σ-game, σ^+-game, and Two-dimensional Additive Cellular Automata

by
Rana Barua and S. Ramakrishnan

1 Introduction

The σ- game is a combinatorial game played on a graph $G = (V,\, E)$ which was intoduced by Sutner in [9]. It is related to a battery-operated toy MERLIN , discussed in [7] by Pelletier. In the σ-game, each vertex assumes one of two states *viz.* 0 or 1. One may think of 0 as the OFF state and 1 as the ON state. An assignment of states to the vertices will be called a *configuration.* Thus a configuration simply gives a description of the states of the vertices at any given instant. If, for instance, the underlying graph is a rectangular grid then a configuration is simply an array of 0's and 1's and can easily be identified with a subset of the set of grid points or with a 0-1 matrix. A *move* in the σ-game consists of *the player* choosing a vertex. If the vertex v is chosen, then the states of *all* the neighbouring vertices change. The *opponent* chooses two configurations X_s (the source configuration) and X_t (the target configuration). To win, the player has to find a sequence of moves that will transform X_s to X_t. Such a sequence of moves will be called a *solution* for $(X_s,\, X_t)$ and when a solution exists $(X_s,\, X_t)$ will be called a *winning pair.* The σ^+-game is defined in much a similar fashion — here a move v will cause the state of v as well as the states of all the neighbouring vertices to change.

One can think of the set of configurations $\mathcal{C}_\mathcal{G}$ as a vector space over $GF(2)$, the trivial field consisting of 0 and 1, where + denotes addition modulo 2. It is not hard to see (*cf.* [9]) that a sequence of moves by the player does not depend on the order in which the vertices are chosen and *hence can be identified with a subset of V. Thus a sequence of moves can be thought of as a configuration.* Denote by $\sigma(Z)$ the configuration obtained *from* the all-zeros configuration $\mathbf{0}$ when the player chooses the configuration Z. Similarly, define $\sigma^+(Z)$ for the σ^+-game. As shown in [9], both $\sigma, \sigma^+ : \mathcal{C}_\mathcal{G} \longmapsto \mathcal{C}_\mathcal{G}$ are linear and

$$\sigma(Z) = A.Z; \quad \sigma^+(Z) = (A + I).Z\,; \tag{1}$$

where A is the adjacency matrix of the graph G. Note that in (1), Z is a configuration and hence can be thought of as a column vector of 0's and 1's. Also, observe that (*cf.* [9]) if X_s is the source configuration chosen by the opponent and Z the configuration chosen by the player, then the resulting configuration is simply $\sigma(Z) + X_s$. Thus Z is a solution for $(X_s\,, X_t)$ *iff*

$$\sigma(Z) + X_s = X_t$$

iff

$$\sigma(Z) = X_s + X_t.$$

Thus the number of solutions for a winning pair $(X_s,\, X_t)$ is 2^k (*respectively,* 2^{k^+}), where k (*resp.,* k^+)is the dimension of the kernel of the linear map σ (*resp.,* σ^+) in the case of the σ-game (*resp.,* σ^+-game).

Sutner [9] has shown that when G is the rectangular grid $P_{m,n}$ on vertices $\{1, 2, ..., m\} \times \{1, 2, ...n\}$, then the number of solutions is 2^k, where $k = \gcd(m + 1, n + 1) - 1$. The problem for σ^+ remained open.

In this article we shall give a different proof of Sutner's result that is, perhaps, more transparent and general. We obtain it by introducing a sequence of polynomials $p_n(\lambda)$ (see below) and then calculating the dimension of the kernel of $p_n(A)$, A being a suitable matrix. Similar polynomials, denoted by π_n, were introduced by Sutner in [8] and their coefficients explicitly obtained. Our main technique for analyzing the σ^+-game is to examine the divisibility properties of these polynomials $p_n(\lambda)$ which were hardly touched upon by Sutner in [8]. Our method yields a simple algorithm for finding the dimension of the kernel of σ^+ and also gives a necessary and sufficient condition for the reversibily of σ^+ thus partially answering a question posed by Sutner in [8].(See 4.2 below.) Furthermore, we explicitly compute the number of solutions of the σ^+-game in the case when one of m, n is of the form $2^k - 1$ (cf.4.6). Lastly, we look at the σ-game and the σ^+-game played on cylinders and tori.

Acknowledgement: We are grateful to a referee for bringing our notice to [8] and for asking us to consider the games played on cylinders and tori.

2 Two-dimensional cellular automata

A two-dimensional cellular automaton (CA, in brief) is a discrete dynamical system consisting of an $m \times n$ array of *cells or sites.* At any given instant, each cell assumes *state* 0 or 1. The cell values evolve synchronously in discrete time step. The state of a cell at time $t+1$ depends on the states of its neighbours (specified in advance) according to a certain local rule. For instance, in the simplest case, the state of each cell at time $t+1$ is the sum (modulo 2) of the states of its nearest *vertical and horizontal* neighbours. Thus, the state of cell (i,j) at time $t+1$, denoted by $c_{i,j}^{t+1}$, is given by

$$c_{i,j}^{t+1} = c_{i-1,j}^{t} + c_{i+1,j}^{t} + c_{i,j-1}^{t} + c_{i,j+1}^{t}\ (\mathrm{mod}2). \tag{2}$$

(Observe that we take $c_{0,j}^{t} = c_{i,0}^{t} = c_{i,n+1}^{t} = c_{m+1,i}^{t} = 0$). (For a detailed study of cellular automata and their various applications one is refered to the fundamental paper of Wolfram [11]. The paper of Martin, Odlyzko and Wolfram [5] gives an excellent algebraic treatment of additive CA).

As in [9] we shall call such an automaton a *σ-automaton*. Define a *configuration* of a CA to be a map from the set of grid points to $\{0,1\}$ so that a configuration can be thought of as an $m \times n$ array or matrix of 0's and 1's. Thus a configuration simply gives the states of the cells at any given instant. If X denotes the configuration at time t, let $T(X)$ denote the configuration at time $t+1$. Then for the σ-automaton on $P_{m,n}$, it is not hard to check that

$$T(X) = A_m.X \quad + \quad X.A_n, \tag{3}$$

where A_m denotes the $m \times m$ tridiagonal matrix

$$\begin{pmatrix} 0 & 1 & 0 & 0 & . & . & . & 0 \\ 1 & 0 & 1 & 0 & . & . & . & 0 \\ 0 & 1 & 0 & 1 & . & . & . & 0 \\ 0 & 0 & 1 & 0 & 1 & . & . & 0 \\ . & . & . & . & . & . & . & . \\ 0 & 0 & . & . & . & 1 & 0 & 1 \\ 0 & 0 & . & . & . & 0 & 1 & 0 \end{pmatrix},$$

over $GF(2)$. Observe that the matrix A_m is simply the matrix that specifies the vertical dependency of each cell. Similarly, the matrix A_n is the matrix specifying the horizontal dependency.The connection with the σ-game is seen as follows. (See [9] for details). In the σ- game played on $P_{m,n}$, if the *source* configuration is the *null* configuration 0 and the player chooses the configuration X, then the state of the cell (i, j) will be affected only by those cells in its neighbourhood that were chosen by the player. Consequently, the state of the $(i,\ j)$th cell $a_{i,j}$ is given by

$$a_{i,j} = x_{i,j-1} + x_{i,j+1} + x_{i-1,j} + x_{i+1,j} (\text{mod} 2);$$

where X is the configuration chosen by the player and $x_{i,j}$ denotes the state of the cell (i, j) which is 1 if chosen by the player; 0 otherwise. Comparing this with equation (2), one easily sees that for the σ-game played on $P_{m,n}$

$$\sigma(X) \quad = \quad A_m.X \quad + \quad X.A_n. \tag{4}$$

Analogously, one can define the σ^+-automaton. Here, the state of a cell at time $t+1$ is the sum (modulo 2) of the states (at time t) of the nearest vertical and horizontal neighbours as well as the state of the cell itself. In the case of the σ^+-automaton, configuration X yields in one time step the configuration

$$\sigma^+(X) \quad = \quad A_m.X \quad + \quad X.A_n^+, \tag{5}$$

or equivalently,

$$\sigma^+(X) \quad = \quad A_m^+.X \quad + \quad X.A_n; \tag{6}$$

where $A_k^+ = A_k + I_k$; I_k being the $k \times k$ identity matrix.

3 The number of solutions on $P_{m,n}$

As observed in the introduction, to find the number of solutions of the σ-game (*respectively*, σ^+-game), it suffices to find the dimension of the kernel of the linear map σ (*respectively*, σ^+). If X is a configuration (regarded as a matrix), let $X_{(i)}$ denote the ith column (regarded as a column vector). Then the following result of Sutner [9] characterizes the configurations in ker(σ), the kernel of σ.

Proposition 3.1 *The configuration X is in the kernel of σ iff each column $X_{(i)}$, $1 < i \leq n$, satisfies the recurrence*

$$X_{(i)} = A_m.X_{(i-1)} + X_{(i-2)}$$

and

$$X_{(n+1)} \stackrel{\text{def}}{=} A_m.X_{(n)} + X_{(n-1)} = 0;$$

where $X_{(0)} = 0$.

Similarly, for the σ^+-game we have

Proposition 3.2 $X \in$ *ker*(σ^+) *iff*

$$X_{(i)} = A_m^+.X_{(i-1)} + X_{(i-2)}, \quad 1 < i \leq n,$$

and

$$X_{(n+1)} \stackrel{\text{def}}{=} A_m^+.X_{(n)} + X_{(n-1)} = 0.$$

Let $p_m(\lambda)$ (*respectively*, $p_m^+(\lambda)$) denote the characteristic polynomial of A_m (*respectively*, A_m^+). The crucial observation is that $p_m(\lambda)$ satisfies a recurrence relation similar to that in Proposition 3.1. (Note that all polynomials are over $GF(2)$. For an explicit description of the coefficients see [8].)

Proposition 3.3 *Let $p_0(\lambda) = 1$ and $p_1(\lambda) = \lambda$. Then $p_n(\lambda)$ is given by the recurrence*

$$p_n(\lambda) = \lambda p_{n-1}(\lambda) + p_{n-2}(\lambda). \tag{7}$$

Proof. $p_n(\lambda) = \quad |A_n - \lambda I_n|$

$$= \begin{vmatrix} \lambda & 1 & 0 & . & . & . & . \\ 1 & \lambda & 1 & 0 & . & . & . \\ 0 & 1 & \lambda & 1 & 0 & . & . \\ . & . & . & . & . & . & . \\ . & . & . & . & 0 & 1 & \lambda \end{vmatrix}$$

$$= \quad \lambda \begin{vmatrix} \lambda & 1 & 0 & . & . & . & . \\ 1 & \lambda & 1 & 0 & . & . & . \\ 0 & 1 & \lambda & 1 & 0 & . & . \\ . & . & . & . & . & . & . \\ . & . & . & . & . & 1 & \lambda \end{vmatrix}_{(n-1)\times(n-1)} + \begin{vmatrix} 1 & 1 & 0 & . & . & . & 0 \\ 0 & \lambda & 1 & 0 & . & . & 0 \\ 0 & 1 & \lambda & 1 & . & . & 0 \\ . & . & . & . & . & . & . \\ . & . & . & . & . & 1 & \lambda \end{vmatrix}_{(n-1)\times(n-1)}$$

$$= \lambda p_{n-1}(\lambda) + \begin{vmatrix} \lambda & 1 & . & . & . \\ 1 & \lambda & 1 & . & . \\ . & . & . & . & . \\ . & . & . & 1 & \lambda \end{vmatrix}_{(n-2)\times(n-2)}$$

$$= \lambda p_{n-1}(\lambda) + \quad p_{n-2}(\lambda). \quad \Box$$

A column (*respectively*, row) n-vector x is said to be in the kernel of an $n \times n$ matrix A if $Ax = 0$ (*resp.*, $xA = 0$). Clearly, for a symmetric matrix the *row* kernel and the *column* kernel are isomorphic.

Propositions 3.1 and 3.3 yield

Theorem 3.4 *There is a one-one correpondence between ker(σ) and the kernel of $p_n(A_m)$.*
(Note that $p_n(A_m)$) is an $m \times m$ symmetric matrix)

Proof If an $m \times n$ matrix X is in ker(σ), then by Proposition 3.1 the column vectors $X_{(i)}$ satisfy the recurrence relation

$$X_{(i)} = A_m X_{(i)} + X_{(i-2)}$$

and

$$X_{(n+1)} \stackrel{\text{def}}{=} A_m X_{(n)} + X_{(n-1)} = 0.$$

We shall show by induction that

$$X_{(i)} = p_{i-1}(A_m).X_{(1)}, \qquad 1 < i \leq n.$$

To see this, observe that
$X_{(i+1)} = A_m X_{(i)} + X_{(i-1)}$
$= A_m.p_{i-1}(A_m).X_{(1)} + p_{i-2}(A_m).X_{(1)}$, by induction hypothesis
$= (A_m.p_{i-1}(A_m) + p_{i-2}(A_m)).X_{(1)}$
$= p_i(A_m).X_{(1)}$, by Proposition 3.3.
Hence,

$$p_n(A_m).X_{(1)} = X_{(n+1)} = 0.$$

So $X_{(1)}$ belongs to the kernel of $p_n(A_m)$. Thus with each $X \in \ker(\sigma)$ we associate the first column vector $X_{(1)}$ which is in the kernel of $p_n(A_m)$. Further, if a column vector X' is in the kernel of $p_n(A_m)$, then we define a sequence $\{Y_i, 1 \leq i \leq n\}$ of column vectors by the recurrence

$$Y_1 = X',$$

$$Y_i = A_m.Y_{i-1} + Y_{i-2}.$$

Then

$$\begin{aligned} Y_{n+1} &\stackrel{\text{def}}{=} A_m.Y_n + Y_{n-1} \\ &= p_n(A_m).Y_{(1)} = p_n(A_m).X' = 0 \end{aligned}$$

By Proposition 3.1, the matrix Y whose columns are Y_i's is in the kernel of σ. Hence the map is onto. To show that it is one-one, let X, Y be in $\ker(\sigma)$ and suppose $X_{(1)} = Y_{(1)}$. Invoking Proposition 3.1 we see that $X_{(i)} = Y_{(i)}$, for all $i, 1 \leq i \leq n$, and hence $X = Y$. So the map is one-one.

This completes the proof.

Given a matrix X, let $X^{(i)}$ denote the ith row vector. Interchanging the role of A_m and A_n and working with row vectors instead of column vectors one can similarly show

Theorem 3.5 *There is a one-one correspondence between ker(σ) and the kernel of $p_m(A_n)$.*

Thus we have

Corollary 3.6 *The kernels of $\sigma, p_n(A_m)$ and $p_m(A_n)$ have the same dimension.*

As an immediate consequence of this we have

Corollary 3.7 *The $m \times m$ matrix $p_{m-1}(A_m)$ is invertible.*

Proof We proof this by induction on m. At the base step, we take $m = 3$. Now,

$$\begin{aligned} p_2(A_3) &= {A_3}^2 + I_3 = \left(A_3^+\right)^2 \\ &= \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \end{aligned}$$

which is clearly invertible. For the inductive step, observe that by Corollary 3.6, the kernel of $p_{m-1}(A_m)$ has the same dimension as that of $p_m(A_{m-1})$. Now

$$p_m(A_{m-1}) = A_{m-1}.p_{m-1}(A_{m-1}) + p_{m-2}(A_{m-1}).$$

By Caley-Hamilton Theorem $p_{m-1}(A_{m-1}) = \mathbf{0}$ and hence

$$p_m(A_{m-1}) = p_{m-2}(A_{m-1}).$$

By induction hypothesis, $p_{m-2}(A_{m-1})$ is invertible. Hence $p_m(A_{m-1})$ is invertible and consequently, $p_{m-1}(A_m)$ is invertible.$\square$

We now show that the dimension of $\ker(\sigma)$ is $\gcd(m+1, n+1) - 1$. But first we prove

Proposition 3.8 *For $n \geq m$ we have the following recurrence*

$$p_n(\lambda) = p_{n-m}(\lambda)p_m(\lambda) + p_{n-m-1}(\lambda)p_{m-1}(\lambda).$$

(Take $p_{-1}(\lambda) = 0$).

Proof We prove this by induction on n. If $n = m+1$ the result is obvious. So assume that $n > m+1$. Now

$$\begin{aligned} p_n(\lambda) &= \lambda p_{n-1}(\lambda) + p_{n-2}(\lambda) \\ &= \lambda\{p_{n-m-1}(\lambda)p_m(\lambda) + p_{n-m-2}(\lambda)p_{m-1}(\lambda)\} \\ &\qquad + \{p_{n-m-2}(\lambda)p_m(\lambda) + p_{n-m-3}(\lambda)p_{m-1}(\lambda)\} \\ &\qquad\qquad \text{(by induction hypothesis)} \\ &= \{\lambda p_{n-m-1}(\lambda) + p_{n-m-2}(\lambda)\}p_m(\lambda) \\ &\qquad + \{\lambda p_{n-m-2}(\lambda) + p_{n-m-3}(\lambda)\}p_{m-1}(\lambda) \\ &= p_{n-m}(\lambda)p_m(\lambda) + p_{n-m-1}(\lambda)p_{m-1}(\lambda). \qquad \square \end{aligned}$$

Corollary 3.9 *For any positive integer k we have*

$$p_{2k}(\lambda) = (p_k(\lambda) + p_{k-1}(\lambda))^2 \tag{8}$$

and

$$p_{2k+1}(\lambda) = \lambda p_k^2(\lambda) \tag{9}$$

Proof We shall prove the second equation, the proof of the first equation is similar.

By Corollary 3.8 we have $p_{2k+1}(\lambda)$
$= p_k(\lambda)p_{k+1}(\lambda) + p_{k-1}(\lambda)p_k(\lambda)$
$= p_k(\lambda)\{p_{k+1}(\lambda) + p_{k-1}(\lambda)\}$
$= p_k(\lambda).\lambda p_k(\lambda)$

by equation (7)

$= \lambda p_k^2(\lambda)$.

We now prove the main result of this section due to Sutner[9].

Theorem 3.10 *The dimension of ker(σ) is gcd($n+1, m+1$) $- 1$.*

In particular, σ is invertible iff gcd($n+1, m+1$) $= 1$ i.e. iff $n+1$ and $m+1$ are relatively prime.

Proof By Corollary 3.6 it suffices to prove that the dimension of the kernel of $p_n(A_m)$ or of the kernel of $p_m(A_n)$ is $\gcd(n+1, m+1) - 1$.

W.l.g. assume $n \geq m$. Let δ denote the required dimension. If $m+1$ divides $n+1$, then $gcd(n+1, m+1) - 1 = m$ and $n+1 = q(m+1)$ for some integer q. By Proposition 3.8, we have

$$p_n(A_m) = p_{n-m}(A_m)p_m(A_m) + p_{n-m-1}(A_m)p_{m-1}(A_m).$$

But $p_m(A_m) = 0$ and by Corollary 3.7 $p_{m-1}(A_m)$ is invertible. Hence δ is equal to the dimension of kernel of $p_{n-m-1}(A_m)$. Repeating the above process $q-1$ times we find that the dimension δ is equal to that of the kernel of $p_m(A_m)$, which is the null $m \times m$ matrix. Hence $\delta = m$ and we are done. So assume that $m+1$ does not divide $n+1$. By the Euclidean algorithm, choose a sequence of integers $r_1 > r_2 > \cdots > r_k = r_{k+1}$ such that for some integers $q_1, q_2, \cdots, q_{k+1}$,

$$n+1 = q_1(m+1) + r_1$$

$$m+1 = q_2 r_1 + r_2$$

$$r_1 = q_3 r_2 + r_3$$

$$\vdots$$

$$r_{k-1} = q_{k+1} r_k + r_{k+1}$$

and

$$r_k = r_{k+1} = gcd(n+1, m+1).$$

We shall prove by induction on i that δ equals to the dimension of the kernel of $p_{r_{i+1}-1}(A_{r_i-1})$. First observe that, by the argument given above, the dimension δ of the kernel of $p_n(A_m)$ is equal to that of the kernel of $p_{n-m-1}(A_m)$, and hence (by repeating the argument q_1 times), to that of the kernel of $p_{n-q_1(m+1)}(A_m) = p_{r_1-1}(A_m)$. But by Corollary 3.6, the dimension of the kernel of $p_{r_1-1}(A_m)$ is the same as that of the kernel of $p_m(A_{r_1-1})$. Thus δ is the dimension of the kernel of $p_m(A_{r_1-1})$. Now if we argue as above with m playing the role of n, $r_1 - 1$ playing the role of m and q_2 playing the role of q_1, we find that δ is equal to the dimension of the kernel of the matrix $p_{r_2-1}(A_{r_1-1})$. The inductive step can be obtained in exactly the same manner. Thus

$$\delta = \text{dimension of} \quad ker(p_{r_{k+1}-1}(A_{r_k-1})).$$

But $r_{k+1} = r_k$ and the use of Caley-Hamilton theorem immediately shows that

$$\delta = r_k - 1 = gcd(n+1, m+1) - 1.$$

This completes the proof.

It is well-known *cf*[4] that the matrix equation

$$A.X + X.B = C$$

has a unique solution iff $f(\lambda)$ and $g(\lambda)$ are relatively prime, where $f(\lambda)$ and $g(\lambda)$ are the characteristic polynomials of A and B respectively. In our case, this means that the linear map σ is invertible iff $p_n(\lambda)$ and $p_m(\lambda)$ are relatively prime. Thus we have the following interesting result.

Theorem 3.11 *$p_n(\lambda)$ and $p_m(\lambda)$ are relatively prime iff $n+1$ and $m+1$ are relatively prime.*

4 The σ^+-game

The analysis of the σ^+-game is very similar to that of the σ-game which was done in Section 3. We state without proof the following which can be established exactly as in the case of the σ- game.

Theorem 4.1 *There is a one-one correspondence between ker(σ^+) and the kernels of $p_n(A_m^+)$ and $p_m(A_n^+)$.*

In particular, the kernels of $(\sigma^+), p_n(A_m^+)$, and $p_m(A_n^+)$ have the same dimension. $\square$

Remark Unlike the σ-game, the above theorem does not give us a nice expression for the number of solutions of the σ^+-game. Nevertheless, it does give us an algorithm to compute the number of solutions. To this end, one simply computes the matrix $p_n(A_m^+)$ (or the matrix $p_m(A_n^+)$) using the recursion in (7) and then find the rank of the resulting matrix. This, however, is not a very efficient algorithm but in certain cases it may be relatively easy provided we know the form of $p_n(\lambda)$. This we shall study below.

Now observe that $p_n^+(\lambda)$, the characteristic polynomial of A_n^+, satisfies

$$p_n^+(\lambda) = p_n(1-\lambda) = p_n(1+\lambda).$$

Since the linear map σ^+ is given by equations (5) or (6), arguing as in Theorem 3.11, we see that σ^+ is one-one iff $p_m(\lambda)$ and $p_n(1+\lambda)$ are relatively prime iff $p_m(1+\lambda)$ and $p_n(\lambda)$ are relatively prime. Thus we have

Theorem 4.2 *The σ^+-game has a unique solution iff $p_m(\lambda)$ and $p_n(1+\lambda)$ are relatively prime iff $p_m(1+\lambda)$ and $p_n(\lambda)$ are relatively prime.* $\square$

Remark Theorem 4.2 gives us an algorithm to test whether the σ^+-game played on the rectangular $m \times n$ grid has a unique solution or not. One simply computes $p_m(\lambda)$ and $p_m(1+\lambda)$ using equation (7) and then test whether these two polynomials are relatively prime.

In order to apply Theorem 4.2 more efficiently in certain situations we obtain some simple properties of the polynomials $p_n(\lambda)$'s which are interesting in their own right. (These polynomials were also introduced in [8] as π_n and some of the results mentioned here were obtained. But the divisibility properties studied here were hardly touched upon in [8].)

Theorem 4.3 *$p_{m-1}(\lambda)$ divides $p_n(\lambda)$ iff $n \equiv m-1 \bmod m$.*

In particular, (putting $m = 2, 3$) λ is a factor of $p_n(\lambda)$ iff n is odd and $(1+\lambda)$ is a factor of $p_n(\lambda)$ iff $n \equiv 2 \bmod 3$.

Similarly, $(1+\lambda+\lambda^2)$ is a factor of $p_n(\lambda)$ iff $n \equiv 4 \bmod 5$.

Proof First observe that by the reccurence in Proposition 3.8 we have

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

Since $p_{m-1}(\lambda)$ and $p_{m-2}(\lambda)$ are relatively prime, by Theorem 3.11, it follows that $p_{m-1}(\lambda)$ divides $p_n(\lambda)$ iff it divides $p_{n-m}(\lambda)$. By Euclidean algorithm, there exist integers q and $r, 0 \leq r < m$, such that

$$n = mq + r$$

Repeating the above argument (q times) we see that $p_{m-1}(\lambda)$ divides $p_n(\lambda)$ iff it divides $p_{n-qm}(\lambda) = p_r(\lambda)$, where $r = 0, 1, \cdots, m-1$. Since $p_{m-1}(\lambda)$ cannot divide $p_r(\lambda)$ for $r < m-1$, r must be $m-1$. Thus $p_n(\lambda)$ divides $p_n(\lambda)$ iff $n \equiv m - 1 \bmod m.\Box$

In the case of 1-dimensional grid *i.e.* when $n = 1$, we have $p_n(1+\lambda) = (1+\lambda)$. Hence, the σ^+-game has a unique solution iff $(1+\lambda)$ is not a factor of $p_m(\lambda)$ *i.e.* iff $m \not\equiv 2 \bmod 3$.

The following can be easily proved by induction. It also follows from the explicit description of the coefficients of $p_n(\lambda)$ given in 3.12 of [8]. (See also 3.14 of [8]).

Theorem 4.4 *1. If $n = 2^k - 2$, then*

$$p_n(\lambda) = \lambda^{2^k - 2} + \lambda^{2^k - 2^2} + \lambda^{2^k - 2^3} + \cdots + 1.$$

2. If $n = 2^k - 1$, then

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

3. If $n = 2^k$, then

$$p_n(\lambda) = \lambda^{2^k} + \lambda^{2^k - 2} + \lambda^{2^k - 2^2} + \cdots + 1$$

Proposition 4.5 *1. If m is of the form $2^k - 1$ and n is of the form $2^l - 1$, then the σ^+-game has a unique solution.*

2. If one of m, n, say m, is of the form $2^k - 1$, then the number of solutions of the σ^+-game is 2^s, where s is the dimension of the kernel of the matrix $(A_n^+)^m$.

3. If m is odd and $n \equiv 2 \bmod 3$(or vice versa*), then σ^+ is* not *invertible*

Similarly, if $m, n \equiv 4 \bmod 5$, then σ^+ is not invertible.

Proof 1. By Theorem 4.2, the σ^+-game has a unique solution iff $p_m(\lambda)$ and $p_n(1+\lambda)$ are relatively prime.By Theorem 4.4, $p_m(\lambda) = \lambda^m$ and $p_n(1+\lambda) = (1+\lambda)^n$. Hence $p_m(\lambda)$ and $p_n(1+\lambda)$ are relatively prime and so σ^+-game has a unique solution.
2. By Theorem 4.1, the number of solutions of the σ^+-game is 2^s, where s is the dimension of the kernel of $p_m(A_n^+) = (A_n^+)^m$, by Theorem 4.4. Hence the result.
3. If m is odd then λ is a factor of $p_m(\lambda)$. Further, if $n \equiv 2 \bmod 3$, then $(1+\lambda)$ is a factor of $p_n(\lambda)$ and hence λ is a factor of $p_n(1+\lambda)$. So, by Theorem 4.2, σ^+ is not invertible.

The last assertion can be proved similarly. □

Remark In the case of the MERLIN graph *cf.* [9, 7] we have $m = n = 3 = 2^2 - 1$ and hence the game has a unique solution.

We now compute the exact number of solutions of the σ^+-game in Proposition 4.5(2).

First observe that A_n^+ is the characteristic matrix [1] of a one-dimensional CA consisting of n-cells which evolve according to **Rule 150** under *null* *boundary conditions.* In other words, the states of the cells evolve synchronously in discrete time steps and the state of each cell at time $t+1$ is simply the sum (modulo 2) of the states of the nearest neighbours and the state of the cell itself at time t. For the boundary cells, the left (right) neighbour of the extreme left (right) cell is assumed to be always in state 0. If $x=(x_1,\cdots,x_n)$ denotes the configuration at time t, then the configuration at time $t+1$ is given by $A_n^+.x^T$. Thus to find the kernel of $(A_n^+)^m$, we need to find all configurations x that evolve to the null configuration in m *time steps* under **Rule 150** with null boundary conditions.

Given a configuration $a=(a_1,\cdots,a_n)$, let

$$a^*=(0,a_1,\cdots,a_n,0,a_n,a_{n-1},\cdots,a_1). \tag{10}$$

Then it is not hard to see *cf.*[5, 4F] that a evolves to the null configuration in m time steps under **Rule 150** with null boundary conditions iff a^* evolves to the null configuration in m time steps under **Rule 150** with *periodic boundary conditions.* Thus to find the cardinality of $\left(A_n^+\right)^m$, it suffices to count the number of configurations of the form (10) that evolve to the null configuration in m time steps under **Rule 150** with periodic boundary conditions.

Let T_N denote the characteristic matrix of an N-cell **Rule 150** CA with periodic boundary conditions. Then *cf.*[1]

$$T_N=\begin{pmatrix} 1 & 1 & 0 & . & . & . & 0 & 1 \\ 1 & 1 & 1 & 0 & . & . & . & 0 \\ 0 & 1 & 1 & 1 & 0 & . & . & 0 \\ . & . & . & . & . & . & . & . \\ 1 & 0 & 0 & . & . & 0 & 1 & 1 \end{pmatrix}$$

Also observe that if $n\not\equiv 2 \bmod 3$, then A_n^+ is invertible. To see this, let μ_n denote the determinant of A_n^+. As in the proof of Proposition 3.3, one can show that

$$\mu_n=\mu_{n-1}+\mu_{n-2}.$$

Hence,

$$\mu_n=\mu_{n-1}+\mu_{n-2}=\mu_{n-2}+\mu_{n-3}+\mu_{n-2}=\mu_{n-3}$$

Since $n\not\equiv 2 \bmod 3$, it follows that $\mu_n=\mu_3$ or μ_4 and hence $\mu_n\neq 0$.

So assume that $n \equiv 2 \bmod 3$. The number of cells in (10) is clearly $2n+2 \equiv 0 \bmod 6$. Put $N = 2n+2$.

For any integer K, let $D_2(K)$ denote the largest integer 2^j that divides K. Call a vector (configuration) $x = (x_1, \cdots, x_N)$ a *palindrome* if the coordinates read the same both ways *i.e.* if $x_i = x_{N+1-i}$. We first prove

1^0. *The kernel of T_N consists of four elements of which two (one of them null) are of the form (10) and two (one null) are palindromes.*

Proof Plainly, $x = (x_1, \cdots, x_N)$ is in the kernel of T_N iff $T_N.x^T = 0$ *i.e.* iff

$$x_N + x_1 + x_2 = 0$$

$$x_1 + x_2 + x_3 = 0$$

$$\cdots$$

$$x_{N-1} + x_N + x_1 = 0$$

This is equivalent to saying that

$$x_1 + x_2 + x_3 = 0$$

and for all $i, 1 \le i \le N$,

$$x_i = x_{(i+3) \bmod N}.$$

Thus there are four choices for the coordinates of x of which exactly one non-null vector is of the form (10) and one non-null vector is a palindrome.□

Let

$$K(m, N) = \{x\colon\ x \text{ is an } N\text{-vector of the form (10) and} \big(T_N\big)^m.x^T = 0\},$$

$$L(m, N) = \{x\colon\ x \text{ is a palindrome and} \big(T_N\big)^m.x^T = 0\}$$

It is easy to see that,

$$K(m+1, N) = \{x\colon\ x \text{ is an } N\text{-vector of the form (10) and} T_N.x^T \in K(m, N)\},$$

$$L(m+1, N) = \{x\colon\ x \text{ is a palindrome and} T_N.x^T \in L(m, N)\}$$

Hence by 1^0,

$$card(K(m,N)) \le 2card(K(m-1,N)) \le \cdots \le 2^{m-1}card(K(1,N)) = 2^m. \tag{11}$$

Similarly, we have

$$card(L(m,N)) \leq 2^m \tag{12}$$

We now prove by induction on $D = D_2(N)$ that
2^0. *If m a power of 2 and $m \leq D_2(N)$, then*

$$card(K(m,N)) = card(L(m,N)) = 2^m.$$

Futhermore, $ker(\big(T_N\big)^D) = ker(\big(T_N\big)^{2D})$ and $card(ker(\big(T_N\big)^D)) = 4^D$.

Proof *Base step: $D = D_2(N) = 2$.*
Since $N \equiv 0 \bmod 6$, it is easy to see that in this case $N \equiv 6 \bmod 12$. Here we need to show that

$$card(K(2,N)) = card(L(2,N)) = 4,$$

$$card(ker(T_N^2)) = 4^2$$

and

$$ker(\big(T_N\big)^2) = ker(\big(T_N\big)^4).$$

It is not hard to check that

$$x = (x_1, x_2, \cdots, x_N) \in ker(\big(T_N\big)^2)$$

iff for all $i, 1 \leq i \leq N$,

$$x_i + x_{(i+2) \bmod N} + x_{(i+4) \bmod N} = 0.$$

or, equivalently, iff

$$x_1 + x_3 + x_5 = 0$$

$$x_2 + x_4 + x_6 = 0$$

and for all $i, 1 \leq i \leq N$,

$$x_i = x_{(i+6) \bmod N}.$$

Thus if x is of the form (10), then $x_1 = 0$ and hence x_2 and x_4 are either both 0 or both 1. Further, since N is of the form $12k+6$ and x is of the form (10), we have $x_{6k+4} = 0$ and so $x_4 = 0$. Hence x_2 and x_6 are either both 0 or both 1. Consequently, there are four choices for the coordinates of x and so $K(2,N)$ has four elements. Finally, note that there are four choices for

x_1, x_3, x_5 and four choices for x_2, x_4, x_6 and hence in all sixteen choices *i.e.* $card(ker(T_N^2)) = 16$.

To see that $L(2, N)$ has four elements, observe that if x is a palindrome whose coordinates satify the equations above, then

$$x_1 = x_{12k+6} = x_6$$

$$x_2 = x_{12k+5} = x_5$$

$$x_3 = x_{12k+4} = x_4$$

and thus the odd coordinates of x are just the even coordinates in reverse order. Since

$$x_1 + x_3 + x_5 = 0$$

there are four choices for the coordinates of x which are in kernel of $\left(T_N\right)^2$ and are palindromes, *i.e.* $card(L(2, N)) = 4$.

Further observe that x is in kernel of $\left(T_N\right)^4$ iff

$$x_1 + x_5 + x_9 = 0$$

$$x_2 + x_6 + x_{10} = 0$$

$$x_3 + x_7 + x_{11} = 0$$

$$x_4 + x_8 + x_{12} = 0$$

and

$$x_i = x_{(i+12) \bmod N}.$$

But $N = 12k + 6$. Thus $x_i = x_{(i+12) \bmod N}$ implies that $x_i = x_{(i+6) \bmod N}$. Hence the preceding equations are equivalent to

$$x_1 + x_5 + x_3 = 0$$

$$x_2 + x_6 + x_4 = 0$$

and

$$x_i = x_{(i+6) \bmod N}.$$

From this it follows that x is in the kernel of $\left(T_N\right)^4$ iff it is in the kernel of $\left(T_N\right)^2$.

This completes the base step.

Inductive step: Let $N \equiv 0 \bmod 3$ such that $D_2(N) = 2d$, with $d \geq 2$. Then, plainly $D_2(N/2) = d$. Put $N/2 = N'$. Fix m of the form 2^k such that $m \leq 2d$. Then $m/2 = 2^{k-1} \leq d$. By induction hypothesis,

$$card(K(m/2, N')) = card(L(m/2, N')) = 2^{m/2}.$$

A little bit of calculation shows that $(T_N)^2$ acting on an N-vector is equivalent to $T_{N'}$ acting on the even coordinates and $T_{N'}$ acting on the odd coordinates. Also, for an N-vector of the form (10), the odd coordinates form an N'-vector of the form (10) and the even coordinates form a palindromic N'-vector. Since T_N acting successively m times is equivalent to $(T_N)^2$ acting successively $m/2$ times, it follows that an N-vector of the (10) is in the kernel of $(T_N)^m$ iff the N'-vector formed with the odd coordinates is of the form (10) and in the kernel of $(T_{N'})^{m/2}$ and the N'-vector formed with the even coordinates is a palindrome in the kernel of $(T_{N'})^{m/2}$. By induction hypothesis, there are $2^{m/2}$ N'-vectors of the form (10) in the kernel of $(T_{N'})^{m/2}$ and $2^{m/2}$ palindromic N'-vectors in the kernel of $(T_{N'})^{m/2}$. Hence there are $2^{m/2} \times 2^{m/2} = 2^m$ N-vectors of the form (10) in the kernel of $(T_N)^m$ *i.e.* $card(K(m, N)) = 2^m$.

To see that $card(L(m, N)) = 2^m$, first observe that if $m < 2d$, then as m and d are both powers of 2, we have $m \leq d$. Hence by induction hypothesis, $card(L(m, N')) = 2^m$. If v is an N'- vector which is a palindrome, then clearly $v{*}v$ (*i.e.* the concatenation) is an N-vector which is also a palindrome. Hence, there are at least 2^m palindromic N-vector which are in the kernel of $(T_N)^m$. But by (12), $card(L(m, N)) \leq 2^m$ and so $card(L(m, N)) = 2^m$.

Now, suppose $m = 2d$. Here we need to show that there are 2^{2d} palindromic N-vectors which are in the kernel of $(T_N^2)^d$. A vector $x = (x_1, \cdots, x_N)$ is a palindrome iff the odd coordinates are the same as the even coordinates in reverse order. Further, T_N^2 applied to an N-vector is equivalent to $T_{N'}$ applied to the odd coordinates and $T_{N'}$ applied to the even coordinates. Thus to find $card(L(2d, N))$ it is enough to find the number of N'-vectors in the kernel of $(T_{N'})^d$. By induction hypothesis, there are $4^d = 2^{2d}$ vectors in the kernel of $(T_{N'})^d$ and hence $card(L(2d, N)) = 2^{2d}$.

Finally, given $x = (x_1, \cdots, x_N)$, let $x_{od} = (x_1, x_3, \cdots, x_{N-1})$ and $x_{ev} = (x_2, x_4, \cdots, x_N)$. Then, x is in kernel of $(T_N)^{4d}$ only if x_{od} and x_{ev} are both in the kernel of $(T_{N'})^{2d}$ *i.e.* only if x_{od} and x_{ev} are in kernel of $(T_{N'})^d$, by induction hypothesis *i.e.* only if x is in the kernel of $(T_{N'})^d$. This shows that

$$ker((T_N)^{4d}) = ker((T_N)^{2d}).$$

A similar argument shows that $card(ker((T_N)^{2d})) = 4^{2d}$.

This completes the proof of the inductive step and hence of 2^0.

We are now in the position to prove the following.

Theorem 4.6 *Suppose m is of the form $2^k - 1$. If $n \not\equiv 2 \bmod 3$, then the σ^+-game has a unique solution. If $n \equiv 2 \bmod 3$, then the number of solutions is $2^{D_2(2n+2)}$ if $D_2(2n+2) < m$ and is 2^m if $m < D_2(2n+2)$.*

Proof By Proposition 4.5(2), to find the number of solutions it is enough to compute the cardinality of the kernel of $(A_n^+)^m$. If $n \not\equiv 2 \bmod 3$, then as already observed, A_n^+ is invertible and hence the σ^+-game has a unique solution.

Now assume that $n \equiv 2 \bmod 3$. Put $m' = m + 1$. As discussed earlier, we need to find the cardinality of $K(m, 2n+2)$, where $2n + 2 \equiv 0 \bmod 6$. Suppose $m < D_2(2n + 2)$. Then $m' \leq D_2(2n + 2)$. Since m' is a power of 2, by 2^0, the cardinality of $K(m', 2n + 2) = 2^{m'}$. By (11),

$$card(K(m', 2n + 2)) \leq 2card(K(m, 2n + 2)) \leq 2.2^m = 2^{m'}.$$

Consequently, $card(K(m, 2n + 2)) = 2^m$. Now, let $m > D_2(2n + 2)$. Since, by 2^0, $ker((T_{2n+2})^m) = ker((T_{2n+2})^{D_2(2n+2)})$ it follows that

$$card(K(m, 2n + 2)) = card(K(D_2(2n + 2), 2n + 2)) = 2^{D_2(2n+2)}.$$

This completes the proof of Theorem 4.6.

As an immediate consequence we have the following which answers a question of Sutner [9, p 34] in the case when m is of the form $2^k - 1$.

Corollary 4.7 *For every m of the form $2^k - 1, m + (m + 1)/2$ is the least positive integer $n \geq m$ such that the dimension of the kernel of σ^+ on $P_{m,n}$ equals m.*

5 Generalizations

Now consider the σ-game (σ^+-game) played on $m \times n$ cylinders or tori.

In the case of the σ-game, respectively σ^+-game, played on an $m \times n$ cylindrical grid, first observe that by cutting along a vertical line, one can think of a configuration as a $0-1$ $n \times m$ matrix. However, equation (4), respectively equation (5), changes to

$$\sigma(X) \quad = \quad A_n.X \quad + \quad X.C_m, \tag{13}$$

respectively,

$$\sigma^+(X) \quad = \quad A_n.X \quad + \quad X.C_m^+, \tag{14}$$

where C_m is the following $m \times m$ circulant matrix over $GF(2)$

$$\begin{pmatrix} 0 & 1 & 0 & 0 & . & . & . & 1 \\ 1 & 0 & 1 & 0 & . & . & . & 0 \\ 0 & 1 & 0 & 1 & . & . & . & 0 \\ 0 & 0 & 1 & 0 & 1 & . & . & 0 \\ . & . & . & . & . & . & . & . \\ 0 & 0 & . & . & . & 1 & 0 & 1 \\ 1 & 0 & . & . & . & 0 & 1 & 0 \end{pmatrix},$$

and $C_m^+ = C_m + I_m$. Arguing as in Theorem 3.5 it is not hard to see that the number of solutions of the σ-game, respectively σ^+-game, in this case is the cardinality of the kernel of $p_n(C_m)$, respectively $p_n(C_m^+)$. It is easy to compute these cardinalities, by the above methods, when n is of the form $2^k - 1$.

Let $q_m(\lambda)$ denote the characteristic polynomial of C_m. Then it is not hard to see (*cf.*[6]) that $q_m(\lambda) = \lambda p_{m-1}(\lambda)$. Now observe that σ is reversible iff $p_n(\lambda)$ and $q_m(\lambda)$ are relatively prime *i.e.* iff λ does not divide $p_n(\lambda)$ and $\gcd(p_n(\lambda), p_{m-1}(\lambda)) = 1$. By Theorems 4.3 and 3.11 this means that n is even and $\gcd(n+1, m) = 1$. (See also Theorem 3.11 of [8]). In the case of the σ^+-game, we have σ^+ is reversible iff $\gcd(p_n(\lambda), q_m(1+\lambda)) = 1$ *i.e.* iff $\gcd(p_n(\lambda), (1+\lambda)p_{m-1}(1+\lambda)) = 1$ *i.e.* iff $(1+\lambda)$ does not divide $p_n(\lambda)$ and $p_n(\lambda), p_{m-1}(1+\lambda)$ are relatively prime. By Theorems 4.2 and 4.3 this means that $n \not\equiv 2 \bmod 3$ and the σ^+-game on the $(m-1) \times n$ rectangular grid is reversible.

It is easy to see that the σ-game played on a torous is always irreversible. In the case of the σ^+-game played on a torous, the equation (5) is replaced by

$$\sigma^+(X) \quad = \quad C_m.X \quad + \quad X.C_n^+, \tag{15}$$

Hence, σ^+ is reversible iff $\gcd(q_m(\lambda), q_n(1+\lambda)) = 1$
iff $\gcd(\lambda p_{m-1}(\lambda), (1+\lambda)p_{n-1}(1+\lambda)) = 1$
iff $(1+\lambda)$ does not divide both $p_{m-1}(\lambda), p_{n-1}(\lambda)$ *and* $\gcd(p_{m-1}(\lambda), p_{n-1}(1+\lambda)) = 1$
iff $m \not\equiv 0 \bmod 3, n \not\equiv 0 \bmod 3$ and $p_{m-1}(\lambda), p_{n-1}(1+\lambda)$ are relatively prime.

References

[1] Rana Barua, Additive cellular automata and matrices over finite fields, *I.S.I. Tech. Report.* No. **17/91**, 1991.

[2] P. C. Fishburn and N. J. A. Sloane, The solution to Berlekamp's switching game, *Discrete Mathematics*, **74**(1989),263-290.

[3] R. E. Hartwig, Resultants and the solution of $AX - XB = -C^*$, *Siam J. of Appl. Math.*, Vol. **23** No.1(1972), 104-117

[4] C. C. MacDuffee, *The Theory of Matrices*, Chelsea Publishing Co., New York, 1956.

[5] O. Martin, A. M. Odlyzko and S. Wolfram, Algebraic properties of cellular automata, *Comm. Math. Phy.* **93**(1984), 219-258.

[6] P. Mazumder, Problems in two-dimensional additive CA, *M.Tech. (C.Sc.) dissertation*, Indian Statistical Institute, 1993.

[7] D. H. Pelletier, Merlin's magic square, *Amer. Math. Monthly*, **94**(1987), 143-150.

[8] K. Sutner, On σ-Automata, *Complex Systems*, Vol. **2**, No. 1 (1988), 1-28.

[9] K. Sutner, The σ-game and cellular automata, *Amer. Math. Monthly*, Jan. 1990, 24-34.

[10] K. Sutner, Linear cellular automata and the Garden-of-Eden, *Math. Intelligencer*, Vol.**11**, No. 2 (1989), 49-53.

[11] S. Wolfram, Statistical Mechanics and cellular automata, *Rev. Modern Phy.* **55**(1983), 601-644.

Stat-Math Division
Indian Statistical Institute
203 B. T. Road, Calcutta INDIA
e-mail: rana@isical.ac.in

Department of Mathematics
University of Miami
Coral Gables, FL 33124, U S A
e-mail: ramakris@cs.cs.miami.edu