JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **23**, No. 4, December 2010

A CHARACTERIZATION OF CYCLE LENGTHS OF CELLULAR AUTOMATA

Jae-Gyeom Kim*

Abstract. In this note, we give a characterization of cycle lengths of uniform cellular automata configured with rules 60 or 102.

1. Introduction

Cellular automata have been demonstrated by many researchers to be a good computational model for physical systems simulation since the concept of cellular automata first introduced by John Von Neumann in the 1950's. And cycle lengths of group cellular automata have been studied [1-9].

In this note, we give a characterization of cycle lengths of uniform cellular automata configured with rules 60 or 102.

2. Preliminaries

A cellular automaton (CA) is an array of sites (cells) where each site is in any one of the permissible states. At each discrete time step (clock cycle) the evolution of a site value depends on some rule (the combinational logic) which is a function of the present states of its k neighbors for a k-neighborhood CA. For 2-state 3-neighborhood CA, the evolution of the (i)th cell can be represented as a function of the present states of $(i-1)$th, (i)th, and $(i+1)$th cells as: $x_i(t+1) = f\{x_{i-1}(t), x_i(t), x_{i+1}(t)\}$, where f represents the combinational logic. For such CA, the modulo-2 logic is always applied.

For 2-state 3-neighborhood CA there are 2^3 distinct neighborhood configurations and 2^{2^3} distinct mappings from all these neighborhood

Received September 07, 2010; Accepted November 09, 2010.
2010 Mathematics Subject Classification: Primary 68Q80.
Key words and phrases: cellular automaton, cycle length.
This Research was supported by Kyungsung University Research Grants in 2010.

configurations to the next states, each mapping representing a CA rule. The CA, characterized by a rule known as rule 60, specifies an evolution from the neighborhood configurations to the next states as:

111	110	101	100	011	010	001	000	
0	0	1	1	1	1	0	0	Decimal 60.

The corresponding combinational logic of rule 60 is given by

$$x_i(t+1) = x_{i-1}(t) \oplus x_i(t),$$

that is, the next state of (i)th cell depends on the present states of its left and self neighbors.

And the CA, characterized by a rule known as rule 102, specifies an evolution from the neighborhood configurations to the next states as:

111	110	101	100	011	010	001	000	
0	1	1	0	0	1	1	0	Decimal 102.

The corresponding combinational logic of rule 102 is given by

$$x_i(t+1) = x_i(t) \oplus x_{i+1}(t),$$

that is, the next state of (i)th cell depends on the present states of self and its right neighbors.

If in a CA the same rule applies to all cells, then the CA is called a uniform CA; otherwise the CA is called a hybrid CA. There can be various boundary conditions; namely, null (where extreme cells are connected to logic '0'), periodic (extreme cells are adjacent), etc. In the sequel, we will always assume null boundary condition unless otherwise specified. If the rule of a CA cell involves only XOR logic, then the rule is called a linear rule. A CA with all the cells having linear rules is called a linear CA. And the number of cells of a CA is called the length of a CA.

The characteristic matrix T of a CA is the transition matrix of the CA. The next state $f_{t+1}(x)$ of a linear CA is given by $f_{t+1}(x) = T \times f_t(x)$, where $f_t(x)$ is the current state and t is the time step. If all the states of the CA form a single or multiple cycles, then it is referred to as a group CA.

Lemma 2.1 ([3]). *A CA is a group CA if and only if $T^m = I$ where T is the characteristic matrix of the CA, I is the identity matrix and m is a positive integer.*

Lemma 2.2 ([9]). *CA rules 60, 102 and 204 form groups for all lengths ℓ with group order $n = 2^a$ where $a = 0, 1, 2, \cdots$. And if the CA rule is 60 or 102 then $\frac{n}{2} < \ell \leq n$.*

3. Cycle lengths of cellular automata

For a uniform CA configured with rule 60, its characteristic matrix T is as follows;

$$(T)_{ij} = \begin{cases} 1, & i = j, \\ 1, & i = j+1, \\ 0, & \text{otherwise}, \end{cases}$$

or

$$T = \begin{pmatrix} 1 & 0 & 0 & & & & \\ 1 & 1 & 0 & & & & \\ 0 & 1 & 1 & 0 & & & \\ & & & \cdot & & & \\ & & & & \cdot & & \\ & & & & & \cdot & \\ & & & & 0 & 1 & 1 & 0 \\ & & & & & 0 & 1 & 1 \end{pmatrix}$$

Considering state transition and cycle lengths in the uniform CA of length ℓ configured with rule 60, a state vector $(0, \cdots, 0, c_t, \cdots, c_1)$ of which first $(\ell - t)$ entries are zero can be identified with the state vector $(c_t, \cdots, c_1)$ in the uniform CA of length t configured with rule 60. When c_t is 1, it is called the first 1 of the state vector $(0, \cdots, 0, c_t, \cdots, c_1)$, and the proper length of the state vector is t.

So we have a lemma.

LEMMA 3.1. *Let $(c_\ell, \cdots, c_1)$ be a state vector in the uniform CA of lengh ℓ configured with rule* 60. *If the proper length of the state vector is t, then the cycle length of the state vector $(c_\ell, \cdots, c_1)$ is the same as the cycle length of the state vector $(c_t, \cdots, c_1)$ in the uniform CA of length t configured with rule* 60.

Now we characterize the (2^a)th power of the characteristic matrix T of a CA configured with rule 60. By mathematical induction, we can easily get T^{2^a} where $a = 1, 2, \cdots$ as follows;

(1)
$$(T^{2^a})_{ij} = \begin{cases} 1, & i = j, \\ 1, & i = j + 2^a, \\ 0, & \text{otherwise}, \end{cases}$$

or

(2) T^{2^a}

$$
= \left(\begin{array}{cccccccccccc}
1 & 0 & 0 & & & & & & & & & 0 \\
0 & 1 & 0 & & & & & & & & & 0 \\
0 & 0 & 1 & & & & & & & & & 0 \\
0 & 0 & 0 & 1 & & & & & \text{0} & & & 0 \\
\vdots & \vdots & \vdots & \cdots & \ddots & & & & & & & \vdots \\
0 & 0 & 0 & \cdots & 0 & 1 & 0 & & & & & 0 \\
1 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 & & & & 0 \\
0 & 1 & 0 & \cdots & 0 & 0 & 0 & 1 & 0 & & & 0 \\
0 & 0 & 1 & \cdots & 0 & 0 & 0 & 0 & 1 & 0 & & 0 \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & 0 & 1 & 0 & 0 & \cdots & \cdots & \cdots & 1
\end{array}\right). \begin{array}{l} \\ \\ \\ \\ \\ \leftarrow (2^a)\text{th row} \\ \\ \\ \\ \\ \\ \\ \end{array}
$$

THEOREM 3.2. *Let $(c_\ell, \cdots, c_1)$ be a state vector in the uniform CA of length ℓ configured with rule 60. Suppose that c_t is the first 1 of the state vector, in other words, the proper length of the state vector is t where $2^a < t \leq 2^{a+1}$. Then the cycle length of the state vector is 2^{a+1}.*

Proof. By Lemma 3.1, the cycle length of the state vector $(c_\ell, \cdots, c_1)$ is the same as the cycle length of the state vector $(c_t, \cdots, c_1)$ in the uniform CA of length t configured with rule 60. Now we have

$$
(T^{2^a}) \begin{pmatrix} c_t \\ \vdots \\ c_{t-2^a+1} \\ c_{t-2^a} \\ \vdots \\ c_1 \end{pmatrix}
$$

$$
= \begin{pmatrix}
1 & 0 & 0 & & & & & & & & & 0 \\
0 & 1 & 0 & & & & & & & & & 0 \\
0 & 0 & 1 & & & & & & & & & 0 \\
0 & 0 & 0 & 1 & & & & \text{\Large 0} & & & & 0 \\
\vdots & \vdots & \vdots & \cdots & \ddots & & & & & & & \vdots \\
0 & 0 & 0 & \cdots & 0 & 1 & 0 & & & & & 0 \\
1 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 & & & & 0 \\
0 & 1 & 0 & \cdots & 0 & 0 & 0 & 1 & 0 & & & 0 \\
0 & 0 & 1 & \cdots & 0 & 0 & 0 & 0 & 1 & 0 & & 0 \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & 0 & 1 & 0 & 0 & \cdots & \cdots & \cdots & 1
\end{pmatrix}
\begin{pmatrix} c_t \\ \vdots \\ c_{t-2^a+1} \\ c_{t-2^a} \\ \vdots \\ c_1 \end{pmatrix}
\quad \text{by (1) and (2)}
$$

$$
= \begin{pmatrix} c_t \\ \vdots \\ c_{t-2^a+1} \\ c_{t-2^a} + c_t \\ \vdots \\ c_1 \end{pmatrix}
$$

$$
\neq \begin{pmatrix} c_t \\ \vdots \\ c_{t-2^a+1} \\ c_{t-2^a} \\ \vdots \\ c_1 \end{pmatrix} \quad \text{because } c_t = 1,
$$

where T is the characteristic matrix of the uniform CA of length t configured with rule 60. This means the cycle length of the state vector $(c_t, \cdots, c_1)$ is greater than 2^a. But the cycle length of the state vector $(c_t, \cdots, c_1)$ is less than or equal to 2^{a+1} by Lemma 2.1 and 2.2. Thus the cycle length of the state vector $(c_t, \cdots, c_1)$ is 2^{a+1} because it should be a divisor of 2^{a+1}. Hence we have the conclusion. □

Corollary 3.3. *For the uniform CA of length ℓ configured with rule* 60 *where $2^a < \ell \leq 2^{a+1}$, the number of state vectors of cycle length 2^{a+1} is $(2^\ell - 2^{2^a})/2^{a+1}$, the number of state vectors of cycle length 2^n is*

$(2^{2^n} - 2^{2^{n-1}})/2^n$ *where* $1 \leq n \leq 2^a$, *and the number of state vectors of cycle length* 1 *is* 2.

Proof. It is a simple counting by Theorem 3.2. □

Theorem 3.2 completely characterize the cycle lengths of state vectors in uniform CA configured with rule 60. And Corollary 3.3 completely characterize the numbers of such state vectors of cycle lenghts. Table 1 shows such numbers explicitly.

Table 1. Cycles of uniform CA configured with rules 60 or 102.

Length of CA	Generated cycles		Length of CA	Generated cycles	
	Length	Number		Length	Number
1	1	2	6	1	2
2	1	2		2	1
	2	1		4	3
3	1	2		8	6
	2	1	7	1	2
	4	1		2	1
4	1	2		4	3
	2	1		8	14
	4	3	8	1	2
5	1	2		2	1
	2	1		4	3
	4	3		8	30
	8	2			

Since the characteristic matrices of uniform CA configured with rules 60 and 102 are the transposes of each other, the discussion on properties related to CA rule 60 in this section is parallel to that on properties related to CA rule 102. So all of the results on CA rule 60 that was discussed in this section is still valid for CA rule 102. In particular, we can have the following theorem and corollary which are parellel to Theorem 3.2 and Corollary 3.3, respectively.

Theorem 3.4. *Let* $(c_1, \cdots, c_\ell)$ *be a state vector in the uniform CA of lengh* ℓ *configured with rule* 102. *Suppose that* c_t *is the last* 1 *of the state vector, in other words, the proper length of the state vector is* t *where* $2^a < t \leq 2^{a+1}$. *Then the cycle length of the state vector is* 2^{a+1}.

Corollary 3.5. *For the uniform CA of length* ℓ *configured with rule* 102 *where* $2^a < \ell \leq 2^{a+1}$, *the number of state vectors of cycle length*

2^{a+1} is $(2^\ell - 2^{2^a})/2^{a+1}$, the number of state vectors of cycle length 2^n is $(2^{2^n} - 2^{2^{n-1}})/2^n$ where $1 \leq n \leq 2^a$, and the number of state vectors of cycle length 1 is 2.

References

[1] P. P. Chaudhuri, D. R. Chowdhury, S. Nandi and S. Chattopadhyay, *Additive celullar automata theory and applications*, **1**, IEEE Computer Society Press, Los Alamitos, California, 1997.

[2] A. K. Das, *Additive cellular automata: Theory and application as a built-in self-test structure*, PhD thesis, I.I.T., Kharagpur, India, 1990.

[3] A. K. Das, A. Ganguly, A. Dasgupta, S. bhawmik and P. P. Chaudhuri, *Efficient characterization of cellular automata*, Proc. IEE (Part E) **15** (1990), no.1, 81–87.

[4] B. Elspas, *The theory of autonomous linear Sequential networks*, TRE Trans. Circuits **CT-6** (1959), 45–60.

[5] P. D. Hortensius, R. D. McLeod and B. W. Podaima, *Cellular automata circuits for built-in self test*, IBM J. Res. & Dev. **34** (1990), 389–405.

[6] J. G. Kim, *On state transition diagrams of cellular automata*, East Asian Math. J. **25** (2009), no.4, 517–525.

[7] S. Nandi, *Additive cellular automata: Theory and application for testable circuit design and data encryption*, PhD thesis, I.I.T., Kharagpur, India, 1994.

[8] S. Nandi, B. K. Kar and P. P. Chaudhuri, *Theory and applications of cellular automata in cryptography*, IEEE Trans. Computers **43** (1994), no. 12, 1346–1357.

[9] W. Pries, A. Thanailakis and H. C. Card, *Group properties of cellular automata and VLSI applications*, IEEE Trans. Computers **C-35** (1986), no. 12, 1013–1024.

*

Department of Mathematics
Kyungsung University
Busan 608-736, Republic of Korea
E-mail: jgkim@ks.ac.kr