)$ is non-invertible iff*

$$\alpha_1 + \cdots + \alpha_k = 0 \ (resp.\ 1)$$

for some choice of α_i's, where α_i is any root of π_{l_i+1} over a field in which all π_{l_i-1}'s split.

In [3] this result is obtained for two dimensions by showing that σ-automaton is invertible iff $\pi_{l_1+1}(x)$ and $\pi_{l_2+1}(x)$ are relatively prime and for the σ^+-automaton $\pi_{l_1}(x)$ and $\pi_{l_2+1}(x)$ must be relatively prime. It turns out that $\pi_{l_1+1}(x)$ and $\pi_{l_2+1}(x)$ are relatively prime iff l_1+1 and l_2+1 are so (see also [13, 14]). For the σ^+-automaton such complete result could not be obtained. For certain special cases sufficiency conditions for invertibility based on number theoretic properties of l_1 and l_2 can be derived. But a general characterisation of this nature seems to be difficult. The above theorem indicates the cause for this difficulty. To obtain a characterisation of invertibility in terms of number theoretic properties we have to characterise in terms of number theoretic properties when a subset sum of roots will lie in the base field. Since the roots in general lie in an extension field, answering this question in general will be difficult.

Lemma 6.1.

- *a) If $l_1,\ldots,l_k$ are all odd, then σ-automaton of k dimensions is non-invertible.*
- *b) If for even k, $\gcd(l_1+1,\ldots,l_k+1)>1$, then σ-automaton on such a grid is non-invertible.*
- *c) If the l_i's are of the form $2^{n_i}-1$ for some n_is, then the σ^+-automaton on such a grid is invertible.*

6.2. Folded and mixed grids

Here we will allow some or all dimensions to have periodic boundary condition. The following is similar to Theorem 4.1.

Theorem 6.2. *Consider a k-dimensional grid $G(l_1,\ldots,l_k)$ with periodic boundary condition in some r $(0\leqslant r\leqslant k)$ dimensions. Then the transition matrix of the σ-automaton on this grid is given by*

$$T = I_{l_1}\otimes I_{l_2}\otimes\cdots\otimes A_{l_k} + I_{l_1}\otimes I_{l_2}\otimes\cdots\otimes A_{l_{k-1}}\otimes I_{l_k} + \cdots + A_{l_1}\otimes I_{l_2}\otimes\cdots\otimes I_{l_k},$$

where

$$A_{l_i} = \begin{cases} S_{l_i} & \text{if there is null boundary condition in the } i\text{th dimension} \\ C_{l_i} & \text{if there is periodic boundary condition in } i\text{th dimension} \end{cases}$$

The matrix for the σ^+-automaton is given by

$$T^{(+)} = T + I_{l_1}\otimes I_{l_2}\otimes\cdots\otimes I_{l_k}.$$

Theorem 6.3. *Consider a mixed grid as in the above theorem. The σ-automaton (resp. σ^+-automaton) on such a grid is non-invertible iff for some $\alpha_1,\ldots,\alpha_k$*

$$\alpha_1\cdot\cdots\cdot\alpha_k = 0 \ (\text{resp. } 1),$$

where α_i is any root of $p_i(x)$, the characteristic polynomial for A_{l_i} and so,

$$p_i(x) = \begin{cases} \pi_{l_i+1}(x) & \text{if the } i\text{th dimension has null boundary condition,} \\ x\pi_{l_i}(x) & \text{if the } i\text{th dimension has periodic boundary condition.} \end{cases}$$

Note that in the above theorem we can replace the characteristic polynomial for A_{l_i} by the minimal polynomial for A_{l_i}. This is because the minimal and characteristic polynomials have the same set of distinct roots. Thus, $p_i(x)$ can be written as

$$p_i(x) = \begin{cases} \pi_{l_i+1}(x) & \text{if the } i\text{th dimension has null boundary condition,} \\ x\pi_{\frac{l_i}{2}}(x) & \text{if the } i\text{th dimension has periodic boundary condition and } l_i \text{ is even,} \\ x\sqrt{\pi_{l_i}}(x) & \text{if the } i\text{th dimension has periodic boundary condition and } l_i \text{ is odd.} \end{cases}$$

Lemma 6.2. *In the underlying grid, if a dimension has length $2^{r_i}-1$ with null boundary condition or length 2^{r_i} with periodic boundary condition, then we can ignore the effect of this dimension on the invertibility of σ or σ^--automaton.*

Lemma 6.3. *For a mixed asymmetric grid, if all dimensions with null boundary condition have lengths of the form $2^{r_i}-1$ and all dimensions with periodic boundary condition have lengths of the form 2^{r_i}, then σ-automaton on such a grid is non-invertible and σ^{-1}-automaton is invertible.*

Similar to Theorem 5.9, one gets

Theorem 6.4. *Consider a k-dimensional mixed grid on $G(l_1,\ldots,l_k)$. Then the characteristic polynomial $Q_k(x)$ for the transition matrix of σ-automaton on such a grid is given by*

$$Q_1(x) = p_1(x),$$

$$Q_i(x) = Res_y(p_i(x+y), Q_{i-1}(y)), 1 < i \leqslant k,$$

where $p_i(x)$ is as in Theorem 6.3.

6.3. Other neighbourhoods

We generalise the concept of nearest neighbourhood to higher dimensions. For the two-dimensional case there are two kinds of nearest-neighbourhood condition – the orthogonal neighbourhood and the diagonal neighbourhood. Our generalisation is based upon the following observation. The orthogonal neighbourhood corresponds to taking one step in one dimension. The diagonal neighbourhood corresponds to taking one step each in two dimensions. Generalising, for a cell in a k-dimensional grid, we let its r-dimensional set of neighbours be the cells which are reachable by taking one step each

in exactly r-dimensions. Since in any dimension we do not allow more than one step the notion of nearest neighbourhood is preserved. Any neighbour of a cell J can also be visualised to be lying on some hyperplane unit distance away from J. We formally express this idea in the following.

Definition 6.1. For a cell $(i_1,\ldots,i_k)$ in a k-dimensional grid, the set of r-dimensional (r-D) nearest neighbours is given by

$$N_r(i_1,\ldots,i_k) = \{(i_1,\ldots,i_{j_1}+1,\ldots,i_{j_r}\pm 1,\ldots,i_k) : 1 \leqslant j_1 < \cdots < j_r \leqslant k\},$$

where $i_j \pm 1$ is taken modulo l_j if the jth dimension has a periodic boundary condition. If the jth dimension has a null boundary condition, then the values -1 and l_j+1 are ignored for the jth dimension.

It is easy to see that the definition exactly corresponds to the idea described above. Also it is clear that $|N_r(i_1,\ldots,i_k)| \leqslant 2^r\binom{k}{r}$ where equality holds for all cells iff all $l_i > 2$ and all dimensions have periodic boundary condition. Such neighbourhoods for multidimensional CA have not been considered before. Martin et al. [7] introduced Type I and Type II neighbourhoods for multidimensional CA. Type I neighbourhood corresponds to our 1-D neighbourhood. Type II neighbours of a cell $J = (i_1,\ldots,i_k)$ are given by the set $\{J\} \cup \bigcup_{1\leqslant r\leqslant k} N_r(J)$. Thus, our definition captures a finer sense of multidimensional neighbourhood.

We now obtain a characterisation of the global rule of an r-D neighbourhood σ-automaton in terms of Kronecker product.

Theorem 6.5. *Consider an r-d neighbourhood σ-automaton on a k-dimensional mixed grid $G(l_1,\ldots,l_k)$. Then the global rule is given by the following matrix:*

$$T_r^{(k)} = \sum_{1\leqslant j_1<\cdots<j_r<\cdots\leqslant k} R_1 \otimes \cdots \otimes R_k,$$

where

$$R_i = \begin{cases} I_{l_i} & \text{if } i \notin \{j_1,\ldots,j_r\},\\ S_{l_i} & \text{if } i \in \{j_1,\ldots,j_r\} \text{ and the } i\text{th dimension has null boundary condition},\\ C_{l_i} & \text{if } i \in \{j_1,\ldots,j_r\} \text{ and the } i\text{th dimension has periodic boundary condition}, \end{cases}$$

For the σ^+-automaton the corresponding global rule is $T_r^{(k)-} = T_r^{(k)} \dotplus I_{l_1\cdots l_k}$.

Proof. Let $T^{(k)}_{j_1,\ldots,j_r}$ be the matrix which corresponds to the local rule which considers neighbours only in the dimensions $j_1,\ldots,j_r$. Then by linearity it follows that

$$T_r^{(k)} = \sum_{1\leqslant j_1<\cdots<j_r\leqslant k} T^{(k)}_{j_1,\ldots,j_r}.$$

Using Lemma 4.1, we can construct a proof similar to that of Theorem 4.1 to show that

$$T^{(k)}_{j_1,\dots,j_k} = R_1 \otimes \dots \otimes R_k,$$

where R_i is as defined in the theorem. Hence the result follows. □

Analogous to Theorem 5.2, we have

Theorem 6.6. *Consider an r-D neighbourhood σ-automaton on a k-dimensional mixed grid $G(l_1,\dots,l_k)$. Then α is a root of the characteristic polynomial of the transition matrix of the σ-automaton iff α is of the form*

$$\sum_{1\leqslant j_1<\dots<j_i<\dots\leqslant k} \alpha_{j_1}\dots\alpha_{j_i} \quad \text{for some choice of } \alpha_1,\dots,\alpha_k.$$

Here α_i is a root of $p_i(x)$, where $p_i(x)$ is as in Theorem 6.3.

Proof. Let ε be an arbitrary scalar and consider the product

$$\begin{aligned}&(I_{l_1} + \varepsilon A_{l_1}) \otimes (I_{l_2} + \varepsilon A_{l_2}) \otimes \dots \otimes (I_{l_k} + \varepsilon A_{l_k})\\ &\quad = I_{l_1} \otimes \dots \otimes I_{l_k} + \varepsilon(I_{l_1} \otimes I_{l_2} \otimes \dots \otimes A_{l_j} + \dots + A_{l_1} \otimes I_{l_2} \otimes \dots \otimes I_{l_k})\\ &\qquad + \dots + \varepsilon^k A_{l_1} \otimes \dots \otimes A_{l_k},\end{aligned}$$

where A_{l_i} is S_{l_i} or C_{l_i} according as the ith dimension has null or periodic boundary condition. The characteristic roots of the left-hand side are

$$(1+\varepsilon\alpha_1)(1+\varepsilon\alpha_2)\dots(1+\varepsilon\alpha_k) = 1 + \varepsilon(\alpha_1+\dots+\alpha_k) + \dots + \varepsilon^k\alpha_1\dots\alpha_k,$$

where α_i is a root of $p_i(x)$.

Let $\underline{x}$ be an eigenvector corresponding to a root. Then,

$$\begin{aligned}&(\underline{x} - (I_{l_1} \otimes \dots \otimes I_{l_k})\underline{x}) + \varepsilon((\alpha_1+\dots+\alpha_k)\underline{x}\\ &\quad -(I_{l_1} \otimes I_{l_2} \otimes \dots \otimes A_{l_j} + \dots + A_{l_1} \otimes I_{l_2} \otimes \dots \otimes I_{l_k})\underline{x})\\ &\quad + \dots + \varepsilon^k((\alpha_1\dots\alpha_k)\underline{x} - (A_{l_1} \otimes \dots \otimes A_{l_k})\underline{x}) = 0.\end{aligned}$$

Since ε is arbitrary, all coefficients of ε^i are 0 $(0\leqslant i\leqslant k)$. From this the result follows. □

Corollary 6.1. *An r-D neighbourhood σ (resp. σ^+)-automaton on a k-dimensional mixed grid is non-invertible iff for some choice of $\alpha_1,\dots,\alpha_k$ we have*

$$\sum_{1\leqslant j_1<\dots<j_i<\dots\leqslant k} \alpha_{j_1}\dots\alpha_{j_i} = 0 \ (\text{resp. } 1)$$

where α_i's are as described in the above theorem.

In particular, we have

Proposition 6.1. *For $G_l(l)$ with null boundary condition, an r-D neighbourhood σ (resp. σ^{-1})-automaton is non-invertible if the coefficient of x^{l-r} in $\pi_{l+1}(x)$ is 0 (resp. 1).*

Proof. Here we have to consider only $\pi_{l+1}(x) = x^l - a_{l-1}x^{l-1} + \cdots + a_0$ with $\sum \alpha_i = a_{l-1}$, $\sum \alpha_1\alpha_2 = a_{l-2}$, …, $\alpha_1 \ldots \alpha_l = a_0$, where α_i's are roots of $\pi_{l+1}(x)$. From this the result follows. □

Remark 6.1. If in the above proposition all dimensions have periodic boundary condition, then we will have to consider the characteristic polynomial for C_l instead of $\pi_{l+1}(x)$.

7. Conclusion and open problems

In this article we have developed necessary and sufficient conditions for the invertibility of σ (σ^{-1})-automata on multidimensional orthogonal grids with different boundary conditions. These conditions have been obtained in terms of the roots of π-polynomials. Also we have tried to relate this to the number theoretic properties of the number of dimensions and lengths of the dimensions.

For symmetric (all dimensions having equal lengths l) σ-automata, we have to consider only one π-polynomial (π_{l+1}). In this case the invertibility is directly related to a sum of subset of the roots of π_{l+1}. In trying to relate this to number theoretic properties, we are able to settle for k (dimension) even or l odd. The case for k odd, l even could not be settled completely (see Section 5.1). This is intimately related to the subset sum of roots of π_{l+1} and settling the invertibility question will also settle the question of when such an arbitrary subset sum will take values in the base field.

For symmetric σ -automata, we could obtain similar results, though a few cases remain unsettled. We were able to extend the subset sum necessary and sufficient condition to asymmetric as well as folded and mixed grids. Also for these grids we have been able to point out special cases where the invertibility can be settled in terms of number theoretic properties. Other cases which remain unsettled can form the subject of further research. We have also generalised the concept of non-orthogonal nearest neighbourhood. Invertibility of σ-automata with such neighbourhood have been characterised in terms of the roots of π-polynomials. However, in this case number theoretic characterisation of invertibilty remains open.

Acknowledgements

The authors are grateful to the referee for several comments, which have greatly improved the presentation of the paper.

References

[1] A.V. Aho, J.D. Ullman, Principles of Compiler Design, Addison-Wesley, Reading, MA, 1977.
[2] S. Barnett, Matrices, Methods and Applications, Clarendon Press, Oxford, 1990.
[3] R. Barua, S. Ramakrishna, σ-game, σ^{-}-game, and two dimensional cellular automata, Theoret. Comput. Sci. 154 (1996) 349–366.
[4] D.R. Chowdhury, Theory and application of additive cellular automata for reliable and testable VLSI circuit design, Ph.D Dissertation, Dept. of Comput. Sci. & Engg., Indian Institute of Technology, Kharagpur, India, 1992.
[5] R. Lidl, H. Niederreiter, Encyclopedia of Mathematics, Finite Fields, Cambridge University Press, Cambridge, 1986.
[6] A. Lindenmayer, Mathematical models for cellular interactions in development, J. Theoret. Biol. 18 (1968) 280–299.
[7] O. Martin, A.M. Odlyzko, S. Wolfram, Algebraic properties of cellular automata, Comm. Math. Phys. 93 (1984) 219–258.
[8] M. Mignotte, Mathematics for Computer Algebra, Springer, Berlin, 1991.
[9] D.H. Pelletier, Merlin's magic square, Amer. Math. Monthly 94 (1987) 143–150.
[10] K. Sutner, On σ-automata, Complex Systems 2 (1988) 1–28.
[11] K. Sutner, Linear cellular automata and the Garden-of-Eden, Math. Intelligencer 11 (1989) 49–53.
[12] M. Serra, et al., The analysis of one dimensional cellular automata and their aliasing properties, IEEE Trans. Comput. Aided Design of Circuits and Systems 9 (1990) 767–778.
[13] K. Sutner, The σ-game and cellular automata, Amer. Math. Monthly 97 (1990) 24–34.
[14] K. Sutner, σ-automata and n-polynomials, Tech. Rep. CS-9408, 6 December, Stevens Institute of Technology, 1994.
[15] K. Sutner, σ-automata and Chebyshev polynomials, see http://www.cs.cmu.edu/~Sutner.
[16] S. Wolfram, Statistical mechanics of cellular automata, Rev. Modern Phys. 55 (1983) 601–644.
[17] S. Wolfram, Theory and Applications of Cellular Automata: Including Selected Papers 1983–1986, World Scientific, Singapore, 1986.