M. Tech. (Computer Science) Dissertation Series

PROBLEMS IN TWO-DIMENSIONAL ADDITIVE CELLULAR AUTOMATA

a dissertation submitted in partial fulfilment of the requirements for the M.Tech. (Computer Science) degree of the Indian Statistical Institute

By

Prateek Mazumdar

under the supervision of

Dr. Rana Barua

and

Dr. Pabitra Pal Chowdhury

INDIAN STATISTICAL INSTITUTE
203, Barrackpore Trunk Road
Calcutta-700 035

ACKNOWLEDGEMENTS

I am indebted to my Supervisors Dr. R. Barua and Dr. P. Pal Chowdhury, for their guidance and assistance, throughout the course of this work. Dr. Barua has always helped me with his own results, and we had long hours of discussions, without which this work would not have been possible. Dr. P. Pal Chowdhury has always kept a keen eye on my progress, and I am particularly grateful to hjm, for his kind assistance. I would like to thank my teacher Prof. K. Sikdar, whose lectures have given me the real flavour of Computer Science. He has also helped me out of my problems during the course of study, whenever I faced one. I also thank S. Ramakrishnan for permitting me to use some of his results.

I am extremely grateful to my friends and classmates, particularly Palash Sarkar and Indranil Ojha, for their help, throughout the course.

I would thank Sri Samir Kumar Chakraborty, who took all the pains to type out the material, in so short a time.

Lastly, I would like to thank I.S.I. for providing me all the facilities without which this work could not have been completed.

Abstract

Cellular automata are simple systems, dynamic in nature, and yet capable of exhibiting extremely complicated behaviour.

The present work deals with, analysing certain features of additive, two-dimensional cellular automata. The properties were studied using matrix algebraic methods. In all our proofs, we have worked, using only one approach, even though other equivalent methods have been discussed briefly.

The work has been mostly theoretical in nature, but the application aspect has not been completely left out. Efficiency of certain special 2-d CA's, regarding the generation of pseudo-random sequences, was investigated.

CONTENTS

Introduction to Cellular Automata

Cellular automata are mathematical idealisations of physical systems , where space and time are discrete and the physical quantities take on a finite set of discrete values. They are discrete dynamical systems which exhibit complex and varied behaviour. A cellular automaton consists of a regular uniform lattice or an array (which could be multi-dimensional and it is the dimension of this array, which is referred to as the dimension of the cellular automata), which in the general case could be infinite in extent. Our discussion would always be restricted to finite cellular automata, i.e., we shall always assume that the extent of the lattices along any dimension, is finite.

The evolution of the cellular automata is in discrete time steps in which each site or cell (which is a position in the lattice) carries a value. The value of the variable in a particular site is affected by the values of the variables at the sites in its neighbourhood (which is a collection of sites specified in advance) on the previous time step according to certain local rule (which is also specified in advance). Thus the variables at each site are updated synchronously,based on the values of the variables in their neighbourhood at the preceeding time step, following the local rules corresponding to each site. We explain the above concept with a simple example. In the simplest case, a cellular automaton consists of a line of sites with each site carrying a value 0 or 1. The rule for evolution could take the value of a site at a particular time step to be the sum modulo two of the values of its nearest neighbours at the previous time step. This (one dimensional) CA is referred to as Rule-90 CA (cf. Wolfram [28]).

We now give a brief introduction to the origination and applicability of cellular automata.

Cellular automata were originated by Von Neumann and Ulam under the name of 'cellular spaces' with the specific purpose of modelling biological self-reproduction. Since then, cellular automata has found a wide range of applications in areas like Physics, Chemistry, Biology, Number Theory and Computer Science.

Physical systems containing various discrete elements with local interactions can be viewed as a system of differential equations with various initial and boundary conditions. This may be conveniently modelled using cellular automaton, by introducing finite differences and discrete variables.

Also cellular automaton can provide models for kinetic aspects of phase transitions (e.g. Harvey et al. **(cf. [28])**, it is possible that crystal growth could be described by aggregation of discrete packets,(Langer [16]) with a local growth inhibition effect associated with local releases of latent heat and thereby treated as a celular automaton.

Many biological systems have also been modelled using cellular automata (Lindenmayer [17], Herman [13], Ulam [30] etc.). The development of structure and patterns in the growth of organisms often appear to be governed by very simple local rules and is therefore reasonably well explained using cellular automaton model.

Cellular automata have also been used to study problems in number theory (Miller [21], Sutton [27]). In a typical case, successive differences in a sequence of numbers (such as primes), reduced with a small modulus, are taken and then the geometry of zero regions is investigated.

In Computer Science, cellular automaton has been used for highly parallel multipliers (Atrubin [2], Cole [8]), sorters (Nishio [20]), etc. They could be used as parallel processing computers. In two dimensions cellular automata have been used extensively for image processing and visual pattern recognition (Deutsch [12], Rosenfeld [23], Sternberg [25]). The computational capabilities have been studied minutely (Codd [7], Burks [6], Banks [3], etc.) and it has been shown that certain cellular automaton are capable of being used as general purpose computers, and hence could be used as general paradigms for parallel computation. Applications of CA in the field of VLSI have also been investigated (see [9]). Thus we see that, since cellular automaton models a variety of physical, biological and computational systems, the mathematical analysis of the general cellular automaton features could yield general results concerning the behaviour of many complex systems.

Formalism

In the following discussions, we shall always restrict ourselves to one and two dimensional cellular automata. Also, we shall consider that each site carries a value 0 or 1 i.e. the states of a site are entries from Z_2.

One dimensional Cellular Automata

Neighbourhood of a 1-d CA :

Definition

A k-neighbourhood system of size 'n', is a sequence $N = \{N_i : 0 \leq i \leq n-1\}$, where each N_i, is a point of Z_n^k. Each neighbourhood of N_i is a k-tuple of points of Z_n and we write $N_i = (n_1^i, n_2^i, \ldots, n_k^i)$ where each $n_j^i \varepsilon Z_n$.

We now give the formal definition of a finite cellular automata.

A 1-dimensional finite cellular automata is quadruple (Q, Z_n, N, F) where :-

(i) Q is a non-empty finite set of cell states.

(ii) $N = \{N_i : 0 \leq i \leq n-1\}$, is a k-neighbourhood system where each N_i is the neighbourhood of the ith cell or site.

(iii) Z_n = ring of integers modulo n, which specifies and enumerates the n cells (sites), in cyclic order.

(iv) $F = \{f_i : 0 \leq i \leq n-1\}$ is a sequence of maps $f_i : Q^k \longrightarrow Q$ called the <u>local rules</u>, f_i being the local rule of the ith cell. (In our case we have $Q = Z_2$.)

<u>Note</u> : In the above definition we have implicitly assumed that the n cells are visited in a cyclic manner, due to the the operation of addition modulo n, in Z_n . That is we have considered that the sequence of n sites are arranged along a <u>circle</u> instead of being arranged along a <u>line</u> so that the first and the last cells are considered to be adjacent. This type of site arrangement is referred to as <u>periodic boundary condition</u> . By virtue of this, any cell or site can have any number of sites ($\leq$ n-1) to its left or right, as its neighbours.

There is another type of boundary condition, which is commonly called <u>null boundary condition</u> ,in which the sites are assumed to be arranged in a linear fashion making the end-points fixed and thus in this case we do not consider the first and the last sites to be adjacent. In such CA the cells to the left of the first and those to the right of the last are assumed to be always in state 0. Thus when we consider a cellular automaton with null boundary conditions, a slight modification of the neighbourhood criterion, in the above definition (as this is the only point where they differ), enables us to extend the same definition, to cellular automata with null boundary conditions.

<u>Definition</u>

The cellular automaton defined above is said to be <u>uniform</u> if every site has the same neighbourhood characteristics and the same local rule, i.e. $f_i = f$ and $N_i = N \; \forall \, i$, $0 \leq i \leq n-1$. In this case the CA will be written as (Q, Z_n, N, F).

If this is not the case then the cellular automaton is said to be <u>hybrid</u>.

<u>Configuration of a Cellular Automaton</u> :

<u>Definition</u>

A map $c : Z_n \rightarrow Q (= Z_2)$,is called a <u>configuration</u> of a cellular automaton. Intuitively the configuration at any time step is the sites carrying their respective values of states at that time step.

We denote by 'C',the set of all possible configurations of the cellular automaton.

Definition

The global transition function or rule induced by each of the local rules,is the map, $T : C \to C$ given by :-

$T(c)(i) = f_i(c(i+n_1^i), c(i+n_2^i), \ldots, c(i+n_k^i))$ where '+' denotes addition modulo n.

Note : This definition is in case of cellular automaton with periodic boundary condition ,as then the neighbours of the ith site are the sites numbered $(i+n_1^i), \ldots, (i+n_k^i)$ and the corresponding states are $c(i+n_1^i), \ldots, c(i+n_k^i)$ where '+' denotes addition modulo n.

In case of a cellular automata with null boundary conditions, this definition can easily be modified appropriately (If the sites are numbered as $0 \ldots n-1$ and if the sum $(i+n_j^i)$ exceeds $n-1$ for some j, then the site value is taken to be 0).

Definition

A cellular automaton is said to be linear or additive , iff each $f_i \varepsilon F$ is so, that is for each 'i',there exists $a_1^i, a_2^i, \ldots, a_k^i \ \varepsilon\ Q$ (if the ith site has a neighbourhood of size k) such that $f_i(x_1, \ldots, x_k) = \sum_{j=1}^{k} a_j^i x_i$. In our case since $Q = Z_2$

this reduces to $f_i(x_1,\ldots,x_k) = \sum_{i=1}^{k} x_i$.

Remark : The set of configurations 'C' is clearly $Q^n = Z_2^n$, which is a vector space over Z_2 .

Theorem ([4])

A cellular automaton $M = (Z_2, Z_n, \{N_i\}, \{f_i\})$ is additive or linear iff its global transition function $T : Z_2^n \to Z_2^n$ is a linear transformation or a vector space homomorphism.

Also given any linear map $G : Z_2^n \to Z_2^n$, G can be realised as a global transition function of some additive cellular automaton over Z_2 .

Not much theoretical development has been achieved in the case of non-linear cellular automata. There has only been some experimental studies on the behaviour of certain special types of non-linear cellular automata ([28]). In case of additive cellular automaton, we can take advantage of the fact that the global transition rule is a linear transformation and then make use of the properties of this linear transformation , to study the evolution of the cellular automaton with time. A number of mathematical techniques exist in order to analyse situations of these types but unfortunately in the non-linear case, since the global transition function is not linear, no such general method exists.

Henceforth, all our discussions will be restricted to the additive case only.

Since the global transition rule in case of an additive CA is a linear transformation, it is characterised by an nxn matrix, where 'n' is the number of sites in the 1-d CA. We regard each configuration as a column vector $\underline{x}$ (nx1) and then the global transition function T, can be written as : $T(\underline{x}) = A\underline{x}$ where A is the matrix of T, taken relative to the cannonical basis, and is called the characteristic matrix of the CA ([4]). This important fact, regarding the global transition function, was observed by Aso and Honda, Sutner and others ([1], [26]). Extensive use of matrix algebra for the study of additive 1-D CA, was done by Das et al. ([10], [11]). Another elegant and important approach due to Martin et al. ([19]), is by the use of the characteristic polynomials. At any time step 't', if the values of the sites are denoted by $a_0^{(t)}, a_1^{(t)}, \ldots, a_{n-1}^{(t)}$, then the configuration of the cellular automaton is represented by the characteristic polynomial $A^{(t)}(x) = \sum_{i=0}^{n-1} a_i^{(t)} x^i$ (coefficient of x^i gives the value of the ith site). Multiplication of the polynomial by x^{-1} (resp. x) modulo the fixed polynomial (x^n-1) yields a polynomial which represents the configuration obtained from the above by a cyclic shift to the left (resp. right). Thus the time evolution of the cellular automaton is obtained by multiplying the characteristic polynomial $A^{(t)}(x)$ by a fixed dipolynomial $T(x)$ (a dipolynomial in x is one in which powers of x as well as x^{-1} are present) and then reducing the product, modulo (x^n-1). Thus, more formally,

$$A^{(t+1)}(x) = [T(x)A^{(t)}(x)]\mathrm{mod}(x^n-1) .$$

The approach by characteristic polynomials has been extensively used by Martin, Wolfram and Odlyzko ([19]), for studying the properties of uniform 1-d additive cellular automaton with periodic boundary conditions. We shall always work with the matrix algebraic approach, since, as was observed by Das et al. ([10]) hybrid additive CA can easily be studied by such methods. From the relation $T(\underline{x}) = A\underline{x}$, it is evident that the time evolution of the cellular automaton is completely characterised by the matrix A and so we need to examine it carefully.

<u>Property</u> ([4]). In case of a 1-d cellular automata with <u>periodic</u> boundary conditions and with <u>uniform</u> local rule, one can show that the characteristic matrix is a <u>circulant</u> matrix (By a circulant matrix, we mean a matrix, each row of which is an 'r' fold cyclic shift of the previous row towards the left or towards the right, for some positive integer, r). The matrix no longer remains circulant, if we consider the same set of local rules but now with <u>null</u> boundary conditions.

We give an example :

Consider the Rule-90 ([28]) 1-d cellular automaton, where each site consists of either 0 or 1 and the rule is to replace the site value at any time step by the sum modulo 2 of the site values of its nearest (i.e. adjacent) neighbours, at the previous time step.

When we consider this rule with <u>periodic</u> boundary conditions, the characteristic matrix A looks like :

$$A = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 1 & 0 \,.. & 0 & 0 \\ 0 & 1 & 0 & 1 \,.. & 0 & 0 \\ \vdots & & & & & \\ 0 & 0 & \cdots\cdots & 1 & 0 & 1 \\ 1 & 0 & \cdots\cdots & 0 & 1 & 0 \end{bmatrix}_{n \times n}$$

Note that the matrix is <u>circulant</u> since each row is a <u>one</u> fold cyclic shift towards the <u>right</u>, of the previous row.

In case of the same automaton but now with <u>null</u> boundary conditions, we can show that :

$$A = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 1 & 0 & 1 \,.. & 0 & 0 \\ \vdots & & & & & \\ 0 & 0 & \cdots\cdots & 1 & 0 & 1 \\ 0 & 0 & \cdots\cdots & 0 & 1 & 0 \end{bmatrix}_{n \times n}$$

The matrix is no longer circulant. (It differs from its periodic counterpart only at the positions $a_{0,n-1}$ and $a_{n-1,0}$, the rest being identical.)

State Transition Graph

Just as in the case of a deterministic or a non-deterministic finite automaton, it is customary to represent the behaviour by means of a state transition graph, same is done in case of cellular automaton too. The state transition graph is easy to visualise and is thus convenient in studying the behaviour of the automaton.

Definition

The state transition graph of a cellular automaton, also referred to as the state transition diagram, is a directed graph, each of whose nodes consist of a particular configuration of the automaton. There is a directed arc from one node to another, iff the configuration represented by the second node, is reachable in one time step (i.e. by one application of the global transition function) from the configuration represented by the first node (note that,this definition is perfectly general, and thus holds for any cellular automaton).

In our case with 1-d CA, if $\underline{x}$ and $\underline{y}$ are configurations represented by two nodes, then there is an arc from $\underline{x}$

to $\underline{y}$, iff $\underline{y} = T(\underline{x})$, where T is the global transition function.

Certain simple properties of the state transition graph are easily observed.

1. Every node in the state transition diagram has outdegree exactly one, whereas the indegrees can differ.

This follows trivially, since 'T' is a well-defined map, therefore every configuration has an unique successor and thus the outdegree of every node in the state transition graph has to be one , but since a particular configuration may have several or no predecessors, the indegrees differ.

2. The state transition graph consists of cycles.

This is true, since there are only finitely many possible configurations, the cellular automaton evolving out from one configuration must ultimately enter into a loop, in which a sequence of configurations are visited repeatedly. This is represented by a directed cycle in the state transition graph.

3. If the cellular automaton is additive , we have identical trees rooted at every configuration on a cycle (see [19]).

The following results have been proved in case of 1-d additive cellular automaton ([19]).

1. In case of a Rule-90 1-d CA with periodic boundary conditions, configurations containing an odd number of sites with value one, can never be generated in the evolution of the cellular automaton. They can only occur as initial states (such configurations which do not have any predecessor, have been named as Garden of Eden configurations).

2. For a Rule-90 1-d CA with periodic boundary conditions, the fraction of the number of configurations having no predecessor, is '$\frac{1}{2}$' for n odd and '$\frac{3}{4}$' for 'n' even (cf. [19]).

3. In case of an additive 1-d CA, two configurations $\underline{x}$ and $\underline{y}$ yield the same configuration after one time step, iff the configuration $\underline{x} - \underline{y}$ yields the null configuration i.e. $\underline{0}$ after one time step (i.e., $T(\underline{x}) = T(\underline{y})$ iff $T(\underline{x}-\underline{y}) = \underline{0}$, which follows from the fact that T is linear).

4. Configurations in a Rule-90 CA with periodic boundary conditions, which have at least one predecessor (i.e. they are not the Garden of Eden configurations), have exactly two predecessors if 'n' is odd and exactly four if 'n' is even .

5. For 'n' odd, in case of a Rule-90 1-d CA with periodic boundary conditions, a tree consisting of a single arc is rooted at every node, on each cycle in the state transition graph.

6. For an additive CA, every reachable configuration, i.e. a configuration with a predecessor, has the same number of predecessors ([19]).

We now look at certain properties of the cycle lengths of 1-d CA's. Later on, we shall show that many of these results carry over to 2-d CA's too.

Definition

For a 1-d cellular automaton, having n-sites, we denote by π_n, the length of largest possible cycle, i.e. the length of a maximal cycle (as we shall see later on, there could be several such cycles which have the maximum possible length).

The following results have been proved ([19]).

1. In case of a uniform, additive 1-d CA with periodic boundary conditions, there is a one-one correspondence between the evolutions of the CA starting with any two configurations having only a single non-zero site (i.e. any two configurations that correspond to a cannonical

basis, by treating the configuration space to be a vector space over Z_2).

As a result of this, the cycle lengths obtained by starting initially with any configuration, which has a single non-zero site, are identical.

2. In case of a uniform, additive 1-d CA with periodic boundary conditions, the lengths of all cycles divide the length of a cycle obtained by starting with an initial seed having only one non-zero site.

Thus it follows that these cycles correspond to the maximum cycle-length π_n, or in other words, these are all maximal cycles.

3. In case of a Rule-90 1-d CA with periodic boundary conditions, having n-sites, if n is of the form '2^k', for some $k > 0$, then $\pi_n = 1$. Also if n is even, but not of the form 2^k, then $\pi_n = 2\pi_{n/2}$.

Definition

Multiplicative order function $ord_n(k)$ is the least positive integer 'j', such that $k^j \equiv 1 \bmod n$. According to the results known from group theory, this definition makes sense only when k and n are relatively prime.

Multiplicative suborder function $\mathrm{sord}_n(k)$ is the least positive integer j such that $k^j \equiv \pm 1 \bmod n$. Again as before, this makes sense only when k and n are relatively prime.

The following result is known to hold ([19]). For a uniform, additive 1-d CA having n-sites and with periodic boundary conditions, if n is odd, then π_n/π^* where $\pi^* = 2^{\mathrm{ord}_n(2)} -1$. If the local rule is symmetric, then we take $\pi^* = 2^{\mathrm{sord}_n(2)} -1$.

This much for 1-d CA. We now focus our attention on 2-d CA's. As before we shall always work with the field Z_2 and consider only additive CA's, i.e. the local rule corresponding to each site will be taken to be additive.

Introduction to 2-dimensional Cellular Automata

In case of 1-d cellular automata we considered the sequence of sites to be arranged on a straight line, or on a circle, accordingly as the choice of boundary conditions was assumed to be null or periodic. A 2-d CA is a generalisation of 1-d CA, where the sites are arranged in a rectangular lattice, which can be thought of as a two-dimensional grid, with connections among the neighbouring cells. Thus a 2-d CA can be thought of an 'mxn' array with 'm' rows, 'n' columns and mn sites. The configuration of a 2-d CA can then be represented by a mxn binary matrix, with each site carrying a value 0 or 1. The evolution of a site may depend either on the orthogonal neighbours (i.e. the horizontal and vertical neighbours), and this is called the Type-I neighbourhood or it could depend on the neighbours which are diagonally adjacent, which is called the Type-II neighbourhood. If f_{ij} denotes the local rule associated with the (i,j)th site ($0 \leq i \leq m-1$, $0 \leq j \leq n-1$), and if $q_{i,j}^{(t)}$ denotes the state of the (i,j)th site at time step 't', then at time step t+1 we have

$$q_{i,j}^{(t+1)} = f_{ij}(q_{i-1,j}^{(t)}, q_{i+1,j}^{(t)}, q_{i,j-1}^{(t)}, q_{i,j+1}^{(t)}, q_{i,j}^{(t)}),$$

in case of a type-I CA, and

$$q_{i,j}^{(t+1)} = f_{ij}(q_{i-1,j-1}^{(t)}, q_{i-1,j+1}^{(t)}, q_{i+1,j-1}^{(t)}, q_{i+1,j+1}^{(t)}, q_{i,j}^{(t)}),$$

in case of a type-II CA.

As in the case of 1-d CA, for a 2-d CA we also have that, each local rule f_{ij} gives rise to the global transition rule T, which is additive iff each f_{ij} is so.

In case of 2-d CA, the configuration space consists of all the 2^{mn} configurations, i.e. all possible mxn binary matrices. As in case of 1-d CA, the configuration space of a 2-d CA is also a vector space over Z_2, where we treat each configuration as a matrix. The dimension of this vector space is mn and the corresponding cannonical basis is the set of configurations E_{ij}, $0 \leq i \leq m-1$, $0 \leq j \leq n-1$ and the matrix E_{ij} has a 1 only at the (i,j)th entry, all other entries being 0's. The global transition function T, which as before, is a mapping from the configuration space into itself, becomes a linear transformation iff the 2-d CA is additive.

We now discuss the nature of boundary conditions, in the context of 2-d CA.

Null boundary conditions :

Here, we consider the fact that, the cells in the rightmost column, have right neighbours which are always in state 0, and cells in the leftmost column have left neighbours also having a constant state 0. Similarly, a cell on the uppermost row of the configuration,has a top neighbour and the one on the lowermost row has a bottom neighbour, both of which are always in state 0.

Periodic boundary conditions :

In this case, we assume that the topmost row is adjacent to the lowermost row and the leftmost column is adjacent to the rightmost column, i.e. if the configuration is an mxn matrix, then (0,j)th site and (m-1,j)th site are considered to be adjacent, as also (i,0)th site and (i,n-1)th site are considered to be adjacent, for all $0 \leq i \leq m-1$ and $0 \leq j \leq n-1$. This is as if the 2-d lattice were folded up cylindrically in the horizontal and vertical directions to make it look like a 'torus'.

Mathematical formulation :

As in the case of 1-d CA, the global behaviour of an additive, uniform 2-d CA could be studied using characteristic polynomials and characteristic matrices.

The characteristic polynomial corresponding to a configuration of a mxn 2-d CA at time step 't' is, ([19])

$A^{(t)}(x,y) = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} a_{ij}^{(t)} x^i y^j$, where $a_{ij}^{(t)}$ represents the site value of the (i,j)th cell at time 't'. As before, this polynomial is multiplied by a fixed polynomial, (which represents the local rule) and the resulting product gives the characteristic polynomial corresponding to the configuration at time step t+1.

If we think of the global transition rule as a linear transformation, and characteristic it by a single matrix, since now each vector corresponds to a mxn matrix, the matrix characterising the linear transformation, will be of dimension mn x mn . This large dimension makes the implementation on a computer, computationally inefficient. To overcome this difficulty we use a very elegant technique due to S. Ramakrishnan ([22]). It can be shown that in case of a Type-I 2-d CA with uniform vertical dependency along each row, and uniform horizontal dependency along each column, the global transition function can be written as : $T(X) = AX + XB$ where X is mxn, A is mxm and B is nxn, which makes $T(X)$ mxn . The matrix A accounts for the vertical dependency, and the matrix B accounts for the horizontal dependency. Thus in this formulation, the two dependencies are dealt with separately.

We explain the above concept, with an example.

Suppose we have a Type-I CA with uniform <Rule-90, Rule-90> local rule, and periodic boundary conditions. We had already introduced Rule-90 in case of 1-d CA, which was sum modulo 2 of the two nearest sites (adjacent ones). By <Rule-90, Rule-90> local rule in a 2-d CA, we shall mean that, the vertical dependency of a site is simply the sum modulo 2 of its nearest neighbours, and this is indicated by the 1st Rule-90; the 2nd Rule-90 implies that, in the horizontal direction, we also consider the same rule, i.e., sum modulo 2 of adjacent sites. So the overall rule becomes sum modulo 2 of the 4 nearest neighbours that are orthogonally adjacent. More formally, this means :

$$q_{ij}^{(t+1)} = (q_{(i-1)\mathrm{mod}\ m,j}^{(t)} + q_{(i+1)\mathrm{mod}\ m,j}^{(t)} + q_{i,(j-1)\mathrm{mod}\ n}^{(t)} + q_{i,(j+1)\mathrm{mod}\ n}^{(t)})\ \mathrm{mod}\ 2,$$

where $q_{ij}^{(t)}$ is the state of the (i,j)th site, at time step 't'. In this case, checking that $T(X) = AX + XB$ holds, is routine, where

$$A = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 1 \\ 1 & 0 & 1 & 0.. & 0 & 0 \\ 0 & 1 & 0 & 1.. & 0 & 0 \\ \vdots & & & & & \\ 0 & 0 & \dots & 1 & 0 & 1 \\ 1 & 0 & \dots & 0 & 1 & 0 \end{bmatrix}_{m \times m}$$

and B is the same matrix, but with dimension nxn .

Another important fact which is evident from the expression $T(X) = AX + XB$, is that, we can treat A and B as the characteristic matrices of the corresponding 1-d CA's and the local rules for these 1-d CA's, are the rules for the vertical and horizontal dependencies of the 2-d CA, treated separately.

Thus we have seen that, the relation $T(X) = AX + XB$ can be viewed as the superposition of two 1-d CA's, by considering the matrices A and B (which characterise the vertical and horizontal dependencies respectively) as the characteristic matrices of two 1-d CA's. Thus it is not unnatural, that many results which hold for 1-d CA's, have a natural extension to their corresponding 2-d counterparts. Some such results will be proved shortly.

In case of Type-II CA, the global transition function can be shown to be of the form, $T(X) = AXB$, which is also a linear transformation. Here too X is $m \times n$, A is $m \times m$ and B is $n \times n$ so that $T(X)$ is $m \times n$. Here again, we assume uniform rule along each row. The discussion regarding boundary conditions is similar, only a little modification is needed in case of periodic boundary conditions as compared to Type-I CA, null boundary conditions being similar. In case of a Type-I 2-d CA with periodic boundary conditions, we had that $(0,j)$th site was adjacent to the $(m-1,j)$th site and the $(i,0)$th site was adjacent to the $(i,n-1)$th site, for all $0 \leq i \leq m-1$ and $0 \leq j \leq n-1$. In case of 2-d CA, since we consider diagonal adjacency instead of orthogonal adjacency, we take $(m-1,(j-1) \bmod n)$th site to be the neighbour of $(0,j)$th site, and $((i-1) \bmod m, n-1)$th site to be the neighbour of $(i,0)$th site. In general, given a site (i,j), the four nearest neighbours are :

$((i-1) \bmod m, (j-1) \bmod n)$, $((i-1) \bmod m, (j+1) \bmod n)$,

$((i+1) \bmod m, (j-1) \bmod n)$, $((i+1) \bmod m, (j+1) \bmod n)$,

in case of <u>periodic</u> boundary conditions.

At this point, it is worthwhile mentioning some of the work in 2-d CA, done by D. Roy Chowdhury, P. Subbarao and P. Pal Chowdhuri ([24]). They extended the theory of 1-d CA built around matrix algebra, to characterise 2-d CA. In the paper emphasis was laid on a special class of additive 2-d CA, known as the restricted vertical neighbourhood (RVN) CA. In this class of 2-d CA's, the vertical dependency of a site is restricted to either the sites on its top or bottom, but not both. The characteristic matrix representing the global transition rule was an mn x mn one if the CA is mxn. The technique involved was to appropriately partition the T matrix into blocks of uniform size, and then the properties of these block matrices were usedto predict the properties of the 2-d CA behaviour. The reason for working with RVN CA's, is that, the characteristic matrix of an RVN CA becomes block-triangular, (so we only have the blocks in the upper or lower triangle, including the diagonal).

Our approach of choosing the global transition rule to be of the form $T(X) = AX + XB$ is somewhat more general than the above and more powerful, as we shall show later. We shall present equivalent proofs of some of the properties of 2-d RVN CA's (that have been previously done using the 'partitioning technique') using the functional form , $T(X) = AX + XB$.

We now turn our attention to some of the properties of 2-d CA's. Many of these results, are the extensions of the results that are known to hold for 1-d CA's, to their corresponding 2-d counterparts.

Theorem 1

(a) Let A and B be the characteristic matrices of a Type-I 2-d CA. Let $X^{(0)}$ represent the initial configuration. Then the configuration $X^{(t)}$, after 't' time steps, is given by :

$$X^{(t)} = A^tX^{(0)} + \binom{t}{1}A^{t-1}X^{(0)}B + \binom{t}{2}A^{t-2}X^{(0)}B^2 + \ldots + X^{(0)}B^t ,$$

where $\binom{t}{j} = ({}^tC_j) \bmod 2$. [Equivalently : $T^t(X) = A^tX + \binom{t}{1}A^{t-1}XB + \ldots + XB^t$, where $T(X) = AX + XB$ for any configuration X]

(b) Let A and B be the characteristic matrices of a Type-II 2-d CA. Then we have : $X^{(t)} = A^tX^{(0)}B^t$ where $X^{(0)}$ is the initial seed. [Equivalently : $T^t(X) = A^tXB^t$ where $T(X) = AXB$ for any configuration X]

Proof.

Part (a). We proceed by induction on 't'.
For $t = 1$ we have $X^{(1)} = T(X^{(0)}) = AX^{(0)} + X^{(0)}B$ and thus the result holds for $t = 1$.

Assume the result to be true for $t = r$, i.e.

$$X^{(r)} = A^r X^{(0)} + \binom{r}{1} A^{r-1} X^{(0)} B + \binom{r}{2} A^{r-2} X^{(0)} B^2 + \dots + X^{(0)} B^r.$$

<u>Case</u> : $t = r+1$

$$X^{(r+1)} = T(X^{(r)}) = AX^{(r)} + X^{(r)}B$$

$$= A(A^r X^{(0)} + \binom{r}{1} A^{r-1} X^{(0)} B + \dots + \binom{r}{j} A^{r-j} X^{(0)} B^j + \dots$$
$$\dots + X^{(0)} B^r)$$
$$+ (A^r X^{(0)} + \binom{r}{1} A^{r-1} X^{(0)} B + \dots + \binom{r}{j} A^{r-j} X^{(0)} B^j + \dots$$
$$\dots + X^{(0)} B^r) B$$
$$= A^{r+1} X^{(0)} + [\binom{r}{0} + \binom{r}{1}] A^r X^{(0)} B + [\binom{r}{1} + \binom{r}{2}] A^{r-1} X^{(0)} B^2 + \dots$$
$$\dots + [\binom{r}{j-1} + \binom{r}{j}] A^{r+1-j} X^{(0)} B^j + \dots + X^{(0)} B^{r+1}.$$

Now we have the following identity :

$$^rC_{j-1} + {}^rC_j = {}^{r+1}C_j .$$

So, $({}^{r+1}C_j) \bmod 2 = ({}^rC_{j-1}) \bmod 2 + ({}^rC_j) \bmod 2$ i.e.,

$\binom{r+1}{j} = \binom{r}{j-1} + \binom{r}{j}$.

Hence $X^{(r+1)} = A^{r+1} X^{(0)} + \binom{r+1}{1} A^r X^{(0)} B + \binom{r+1}{2} A^{r-1} X^{(0)} B^2 + \dots$
$\dots + X^{(0)} B^{r+1}$.

So the result is true by induction for all $t > 0$.

Corollary 1.1

If 't' is of the form 2^k for some $k > 0$, then $X^{(t)} = A^t X^{(0)} + X^{(0)} B^t$.

Proof.

According to Knuth ([14]), if 't' is of the form 2^k then $({}^tC_j) \bmod 2 = 0$ where $1 \leq j \leq t-1$. Thus $\binom{t}{j} = 0$ $1 \leq j \leq t-1$ and hence the expression for $X^{(t)}$ derived above, reduces to :

$$X^{(t)} = A^t X^{(0)} + X^{(0)} B^t \quad \text{if} \quad t = 2^k \ (k > 0)$$

Part (b). Since $T(X) = AXB$, so $T^2(X) = T(T(X)) = T(AXB) = A(AXB)B = A^2XB^2$, and in this manner we can easily show, $T^t(X) = A^t X B^t$, for any $t > 0$. This is equivalent to saying, $X^{(t)} = A^t X^{(0)} B^t$. Hence the proof.

We know that for an mxn additive 2-d CA. The set of all configurations, which are 2^{mn} in number, form a vector space over Z_2 . The cannonical basis for this space, is given by the configurations E_{ij}, where $0 \leq i \leq m-1$ and $0 \leq j \leq n-1$ and the (i,j)th entry of E_{ij} is 1 , all other entries being 0's.

Theorem 2.

There is a one-to-one correspondence between the evolutions of a uniform 2-d CA with periodic boundary conditions, starting with any two basis configurations.

Proof.

Case 1. The CA is a Type-I CA.
Then the global transition function, which is a linear transformation, is given by $T(X) = AX + XB$, where A is $m \times m$, X is $m \times n$ and B is $n \times n$. We prove the Theorem by showing that, there is a one-to-one correspondence between the evolutions starting with E_{ij}, for any i,j $(0 \leq i \leq m-1$ and $0 \leq j \leq n-1)$ and E_{00}.

In the expression $T(X) = AX + XB$, we know that the matrices A and B correspond to the vertical and horizontal dependencies respectively. Due to the uniformity of the CA rule, it is easy to see that,

$a_{ij} = 1$, iff $a_{(i+k) \bmod m,\ (j+k) \bmod m} = 1$, where $0 \leq i,j,k \leq m-1$.
Hence, we have $a_{ij} = a_{(i+k) \bmod m,\ (j+k) \bmod m}$. Similarly,
$b_{ij} = b_{(i+k) \bmod n,\ (j+k) \bmod n}$.
Let us now fix i and j, $(0 \leq i \leq m-1$ and $0 \leq j \leq n-1)$.
Define an $m \times m$ matrix U such that

$u_{(i+k)\bmod m,k} = 1$ for $0 \le k \le m-1$ and all other entries are 0's.

Similarly define an nxn matrix V such that, $v_{k,(j+k)\bmod n} = 1$, $0 \le k \le n-1$ and all other entries are zeroes.
By the very construction of the matrix U, each row has exactly one '1', and no two rows have 1's in the same column. So all rows of U are linearly independent and hence U is invertible.
Also, similarly we can show that V is invertible.
Now a direct computation reveals that $E_{ij} = U\, E_{00}\, V$, by the constructions of U and V.
Now we show that, U commutes with A.
Fix p,q such that $0 \le p, q \le m-1$. We proceed to show that, (p,q)th element of the matrices UA and AU, are the same.
The (p,q)th element of UA, is the inner product of the pth row of U and the qth column of A.
Now we have an unique integer k, $0 \le k \le m-1$, such that $p = (i+k)\bmod m$. But then by the construction of U, $u_{p,k} = 1$ and $u_{p,r} = 0 \quad \forall \quad r \ne k$.

Therefore, (p,q)th element of UA is :

$$[u_{p,0}, u_{p,1}, \ldots, u_{p,m-1}] \begin{bmatrix} a_{0,q} \\ a_{1,q} \\ \vdots \\ a_{m-1,q} \end{bmatrix}$$

$= u_{p,k}a_{k,q}$ as all other $u_{p,r}$'s are = 0

$= a_{k,q}$ [since $u_{p,k} = 1$].

Similarly (p,q)th element of AU is :

$$[a_{p,0}, a_{p,1}, \ldots, a_{p,m-1}] \begin{bmatrix} u_{0,q} \\ u_{1,q} \\ \vdots \\ u_{m-1,q} \end{bmatrix}$$

We have only, $u_{(i+q)\text{mod } m,\ q} = 1$ and all other $u_{r,q}$'s = 0.

Thus the (p,q)th element of AU is $a_{p,(i+q)\text{mod } m}$.

But we have $a_{k,q} = a_{(i+k)\text{mod } m,\ (i+q)\text{mod } m}$ [shown before]

So, $a_{k,q} = a_{p,(i+q)\text{mod } m}$ [since $p = (i+k)\text{mod } m$].

Hence, AU = UA.

Exactly in a similar manner, VB = BV.

Thus we have $T(E_{ij}) = AE_{ij} + E_{ij}B$

$= AUE_{00}V + UE_{00}VB$

$= UAE_{00}V + UE_{00}BV$

$= U(AE_{00} + E_{00}B)V = UT(E_{00})V$

and in this way : $T^r(E_{ij}) = UT^r(E_{00})V \quad \forall\ r \geq 0$.

So if we define a map ϕ, from the set of configurations in the evolution of E_{ij} into the set of configurations in the evolution of E_{00}, as follows :

$$\phi(T^r(E_{ij})) = T^r(E_{00}) .$$

Then ϕ is well-defined and one-one, since

$$\phi(T^r(E_{ij})) = \phi(T^s(E_{ij}))$$

iff $T^r(E_{00}) = T^s(E_{00})$

iff $UT^r(E_{00})V = UT^s(E_{00})V$, [since U^{-1} and V^{-1} exists]

iff $T^r(E_{ij}) = T^s(E_{ij})$

and ϕ is trivially onto. Thus ϕ is the desired one-one correspondence.

Case 2. The CA is a Type-II CA.

Then $T(X) = AXB$ and in the same way, $E_{ij} = UE_{00}V$, $AU = UA$ and $BV = VB$. So $T(E_{ij}) = AE_{ij}B = AUE_{00}VB = UAE_{00}BV = UT(E_{00})V$, and in this way we have, $T^r(E_{ij}) = UT^r(E_{00})V$, for any $r > 0$. The proof of the remaining part is same as in the case of Type-I CA. Hence the theorem.

Corollary 2.1

In case of the above 2-d CA, the cycle lengths obtained by starting with any basis configuration, are identical.

Proof.

This is a direct consequence of the 1-1 correspondence between the evolutions of any two basis configurations, as was proved in the Theorem.

As a consequence of the above result, we have the following theorem.

Theorem 3.

For uniform 2-d CA with periodic boundary conditions, the cycle length encountered, by starting with an arbitrary configuration, is a divisor of the cycle length 'π', which is obtained by starting with any of the basis configurations E_{ij}.

Proof.

Let X be a configuration on an arbitrary cycle of length π_1. We are to show that , π_1/π .

Since the configurations E_{ij}, (described before) with $0 \leq i \leq m-1$ and $0 \leq j \leq n-1$, form the cannonical basis of the configuration space, we can represent X as a linear combination of E_{ij}'s. Thus $X = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \varepsilon_{ij} E_{ij}$, where $\varepsilon_{ij} = 0$ or 1.
If T is the global transition function, which is a linear transformation, we have :

$$T(X) = T\left(\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \varepsilon_{ij} E_{ij}\right) = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \varepsilon_{ij} T(E_{ij}).$$

Similarly, $T^2(X) = T(T(X)) = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \varepsilon_{ij} T^2(E_{ij})$, and thus in this way, we have for any $r > 0$,

$$T^r(X) = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \varepsilon_{ij} T^r(E_{ij}). \qquad \ldots(1)$$

Now since we have shown that, there is a one-one correspondence between the evolutions of any two E_{ij}'s, we assume that each E_{ij} enters into a cycle after exactly 'h' steps , i.e. 'h' is the least positive integer for which $T^{\pi+h}(E_{ij}) = T^h(E_{ij})$ $0 \le i \le m-1$, $0 \le j \le n-1$. Then $T^{\pi+2h}(E_{ij}) = T^h(T^{\pi+h}(E_{ij}))$ $= T^h(T^h(E_{ij})) = T^{2h}(E_{ij})$.

Thus we have in this way, $T^{\pi+rh}(E_{ij}) = T^{rh}(E_{ij})$ $\qquad \ldots(2)$

for any $r > 0$.

Now as X lies on a cycle of length π_1, so π_1 is the least positive integer for which $T^{\pi_1}(X) = X$. But then, $T^{r\pi_1}(X) = X$ for any $r > 0$. So we have using **(1)**:

$$T^{r\pi_1}(X) = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \varepsilon_{ij} T^{r\pi_1}(E_{ij}) .$$

Therefore $X = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \varepsilon_{ij} T^{r\pi_1}(E_{ij})$, for any $r > 0$. $\qquad \ldots(3)$

Now we consider, $T^{\pi+\pi_1 h}(X)$.

By virtue of (1) : $T^{\pi+\pi_1 h}(X) = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \varepsilon_{ij} T^{\pi+\pi_1 h}(E_{ij})$.

Again by virtue of (2) : $T^{\pi+\pi_1 h}(E_{ij}) = T^{\pi_1 h}(E_{ij})$

Therefore $T^{\pi+\pi_1 h}(X) = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \varepsilon_{ij} T^{\pi_1 h}(E_{ij}) = X$, by virtue of (3).

Thus $T^{\pi+\pi_1 h}(X) = X$.

By division algorithm, it is possible to find integers q and t, such that, $\pi = q\pi_1+t$, $0 \leq t \leq \pi_1-1$.

Claim $t = 0$.

From $T^{\pi+\pi_1 h}(X) = X$ we have :

$$T^{(q+h)\pi_1+t}(X) = X$$

or, $$T^t(T^{(q+h)\pi_1}(X)) = X .$$

Since $T^{r\pi_1}(X) = X$ for any $r > 0$, we have : $T^t(X) = X$. If $t \neq 0$, then $0 < t < \pi_1$, which means that, the length of the cycle on which X lies, is $\leq t < \pi_1$, contradicting the fact that, π_1 is the cycle length. Hence $t = 0$. Then $\pi = q\pi_1 \Rightarrow \pi_1/\pi$. The proof follows.

Corollary 3.1.

The cycle length obtained by starting with any basis configuration is the maximum cycle length $\pi_{m,n}$, of the 2-d mxn CA.

Proof.

If π is the desired cycle length, then by the above theorem $\pi_{m,n}/\pi$. So $\pi_{m,n} \leq \pi$ and also as $\pi_{m,n}$ is the maximum cycle length, $\pi \leq \pi_{m,n}$. Hence $\pi = \pi_{m,n}$. The proof follows.

Theorem 4. (cf. [19 : 4.7])

In case of a mxn 2-d CA with symmetric and uniform local rules and with periodic boundary conditions, let the characteristic matrices be A and B. Let A and B, correspond to 1-d CA's of maximum cycle lengths π_m and π_n respectively. Then if $\pi_{m,n}$ is the maximum cycle length of the 2-d CA, we have : ℓ.c.m. $(\pi_m, \pi_n)/\pi_{m,n}$.

Proof.

Let T be the global transition function. 'A' accounts for the vertical dependency and 'B' for the horizontal dependency. By symmetric local rules, we have that the matrices A and B are symmetric, and the dependency of a site, on the number of sites towards its right (resp. top), is the same as that towards its left (resp. bottom). But this means, each row (and hence column) of A and B must contain an even number of 1's.

Let $\underline{x}$ (mx1) be a 1-d CA configuration with characteristic matrix A, such that $\underline{x}$ lies on a maximal cycle of length π_m . So π_m is the least positive integer for which $A^{\pi_m}\underline{x} = \underline{x}$. Let us choose a mxn 2-d configuration X as follows :

$X = (\underline{x}, \underline{x}, \ldots, \underline{x})$ (n-tuple). Then X has the property that, every row of X is either all 0's or all 1's.

Now in $T(X) = AX + XB$, let us evaluate the product XB. Any element of XB, is the inner product of a row of X and a column of B. If the row of X is all 0's, then the result trivially vanishes. If the row is all 1's, then the result is simply the sum modulo 2 of the entries in a column of B. But as any column of B has an even number of 1's, the sum vanishes over Z_2. Thus we have shown that $XB = 0$. So, $T(X) = AX$.

Now $T^{\pi_m}(\underline{x}) = A^{\pi_m}\underline{x} = \underline{x}$

i.e. $T^{\pi_m}(X) = A^{\pi_m}(\underline{x}, \underline{x}, \ldots, \underline{x})$

$$= (A^{\pi_m}\underline{x}, A^{\pi_m}\underline{x}, \ldots, A^{\pi_m}\underline{x})$$

$$= (\underline{x}, \underline{x}, \ldots, \underline{x}) = X \text{ and}$$

π_m is the least integer for which this is so. Hence X lies on a cycle of length π_m, in the 2-d CA. Since $\pi_{m,n}$ is the largest cycle length, by Theorem 3 we have $\pi_m / \pi_{m,n}$. We could show in a similar manner that $\pi_n / \pi_{m,n}$.

So $\ell.c.m.\ (\pi_m, \pi_n) / \pi_{m,n}$. Hence the proof.

<u>Lemma 5.1</u>.

If the global transition function 'T', of a <u>general</u>, <u>additive</u> CA is <u>invertible</u>, then there exists a positive integer 'r' such that $T^r = I$, where I denotes the identity mapping.

Proof.

Let X be an arbitrary configuration. Consider the sequence $X, T(X), T^2(X), \ldots$. Since the configuration space is finite, so the above sequence cannot be infinite i.e. there exists integers i and j, $i > j$, for which $T^i(X) = T^j(X)$. Since T is invertible this means $T^{i-j}(X) = X$ (operating by T^{-j}). Since $i-j > 0$ we have that corresponding to each configuration X, we have a least positive integer r_X that satisfies $T^{r_X}(X) = X$.

If the configuration space is 'C', let $r = \ell.c.m. \{ r_X : X \in C \}$. Then trivially , $T^r(X) = X, \; \forall \; x \in C$ which means that $T^r = I$. Hence the proof.

Theorem 5.

For a general, invertible, additive CA, if 'r' is the least positive integer such that $T^r = I$, then 'r' is the least common multiple of all the cycle-lengths in the CA.

(Note : This theorem does not make any reference about the dimension of the CA . It is a perfectly general result).

Proof.

If π_1 is any cycle length, we show that π_1 divides 'r' . Let X be a configuration on the cycle of length π_1. So π_1 is the least positive integer for which $T^{\pi_1}(X) = X$. Now $T^r = I$. Therefore $T^r(X) = X$. Evidently then $\pi_1 \leq r$. By division algorithm, we have, $r = q\pi_1 + t$ for some integers q and t, with $0 \leq t < \pi_1$. Then, $X = T^r(X) = T^{q\pi_1+t}(X)$ $= T^t[T^{q\pi_1}(X)]$. Since $T^{\pi_1}(X) = X$ and T is invertible, so $T^{q\pi_1}(X) = X$, if 'q' is any integer.

Thus $T^r(X) = T^t(X)$ i.e. $T^t(X) = X$.

If $t \neq 0$ then $0 < t < \pi_1$ and $T^t(X) = X$, which contradicts the choice of π_1. So $t = 0$ and thus π_1/r. Since π_1 is the length of an arbitrary cycle, we have shown that, **each** cycle length divides 'r'. Hence if $\ell = \ell$.c.m. of all cycle lengths, then ℓ/r. Our next aim is to show that, r/ℓ. Let $X \neq \underline{O}$ (the null configuration) be any configuration. We consider the sequence $X, T(X), T^2(X), \ldots$ and then by imitating the proof of Lemma 5.1 we find that there exists a least positive integer k, for which $T^k(X) = X$. But then X lies on a cycle of length k, and as $\ell = \ell$.c.m. of all cycle lengths, $\ell = tk$ for some integer $t > 0$. Then $T^\ell(X) = T^{tk}(X) = X$, and trivially $T^\ell(\underline{O}) = \underline{O}$. So $T^\ell(X) = X$, for any configuration X, which means $T^\ell = I$. As 'r' is the least positive integer for which this is so, we must have r/ℓ. The proof follows.

Corollary 5.1.

Let 'r' be as in Theorem 5. If in particular, the CA in Theorem 5 is a uniform mxn 2-d CA, with periodic boundary conditions, then $r = \pi_{m,n}$ (the length of the largest cycle).

Proof.

By Theorem 5, r = ℓ.c.m. of all cycle lengths. Also by Theorem 3 each cycle length of the chosen CA, divides $\pi_{m,n}$ and so the ℓ.c.m. of all these lengths is equal to $\pi_{m,n}$. The proof follows.

Definition.

By the height of an additive CA we shall mean the height of the tree,rooted at the null configuration, in the state transition graph. This definition is meaningful, since it has already been stated ([19]) that trees on each node of a cycle in the state transition graph, are identical.

Theorem 6.

In a symmetric, uniform 2-d CA with periodic boundary conditions, let the global transition rule T be given by $T(X) = AX + XB$. If h_1 and h_2 are the heights of the corresponding 1-d CA's with characteristic matrices A and B respectively, and 'h' is the height of the 2-d CA, then $h \geq \max(h_1, h_2)$.

Proof.

In case of the 1-d CA with A as the characteristic matrix, let $\underline{x}(m\times 1)$ be a configuration that reaches the null configuration after h_1 time steps, i.e. 'h_1' is the least positive integer, such that $A^{h_1}\underline{x} = \underline{O}$. Let X be the 2-d configuration $(\underline{x},\underline{x},\ldots,\underline{x})$ (n-tuple), which is $m\times n$. Then exactly as in the proof of Theorem 4, we have $XB = O$. Thus $T(X) = AX$.

Now $A^{h_1}\underline{x} = \underline{O}$, so $T^{h_1}(X) = A^{h_1}X = A^{h_1}(\underline{x},\underline{x},\ldots,\underline{x})$ $= (A^{h_1}\underline{x},A^{h_1}\underline{x},\ldots,A^{h_1}\underline{x}) = (\underline{O},\underline{O},\ldots,\underline{O})$, the null configuration of the 2-d CA.

So the 2-d configuration X evolves to the null configuration after h_1 time steps; therefore $h \geq h_1$. Exactly in a similar manner, $h \geq h_2$. Thus $h \geq \max(h_1,h_2)$. Hence the proof.

Theorem 7.

In case of a $m\times n$ Type-II 2-d CA with symmetric and uniform local rules, and with periodic boundary conditions, a configuration which has all rows identical or all columns identical, is a predecessor of the null configuration.

Proof.

Here $T(X) = AXB$ where A is $m\times m$, X is $m\times n$ and B is $n\times n$.

Now if all columns of X are identical, then $X = (\underline{x}, \underline{x}, \ldots, \underline{x})$, where $\underline{x}$ is $m \times 1$. Then, as in Theorem 4, $XB = O$. So $T(X) = O$. If all rows of X are identical then in a similar way : $AX = O$ and thus $T(X) = O$. Hence the proof.

Corollary 7.1

The kernel of the global transition rule T of the CA described in Theorem 7, has at least $2^m + 2^n - 2$ elements.

Proof.

By Theorem 7, configurations with all rows identical or all columns identical are in Ker(T). So if r is the number of configurations with all rows equal or all columns equal, then $|Ker(T)| \geq r$.

Let C_1 represent the set of configurations with all rows identical and C_2 represent those with all columns identical. Then evidently, $|C_1| = 2^n$ and $|C_2| = 2^m$ where, m = no. of rows and n = no. of columns. $C_1 \cap C_2$ consists of all 0's or all 1's configuration. So $|C_1 \cap C_2| = 2$.

Now $r = |C_1 \cup C_2| = |C_1| + |C_2| - |C_1 \cap C_2| = 2^n + 2^m - 2$.

So, $|Ker(T)| \geq 2^m + 2^n - 2$. Hence the proof.

Theorem 8.

In case of $m \times n$ <Rule-90, Rule-90> 2-d CA with periodic boundary conditions, the all 1's configuration is a predecessor of the null configuration (cf. [19] for the 1-d case).

Proof.

If T is the global transition rule, $T(X) = AX + XB$ where, in case of <Rule-90, Rule-90> the matrices A and B are as follows :

$$A = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ \vdots & & & & & \\ 0 & 0 & \dots & 1 & 0 & 1 \\ 1 & 0 & \dots & 0 & 1 & 0 \end{bmatrix}_{m \times m}$$

and B is the same matrix with dimension $n \times n$. Substituting

$$X = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 \\ \vdots & & & \\ 1 & 1 & \dots & 1 \end{bmatrix}_{m \times n} ,$$

it is only a matter of routine checking, that $AX + XB$ evaluates to the null matrix. Hence the proof.

Corollary 8.1

<Rule-90, Rule-90> 2-d CA with periodic boundary conditions, is never invertible.

Proof.

The CA would be invertible iff T is so, i.e. Ker(T) = $\{\underset{\sim}{0}\}$. But by the above theorem

$$\begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \\ \vdots & & & \\ 1 & 1 & \cdots & 1 \end{bmatrix}_{m\times n} \in \mathrm{Ker}(T)$$

and thus Ker(T) $\neq \{\underset{\sim}{0}\}$. The proof follows.

As in the case of 1-d Rule-90 CA we have the following :

Theorem 9.

In a <Rule-90, Rule-90> 2-d CA with periodic boundary conditions; configurations that have a value 1, at an odd number of sites, cannot be reachable.

Proof.

It is sufficient to show that, the configurations that are reachable in one time step, i.e. by one application of T, always have an even number of 1's.

We have T(X) = AX + XB , where

$$A = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & & & & & \\ 0 & 0 & 0 & \cdots 1 & 0 & 1 \\ 1 & 0 & 0 & \cdots 0 & 1 & 0 \end{bmatrix}_{m\times m}$$

and B is the same matrix but with dimension $n \times n$.

Then we easily see that the $(i,j)\underline{th}$ entry of $T(X)$ is

$$x_{i,(j-1)\bmod n} + x_{i,(j+1)\bmod n} + x_{(i-1)\bmod m,j} + x_{(i+1)\bmod m,j}$$

(The sum is taken modulo 2).

We now compute the sum of all the entries of $T(X)$.

The sum is :

$$\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[x_{i,(j-1)\bmod n} + x_{i,(j+1)\bmod n} + x_{(i-1)\bmod m,j} + x_{(i+1)\bmod m,j}]$$

$$= \sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[x_{i,(j-1)\bmod n} + x_{i,(j+1)\bmod n}] + \sum_{j=0}^{n-1}\sum_{i=0}^{m-1}[x_{(i-1)\bmod m,j} + x_{(i+1)\bmod m,j}]$$

We evaluate : $\sum_{j=0}^{n-1}[x_{i,(j-1)\bmod n} + x_{i,(j+1)\bmod n}]$

$$= (x_{i,n-1} + x_{i,1})+(x_{i,0} + x_{i,2})+(x_{i,1} + x_{i,3}) + \cdots$$
$$\cdots + (x_{i,n-3} + x_{i,n-1})+(x_{i,n-2} + x_{i,0})$$

Rearranging we get :

$$(x_{i,0} + x_{i,0})+(x_{i,1} + x_{i,1}) +\cdots+ (x_{i,n-1} + x_{i,n-1}) = 0 .$$

(As the sum is taken modulo 2.)

Similarly $\sum_{i=0}^{m-1} [x_{(i-1)\bmod m,j} + x_{(i+1)\bmod m,j}] = 0 .$

Thus the sum of all entries of $T(X)$ is 0 and this is possible iff, $T(X)$ contains an even number of 1's. Hence the proof.

Corollary 9.1

In the state transition diagram, the tree rooted at the null configuration (and hence at each configuration on each cycle), consists of $k-1$ arcs, where $|Ker(T)| = k$, if $m+n$ is odd .

Proof.

As in the 1-d case, we assume that the trees are balanced. By Theorem 8, all 1's configuration is a predecessor of the null configuration. So by Theorem 9, if $m+n$ is odd, then the all 1's configuration has no predecessor. The proof follows.

We next deduce the following result of Martin et al. ([19]) using our method.

Theorem 10.

For an uniform, mxn 2-d CA with periodic boundary conditions, if $\pi_{m,n}$ denotes the maximum cycle-length , then $\pi_{m,n}/\pi^*$, where : $\pi^* = 2^{\ell.c.m.(ord_m(2),\, ord_n(2))} - 1$ in general; and if the local rules are symmetric, we have : $\pi^* = 2^{\ell.c.m.(sord_m(2),\, sord_n(2))} - 1$.

(Note : For $ord_m(2)$ and $ord_n(2)$ to be defined, we need both m and n to be odd.)

Proof.

We have assumed additive, uniform local rules, so, our global transition function T is given by $T(X) = AX + XB$, where A gives the vertical dependency and B gives the horizontal dependency. We consider A which is an $m \times m$ matrix. Let the vertical dependency of each site x_{ij} in the most general case be as follows : x_{ij} is replaced by :
$\varepsilon_0 x_{i,j} + \varepsilon_1 x_{(i-1) \bmod m, j} + \dots + \varepsilon_{m-1} x_{(i-m+1) \bmod m, j}$, where each ε_k is either 0 or 1. Since the local rule is same for every cell, we have that ε_k's are independent of i and j. Thus given an arbitrary configuration $X = (x_{ij})$, the (i,j)th entry of AX is $\varepsilon_0 x_{ij} + \varepsilon_1 x_{(i-1) \bmod m, j} + \dots + \varepsilon_{m-1} x_{(i-m+1) \bmod m, j}$ (modulo 'm' operation is taken due to periodic boundary conditions).

We now proceed to express A in a particular form. Let 'C' be the $m \times m$ matrix

$$C = \begin{bmatrix} 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \dots 1 & 0 \end{bmatrix}$$

If we choose any mxl column vector :

$$\underline{x} = \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{m-1} \end{bmatrix} \quad \text{then we have} \quad C\underline{x} = \begin{bmatrix} x_{m-1} \\ x_0 \\ x_1 \\ \vdots \\ x_{m-2} \end{bmatrix} \quad \text{i.e. one}$$

application of 'C' produces a 1-fold cyclic shift, of the column vector, towards the bottom. Thus if we consider $C^r\underline{x}$ for any $r > 0$, the shift is r-fold. Keeping this property of 'C' in mind, we now show that

$$A = \varepsilon_0 I + \varepsilon_1 C + \varepsilon_2 C^2 + \dots + \varepsilon_{m-1} C^{m-1} .$$

Let $X = (x_{ij})$ be any configuration. We can write X as $X = (\underline{x}_0, \underline{x}_1, \dots, \underline{x}_{n-1})$ where

$$\underline{x}_j = \begin{bmatrix} x_{0j} \\ x_{1j} \\ \vdots \\ x_{m-1,j} \end{bmatrix} .$$

If $D = \varepsilon_0 I + \varepsilon_1 C + \dots + \varepsilon_{m-1} C^{m-1}$, then $DX = (D\underline{x}_0, D\underline{x}_1, \dots, D\underline{x}_{n-1})$. Thus (i,j)th element of DX is the element in the ith row of $D\underline{x}_j$. Since element in the ith row of $C^r\underline{x}_j$ is the element in row (i-r)mod m, of the vector $\underline{x}_j$ (as $C^r\underline{x}_j$ is a r-fold cyclic shift of $\underline{x}_j$, we have that the element in the ith row of $D\underline{x}_j$ is $\sum_{r=0}^{m-1} \varepsilon_r x_{(i-r) \bmod m, j}$

$= \varepsilon_0 x_{i,j} + \varepsilon_1 x_{(i-1) \bmod m, j} + \cdots + \varepsilon_{m-1} x_{(i-m+1) \bmod m, j}$.

Thus we have shown that, (i,j)th element of DX is same as the (i,j)th element of AX, for any configuration X ; which proves D = A. Hence $A = \varepsilon_0 I + \varepsilon_1 C + \varepsilon_2 C^2 + \ldots + \varepsilon_{m-1} C^{m-1}$. We can see that C is invertible, as all its rows are linearly independent. The characteristic polynomial for C is given by, $\det(C-\lambda I_m) = \det(C+\lambda I_m)$. [$I_m$ is the mxm identity matrix].

$$= \begin{vmatrix} \lambda & 0 & 0 & \ldots & 1 \\ 1 & \lambda & 0 & \ldots & 0 \\ 0 & 1 & \lambda & \ldots & 0 \\ \vdots & & & & \\ 0 & \ldots & \ldots & 1 & \lambda \end{vmatrix}_{m \times m} = \lambda \begin{vmatrix} \lambda & 0 & 0 & \ldots & 0 \\ 1 & \lambda & 0 & \ldots & 0 \\ 0 & 1 & \lambda & \ldots & 0 \\ \vdots & & & & \\ 0 & 0 & \ldots & 1 & \lambda \end{vmatrix}_{(m-1)\times(m-1)}$$

$$+ \begin{vmatrix} 1 & \lambda & 0 & \ldots & 0 \\ 0 & 1 & \lambda & \ldots & 0 \\ \vdots & & & & \\ 0 & \ldots & \ldots & 0 & 1 \end{vmatrix}_{(m-1)\times(m-1)}$$

(Expanding by the first row)

The first (m-1)x(m-1) matrix is upper triangular and the second one is lower triangular. So the determinant is simply the product of diagonal elements. So $\det(C-\lambda I_m) = \lambda . \lambda^{m-1} + 1 = \lambda^m + 1$ $= \lambda^m - 1$ [we are in Z_2].

Therefore by Cayely-Hamilton theorem, $C^m - I = 0$ (null matrix) i.e. $C^m = I_m$.

Since $A = \varepsilon_0 I + \varepsilon_1 C + \varepsilon_2 C^2 + \dots + \varepsilon_{m-1} C^{m-1}$, we have

$$A^{2^{\mathrm{ord}_m(2)}} = \sum_{r=0}^{m-1} \varepsilon_r^{2^{\mathrm{ord}_m(2)}} C^{r.2^{\mathrm{ord}_m(2)}} \quad \text{(since we are in } Z_2\text{)}.$$

Also since $\varepsilon_r \in Z_2$, $\varepsilon_r^{2^k} \equiv \varepsilon_r \bmod 2$, for all $k > 0$.

So $$A^{2^{\mathrm{ord}_m(2)}} = \sum_{r=0}^{m-1} \varepsilon_r C^{r.2^{\mathrm{ord}_m(2)}}.$$

If $\mathrm{ord}_m(2) = j$, then $2^j \equiv 1 \bmod m$, i.e. $2^{\mathrm{ord}_m(2)} = km + 1$ for some k.

Thus $C^{r.2^{\mathrm{ord}_m(2)}} = C^{r(km+1)} = (C^m)^{rk} C^r = (I_m)^{rk} C^r = C^r$.

Hence, $$A^{2^{\mathrm{ord}_m(k)}} = \sum_{r=0}^{m-1} \varepsilon_r C^r = A.$$

One can similarly show that, $B^{2^{\mathrm{ord}_n(k)}} = B$.

Let us write, $f(C) = \sum_{r=0}^{m-1} \varepsilon_r C^r = A[C^0 = I_m]$.

If we have the uniform local rule to be symmetric, it is easy to see that, $f(C) = f(C^{-1})$, i.e. $A = \sum_{r=0}^{m-1} \varepsilon_r C^{-r}$.

Then as before, $$A^{2^{\mathrm{sord}_m(2)}} = \sum_{r=0}^{m-1} \varepsilon_r C^{-r.2^{\mathrm{sord}_m(2)}}.$$

If $\mathrm{sord}_m(2) = j$ then $2^j \equiv \pm 1 \bmod m$.

So $A^{2^{\mathrm{sord}_m(2)}} = \sum_{r=0}^{m-1} \varepsilon_r C^{-r(km\pm 1)}$ [as $2^{\mathrm{sord}_m(2)} = km\pm 1$, for some k]

$= \sum_{r=0}^{m-1} \varepsilon_r C^{-rkm} C^{-r}$ or $\sum_{r=0}^{m-1} \varepsilon_r C^{-rkm} C^{r}$

$= \sum_{r=0}^{m-1} \varepsilon_r C^{-r}$ or $\sum_{r=0}^{m-1} \varepsilon_r C^{r}$ [as $C^m = I_m$, $C^{-rkm} = I_m$]

Since due to symmetry : $\sum_{r=0}^{m-1} \varepsilon_r C^{-r} = A = \sum_{r=0}^{m-1} \varepsilon_r C^{r}$, we have

$A^{2^{\mathrm{sord}_m(2)}} = A$. Similarly, $B^{2^{\mathrm{sord}_n(2)}} = B$.

Let $\ell = 2^{\mathrm{ord}_m(2)}$ (resp. $2^{\mathrm{sord}_m(2)}$).

Since $A^{\ell} = A$, it is easy to check by induction that $A^{\ell^k} = A$, for any $k > 0$.

Now $\pi^* + 1 = 2^{\ell.c.m.(\mathrm{ord}_m(2),\ \mathrm{ord}_n(2))}$

(resp. $2^{\ell.c.m.(\mathrm{sord}_m(2),\ \mathrm{sord}_n(2))}$).

There is an integer k_1 such that,

$\ell.c.m.(\mathrm{ord}_m(2), \mathrm{ord}_n(2))$ (resp. $\ell.c.m.(\mathrm{sord}_m(2), \mathrm{sord}_n(2))$)

$= k_1\, \mathrm{ord}_m(2)$ (resp. $k_1 \mathrm{sord}_m(2)$).

So, $A^{\pi^* + 1} = A^{2^{k_1 \mathrm{ord}_m(2)}}$ (resp. $A^{2^{k_1 \mathrm{sord}_m(2)}}$)

$= A^{\ell^{k_1}} = A$.

Similarly, $B^{\pi^* + 1} = B$.

Now as, $\pi^* + 1$ is a power of 2, we have by Corollary 1.1 that : $T^{\pi^*+1}(X) = A^{\pi^*+1}X + XB^{\pi^*+1}$.

Hence, $T^{\pi^*+1}(X) = AX + XB = T(X)$.

Thus we have shown that, given any configuration, there is a repeatation after π^* steps, and in particular a configuration lying on a maximal cycle, (of length $\pi_{m,n}$) also repeats itself after π^* steps. Hence by Theorem 3 we have, $\pi_{m,n}/\pi^*$. The proof follows.

Corollary 10.1

For mxn <Rule-90, Rule-90> 2-d CA with periodic boundary conditions, if $m = 2^p$ and $n = 2^q$, for some integers $p,q > 0$, then $\pi_{m,n} = 1$. (Similar to the 1-d case ([19])).

Proof.

If we can show that, in the above CA, every configuration ultimately evolves to the null configuration, then we are done.

Now as A is the Rule-90 matrix of a 1-d CA, imitating the proof of Theorem 10, one can easily verify that, A can be written as $C + C^{-1}$, where 'C' is the matrix, as described in Theorem 10. (Equivalently, $A = C + C^{m-1}$, as $C^m = I_m$, the mxm identity matrix.) Since A is mxm , so we use the notation, C_m instead of 'C'. Thus $A = C_m + C_m^{-1}$. Similarly $B = C_n + C_n^{-1}$. Hence

$$T(X) = (C_m + C_m^{-1}) X + X (C_n + C_n^{-1}).$$

Without loss of generality, we assume that, $p \geq q$. Since $m = 2^p$, by Corollary 1.1, we have, $T^m(X) = A^m X + XB^m$ $= (C_m + C_m^{-1})^m X + X(C_n + C_n^{-1})^m$, i.e. $T^m(X) = (C_m^m + C_m^{-m})X + X(C_n^m + C_n^{-m})$ [as we are in Z_2].

Since $C_m^m = I_m, C_m^m + C_m^{-m} = 0$ (null matrix) and thus, $T^m(X) = X(C_n^m + C_n^{-m})$. Since $p \geq q$, let $p = q + r$, where $r \geq 0$. But as $C_n^n = I$, so $C_n^{2^q} = I_n$, so, $C_n^m = C_n^{2^p} = C_n^{2^{q+r}}$ $= (C_n^{2^q})^{2^r} = (I_n)^{2^r} = I_n$.

Thus, $T^m(X) = X(I_n + I_n) = 0$, for any configuration X . The proof follows.

In some of our proofs given above, we had come across situations, where the global transition rule T of the 2-d CA is invertible. We shall now consider the case of invertibility, a bit more closely. This case is of interest, since, if T is invertible, all configurations other than the null configuration, lie on some cycle and thus there are no trees in the state transition graph. This case is of interest since in certain CA applications such as pseudo-random sequence generation ([29]), long cycle lengths are desirable. In case T is invertible, there is a possibility that excepting the null configuration, all other configurations could lie on one cycle, giving a very large cycle length.

Since, practically always we have been working with the global transition rule of the form $T(X) = AX + XB$, we would like to investigate the invertibility of T, from properties of A and B.

Definition

The characteristic polynomial for an nxn matrix A is defined as $\det(A-\lambda I_n)$ where I_n is the nxn identity matrix. Since we are always working with Z_2, we may rewrite it as $\det(A+\lambda I_n)$.

Theorem 11 ([18])

For a 2-d CA with global transition rule T of the form $T(X) = AX + XB$, T is invertible, iff the characteristic polynomials of A and B are relatively prime (over Z_2).

We now proceed to determine the characteristic polynomials for a <Rule-90, Rule-90> 2-d CA with both periodic and null boundary conditions.

Theorem 12 ([5])

If 'A' is the Rule-90 matrix of a 1-d CA with null boundary conditions, then the characteristic polynomial of A, denoted by $q_n(\lambda)$ where 'n' is the dimensionality of A, satisfies the recurrence relation : $q_n(\lambda) = \lambda q_{n-1}(\lambda) + q_{n-2}(\lambda)$.

Proof.

$$q_n(\lambda) = \det(A + \lambda I_n).$$

In this case we have seen before that A is of the form :

$$A = \begin{vmatrix} 0 & 1 & 0 & \dots & 0 & 0 \\ 1 & 0 & 1 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \vdots & & & & & \\ 0 & 0 & \dots & 1 & 0 & 1 \\ 0 & 0 & \dots & \dots & 1 & 0 \end{vmatrix}_{n \times n}$$

Therefore, $$q_n(\lambda) = \begin{vmatrix} \lambda & 1 & 0 & \dots & 0 & 0 \\ 1 & \lambda & 1 & \dots & 0 & 0 \\ 0 & 1 & \lambda & \dots & 0 & 0 \\ \vdots & & & & & \\ 0 & 0 & \dots & 1 & \lambda & 1 \\ 0 & 0 & \dots & \dots & 1 & \lambda \end{vmatrix}_{n \times n}$$

Expanding by the first row yields :

$$q_n(\lambda) = \lambda \begin{vmatrix} \lambda & 1 & 0 & \dots & 0 \\ 1 & \lambda & 1 & \dots & 0 \\ \vdots & & & & \\ 0 & 0 & \dots & 1 & \lambda \end{vmatrix}_{(n-1)\times(n-1)} + \begin{vmatrix} 1 & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \dots & 0 \\ \vdots & & & & \\ 0 & 0 & \dots & 1 & \lambda \end{vmatrix}_{(n-1)\times(n-1)}$$

$$= \lambda q_{n-1}(\lambda) + \begin{vmatrix} \lambda & 1 & 0 & \dots & 0 \\ 1 & \lambda & 1 & \dots & 0 \\ \vdots & & & & \\ 0 & 0 & \dots & 1 & \lambda \end{vmatrix}_{(n-2)x(n-2)}$$

(Expanding the second (n-1)x(n-1) determinant by the 1st column)

So $q_n(\lambda) = \lambda q_{n-1}(\lambda) + q_{n-2}(\lambda)$. The proof follows.

Notation : $q_n(\lambda)$ is the characteristic polynomial of a Rule-90 1-d CA having 'n' sites with null boundary conditions. Let $\dot{p}_n(\lambda)$ be the characteristic polynomial of the same 1-d CA but now with periodic boundary conditions.

Then we have the following result :

Theorem 13

If 'A' is the Rule-90 matrix of a 1-d CA with periodic boundary conditions, then the characteristic polynomial of A, denoted by $p_n(\lambda)$, where 'n' is the dimensionality of A, satisfies the recurrence relation : $p_n(\lambda) = \lambda q_{n-1}(\lambda)$.

Proof.

In this case A looks like :

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & 1 & \dots & 0 & 0 \\ \vdots & & & & & & \\ 0 & 0 & 0 & 0 & \dots 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & \dots 0 & 1 & 0 \end{bmatrix}_{nxn}$$

$$\text{So,}\quad p_n(\lambda) = \begin{vmatrix} \lambda & 1 & 0 & \cdots & 0 & 1 \\ 1 & \lambda & 1 & \cdots & 0 & 0 \\ 0 & 1 & \lambda & \cdots & 0 & 0 \\ \vdots & & & & & \\ 0 & 0 & 0 & \cdots 1 & \lambda & 1 \\ 1 & 0 & 0 & \cdots 0 & 1 & \lambda \end{vmatrix}_{n\times n}$$

Expanding by the 1st row :

$$p_n(\lambda) = \lambda \begin{vmatrix} \lambda & 1 & \cdots & 0 & 0 \\ 1 & \lambda & \cdots & 0 & 0 \\ 0 & 1 & \lambda \cdots & 0 & 0 \\ \vdots & & & & \\ 1 & 0 & 0 \cdots & 1 & \lambda \end{vmatrix}_{(n-1)\times(n-1)} + \begin{vmatrix} 1 & 1 & \cdots & 0 & 0 \\ 0 & \lambda & 1 \cdots & 0 & 0 \\ \vdots & & & & \\ 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 1 & \lambda \end{vmatrix}_{(n-1)\times(n-1)}$$

$$+ \begin{vmatrix} 1 & \lambda & 1 & \cdots & 0 \\ 0 & 1 & \lambda & \cdots & 0 \\ \vdots & & & & \\ 1 & 0 & \cdots & 0 & 1 \end{vmatrix}_{(n-1)\times(n-1)}$$

The 1st $(n-1)\times(n-1)$ determinant can be easily seen to be $q_{n-1}(\lambda)$ (refer to the proof of Theorem 12).

Expanding the second determinant by the 1st column we get :

$$\begin{vmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 1 & \lambda & 1 & \cdots & 0 \\ \vdots & & & & \\ 0 & \cdots & & 1 & \lambda \end{vmatrix}_{(n-2)\times(n-2)} + \begin{vmatrix} 1 & 0 & \cdots & 0 \\ \lambda & 1 & 0 \cdots & 0 \\ \vdots & & & \\ 0 & 0 & 0 \cdots & 1 \end{vmatrix}_{(n-2)\times(n-2)}$$

Now the 1st (n-2)x(n-2) determinant is clearly $q_{n-2}(\lambda)$ and the second one being lower triangular, the determinant is simply the product of the diagonal elements and is thus 1. Also expanding the third (n-1)x(n-1) determinant by the first column we find it to be equal to $1 + q_{n-2}(\lambda)$.

Thus ultimately :

$$p_n(\lambda) = \lambda q_{n-1}(\lambda) + 1 + q_{n-2}(\lambda) + q_{n-2}(\lambda) + 1$$

$$= \lambda q_{n-1}(\lambda) \text{ [as we are in } Z_2].$$

Hence the proof.

Remarks : In case of a mxn <Rule-90, Rule-90> 2-d CA, with periodic boundary conditions, since the characteristic matrices A and B in $T(X) = AX + XB$, are Rule-90 1-d CA matrices with periodic boundary conditions; their characteristic polynomials are $p_m(\lambda)$ and $p_n(\lambda)$ respectively. Since $p_m(\lambda) = \lambda q_{m-1}(\lambda)$ and $p_n(\lambda) = \lambda q_{n-1}(\lambda)$, it follows that $p_m(\lambda)$ and $p_n(\lambda)$ are not relatively prime and thus by Theorem 11, T is not invertible. This is an alternative proof of Corollary 8.1.

In this case we have not been able to compute the dimension of the kernel of T, which would give the number of predecessors of the null configuration. However, instead of periodic, if we choose null boundary conditions, then we have the following result due to Sutner ([26]) (Also see ([5]) for an alternative simple proof).

Theorem 14

For an mxn <Rule-90, Rule-90> 2-d CA with null boundary conditions, the dimension of the kernel of T is given by :

$$\text{h.c.f.}(m+1,\ n+1) - 1 ,$$

and thus the number of predecessors of the null configuration is $2^{\text{h.c.f.}(m+1,n+1)-1}$.

In particular the CA is invertible iff h.c.f.(m+1,n+1) = 1 i.e. iff m+1 and n+1 are relatively prime.

Remarks : The second assertion is verified from Table 1 where we see that whenever m+1 and n+1 are relatively prime, the height of the tree is 0. (Look up Table 1 for results on o-e-n)

The following results can now be proved by induction ([5]) :

Theorem 15

(a) λ is a factor of $q_n(\lambda)$ iff 'n' is odd.

(b) $(1+\lambda)$ is a factor of $q_n(\lambda)$ iff $n \equiv 2 \bmod 3$, i.e. iff $n = 3k+2$, for some $k \geq 0$.

(c) (i) If $n = 2^k-2$, for some $k > 0$ then

$$q_n(\lambda) = \lambda^{2^k-2} + \lambda^{2^k-2^2} + \ldots + 1$$

(ii) If $n = 2^k - 1$, then

$$q_n(\lambda) = \lambda^n$$

(iii) If $n = 2^k$, then

$$q_n(\lambda) = \lambda^{2^k} + \lambda^{2^k-2} + \lambda^{2^k-2^2} + \dots + 1$$

and $p_n(\lambda) = \lambda^n$

We had introduced Rule-90 earlier. We now introduce Rule-150 ([28]) along with it. In case of Rule-90 1-d CA the local rule consisted of adding modulo 2, the site values of the two nearest (adjacent) neighbours. Both periodic and null boundary conditions were discussed. In case of Rule-150, the rule for any site is to consider sum modulo 2 of the site values of the two nearest neighbours <u>along with the site value of its own</u>. In the Rule-90 matrix, both in the periodic and null boundary conditions, the diagonal entries were 0's. The Rule-150 matrix in both the cases will be the corresponding Rule-90 matrix with all diagonal entries as 1's. For example, the nxn Rule-150 matrix looks like :

$$\begin{bmatrix} 1 & 1 & 0 & & \dots & 1 \\ 1 & 1 & 1 & 0 & \dots & 0 \\ 0 & 1 & 1 & 1 & 0\dots & 0 \\ \vdots & & & & & \\ 1 & 0 & 0 & \dots\dots & 1 & 1 \end{bmatrix}_{n \times n}$$

in case of periodic boundary conditions.

In case of null boundary conditions, the matrix remains same, only that the entries at positions (0, n-1) and (n-1, 0) become 1.

The following is then trivial:
The characteristic polynomial for a $n \times n$ Rule-150 matrix is $p_n(1+\lambda)$ for <u>periodic</u> boundary conditions and $q_n(1+\lambda)$ for <u>null</u> boundary conditions.

<u>Theorem 16</u>

(a) In a $m \times n$ <Rule-90, Rule-150> 2-d CA with <u>null</u> boundary conditions, if $m = 2^k-1$ and $n = 2^\ell-1$, for some integers $k, \ell > 0$, then the global transition function T is invertible.

(b) In a $m \times n$ <Rule-90, Rule-150> 2-d CA with <u>periodic</u> boundary conditions, if $m = 2^k$ and $n = 2^r$, for some $k, r > 0$, then T is invertible.

<u>Proof</u>.

<u>Part (a).</u> $T(X) = AX + XB$.

Characteristic matrix of A is $q_m(\lambda)$ and that for B is $q_n(1+\lambda)$.

Now as $m = 2^k-1$ and $n = 2^\ell-1$, by part (ii) of Theorem 15(c) : $q_m(\lambda) = \lambda^m$ and $q_n(\lambda) = \lambda^n$.

Thus $q_n(1+\lambda) = (1+\lambda)^n$. Since the polynomials λ^m and $(1+\lambda)^n$ are relatively prime, we have using Theorem 11, T is invertible.

(b) $T(X) = AX + XB$. In this case the characteristic polynomial for A is $p_m(\lambda)$ and that for B is $p_n(1+\lambda)$. Since $m = 2^k$ and $n = 2^r$, we find using part (iii) of Theorem 15(c) that $p_n(\lambda) = \lambda^n$ and $p_m(\lambda) = \lambda^m$. So, $p_n(1+\lambda) = (1+\lambda)^n$.

Again as λ^m and $(1+\lambda)^n$ are relatively prime, using Theorem 11, the result follows.

Hence the proof.

Earlier, we had mentioned about a special case of 2-d CA known as, <u>Restricted Vertical Neighbourhood</u> (RVN) CA ([24]). We now present equivalent proofs of certain properties using our approach of choosing the transition function as, $T(X) = AX + XB$. Now in our terminology, the vertical dependency is given by the matrix A. It is a simple observation that A has non-zero entries only in its lower (resp. upper) triangular portion if the vertical dependency is restricted to the <u>top</u> (resp. <u>bottom</u>). The diagonal elements are always zeroes. The matrix B could be any matrix. Having characterised the RVN in terms of the matrix A, the following result is now easy to prove :

<u>Theorem 17</u>

An mxn RVN 2-d CA whose global transition function T is given by $T(X) = AX + XB$, is invertible iff the matrix B is so.

Proof.

As we had mentioned previously, the matrix A is upper or lower diagonal with all the diagonal entries being 0's . Let $p(\lambda)$ and $q(\lambda)$ be the characteristic polynomials of A and B respectively. Since A is an mxm triangular matrix with diagonal entries 0, so the matrix $A + \lambda I_m$ will be a triangular matrix with all diagonal entries λ, (I_m is the mxm identity matrix) and so $\det(A + \lambda I_m)$ will simply be the product of the diagonal elements. Thus we have $p(\lambda) = \lambda^m$. Now according to Theorem 11, T is invertible iff $p(\lambda)$ and $q(\lambda)$ are relatively prime, i.e. iff λ^m and $q(\lambda)$ are relatively prime, i.e. iff λ and $q(\lambda)$ are relatively prime, i.e. iff λ is not a divisor of $q(\lambda)$, i.e. iff $\lambda = 0$ is not a root of $q(\lambda)$, i.e. iff 0 is not an eigenvalue of B, i.e. iff B is invertible. Hence the proof.

We now deduce one of the results related to cycle-lengths of RVN CA obtained in ([24]).

Theorem 18

For an mxn invertible RVN CA characterised by $T(X) = AX + XB$, the cycle-lengths will be divisors of ℓ.c.m.(r,k) where $k = 2^{\lceil \log_2 m \rceil}$ and 'r' is the least positive integer for which $B^r = I_n$.

Proof.

If X is any configuration, and we can show that $T^{\ell cm(r,k)}(X) = X$, then we will have proved the theorem. We have already shown in Theorem 17, that the characteristic polynomial for A is λ^m . By Cayley-Hamilton theorem we thus have, $A^m = O$.

Now by Corollary 1.1., since $k = 2^{\lceil \log_2 m \rceil}$ we have, $T^k(X) = A^k X + XB^k$. Now as $\lceil \log_2 m \rceil \geq \log_2 m$, so we have $2^{\lceil \log_2 m \rceil} \geq m$ i.e. $k \geq m$. Since $A^m = O$, therefore $A^k = O$. So, $T^k(X) = XB^k$. It can now be easily checked by induction that $T^{tk}(X) = XB^{tk}$ for any $t > 0$. Now if $\ell = \ell.c.m.(r,k)$, we can find integers t_1 and t_2 such that $\ell = t_1 r = t_2 k$. Since $T^{t_2 k}(X) = XB^{t_2 k}$, so $T^{\ell}(X) = XB^{t_1 r} = X(B^r)^{t_1} = X(I_n)^{t_1} = X$. The proof follows.

Implementation and application aspects:

From the preceeding discussions, it is very clear that, the height and cycle length of a CA, play a key role concerning its behaviour. Unfortunately, our theoretical knowledge about these two facts is very limited. Even for a Rule-90 CA, which has such a simple local rule, and of which Wolfram ([28]) has made so extensive a study, a general expression regarding the cycle length is yet to be found, though its asymptotic behaviour is known. This was in case of a 1-d CA. Analysis of 2-d CA features is yet more complicated. This suggests that, deriving properties merely by intuition, is not always feasible. One needs to have some concrete numerical information at his disposal, as this could possibly throw light upon some facts concerning the CA behaviour, which could subsequently be established.

So we simulated the following uniform CA's (eight in number) on the computer. We describe them in brief.

(a) Type-I CA's (Results displayed in Table 1)

(i) o-e-p :

Local rule : Add modulo 2, the values of all four nearest orthogonal neighbours (i.e. <Rule-90, Rule-90>) assuming periodic boundary conditions.

(ii) o-e-n :

Same as the previous case, but now with null boundary conditions.

(iii) <u>o-i-p</u> :

Local rule : Add modulo 2, the values at all four nearest orthogonal neighbours, including its own (i.e. <Rule-90, Rule-150>), assuming <u>periodic</u> boundary conditions.

(iv) <u>o-i-n</u> :

Same as the previous CA, but now with <u>null</u> boundary conditions.

(b) Type-II CA's (Results displayed in Table 2)

(i) <u>d-e-p</u> :

Local rule : Add modulo 2, the values of all four nearest diagonal neighbours, assuming <u>periodic</u> boundary conditions.

(ii) <u>d-e-n</u> :

Same as the previous case, but now with <u>null</u> boundary conditions.

(iii) <u>d-i-p</u> :

Local rule : Add modulo 2, the values at all four nearest diagonal neighbours, also including its own, assuming <u>periodic</u> boundary conditions.

(iv) <u>d-i-n</u> :

Same as the previous case, but now with <u>null</u> boundary conditions.

Generating Pseudo-random sequences using Cellular Automata

Let us very briefly discuss the applicability of CA as, possible pseudo-random number generators.

By far, one of the most popular random number generators is the linear congruential sequence ([15]), where the desired sequence of random numbers x_n , is obtained by setting :

$$X_{n+1} = (aX_n + c) \bmod m \quad (n \geq 0),$$

where : $0 \leq a < m$, ('a' is called the 'multiplier')

$0 \leq c < m$, ('c' is called the 'increment')

and $0 \leq X_0 < m$, ('X_0' is called the 'starting value').

The integers m,a,c,X_0; are chosen in such a way that the periodicity of the random sequence is large.

Apparently, this seems to bear no relation with CA, but it was the genius of Wolfram to observe that the rule $X_{n+1} = (aX_n + c) \bmod m$ is nothing but a 1-d CA rule. Since then he has made an extensive study of CA applications in pseudo-random sequence generation ([29]).

We would like to use 2-d CA for generating such pseudo-random sequences . Now, instead of generating a pseudo-random sequence of numbers, we would like to generate a pseudo-random sequence of matrices. The CA which does it will be said to be a pseudo-random pattern generator. Use of 2-d CA for pseudo-random pattern generation, has been studied extensively by D. Roy Chowdhury et al. ([24]). Using hybrid CA (with null boundary conditions), the pseudo-random patterns obtained by them, seemed to have passed most of the randomness tests, as given in Knuth ([15]).

We tried the same, with some simple uniform 2-d CA's, with both periodic and null boundary conditions. The CA's chosen were the one's mentioned earlier, namely, o-e-p, o-e-n, o-i-p; o-i-n, d-e-p, d-e-n, d-i-p, d-i-n; with E_{00} as the seed.

The patterns were tested for randomness, using some of the tests like Equidistribution-test, Serial-test, Permutation-test, etc. and in most cases, they failed to pass these tests.

This seems to suggest that, in order to obtain good pseudo-random patterns using 2-d CA's, one would have to use totally hybrid CA's, rather than uniform CA's with total dependencies (i.e. depending on each nearest neighbour).

Conclusion

In our work, we characterised two-dimensional additive cellular automata, using the functional forms $T(X) = AX + XB$, and $T(X)$ AXB. A great deal of emphasis was laid upon showing that, these functional forms are powerful tools, for deriving important results. Our claim is justified, as we were able to translate many existing proofs, done using other methods, into an equivalent proof, using our method. Along with these, we also proved certain additional results by our method.

We hope that, this method will turn out to be an important tool in the study of additive two-dimensional cellular automata.

Table 1

Dimension (mxn)	o-e-p height	o-e-p cycle length	o-e-n height	o-e-n cycle length	o-i-p height	o-i-p cycle length	o-i-n height	o-i-n cycle length
3x4	2	2	0	12	2	2	0	12
3x5	1	3	3	4	1	3	4	4
3x6	2	2	0	28	2	2	0	28
3x7	1	7	8	1	1	7	0	8
3x8	4	4	0	28	4	4	4	28
3x9	1	7	3	12	1	7	0	12
3x10	1	6	0	124	1	6	0	124
3x11	1	31	4	8	1	31	8	4
3x12	4	4	0	252	4	4	0	84
3x13	1	63	3	28	1	63	0	28
3x14	1	14	0	60	1	14	0	60
3x15	1	15	16	1	1	15	0	16
4x4	2	1	2	2	0	2	2	2
4x5	2	6	0	12	0	6	0	12
4x6	2	2	0	126	2	2	0	126
4x7	2	14	0	24	0	14	0	24
4x8	4	1	0	126	0	4	0	126
4x9	2	14	4	12	2	14	4	12
4x10	2	6	0	682	0	6	0	682
4x11	2	62	0	24	0	62	0	24
4x12	2	4	0	126	4	2	0	126
4x13	2	126	0	252	0	42	0	252
4x14	2	14	2	30	0	14	2	30
4x15	2	30	0	48	2	30	0	48

Table 1 (Contd.)

Dimension (mxn)	o-e-p		o-e-n		o-i-p		o-i-n	
	height	cycle length	height	cycle length	height	cycle length	height	cycle length
5x5	1	3	4	4	1	3	4	4
5x6	1	6	0	28	2	6	0	28
5x7	1	63	7	8	0	63	8	8
5x8	4	12	4	28	0	12	2	28
5x9	1	63	1	12	1	63	4	12
5x10	2	6	0	124	2	6	0	124
5x11	1	1023	8	8	0	1023	8	8
5x12	2	12	0	252	4	12	0	252
5x13	1	63	1	28	0	63	4	28
5x14	1	126	4	60	0	126	2	60
5x15	1	15	15	16	1	15	16	16
6x6	2	2	2	14	2	2	0	14
6x7	1	14	0	56	2	14	0	56
6x8	4	4	0	14	4	4	2	14
6x9	2	14	-	-	2	14	0	252
6x10	1	6	-	-	2	6	-	-
6x11	1	62	-	-	2	62	0	56
6x12	4	4	0	126	4	4	0	126
6x13	1	126	4	28	2	126	0	28
6x14	1	14	-	-	2	14	-	-
6x15	2	30	-	-	2	30	0	112

Table 1 (Contd.)

Dimension (mxn)	o-e-p		o-e-n		o-i-p		o-i-n	
	height	cycle length	height	cycle length	height	cycle length	height	cycle length
7x7	1	7	8	1	0	7	0	8
7x8	4	28	0	56	0	28	8	56
7x9	1	7	7	24	1	7	0	24
7x10	1	126	0	248	0	126	0	248
7x11	-	-	8	8	-	-	8	8
7x12	2	28	0	504	4	28	0	168
7x13	1	63	7	56	0	63	0	56
7x14	2	14	0	120	0	14	8	120
7x15	-	-	16	1	-	-	0	16

Table 2

Dimension (mxn)	d-e-p height	d-e-p cycle length	d-e-n height	d-e-n cycle length	d-i-p height	d-i-p cycle length	d-i-n height	d-i-n cycle length
3x4	2	1	3	1	0	2	0	4
3x5	1	3	3	1	0	3	0	4
3x6	1	2	3	1	2	1	0	4
3x7	1	7	3	1	0	7	0	4
3x8	4	1	3	1	0	4	0	4
3x9	1	7	3	1	1	7	0	4
3x10	1	6	3	1	0	6	0	4
3x11	1	31	3	1	0	31	0	4
3x12	2	4	3	1	4	2	0	4
3x13	1	63	3	1	0	21	0	4
3x14	1	14	3	1	0	14	0	4
3x15	1	15	3	1	1	15	0	4
4x4	2	1	0	6	0	2	2	6
4x5	2	1	1	12	0	2	0	12
4x6	2	1	0	42	0	2	0	126
4x7	2	1	7	1	0	2	0	8
4x8	2	1	0	42	0	2	0	126
4x9	2	1	1	12	0	2	4	12
4x10	2	1	0	186	0	2	0	2046
4x11	2	1	3	24	0	2	0	24
4x12	2	1	0	126	0	2	0	126
4x13	2	1	1	84	0	2	0	252
4x14	2	1	0	30	0	2	2	30
4x15	2	1	15	1	0	2	0	16

Table 2 (Contd.)

Dimension (mxn)	d-e-p		d-e-n		d-i-p		d-i-n	
	height	cycle length	height	cycle length	height	cycle length	height	cycle length
5x5	1	3	1	4	1	3	4	1
5x6	1	6	1	28	0	6	0	28
5x7	1	21	7	1	0	63	0	8
5x8	4	1	1	28	0	4	4	28
5x9	1	21	1	12	0	63	0	12
5x10	1	6	1	124	2	6	0	124
5x11	1	93	3	8	0	1023	8	4
5x12	2	12	1	252	0	12	0	84
5x13	1	63	1	28	0	63	0	28
5x14	1	42	1	60	0	126	4	60
5x15	1	15	15	1	1	15	0	16
6x6	1	2	0	14	2	1	0	14
6x7	1	14	7	1	0	14	0	8
6x8	4	1	0	14	0	4	2	14
6x9	1	14	1	84	2	14	0	252
6x10	1	6	0	434	0	6	-	-
6x11	1	62	3	56	0	62	0	56
6x12	2	4	0	126	4	2	0	126
6x13	1	126	1	28	0	42	0	28
6x14	1	14	0	210	0	14	-	-
6x15	1	30	15	1	2	30	0	16

Table 2 (Contd.)

Dimension (mxn)	d-e-p		d-e-n		d-i-p		d-i-n	
	height	cycle length	height	cycle length	height	cycle length	height	cycle length
7x7	1	7	7	1	0	7	0	8
7x8	4	1	7	1	0	4	0	8
7x9	1	7	7	1	1	7	0	8
7x10	1	42	7	1	0	126	0	8
7x11	1	217	7	1	-	-	0	8
7x12	2	28	7	1	0	28	0	8
7x13	1	63	7	1	0	63	0	8
7x14	1	14	7	1	0	14	0	8
7x15	1	105	7	1	-	-	0	8

The list of abbreviations used is given in the next page.

Abbreviations Used

o-e-p : Orthogonal, Excluding, Periodic.

Local rule : Sum modulo 2 of four nearest orthogonal neighbours, assuming periodic boundary conditions.

o-e-n : Orthogonal, Excluding, Null.

Local rule : Same as the previous case, only that the boundary condition is null .

o-i-p : Orthogonal, Including, Periodic.

Local rule : Sum modulo 2 of four nearest orthogonal neighbours, including itself, assuming periodic boundary conditions.

o-i-n : Orthogonal, Including, Null.

Local rule : Same as the previous case, only that the boundary condition is null.

d-e-p : Diagonal, Excluding, Periodic

Local rule : Sum modulo 2 of four nearest diagonal neighbours, assuming periodic boundary conditions.

d-e-n : Diagonal, Excluding, Null.

Local rule : Same as the previous case, only that the boundary condition is null.

d-i-p : Diagonal, Including, Periodic.

Local rule : Sum modulo 2 of four nearest diagonal neighbours, including itself, assuming <u>periodic</u> boundary conditions.

d-i-n : Diagonal, Including, Null.

Local rule : Same as the previous case, only that the boundary condition is <u>null</u>.

Note : The blank entries in the above tables are due to the fact that, the cycle lengths in these cases were very large, so, the computations had to be abandoned, and thus the reading was not available.

In all the cases we have taken E_{00} to be the starting configuration. From Corollary 3.1, we know that the cycle lengths of the CA's ; o-e-p, o-i-p, d-e-p, d-i-p, are all maximum cycle lengths. We do not know whether the cycle lengths in the tables of o-e-n, o-i-n, d-e-n, d-i-n, are the maximum cycle lengths.

List of References

1. A so, H. and N. Honda, Dynamical characteristics of linear cellular automata, JCCS, Vol. 30 (1985), 291-317.

2. Atrubin, A.J., 'A one dimensional real-time iterative multiplier', IEEE Trans. Comput. EC-14 (1965), 394.

3. Banks, E.R., 'Information processing and transmission in cellular automata,' MIT Project MAC report no. TR-81, 1971.

4. Barua, R. and Pabitra Pal Chowdhury, Finite cellular automata and linearity. Proc. National Seminar on TCS, Ed - P.S. Thiagarajan, 1991.

5. Barua, R. and S. Ramakrishnan, σ-game, σ^{+}-game and 2-d additive CA, handwritten notes, 1993.

6. Burks, A.W. Essays on cellular automata (University of Illinois, Urbana), 1970.

7. Codd, E.F. Cellular Automata (Academic, New York), 1968.

8. Cole, S.N., 'Real-time computation by n-dimensional iterative arrays of finite state machines', IEEE Trans. Comput. C-18 (1969), 349.

9. Das, A.K. and P. Pal Chaudhuri. An efficient on-chip deterministic test pattern generation scheme. Euromicro Journal, Microprocessing and Microprogramming, 26 (1989), 195-204.

10. Das, A.K., Additive Cellular Automata : Theory and Application as a Built-in Self-test Structure. Ph.D. thesis, I.I.T. Kharagpur, 1990.

11. Das, A.K. and P. Pal Chaudhuri, Efficient characterisation of cellular automata. Proc. IEEE (Part E), 137 (1990), 81-87.

12. Deutsch, E.S., 'Thinning algorithms on rectangular, hexagonal and triangular arrays', Commun. ACM 15(1972), 827.

13. Herman, G.T., 'Computing ability of a developmental model for filamentous organisms,' J. Theor. Biol. 25 (1969), 421.

14. Knuth, D.E. Vol-I, Fundamental Algorithms.

15. Knuth, D.E. Vol.-II, Seminumerical Algorithms.

16. Langer, J.S., 'Instabilities and pattern formation in crystal growth', Rev. Mod. Phys. 52 (1980), 1.

17. Lindenmayer, A., 'Mathematical models for cellular interactions in development,' J. Theoret. Biol. 18 (1968), 280.

18. Mac Duffee, C.C., The theory of matrices, Chelsee Publishing Co., New York, 1956.

19. Martin, O., A. Odlyzko and S. Wolfram, 'Algebraic properties of cellular automata,' Commun. Math. Phys. 93 (1984), 219-258.

20. Nishio, H., 'Real time sorting of binary numbers by 1-dimensional cellular automata', Kyoto University report, 1981.

21. Miller, J.C.P., 'Periodic forests of stunted trees', Philos. Trans. R. Soc. London, Ser. A 293 (1970), 63 .

22. Ramakrishnan, S., Personal Communication.

23. Rosenfeld, A., Picture Languages. Academic, New York (1979).

24. Roy Chowdhury, D., P. Subbarao and P. Pal Chaudhuri, 'On the characterisation of 2-d cellular automata using matrix algebra', Information Sciences (to appear).

25. Sternberg, S.R., 'Language and architecture for parallel image processing', in Pattern Recognition in Practice, edited by E.S. Gelesma and L.N. Kanal (North-Holland, Amsterdam),(1980), 35.

26. Sutner, K., The σ-game and cellular automata, Amer. Math. Monthly, Jan. 1990.

27. Sutton, C., 'Forests and numbers and thinking backwards', New Sci. 90 (1981), 209.

28. Wolfram, S., 'Statistical mechanics of cellular automata,' Rev. Mod. Phys. 55 (1983), 601.

29. Wolfram, S., 'Random sequence generation by cellular automata', Adv. Applied Math. 7 (1986), 123.

30. Ulam, S., 'Some ideas and prospects in biomathematics', Ann. Rev. Bio. (1974), 255.