J. KSIAM **Vol.3,** No. 2, 137-145, 1999

Some Properties of Maximum Length Cellular Automata*

Sung-Jin Cho*, Han-Doo Kim ** and Un-Sook Choi*

Abstract

In this paper, We consider two-dimensional Maximum Length Cellular Automata (2-D MLCA) as an extension of the 1-D MLCA. 2-D MLCA can display much better random patterns than those generated by 1-D CA and LFSR. To generate random pattern, a CA should have a maximum length cycle. So, it is necessary to find MLCA that the characteristic polynomial of the transition matrix is primitive. New boundary conditions of 3 types are proposed and some rules having primitive polynomials of 2-D MLCA are found.

I . Introduction

Cellular Automata have been introduced by Von Neumann and Ulam as models of self-organizing and self-reproducing behaviors [12]. A Cellular Automaton is a discrete dynamical system, which consists of a uniform array of memories called cells. The states of cells in the array are updated according to a rule : the state of a cell at a given time depends only on its own state and the states of its nearby neighbors at the previous step [15]. A CA is a necessity in many application areas such as test pattern generation, pseudorandom number generation, cryptography, error correcting codes and signature analysis [1,4,5,6,8,9,11,13,14]. In 2-D CA, cells are arranged in a two-dimensional grid with connections among the neighboring cells. The next state of a cell depends on its four neighbors and itself (five-neighborhood dependency) [5]. A 2-D CA as an extension of the 1-D CA can display

---

1991 Mathematics Subject Classification: 94

Key Words and Phrases. Cellular automata, primitive polynomials, maximum length,

* This research was partially supported by the Ministry of Information and Communications under a Grant from the University Basic Research Fund in 1998.

much better random patterns than those generated by 1-D CA and LFSR. Since a CA has a regular uniform array of nearest neighbor interconnection with combinational logic, it can effectively generate random patterns which have good randomness characteristics.

CA and LFSR are special forms of linear finite state machines (LFSM's) [2]. Every LFSM is represented by a transition matrix over GF(2), and every transition matrix has a characteristic polynomial. Since the characteristic polynomial represents certain properties of the LFSM, finding a particular type of LFSM with a specific characteristic polynomial is an important problem [3]. A CA can be used for random pattern generation. Good randomness is guaranteed when CA has maximum length. A CA has a maximum length if and only if the characteristic polynomial of the transition matrix is primitive. It is a major problem to find CA with primitive polynomial. But it is very difficult to find CA with primitive polynomial.

In this papaer we introduce 2-D IBCA with several types and study maximum length CA with primitive polynomials, which can generate effective random patterns.

II. Preliminaries

The following definitions are well-known.

Definition 2.1> A 1-D CA consists of a number of cells arranged in a regular fashion, where the state transitions of the cells depend on the state of its neighbors [7,15]. In other words, a 1-D CA is a regular structure consisting of an array of memory elements (D-flip flop) and a combinational logic determining the next states of the memory elements. For a local neighborhood 1-D CA, the next state of a particular cell is usually assumed to depend only on itself and on its two neighbors (3- neighborhood dependency). The state q of the i-th cell at time $t+1$ can be noted as

$$q_i^{t+1} = g(q_i^t, q_{i-1}^t, q_{i+1}^t)$$

where q_i^t denotes the state of i-th cell at time t, and g is the next state transition function called the rule of the 1-D CA.

Definition 2.2> a) If the rule of a CA cell involves only XOR logic, then it is called a linear rule. A CA with all the cells having linear rules is called a linear CA.

b) If all the CA cells obey the same rule, then the CA is said to be a uniform CA ; otherwise, it is a hybrid CA.

c) A 1-D CA is said to be a Null Boundary 1-D CA (1-D NBCA) if the left(right) neighbor of the left(right)-most terminal cell is connected to logic 0-state.

d) A 1-D CA is said to be an Intermediate Boundary 1-D CA (1-D IBCA) if the next state of the left(right)-most cell depends on itself, its right(left) neighbor, and the one next to (before) it.

Definition 2.3> A primitive polynomial $p(x)$ of degree n is an irreducible polynomial such that the minimum value of m for which $p(x)$ divides $x^m + 1$ is $2^n - 1$.

It is well-known that a CA has a maximum length if and only if the characteristic polynomial of the transition matrix is primitive [2].

Example 2.4> a) The polynomial $x^4+x^3+x^2+x+1$ is irreducible but not primitive.

b) The polynomial $x^{32}+x^{29}+x^{28}+x^{27}+x^{25}+x^{24}+x^{21}+x^{20}+x^{18}+x^{16}$ $+x^{15}+x^{14}+x^{12}+x^6+x^5+x^4+x^2+x+1$ is primitive.

Ⅲ. Main Results

Definition 3.1 [5]> A 2-D CA is a generalization of 1-D CA, where the cells are arranged in a two-dimensional grid with connections among the neighboring cells. A 2-D CA is composed of mn cells organized as an $m \times n$ array with m rows and n columns. The state transition of the 2-D CA can be represented by an $mn \times mn$ binary matrix. The next state of a cell depends on its four neighbors(top, left, bottom, right) and itself (five-neighborhood dependency). Thus, the next state q of the (i, j)-th cell of a 2-D CA is given by

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

From now we consider only 2-D CA with a linear neighborhood relationship (XOR function). For the five neighborhood dependency, rule can be expressed as a 5-bit number (self, top, left, bottom, right), where each bit signifies the presence of the corresponding dependency.

Example 3.2> Rule matrix $R = \begin{bmatrix} 7 & 29 & 7 \\ 29 & 29 & 7 \\ 29 & 29 & 7 \end{bmatrix}$ and the T matrix for this rule is

$$T = \begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

Now, we propose new definitions about boundary condition in 2-D CA.

Definition 3.3> Boundary conditions can be classified as following.

a) Class 1 : Null Boundary 2-D CA

- The boundary values are all zero as shown in Fig. 1.

b) Class 2 : Intermediate Boundary 2-D CA

- Boundary conditions are divided into three types by different boundary value of left (right) -most cell in each row. And boundary values of top and bottom are zero.

① Type 1 : Pure 2-D IBCA

- Intermediate boundary condition is applied to only a_{11} and a_{mn}.

The rest of boundary cells have null boundary conditions.

And a_{13} be the left neighbor of a_{11} and a_{mn-2} are the right neighbor of a_{mn}

② Type 2 : Inner 2-D IBCA

- Intermediate boundary condition is applied to only a_{i1} and a_{in} where $i = 1, \cdots, m$. That is, left neighbor of a_{i1} is a_{i3} and right neighbor of a_{in} is a_{in-2}.

③ Type 3 : Outer 2-D IBCA

- a_{11}, a_{mn} cells obey Type 1.

Left neighbor of a_{i1} is a_{i-1n} and right neighbor of a_{in} is a_{i+11}.

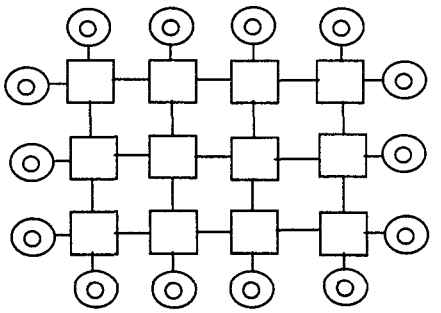


Fig. 1. 2-D NBCA

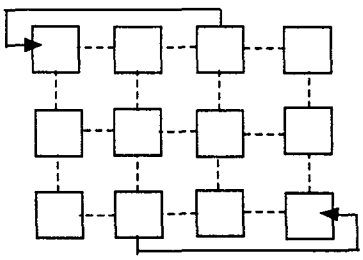


Fig. 2. Type 1 : Pure 2-D IBCA

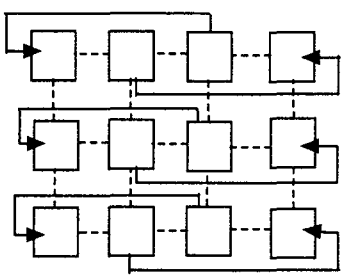


Fig. 3. Type 2 : Inner 2-D IBCA

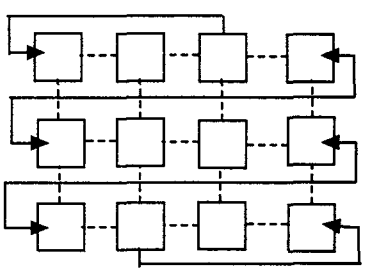


Fig. 4. Type 3 : Outer 2-D IBCA

Example 3.4>

$$R_1 = \begin{bmatrix} 7 & 14 & 7 & 14 & 7 & 14 & 7 & 14 \\ 14 & 7 & 14 & 7 & 14 & 7 & 14 & 7 \\ 7 & 14 & 7 & 14 & 7 & 14 & 7 & 14 \\ 14 & 7 & 14 & 7 & 14 & 7 & 14 & 7 \end{bmatrix}$$ with Type 1 and

$$R_2 = \begin{bmatrix} 21 & 5 & 21 & 21 & 21 & 21 & 5 & 21 \\ 21 & 21 & 21 & 5 & 21 & 21 & 21 & 21 \\ 21 & 5 & 5 & 21 & 21 & 21 & 21 & 5 \\ 5 & 21 & 5 & 5 & 5 & 21 & 21 & 5 \end{bmatrix}$$ with Type 3.

These two rules have the primitive polynomials:

$x^{32}+x^{29}+x^{28}+x^{27}+x^{25}+x^{24}+x^{21}+x^{20}+x^{18}+x^{16}$
$+x^{15}+x^{14}+x^{12}+x^{6}+x^{5}+x^{4}+x^{2}+x+1$ and $x^{32}+x^{31}+x^{30}+x^{10}+1$ respectively.

The following theorem establishes the fact that there exists at least one 2-D IBCA with type 1 corresponding to a 2-D NBCA with type 1, both having the same characteristic polynomial.

Theorem 3.5> Let $R = (R_{ij})$ be a $m \times n$ 7/29 hybrid 2-D CA with null boundary condition such that R_{21} and R_{mn-1} (resp. R_{21} and R_{m-1n}) are independent of the top(resp. bottom). Then there exists a 2-D IBCA with type 1 having the same characteristic polynomial.

Proof. The characteristic matrix of R is given by

$$R_{NBCA} = \begin{bmatrix} g_{11} & 1 & 0 & b_{11} & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & g_{12} & 1 & 0 & b_{12} & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & g_{13} & 1 & 0 & b_{13} & \cdots & 0 & 0 & 0 & 0 & 0 & 0 \\ & & & \ddots & & & & & & & & & \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & t_{m,n-2} & 0 & 0 & g_{m,n-2} & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & t_{m,n-1} & 0 & 1 & g_{m,n-1} & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & t_{m,n} & 0 & 1 & g_{m,n} \end{bmatrix}_{mn \times mn}$$

where $g_{ij} = \begin{cases} 0, & \text{if } R_{ij} \text{ is } 7 \\ 1, & \text{if } R_{ij} \text{ is } 29 \end{cases}$, $t_{ij} = \begin{cases} 0, & \text{if } R_{ij} \text{ is } 7 \\ 1, & \text{if } R_{ij} \text{ is } 29 \end{cases}$ and

$$b_{ij} = \begin{cases} 1, & \text{if } R_{ij} \text{ is } 7 \\ 0, & \text{if } R_{ij} \text{ is } 29 \end{cases}$$

The characteristic polynomial of R_{NBCA} is $det(R_{NBCA} + xI)$.

$$R_{NBCA} + xI = \begin{bmatrix} g_{11}+x & 1 & 0 & b_{11} & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & g_{12}+x & 1 & 0 & b_{12} & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & g_{13}+x & 1 & 0 & b_{13} & \cdots & 0 & 0 & 0 & 0 & 0 & 0 \\ & & & \ddots & & & & & & & & & \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & t_{m,n-2} & 0 & 0 & g_{m,n-2}+x & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & t_{m,n-1} & 0 & 1 & g_{m,n-1}+x & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & 0 & t_{m,n} & 0 & 1 & g_{m,n}+x \end{bmatrix}$$

Row(1)+Row(2)→Row(1) , Row(mn)+Row(mn-1)→Row(mn)

$$\Rightarrow \begin{bmatrix} 1+g_{11}+x & 1+g_{12}+x & 1 & b_{11} & b_{12} & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & g_{12}+x & 1 & 0 & b_{12} & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & g_{13}+x & 1 & 0 & b_{13} & \cdots & 0 & 0 & 0 & 0 & 0 & 0 \\ & & & \ddots & & & & & & & & & \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & t_{m,n-2} & 0 & 0 & g_{m,n-2}+x & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & t_{m,n-1} & 0 & 1 & g_{m,n-1}+x & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & t_{m,n-1} & t_{m,n} & 1 & 1+g_{m,n-1}+x & 1+g_{m,n}+x \end{bmatrix}$$

Col.(1)+Col.(2)→Col.(2) , Col.(mn)+Col.(mn-1)→Col.(mn-1)

$$\Rightarrow \begin{bmatrix} 1+g_{11}+x & g_{11}+g_{12} & 1 & b_{11} & b_{12} & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1+g_{12}+x & 1 & 0 & b_{12} & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & g_{13}+x & 1 & 0 & b_{13} & \cdots & 0 & 0 & 0 & 0 & 0 & 0 \\ & & & \ddots & & & & & & & & & \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & t_{m,n-2} & 0 & 0 & g_{m,n-2}+x & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & t_{m,n-1} & 0 & 1 & 1+g_{m,n-1}+x & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & t_{m,n-1} & t_{m,n} & 1 & g_{m,n-1}+g_{m,n} & 1+g_{m,n}+x \end{bmatrix}$$

$$\Rightarrow \begin{bmatrix} 1+g_{11} & g_{11}+g_{12} & 1 & b_{11} & b_{12} & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1+g_{12} & 1 & 0 & b_{12} & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & g_{13} & 1 & 0 & b_{13} & \cdots & 0 & 0 & 0 & 0 & 0 & 0 \\ & & & \ddots & & & & & & & & & \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & t_{m,n-2} & 0 & 0 & g_{m,n-2} & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & t_{m,n-1} & 0 & 1 & 1+g_{m,n-1} & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & \cdots & 0 & t_{m,n-1} & t_{m,n} & 1 & g_{m,n-1}+g_{m,n} & 1+g_{m,n} \end{bmatrix} + xI$$

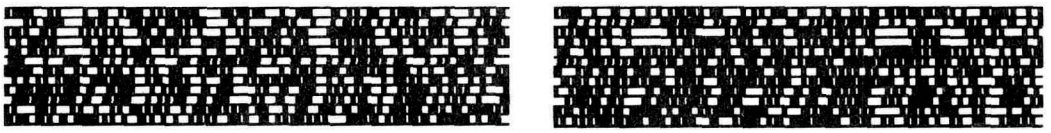
$\Rightarrow R_{IBCA} + xI$

R_{IBCA} is the matrix representation of 2-D IBCA and hence the proof is completed.

Example 3.6> $R = \begin{bmatrix} 7 & 29 & 7 & 29 \\ 7 & 29 & 7 & 29 \\ 7 & 29 & 7 & 29 \end{bmatrix}$ with null boundary condition has the primitive polynomial $1 + x^5 + x^8 + x^9 + x^{12}$.

From the above Theorem we obtain 2-D IBCA R' with type 1 as follows.

$$R' = \begin{bmatrix} 23 & 13 & 7 & 29 \\ 7 & 29 & 7 & 29 \\ 7 & 29 & 23 & 13 \end{bmatrix}$$



(a) 12-cell 2-D NBCA (b) 12-cell 2-D IBCA

Fig. 5. State Time Diagrams for 2-D NBCA and 2-D IBCA

Ⅳ. Conclusion

In this paper, we consider 2-D MLCA as extensions of 1-D MLCA. Some examples of 2-D MLCA are shown and new boundary conditions of 3 types are introduced. Several configurations are shown under the some conditions. The 2-D MLCA can be used for random pattern generation. To generate better random pattern, MLCA should satisfy the condition that the characteristic polynomial of the transition matrix is primitive. This paper presents some rules having primitive polynomials of the 2-D MLCA.

References

[1] P.H. Bardell, "Analysis of cellular automata used as pseudorandom pattern generators", *Proc. IEEE int. Test. Conf.*, pp.762-767, 1990.

[2] T.L. Booth, *Sequential Machines and Automata Theory*, John Wiely & Sons, London, 1967.

[3] Kevin Cattell and Jon C. Muzio, "Synthesis of One-Dimensional Linear Hybrid Cellular Automata", *IEEE Trans. Computer-Aided Design,* Vol. 15, No. 3, 1996

[4] D.R. Chowdhury, S. Basu, I. S. Gupta and P. P. Chaudhuri, "Design of CAUCC-cellular automata based error correcting code", *IEEE Trans. Comput.*, Vol.43, pp.759-764, 1994.

[5] D.R. Chowdhury, P. Subbarao and P. P. Chaudhuri, " Characterization of two dimensional cellular automata using matrix algebra", *Information Sciences*, Vol. 71, pp. 289-314, 1993

[6] T. Damarla and A. Sathaye, "Application of one-dimensional cellular

automata and linear feedback shift registers for pseudo exhaustive testing", *IEEE. Trans. Computer-Aided Design*, Vol. 12, pp. 1580-1591, 1993.

[7] A.K. Das and P.P. Chaudhuri, " Efficient characterization of cellular automata" *Proc. IEE(Part E)*, Vol. 137, No.1, pp. 81-87, Jan. 1990.

[8] A. K. Das and P. P. Chaudhuri, "Vector space theoritic analysis of additive cellular automata and its application for pseudo-exhaustive test pattern generation", *IEEE Trans. Compute.*, Vol. 42, pp. 340-352, 1993.

[9] P.D. Hortensius, R.D. McLeod and H.C. Card, "Cellular automata based signature analysis for built-in self-test", *IEEE Trans. Comput.*, Vol. 39, pp. 1273-1283, 1990.

[10] D.M. Miller, J.C. Muzio, M. Serra, X. Sun, S. Zhang and R.D. McLeod "Cellular automata techniques for compaction based BIST", *Proc. IEEE Int. Symp. Circuits Syst.*, pp. 1893-1896, 1991.

[11] D.M. Miller and S. Zhang, "A study of the fault coverage of LFSR and CA pseudo-random test pattern generators", *Proc. 5th Technical Workshop New Directions IC Testing,* 1991.

[12] J. Von Neumann, *Theory of self-reproducing automata,* University of Illinois Press, Urbana, 1966.

[13] M. Serra, T. Slater, J.C. Muzio and D.M. Miller, "The analysis of one dimensional linear cellular automata and their aliasing properties", *IEEE Trans Computer-Aided Design*, Vol. 9, pp. 767-778, 1990.

[14] P. Tsalides, T. A. York and A. Thanailakis, "Pseudorandom number generators for systems based on linear cellular automata", *IEE Proc(Part E) Computers Digital Techniques,* Vol. 138, pp.241-249, 1991.

[15] S. Wolfram, " Statistical mechanics of cellular automata", *Rev. Modern Physics,* Vol. 55, No. 3, July 1983.

* Dept. of Applied Mathematics, Pukyong National University

**Dept. of Mathematics, Inje University