Complex Systems **3** (1989) 209–227

Algebraic Theory of Bounded One-dimensional Cellular Automata

N. Pitsianis
G.L. Bleris
Solid State Section, Physics Department, University of Thessaloniki, 54006 Thessaloniki, Greece

Ph. Tsalides
A. Thanailakis
Laboratory of Electrotechnical and Electronic Materials Technology, Department of Electrical Engineering, School of Engineering, Democritus University of Thrace, 67100 Xanthi, Greece

H.C. Card
VLSI Research Laboratory, Department of Electrical Engineering, University of Manitoba, Winnipeg, Manitoba, Canada, R3T 2N2

Abstract. A formal mathematical presentation of various algebraic properties of rule 90 elementary one-dimensional cellular automata (CA) with null boundary conditions is given. The CA global rule transition matrix is given and its characteristic polynomial is formally obtained. Mathematical relationships between the CA register lengths and the orders of the corresponding group or semigroup algebraic structures are derived.

1. Introduction

The principles of cellular automata (CA) as discrete systems capable of self-organization, replication, and simulation of biological systems were established by the early work of Von Neumann [1].

Applications of CA in manipulation of pictorial data have recently been developed by Preston and Duff [2].

Various aspects and applications of CA have been presented in a recent publication by Wolfram [3] and also in [4].

Some of the algebraic properties of one-dimensional deterministic CA with periodic boundary conditions have recently been studied by Martin et al. [5], using properties of the CA global state polynomials over finite fields. Pu-hua and Yu He [6] have also studied such CA exploiting the properties of

circulant matrices on finite fields. This method, however, cannot be applied in the case of null bounded CA.

Present VLSI integration levels have reached the point where CA structures of high complexity may be implemented. As an alternative to conventional radix arithmetic processors these CA structures are capable of highly-parallel computation. Pries et al. [7,8] have recently demonstrated that CA may be used as modulo arithmetic units based on the group properties of one-dimensional CA.

Simulation results on the group and semigroup properties of one-dimensional, null bounded, rule 90 and rule 150 (in Wolfram's notation [9]) CA obtained by Thanailakis et al. [10] have shown that the global symmetries of CA with different length N (number of cell sites) lead to various relationships between the group or semigroup order and the CA length. However, due to computational limitations, it is very difficult to establish such relationships by means of simulation, especially when relatively long CA are involved. On the other hand, VLSI implementation of CA systems requires a complete mathematical description of their behavior. There is, therefore, a need for detailed studies of the algebraic properties of CA systems as they evolve according to deterministic rules, and the present work constitutes a contribution in this particular direction.

This paper presents a formal mathematical treatment, based on the characteristic polynomials of the CA global rule transition matrices, of various properties of rule 90 one-dimensional, null bounded, CA exhibiting group or semigroup algebraic structures. More specifically, in section 2 a general description of the one-dimensional CA notation is given. In section 3, the algebraic theory of one-dimensional CA is presented, in terms of the CA global rule transition matrix, and various important formal results are derived. Finally, the last section draws conclusions from the results obtained. To our knowledge, no previous investigations of this nature have appeared in the literature.

2. Description of one-dimensional cellular automata

A one-dimensional cellular automaton is a uniform array of identical cells of infinite or finite extent in one dimensional interconnection scheme, with a discrete variable at each cell (local state). The global state of a cellular automaton is specified by the values of all cells at a given time. In the following, we consider finite one-dimensional CA with cell values $\in Z_2$, with no memory associated with the cell beyond the previous time step (clock cycle). The value taken by a particular cell at any given clock cycle is affected (according to a specific local rule) by the values of cells in its neighborhood on the previous clock cycle. The neighborhood of a cell is taken to be the cells immediately adjacent to it on the left and right.

Figure 1 shows a one-dimensional CA with length N (N cells) and null boundary conditions. Null boundaries have been chosen, because in VLSI implementations we prefer to hold the end inputs at a constant value (grounded

Figure 1: Schematic of a one-dimensional CA illustrating the connection scheme for null boundary conditions.

in this particular case).

If $\alpha_i^{(t)} \in \{0,1\}$ is the value of the ith cell on clock cycle t, the global state of the cellular automaton with length N may be represented by a polynomial of the form

$$A^{(t)}(x) = \sum_{i=0}^{N-1} \alpha_i^{(t)} \cdot x^i \tag{2.1}$$

The total number of possible global states for such a CA is 2^N.

The local rule may be expressed by the Boolean function

$$T(x) = \beta_{i-1} x^{i-1} * \beta_{i+1} x^{i+1} \tag{2.2}$$

where the symbol $*$ is used to define a binary operation, and $\beta \in \{0,1\}$. In this paper, we have used the specific form of equation (2.2)

$$T(x) = x^{i-1} + x^{i+1} \pmod 2 \tag{2.3}$$

defining rule 90 in Wolfram's notation [9]. Therefore, the local state $\alpha_i^{(t+1)}$ of the ith cell on clock cycle $t+1$ is given by

$$\alpha_i^{(t+1)} = \alpha_{i-1}^{(t)} + \alpha_{i+1}^{(t)} \pmod 2 \tag{2.4}$$

The time evolution of a global state for one time step is defined [8] by

$$A^{(t+1)}(x) = T(x)\, A^{(t)}(x) \text{ trunc } (x^N + x^{-1}) \tag{2.5}$$

The time evolution, according to equation (2.5), in successive time steps, provides a mapping of the set of 2^N possible global states onto itself.

3. Algebraic theory of one-dimensional CA

3.1 Matrix representation of the global rule

The transformation (according to rule 90) of a CA global state in one clock cycle may be represented by the matrix operation

$$S^{(t+1)} = M_N . S^{(t)} \pmod 2 \tag{3.1}$$

where M_N is an $N \times N$ square matrix representing the CA (of length N) global rule; $S^{(t)}$ is the $(N \times 1)$ global state column vector, on clock cycle t; and $S^{(t+1)}$ is the corresponding global state column vector, on clock cycle $t+1$. Note that in the result (3.1), and all subsequent expressions in this paper, mod2 arithmetic is implied.

The global state column vectors $S^{(t)}$ and $S^{(t+1)}$ are defined as follows:

$$S^{(t)} = \begin{bmatrix} \alpha_{N-1}^{(t)} \\ \alpha_{N-2}^{(t)} \\ \vdots \\ \alpha_1^{(t)} \\ \alpha_0^{(t)} \end{bmatrix} \tag{3.2}$$

and

$$S^{(t+1)} = \begin{bmatrix} \alpha_{N-1}^{(t+1)} \\ \alpha_{N-2}^{(t+1)} \\ \vdots \\ \alpha_1^{(t+1)} \\ \alpha_0^{(t+1)} \end{bmatrix} \tag{3.3}$$

where the elements of these column vectors are the coefficients α_i of the corresponding polynomials in equation (2.1), and the global rule transition matrix M_N has the form [10]

$$M_N = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & . & . & . \\ 1 & 0 & 1 & 0 & 0 & 0 & . & . & . \\ 0 & 1 & 0 & 1 & 0 & 0 & . & . & . \\ 0 & 0 & 1 & 0 & 1 & 0 & . & . & . \\ . & . & . & . & . & . & . & . & . \\ 0 & . & . & . & . & 0 & 1 & 0 & 1 \\ 0 & . & . & . & . & 0 & 0 & 1 & 0 \end{bmatrix}_{N \times N} \tag{3.4}$$

The global state $S^{(t=k)}$, on clock cycle $t = k$, may directly be obtained from the initial state $S^{(t=0)}$ by the relation

$$S^{(t=k)} = M_N^k \cdot S^{(t=0)} \tag{3.5}$$

where M_N^k is the kth power of the (mod2) $N \times N$ rule matrix M_N.

The set of $N \times N$ matrices

$$F = \{M_N, M_N^2, M_N^3, \ldots, M_N^k\} \tag{3.6}$$

where k is a positive integer with a value depending on the CA length N, characterizes completely the properties of the one-dimensional, null bounded, CA of different lengths.

The behavior of a rule 90 CA has been found [10] to depend on the CA length as follows:

1. if Nmod2 $= 0$, F forms a cyclic group structure, with a corresponding group order ${}^{o}G = k$, where k satisfies the relation

$$M_N^k = I \tag{3.7}$$

and I is the $N \times N$ identity matrix, and

2. if Nmod2 $\neq 0$, F forms a semigroup algebraic structure of order ${}^{o}S = k - 1$, where

$$M_N^k = M_N^{q \leq k-1} \tag{3.8}$$

Figures 2(a) and (b) show the types of state transition graph [11] obtained for rule 90, group and semigroup algebraic structures, respectively. The nodes represent the corresponding global states, whereas each arc represents the global rule transition matrix. The order ${}^{o}G$ of the corresponding group algebraic structure for a CA of length N is equal to the number of states in the cycle (or cycles) with the maximum length. The value of the parameter q, in equation (3.8), is equal to the tail-tree height of the corresponding semigroup state transition graph. The value of the parameter k is equal to the number of arcs in the loop (or loops) with the maximum length obtained plus the height of the tail-trees rooted at the loop states.

The accessible range of N over which the group and semigroup properties can be studied using the matrix representation of the global rule is limited, due to the fact that the computation time increases prohibitively when N exceeds some value [10]. The accessible range of N may considerably be extended by employing the characteristic polynomial of the global rule transition matrix, which we will now derive.

Lemma 1. *Given a global rule transition matrix M_N for a finite 1-D, null bounded, rule 90 CA of length N, the corresponding characteristic polynomial, $P_N(\lambda)$, is recursively given by*

$$P_N(\lambda) = \lambda P_{N-1}(\lambda) + P_{N-2}(\lambda) \tag{3.9}$$

Proof. The characteristic polynomial of the global rule matrix is given by

$$P_N(\lambda) = |M_N + \lambda I| = \begin{vmatrix} -\lambda & 1 & 0 & 0 & 0 & 0 & \cdot & \cdot & \cdot \\ 1 & -\lambda & 1 & 0 & 0 & 0 & \cdot & \cdot & \cdot \\ 0 & 1 & -\lambda & 1 & 0 & 0 & \cdot & \cdot & \cdot \\ 0 & 0 & 1 & -\lambda & 1 & 0 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & 1 & -\lambda & 1 \\ 0 & \cdot & \cdot & \cdot & \cdot & 0 & 0 & 1 & -\lambda \end{vmatrix}_{N \times N} \tag{3.10}$$

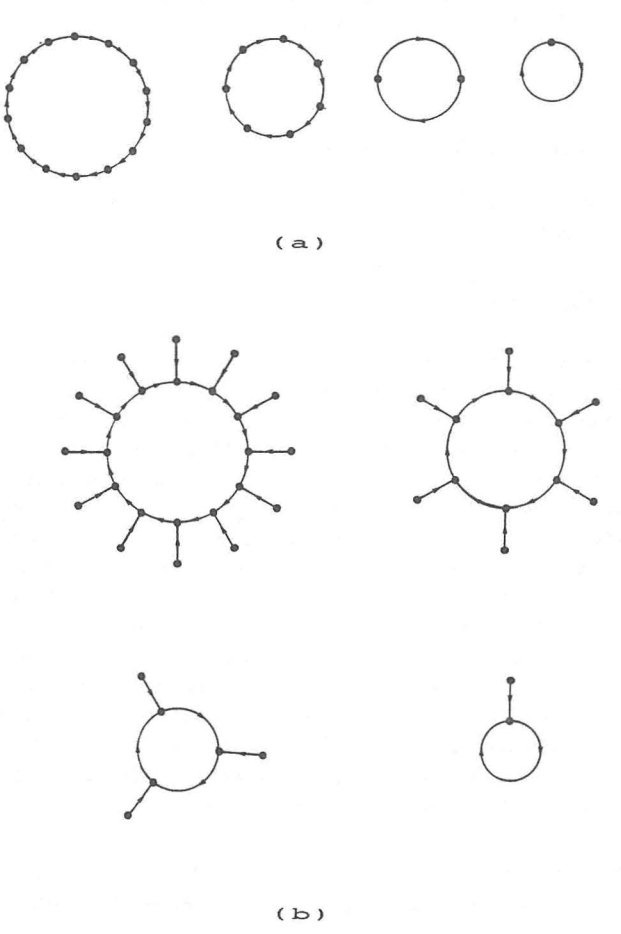

Figure 2: (a) The global state transition graph for a rule 90, null bounded, one-dimensional CA of length $N = 8$. Group algebraic structure of order ${}^0G = 14$ (the entire state transition graph consists of 17 cycles of 14 states, 2 cycles of 7 states, 1 cycle of 2 states, and 2 cycles of 1 state). (b) The global state transition graph for a rule 90, null bounded, one-dimensional CA of length $N = 9$. Semigroup algebraic structure of order ${}^0S = k - 1 = 12$, tail-tree height $q = 1$ and maximum number of loop states $(k - q) = 12$ (the entire state transition graph consists of 20 loops of 12 states, 2 loops of 6 states, 1 loop of 3 states, and 1 loop of 1 state. At each loop state is rooted a tail-tree of height $q = 1$).

$$= -\lambda \begin{vmatrix} -\lambda & 1 & 0 & 0 & 0 & \cdot & \cdot & \cdot \\ 1 & -\lambda & 1 & 0 & 0 & \cdot & \cdot & \cdot \\ 0 & 1 & -\lambda & 1 & 0 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & 0 & 1 & -\lambda & 1 \\ 0 & \cdot & \cdot & \cdot & 0 & 0 & 1 & -\lambda \end{vmatrix}_{(N-1)\times(N-1)}$$

$$- \begin{vmatrix} 1 & 1 & 0 & 0 & 0 & \cdot & \cdot & \cdot \\ 0 & -\lambda & 1 & 0 & 0 & \cdot & \cdot & \cdot \\ 0 & 1 & -\lambda & 1 & 0 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & \cdot & \cdot & \cdot & 0 & 1 & -\lambda & 1 \\ 0 & \cdot & \cdot & \cdot & 0 & 0 & 1 & -\lambda \end{vmatrix}_{(N-1)\times(N-1)}$$

Hence

$$P_N(\lambda) = \lambda P_{N-1}(\lambda) + P_{N-2}(\lambda)$$

It is important, however, to be able to obtain directly the non recursive form of the characteristic polynomial

$$P_N(\lambda) = \lambda^N + c_{N-1}\lambda^{N-1} + \ldots c_1\lambda + c_0 \tag{3.11}$$

where $c_r \in \{0,1\}$. In this respect, the following theorem holds:

Theorem 1. *Given a global rule transition matrix M_N for a null bounded rule 90 CA of length N, the corresponding characteristic polynomial, $P_N(\lambda)$, is directly given by the relation*

$$P_N(\lambda) = \frac{1}{2^N} \sum_{j=0}^{j=[N/2]} \binom{N+1}{2j+1} \lambda^{N-2j}(\lambda^2+4)^j \tag{3.12}$$

where $[N/2]$ represents the integral part of the number $N/2$, and $\binom{N+1}{2j+1}$ represents the number of all possible combinations of $N+1$ elements into a sequence of $2j+1$ elements.

Proof. Equation (3.9) of lemma 1 may be written in the general form

$$P_N - \lambda P_{N-1} - P_{N-2} = 0 \tag{3.13}$$

The solution of equation (3.13), considered as a finite difference equation, is

$$A\rho_1^N + B\rho_2^N = P_N \tag{3.14}$$

with initial conditions

$$P_0 = 1 \quad \text{and} \quad P_1 = \lambda \tag{3.15}$$

where

$$\rho_{1,2} = \frac{\lambda \pm (\lambda^2+4)^{1/2}}{2} = \frac{\lambda \pm \Delta^{1/2}}{2} \tag{3.16}$$

are roots of the well known equation $y^2 - \lambda y - 1 = 0$. From equations (3.14) and (3.15) we get

$$A = \frac{\lambda - \rho_2}{\rho_1 - \rho_2} = \frac{\lambda + \Delta^{1/2}}{2\Delta^{1/2}} \tag{3.17}$$

and

$$B = 1 - A = \frac{-\lambda + \Delta^{1/2}}{2\Delta^{1/2}} \tag{3.18}$$

From equations (3.14), (3.16), (3.17), and (3.18) we finally obtain

$$P_N(\lambda) = \frac{1}{2^N} \sum_{j=0}^{j=[N/2]} \binom{N+1}{2j+1} \lambda^{N-2j} (\lambda^2+4)^j$$

3.2 Formal results

Detailed results obtained from studies of a large variety of group and semigroup structures, together with the various types of state transformations resulting from the action of rule 90 CA evolution, may be found in [10,11].

Table 1 shows the orders ${}^0G$ of group structures for various lengths N. It can be seen that the values of ${}^0G_N$ for $N = 2^n$, where $n = 1, 2, 3, \ldots$, constitute the lower bound for the range of allowed values of ${}^0G$, whereas the values ${}^0G_N = 2(2^{N/2} - 1)$ constitute the upper bound [10].

It is also apparent from table 1 that there is a great number of classes of rule 90, null bounded, 1-D CA satisfying different functional dependencies for their lengths and the corresponding group orders. It is highly desirable to have formal results regarding these dependences and the contribution of the present paper, in this respect, will now be presented and discussed.

Now we will prove the results related to the lower bound referred to above.

Lemma 2. *If $P_N(\lambda)$ is the characteristic polynomial of the global rule transition matrix for a rule 90, null bounded, 1-D CA of length N, then*

$$P_N^2(\lambda) = P_N(\lambda^2) \tag{3.19}$$

Proof. Since $P_N^2(\lambda) = \sum_r c_r^2 \lambda^{2r}$, and $c_r^2 = c_r$, it is obvious that

$$P_N^2(\lambda) = \sum_r c_r \lambda^{2r} = P_N(\lambda^2)$$

Lemma 3. *The characteristic polynomial $P_{2N+1}(\lambda)$, where $N \geq 2$, is recursively generated by the relation*

$$P_{2N+1}(\lambda) = \lambda P_N^2(\lambda) \tag{3.20}$$

N	${}^0G$	N	${}^0G$	N	${}^0G$	N	${}^0G$	N	${}^0G$
2	2	80	$> 10^5$	158	$> 10^5$	236	$> 10^5$	314	8190
4	6	82	$> 10^5$	160	$> 10^5$	238	$> 10^5$	316	$> 10^5$
6	14	84	510	162	$> 10^5$	240	8190	318	$> 10^5$
8	14	86	$> 10^5$	164	$> 10^5$	242	$> 10^5$	320	$> 10^5$
10	62	88	4094	166	$> 10^5$	244	$> 10^5$	322	$> 10^5$
12	126	90	8190	168	$> 10^5$	246	$> 10^5$	324	$> 10^5$
14	30	92	2046	170	1022	248	$> 10^5$	326	$> 10^5$
16	30	94	$> 10^5$	172	$> 10^5$	250	$> 10^5$	328	$> 10^5$
18	1022	96	$> 10^5$	174	$> 10^5$	252	$> 10^5$	330	65534
20	126	98	65534	176	$> 10^5$	254	510	332	$> 10^5$
22	4094	100	$> 10^5$	178	$> 10^5$	256	510	334	$> 10^5$
24	2046	102	$> 10^5$	180	$> 10^5$	258	$> 10^5$	336	$> 10^5$
26	1022	104	8190	182	$> 10^5$	260	$> 10^5$	338	$> 10^5$
28	32766	106	$> 10^5$	184	$> 10^5$	262	$> 10^5$	340	2046
30	62	108	$> 10^5$	186	$> 10^5$	264	$> 10^5$	342	$> 10^5$
32	62	110	$> 10^5$	188	$> 10^5$	266	$> 10^5$	344	$> 10^5$
34	8190	112	32766	190	$> 10^5$	268	$> 10^5$	346	$> 10^5$
36	174762	114	$> 10^5$	192	$> 10^5$	270	$> 10^5$	348	$> 10^5$
38	8190	116	8190	194	8190	272	8190	350	$> 10^5$
40	2046	118	$> 10^5$	196	$> 10^5$	274	$> 10^5$	352	$> 10^5$
42	254	120	$> 10^5$	198	$> 10^5$	276	$> 10^5$	354	$> 10^5$
44	8190	122	$> 10^5$	200	$> 10^5$	278	$> 10^5$	356	$> 10^5$
46	$> 10^5$	124	$> 10^5$	202	$> 10^5$	280	$> 10^5$	358	$> 10^5$
48	$> 10^5$	126	254	204	2046	282	$> 10^5$	360	$> 10^5$
50	510	128	254	206	$> 10^5$	284	$> 10^5$	362	$> 10^5$
52	$> 10^5$	130	$> 10^5$	208	$> 10^5$	286	$> 10^5$	364	$> 10^5$
54	$> 10^5$	132	$> 10^5$	210	$> 10^5$	288	$> 10^5$	366	$> 10^5$
56	1022	134	$> 10^5$	212	$> 10^5$	290	$> 10^5$	368	$> 10^5$
58	$> 10^5$	136	$> 10^5$	214	$> 10^5$	292	$> 10^5$	370	$> 10^5$
60	$> 10^5$	138	$> 10^5$	216	65534	294	$> 10^5$	372	$> 10^5$
62	126	140	$> 10^5$	218	$> 10^5$	296	$> 10^5$	374	$> 10^5$
64	126	142	$> 10^5$	220	$> 10^5$	298	$> 10^5$	376	$> 10^5$
66	$> 10^5$	144	32766	222	$> 10^5$	300	$> 10^5$	378	$> 10^5$
68	$> 10^5$	146	$> 10^5$	224	$> 10^5$	302	$> 10^5$	380	32766
70	$> 10^5$	148	$> 10^5$	226	$> 10^5$	304	$> 10^5$	382	$> 10^5$
72	1022	150	65534	228	$> 10^5$	306	$> 10^5$	384	$> 10^5$
74	$> 10^5$	152	$> 10^5$	230	$> 10^5$	308	$> 10^5$		
76	$> 10^5$	154	$> 10^5$	232	$> 10^5$	310	$> 10^5$		
78	$> 10^5$	156	$> 10^5$	234	$> 10^5$	312	$> 10^5$		

Table 1: Order ${}^0G$ of group algebraic structures versus CA length N for rule 90, null bounded, one-dimensional CA. The symbol $> 10^5$ means that the value of ${}^0G$ is greater than 10^5 but it has not been experimentally determined, due to computational limitations.

Proof. We shall prove this lemma by induction on N. We assume the lemma proved for $N \leq v$, and we shall prove it for $N = v + 1$. Equation (3.9) of lemma 1 may also be written in the form

$$P_{2N+1}(\lambda) = \lambda P_{2N}(\lambda) + P_{2N-1}(\lambda) \tag{3.21}$$

For $N = v + 1$ we get

$$\begin{aligned} P_{2v+3}(\lambda) &= \lambda P_{2v+2}(\lambda) + P_{2v+1}(\lambda) \\ &= \lambda^2 P_{2v+1}(\lambda) + P_{2v-1}(\lambda) \end{aligned} \tag{3.22}$$

Equation (3.20) is true for $N = v - 1$, and also for $N = v$, leading to

$$P_{2v-1}(\lambda) = \lambda P_{v-1}^2(\lambda) \tag{3.23}$$

and

$$P_{2v+1}(\lambda) = \lambda P_v^2(\lambda) \tag{3.24}$$

respectively.

From equations (3.22), (3.23), and (3.24) we have

$$\begin{aligned} P_{2v+3}(\lambda) &= \lambda^2 P_{2v+1}(\lambda) + \lambda P_{v-1}^2(\lambda) \\ &= \lambda[\lambda P_{2v+1}(\lambda) + P_{v-1}^2(\lambda)] \\ &= \lambda[\lambda^2 P_v^2(\lambda) + P_{v-1}^2(\lambda)] \\ &= \lambda P_{v+1}^2(\lambda) \end{aligned} \tag{3.25}$$

Lemma 4. *The characteristic polynomial $P_{2N+1}(\lambda)$ is recursively generated by the relation*

$$P_{2N+1}(\lambda) = \lambda P_N(\lambda^2) \tag{3.26}$$

Proof. This result may easily be proved by combining lemma 2 and lemma 3.

Lemma 5. *Given a global rule transition matrix M_{2N} for a null bounded rule 90 CA of length $2N$, the corresponding characteristic polynomial, $P_{2N}(\lambda)$, is recursively given by*

$$P_{2N}(\lambda) = P_N^2(\lambda) + P_{N-1}^2(\lambda) \tag{3.27}$$

Proof. We shall prove this lemma by induction on N. We assume the lemma proved for $N = v$, and we shall prove it for $N = v+1$. For $N = v+1$, combining lemma 1 and lemma 3, we obtain

$$\begin{aligned} P_{2(v+1)}(\lambda) &= \lambda P_{2v+1}(\lambda) + P_{2v}(\lambda) \\ &= \lambda^2 P_v^2(\lambda) + P_{2v}(\lambda) \end{aligned} \tag{3.28}$$

Equation (3.27) is true for $N = v$ leading to

$$P_{2v}(\lambda) = P_v^2(\lambda) + P_{v-1}^2(\lambda) \tag{3.29}$$

From equations (3.28) and (3.29) we have

$$\begin{aligned} P_{2(v+1)}(\lambda) &= \lambda^2 P_v^2(\lambda) + P_v^2(\lambda) + P_{v-1}^2(\lambda) \\ &= P_{v+1}^2(\lambda) + P_v^2(\lambda) \end{aligned}$$

Lemma 6. *The characteristic polynomial $P_N(\lambda)$ of a rule 90 null bounded CA of length $N = 2^n - 1$, where $n = 1, 2, 3, \ldots$, is given by*

$$P_{N=2^n-1}(\lambda) = \lambda^{N=2^n-1} \tag{3.30}$$

Proof. We shall prove this lemma by induction on n. We assume the lemma proved for $n = v$, and we shall prove it for $n = v + 1$.

According to lemma 3, for $n = v + 1$ we have

$$P_{2^{v+1}-1}(\lambda) = P_{2(2^v-1)+1}(\lambda) = \lambda P_{2^v-1}^2(\lambda) \tag{3.31}$$

Equation (3.30) is true for $n = v$ leading to

$$P_{2^v-1}(\lambda) = \lambda^{2^v-1} \tag{3.32}$$

From equations (3.31) and (3.32) we obtain

$$\begin{aligned} P_{2^{v+1}-1}(\lambda) &= \lambda[\lambda^{2^v-1}]^2 \\ &= \lambda^{2^{v+1}-1} \end{aligned}$$

Lemma 7. *The characteristic polynomial $P_N(\lambda)$ of a rule 90 null bounded CA of length $N = 2^{n+1}$, where $n = 1, 2, 3, \ldots$, is given by*

$$P_{2^{n+1}}(\lambda) = P_{2^n}^2(\lambda) + \lambda^{2^{n+1}-2} \tag{3.33}$$

Proof. Combining lemma 5 and lemma 6, we obtain

$$\begin{aligned} P_{2^{n+1}}(\lambda) &= P_{2(2^n)}(\lambda) \\ &= P_{2^n}^2(\lambda) + P_{2^n-1}^2(\lambda) \\ &= P_{2^n}^2(\lambda) + \lambda^{2^{n+1}-2} \end{aligned}$$

Lemma 8. *The characteristic polynomial $P_N(\lambda)$ of a rule 90 null bounded CA of length $N = 2^n$, where $n = 1, 2, 3, \ldots$, is given by*

$$P_{N=2^n}(\lambda) = \lambda^{2^n} + \lambda^{2^n-2} + \lambda^{2^n-2^2} + \ldots + \lambda^{2^n-2^{n-1}} + 1 \tag{3.34}$$

Proof. We shall prove this lemma by induction on n. We assume the lemma proved for $n = v$, and we shall prove it for $n = v + 1$.

From lemma 7 we have

$$P_{2^{n+1}}(\lambda) = P_{2^n}^2(\lambda) + \lambda^{2^{n+1}-2}$$

According to lemma 2, the above equation may be written

$$P_{2^{n+1}}(\lambda) = P_{2^n}(\lambda^2) + \lambda^{2^{n+1}-2} \tag{3.35}$$

Since we have assumed that equation (3.34) is true for $n = v$, equation (3.35) takes the form

$$\begin{aligned} P_{2^{v+1}}(\lambda) &= \lambda^{2^{v+1}} + \lambda^{2^{v+1}-2^2} + \lambda^{2^{v+1}-2^3} + \ldots + \lambda^{2^{v+1}-2^v} + 1 + \lambda^{2^{v+1}-2} \\ &= \lambda^{2^{v+1}} + \lambda^{2^{v+1}-2} + \lambda^{2^{v+1}-2^2} + \ldots + \lambda^{2^{v+1}-2^v} + 1 \end{aligned}$$

Lemma 9. *Given a global rule transition matrix $M_{N=2^n}$ for a null bounded rule 90 CA of length $N = 2^n$, where $n = 1, 2, 3, \ldots$, then*

$$P_{2^{n+1}}(M_{2^n}) = I \tag{3.36}$$

where I is the $(2^n \times 2^n)$ identity matrix.

Proof. From lemma 8 we have

$$\begin{aligned} P_{2^{n+1}}(M_{2^n}) &= M_{2^n}^{2^{n+1}} + M_{2^n}^{2^{n+1}-2} + M_{2^n}^{2^{n+1}-2^2} + \ldots + M_{2^n}^{2^{n+1}-2^n} + I \\ &= M_{2^n}^{2^{n+1}-2^n}\left[M_{2^n}^{2^n} + M_{2^n}^{2^n-2} + \ldots + I\right] + I \\ &= M_{2^n}^{2^{n+1}-2^n} P_{2^n}(M_{2^n}) + I \end{aligned}$$

According to the Cayley-Hamilton theorem [12], $P_{2^n}(M_{2^n}) = 0$, and, therefore

$$P_{2^{n+1}}(M_{2^n}) = I$$

Theorem 2. *If the length of rule 90, null bounded, 1-D CA is of the form $N = 2^n$, where $n = 1, 2, 3, \ldots$, then the order of the corresponding group algebraic structure is given by the relation*

$${}^0G_{N=2^n} = 2^{n+1} - 2 = 2(N-1) \tag{3.37}$$

Proof. From lemma 7 we have

$$P_{2^{n+1}}(M_{2^n}) = [P_{2^n}(M_{2^n})]^2 + M_{2^n}^{2^{n+1}-2}$$

Using lemma 9 and the Cayley-Hamilton theorem the above equation reduces to

$$M_{2^n}^{2^{n+1}-2} = I$$

Therefore, the corresponding group order is

$${}^0G_{N=2^n} = 2^{n+1} - 2 = 2(N-1)$$

Corollary 1. *For rule 90, null bounded, 1-D CA with length $N = 2^n$, where $n = 1, 2, 3, \ldots$, the order ${}^0G$ of the corresponding group structure is recursively given by*

$${}^0G_{N'=2^{n+1}} = 2({}^0G_{N=2^n} + 1) \tag{3.38}$$

Proof. From theorem 2 we have

$$\begin{aligned} {}^0G_{N'=2^{n+1}} &= 2^{n+2}-2 \\ &= 2(2^{n+1}-1) \\ &= 2({}^0G_{N=2^n}+1) \end{aligned}$$

Now we will deal with the set of CA lengths satisfying the relation $N = 2^n - 2$, where $n = 3, 4, 5, \ldots$.

Lemma 10. *The characteristic polynomial $P_N(\lambda)$ of a rule 90 null bounded CA of length $N = 2^n - 2$, where $n = 3, 4, 5, \ldots$, is given by*

$$P_{N=2^n-2}(\lambda) = \lambda^{2^n-2} + \lambda^{2^n-2^2} + \ldots + \lambda^{2^{n-1}} + 1 \qquad (3.39)$$

Proof. Equation (3.9) of lemma 1 may, for $N = 2^n$, be written in the form

$$P_{2^n-2}(\lambda) = \lambda P_{2^n-1}(\lambda) + P_{2^n}(\lambda) \qquad (3.40)$$

From equation (3.40) and lemmas 6 and 8 we obtain

$$\begin{aligned} P_{2^n-2}(\lambda) &= \lambda.\lambda^{2^n-1} + \lambda^{2^n} + \lambda^{2^n-2} + \ldots + \lambda^{2^{n-1}} + 1 \\ &= \lambda^{2^n-2} + \lambda^{2^n-2^2} + \ldots + \lambda^{2^{n-1}} + 1 \end{aligned}$$

Theorem 3. *If the length of rule 90, null bounded, 1-D CA is of the form $N = 2^n - 2$, where $n = 3, 4, 5, \ldots$, then the corresponding group order is given by the relation*

$${}^0G_{N=2^n-2} = 2(N+1) \qquad (3.41)$$

Proof. From lemma 10 and the Cayley-Hamilton theorem we have

$$M_N^{2^n-2} + M_N^{2^n-2^2} + \ldots + M_N^{2^{n-1}} + I = 0$$

Hence

$$M_N^{2^n-2} = M_N^{2^n-2^2} + \ldots + M_N^{2^{n-1}} + I$$

or

$$\begin{aligned} M_N^{2^{n+1}-2} &= M_N^{2^n}\left[M_N^{2^n-2^2} + \ldots + M_N^{2^{n-1}-2} + I\right] \\ &= M_N^{2^{n+1}-2^2} + \ldots + M_N^{2^n+2^{n-1}} + M_N^{2^n} \\ &= \left[M_N^{2^n-2} + M_N^{2^n-2^2} + \ldots + M_N^{2^{n-1}}\right]^2 \\ &= \left[P_{N=2^n-2}(M_N) + I\right]^2 = I \end{aligned}$$

Therefore, the corresponding group order is

$${}^0G_{N=2^n-2} = 2^{n+1} - 2 = 2(N+1)$$

We will now present the results related to semigroup algebraic structures.

Theorem 4. *If the length of rule 90, null bounded, 1-D CA is of the form* $N = 2^n - 1$, *where* $n = 1, 2, 3, \ldots$, *then the order of the corresponding semigroup algebraic structure is given by the relation*

$$^0S_{N=2^n-1} = N \tag{3.42}$$

Proof. From lemma 6 and the Cayley-Hamilton theorem we have

$$M_{N=2^n-1}^{2^n-1} = 0$$

Hence, the value of the parameter q of equation (3.8) is [10]

$$q = 2^n - 1$$

Therefore, the corresponding semigroup order is

$$^0S_{N=2^n-1} = 2^n - 1 = N$$

The state transition graph for such CA is of the pure binary tree type [10].

For any given CA length N such that $N \bmod 2 = 0$, the quantity $N_{\text{initial}} \equiv N_{m=1} = 2N + 1$ serves as the initial length for a corresponding class of CA, exhibiting semigroup algebraic structure, within which the CA lengths satisfy the relation

$$N_{m+1} = 2N_m + 1 \tag{3.43}$$

where $m = 1, 2, 3, \ldots$.

We will now present some results related to such classes of CA semigroup structures.

Theorem 5. *For rule 90, null bounded, 1-D CA semigroup structures with lengths* $N_{\text{initial}} \equiv N_{m=1} = 2N + 1$, *where* $N \bmod 2 = 0$, *the corresponding value,* $q_{\text{initial}} \equiv q_{N_{m=1}}$ *of the parameter* q *in equation (3.8) is*

$$q_{\text{initial}} = 1$$

and the corresponding value $k_{\text{initial}} \equiv k_{N_{m=1}}$ *of the parameter* k *in equation (3.8) is*

$$k_{\text{initial}} = 2^0G_{N=\frac{N_{\text{initial}}-1}{2}} + 1$$

where ^0G_N *is the group order of the CA with length* N.

Proof. For rule 90 CA group algebraic structures, the characteristic polynomial $P_N(\lambda)$ is given by equation (3.11), where $c_0 = 1$ [10]. Equation (3.11) may be written in the form

$$\lambda^{^0G_N-N}.P_N(\lambda) = \lambda^{^0G_N} + c_{N-1}\lambda^{^0G_N-1} + \ldots + c_1\lambda^{^0G_N-N+1} + \lambda^{^0G_N-N}$$

or

$$\lambda^{0G_N-N}.P_N(\lambda) = \lambda^{0G_N} + P_N(\lambda).Q(\lambda) + R(\lambda) \tag{3.44}$$

where $Q(\lambda)$ and $R(\lambda)$ are the quotient and the remainder, respectively, of the polynomial division

$$\frac{P_N(\lambda).Q(\lambda)+R(\lambda)\equiv F(\lambda)=c_{N-1}\lambda^{0G_N-1}+\ldots+c_1\lambda^{0G_N-N+1}+\lambda^{0G_N-N}}{P_N(\lambda) = \lambda^N + c_{N-1}\lambda^{N-1} + \ldots + c_1\lambda + 1} \tag{3.45}$$

It can easily be proved that for any rule 90 CA group structure the remainder $R(\lambda) = 1$.

Replacing λ by the semigroup transition matrix M_{2N+1}, lemma 4 reduces to

$$P_{2N+1}(M_{2N+1}) = M_{2N+1}.P_N(M_{2N+1}^2) = 0 \tag{3.46}$$

Now, replacing λ in equation (3.44) by M_{2N+1}^2 we obtain

$$M_{2N+1}^{2(^0G_N-N)}.P_N(M_{2N+1}^2) = M_{2N+1}^{2^0G_N} + P_N(M_{2N+1}^2).Q(M_{2N+1}^2) + I \tag{3.47}$$

Taking into account that the quotient $Q(M_{2N+1}^2)$ is of the form

$$Q(M_{2N+1}^2) = c_{2(^0G_N-1-N)}M_{2N+1}^{2(^0G_N-1-N)} + \ldots + I$$

and using equation (3.45), equation (3.46) reduces to

$$0 = M_{2N+1}^{2^0G_N} + P_N(M_{2N+1}^2) + I$$

or

$$M_{2N+1}^{2^0G_N+1} = M_{2N+1}$$

Hence

$$q_{\text{initial}} = 1$$

and

$$k_{\text{initial}} = 2^0G_N + 1$$

We will now present some results regarding the semigroup properties of CA belonging to classes described by equation (3.43).

Theorem 6. *If for a rule 90, null bounded, 1-D CA of length* N_m, $M_{N_m}^k = M_{N_m}^q$ *then for a CA length* $N_{m+1} = 2N_m + 1$, *where* $m = 1, 2, 3, \ldots$, *the following relation holds:*

$$M_{N_{m+1}}^{2k+1} = M_{N_{m+1}}^{2q+1}$$

Proof. For a rule 90 CA semigroup algebraic structure the general form of the characteristic polynomial $P_N(\lambda)$ of equation (3.11) reduces [10] to

$$P_{N_m}(\lambda) = \lambda^{N_m} + c_{N_m-1}\lambda^{N_M-1} + \ldots + \lambda^{r=q}$$

Hence

$$\lambda^{k-N_m} P_{N_m}(\lambda) = \lambda^k + c_{N_m-1}\lambda^{k-1} + \ldots \lambda^{k-N_m+q}$$

or, by analogy to equation (3.44),

$$\lambda^{k-N_m} P_{N_m}(\lambda) = \lambda^k + P_{N_m}(\lambda)Q(\lambda) + R(\lambda) \tag{3.48}$$

It can easily be proved that for any rule 90 CA semigroup structure the remainder $R(\lambda)$ is a monomial of the form

$$R(\lambda) = \lambda^q \tag{3.49}$$

Therefore, equation (3.47) may be written

$$\lambda^{k-N_m}.P_{N_m}(\lambda) = \lambda^k + P_{N_m}(\lambda)Q(\lambda) + \lambda^q \tag{3.50}$$

Replacing λ in equation (3.49) by $M^2_{2N_m+1}$ we obtain

$$\begin{aligned} M^{2(k-N_m)}_{2N_m+1}.P_{N_m}(M^2_{2N_m+1}) &= M^{2k}_{2N_m+1} && (3.51)\\ &+ P_{N_m}(M^2_{2N_M+1}).Q(M^2_{2N_M+1}) && (3.52)\\ &+ M^{2q}_{2N_m+1} \end{aligned}$$

From lemma 4 we have

$$P_{2N_m+1}(M_{2N_m+1}) = M_{2N_m+1}.P_{N_m}(M^2_{2N_m+1}) = 0 \tag{3.53}$$

From equations (3.51) and (3.52), taking into account that

$$Q(M^2_{2N_m+1}) = c_{2(k-1-N_m)}M^{2(k-1-N_m)}_{2N_m+1} + \ldots + I$$

we obtain

$$M^{2k}_{2N_m+1} + P_{N_m}(M^2_{2N_m+1}) + M^{2q}_{2N_m+1} = 0$$

and, hence,

$$M^{2k+1}_{2N_m+1} = M^{2q+1}_{2N_m+1}$$

Corollary 2. *If q_{2N_m+1} and q_{N_m} are the tail-tree heights in the state transition graphs for CA lengths $2N_m + 1$ and N_m, respectively, then*

$$q_{2N_m+1} = 2_{q_{N_m}} + 1$$

Proof. The result follows from theorem 6.

Corollary 3. *If k_{2N_m+1} and k_{N_m} are the kth power of the global rule transition matrices M_{2N_m+1} and M_{N_m} for CA lengths $2N_m+1$ and N_m, respectively, then*

$$k_{2N_m+1} = 2k_{N_m} + 1$$

Proof. This result follows from theorem 6.

Corollary 4. *If* $(k-q)_{2N_m+1}$ *and* $(k-1)_{N_m}$ *are the number of loop-states in the state transition graphs for CA lengths* $2N_m+1$ *and* N_m*, respectively, then*

$$(k-q)_{2N_m+1} = 2(k-q)_{N_m}$$

Proof. This result follows from corollaries 2 and 3.

Corollary 5. *If* ${}^0S_{2N_m+1}$ *and* ${}^0S_{N_m}$ *are the semigroup orders for CA lengths* $2N_m+1$ *and* N_m*, respectively, then*

$${}^0S_{2N_m+1} = 2({}^0S_{N_m} + 1)$$

Proof. We have already pointed out that ${}^0S = k-1$. Therefore, taking into account corollary 3, we have

$${}^0S_{2N_m+1} = k_{2N_m+1} - 1 \quad \text{and} \quad {}^0S_{N_m} = k_{N_m} - 1$$

Hence

$$\begin{aligned} {}^0S_{2N_m+1} &= (2k_{N_m}+1) - 1 \\ &= 2({}^0S_{N_m} + 1) \end{aligned}$$

It is apparent from corollaries 2, 3, 4, and 5 that all odd CA lengths $N_{\text{initial}} \equiv N_{m=1} = 2N+1$, with $N \bmod 2 = 0$, serve as initial values for corresponding classes of semigroup CA structures, within each of which the following recursive relations hold:

$$\begin{aligned} N_{m+1} &= 2N_m + 1 \\ q_{N_{m+1}} &= 2q_{N_m} + 1 \\ k_{N_{m+1}} &= 2k_{N_m} + 1 \end{aligned} \tag{3.54}$$

$$(k-q)_{N_{m+1}} = 2(k-q)_{N_m}$$

and

$${}^0S_{N_{m+1}} = 2({}^0S_{N_m} + 1)$$

where $m = 1, 2, 3, \ldots$. The results of equation (3.53) are in agreement with the experimental results shown in table 2 [11].

N	$\frac{S}{N}$	q_N	$(k-q)_N$	N	$\frac{S}{N}$	q_N	$(k-q)_N$
5	4	1	4	35	58	3	56
7	7	7	1(BT)	37	2044	1	2044
9	12	1	12	39	54	7	48
11	10	3	8	41	252	1	252
13	28	1	28	43	250	3	248
15	15	15	1(BT)	45	8188	1	8188
17	28	1	28	47	46	15	32
19	26	3	24	49	4092	1	4092
21	24	1	124	51	506	3	504
23	22	7	16	53	2044	1	2044
25	252	1	252	55	118	7	112
27	58	3	56	57	65532	1	65532
29	60	1	60	59	122	3	120
31	31	31	1(BT)	61	124	1	124
33	60	1	60	63	63	63	1(BT)

Table 2: Order ${}^0S_N$ of semigroup algebraic structures and state transition graph-related parameters versus CA length N for rule 90, null bounded, one-dimensional CA. BT = Binary tree.

4. Concluding remarks

A formal mathematical presentation of various algebraic properties of rule 90, null bounded, 1-D cellular automata is given in this paper.

The global rule transition matrix of 1-D CA is given, and its characteristic polynomial is formally obtained.

Direct relationships between the CA lengths $N = 2^n$, where $n = 1, 2, 3, \ldots$, and the orders of the corresponding group algebraic structures ${}^0G_N$-constituting the lower bound for the range of allowed values of ${}^0G-$ as well as between the lengths $N = 2^n - 2$, where $n = 3, 4, 5, \ldots$, and the corresponding group orders ${}^0G_N$ are derived.

The direct relationship between the CA lengths $N = 2^n - 1$, where $n = 1, 2, 3, \ldots$, and the orders of the corresponding semigroup algebraic structures ${}^0S_N$ is formally obtained.

All odd CA lengths N_{initial} $(\equiv N_{m=1}) = 2N + 1$, with $N \bmod 2 = 0$, serve as initial values for corresponding classes of semigroup algebraic structures. The corresponding values q_{initial} $(\equiv q_{N_{m=1}})$ and k_{initial} $(\equiv k_{N_{m=1}})$ are given by the relations

$$q_{\text{initial}} = 1$$

and

$$k_{\text{initial}} = 2^0G_{\frac{N_{\text{initial}}-1}{2}} + 1$$

respectively, where ${}^0G_{\frac{N_{\text{initial}}-1}{2}}$ is the group order of the CA with length $(N_{\text{initial}} - 1)/2$.

Within each of the above classes the following recursive relations were found to hold:

$$\begin{aligned} N_{m+1} &= 2N_m + 1 \\ q_{N_{m+1}} &= 2_{q_{N_m}} + 1 \\ k_{N_{m+1}} &= 2k_{N_m} + 1 \\ (k-q)_{N_{m+1}} &= 2(k-q)_{N_m} \end{aligned}$$

and

$${}^0S_{N_{m+1}} = 2({}^0S_{N_m} + 1)$$

where $m = 1, 2, 3, \ldots$.

References

[1] J. Von Neumann, *Theory of Self-Reproducing Automata*, A.W. Burks, ed. (University of Illinois Press, Urbana, 1966).

[2] K. Preston Jr. and M.J.B. Duff, *Modern Cellular Automata Theory and Applications* (Plenum Press, New York, 1984).

[3] S. Wolfram, *Theory and Applications of Cellular Automata* (World Scientific Publishing Co. Pte. Ltd., Singapore, 1987).

[4] D. Farmer, T. Toffoli, and S. Wolfram, "Cellular Automata," *Physica D*, **10D** (1984).

[5] O. Martin, A. Odlyzko, and S. Wolfram, "Algebraic Properties of Cellular Automata," *Commun. Math. Phys.*, **93** (1984) 219–258.

[6] G. Pu-hua and Ye He, "Exact Results for Deterministic Cellular Automata with Additive Rules," *Journal of Statistical Physics*, **43** (1986) 463–478.

[7] W. Pries, R.D. McLeod, A. Thanailakis, and H.C. Card, "Formal properties of cellular automata as VLSI finite state machines," *Proceedings of the Canadian VLSI Conference* (1985) 205–208.

[8] W. Pries, A. Thanailakis, and H.C. Card, "Group properties of cellular automata and VLSI applications," *IEEE Trans. Comp.*, **C-35** (1986) 1013–1024.

[9] S. Wolfram, "Statistical mechanics of cellular automata," *Rev. Mod. Phys.*, **55** (1983) 601–644.

[10] A. Thanailakis, W. Pries, C.J. Zarowski, and H.C. Card, "Algebraic structure of linear cellular automata," to be published.

[11] A. Thanailakis, C.J. Zarowski, W. Pries, and H.C. Card, "Algebraic structure of VLSI finite state machines based on linear cellular automata." Internal report, Department of Electrical Engineering, University of Manitoba, 1985.

[12] L. Mirsky, *An Introduction to Linear Algebra* (Dover, New York, 1982).