East Asian Mathematical Journal
Vol. 25 (2009), No. 4, pp. 517–525

ON STATE TRANSITION DIAGRAMS OF CELLULAR AUTOMATA

Jae-Gyeom Kim

Abstract. We discuss group orders and lengths of cycles of state transition diagrams of cellular automata.

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. Many parts of the theory of cellular automata have been developed by researchers who are not mathematicians. And we could find some logical errors in the literatures [1, 4]. In fact, the errors in [4] have been repeated in [1]. Recently, some of such errors were pointed out and parts of them were modified [3].

In this note, we will modify some more parts of them and discuss lengths of cycles of state transition diagrams of cellular automata. For the purpose, we will use terminologies and notations just as in [4]. In section 2, we will give some terminologies and notations in [4] and quote some contents from [4].

2. Preliminaries and quotation

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 state 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 2-state 3-neighborhood CA there are 2^3 distinct neighborhood configurations and 2^{2^3} distinct mappings from all these neighborhood configurations to the next state, each mapping representing a CA rule. The CA, characterized by

Received July 24, 2009; Accepted November 16, 2009.
2000 *Mathematics Subject Classification.* 68Q80.
Key words and phrases. cellular automaton, group cellular automaton.
This Research was supported by Kyungsung University Research Grants in 2009.

a rule known as rule 60, specifies an evolution from neighborhood configuration to the next state 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

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

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

A CA characterized by EXOR and/or EXNOR dependence is called an additive CA. If in a CA the neighborhood dependence is EXOR, then it is called a noncomplemented CA and the corresponding rule is referred to as a noncomplemented rule. For neighborhood dependence of EXNOR (where there is an inversion of the modulo-2 logic), the CA is called a complemented CA. The corresponding rule involving the EXNOR function is called a complemented rule. In a complemented CA, single or multiple cells may employ a complemented rule with EXNOR function. There exist 16 additive rules which are: Rule 0, 15, 51, 60, 85, 90, 102, 105, 150, 153, 165, 170, 195, 204, 240 and 255.

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.

The logic functions for three complemented rules 195, 163 and 51 and the corresponding noncomplemented rules are also noted in Table 1.

Table 1. Logic functions

complemented			noncomplemented	
Rule	logic function	dependency	rule	logic function
195	$\overline{x_{i-1}(t) \oplus x_i(t)}$	left & self	60	$x_{i-1}(t) \oplus x_i(t)$
153	$\overline{x_i(t) \oplus x_{i+1}(t)}$	self & right	102	$x_i(t) \oplus x_{i+1}(t)$
51	$\overline{x_i(t)}$	self	204	$x_i(t)$

The characteristic matrix T of a CA is the transition matrix of the CA. The next state $f_{t+1}(x)$ of an additive CA is given by $f_{t+1}(x) = T \times f_t(x)$, where $f_t(x)$ is the current state, 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. [2] *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. [2] *Let $\overline{T}^m$ denote the application of the complemented rule $\overline{T}$ for m successive cycles, then*

$$[\overline{T}^m][f(x)] = [I + T + T^2 + \cdots + T^{m-1}][F(x)] + [T^m][f(x)]$$

where T is the characteristic matrix of the corresponding noncomplemented rule and $[F(x)]$ is an ℓ-dimensional vector ($\ell =$ number of cells) responsible for inversion after EXORing. $F(x)$ has '1' entries (i.e., nonzero entries) for CA cell positions where EXNOR function is employed.

Lemma 2.3. [2] *The complement of a group CA is also a group CA.*

Lemma 2.4. [5] *CA rules* 60, 102 *and* 204 *form groups for all lengths ℓ with group order $O(G) = n = 2^a$ where $a = 0,\ 1,\ 2,\ \cdots$. And if the CA rule is* 60 *or* 102 *then $\frac{n}{2} < \ell \leq n$.*

Lemma 2.4 provides the CA rules that generate cycles of length 2^a, $a = 0,\ 1,\ 2,\ \cdots$. The following lemma establishes the corresponding results for uniform CA's with complemented rules 51, 153, and 195. The corresponding noncomplemented rules are 204, 102 and 60.

Lemma 2.5. [4] *Complemented CA rules* 195, 153 *and* 51 *form groups for all lengths with group order $O(G) = m = 2^a$ where $a = 0,\ 1,\ 2,\ \cdots$.*

Proof. [4]. Consider a CA with rule R and characteristic matrix T, where R is a combination of the rules 60, 102, and 204. Then, as per Lemma 2.2, the corresponding complemented CA, with characteristic matrix $\overline{T}$, may be expressed as:

$$[\overline{T}^m][f(x)] = [I + T + T^2 + \cdots + T^{m-1}][F(x)] + [T^m][f(x)]. \tag{1}$$

The fact that R is a group CA rule implies that $T^n = I$ for n as some integral power of 2 (Lemma 2.4). As per Lemma 2.3, complement of a group CA is also a group CA. So,

$$[\overline{T}^m][f(x)] = [f(x)], \tag{2}$$

where m is the cycle length of the complemented CA. From (1) and (2),

$$[T^m + I][f(x)] = [I + T + T^2 + \cdots + T^{m-1}][F(x)]$$
$$\Rightarrow [T + I][I + T + T^2 + \cdots + T^{m-1}][f(x)] = [I + T + T^2 + \cdots + T^{m-1}][F(x)]$$

Assume $I + T + T^2 + \cdots + T^{m-1} \neq 0$, consequently

$$[T + I][f(x)] = [F(x)]. \tag{3}$$

If the CA under consideration consists of ℓ number of cells, then (3) is a system of ℓ linear equations, and the condition for its solution to exist is

$$rank[T + I] = rank[T + I|F(x)].$$

In the case of R, being any combination of rules 60, 102 and 204, it can be directly shown that $rank[T + I] < \ell$, owing to fact that one row of matrix $T + I$

is null in such a case. Also, since each entry of $F(x)$ is 1 (as in the case of all complemented rules), it follows that

$$rank[T+I] \neq rank[T+I|F(x)].$$

This is a contradiction and, hence, it follows that

$$I+T+T^2+\cdots+T^{m-1}=0 \tag{4}$$

$$\Rightarrow \overline{T}^m[f(x)] = T^m[f(x)] = f(x) \tag{5}$$

$$\Rightarrow T^m = I.$$

Let $m = bn$, where b is nonzero positive integer. For $b = 2$,

$$\begin{aligned}
&I+T+T^2+\cdots+T^{m-1} \quad (\text{as } m=2n)\\
&= I+T+T^2+\cdots+T^{n-1}+T^n+T^{n+1}+T^{n+2}+\cdots+T^{2n-1}\\
&= [I+T+T^2+\cdots+T^{n-1}]+[I+T+T^2+\cdots+T^{n-1}] \quad (\text{as } T^n=I)\\
&= 0 \quad (\text{since modulo-2 summation is involved}).
\end{aligned}$$

So, the relation (4) always satisfies for $b = 2$. For particular values of T, relation (4) may hold for $b = 1$. Hence, the value of m is either n or $2n$.

Now we need to show that m is a nonzero positive integral power of 2. As per Lemma 2.4, n is of the form 2^a, ($a = 0, 1, 2, \cdots$). We consider the following two cases.

Case 1 : for $n = 2^0 = 1$

$$\Rightarrow T = I$$

$$\Rightarrow I+T=0 \tag{6}$$

Considering equations (4) and (6) we arrive at the conclusion that $m = 2$ for $n = 1$.

Case 2 : for $n = 2^a$, ($a = 1\ ,\ 2\ ,\ 3\ ,\ \cdots$);

we know that m is either n or $2n$.

So m is also a nonzero positive integral power of 2. □

Theorem 2.6. [4] *If a null boundary uniform or hybrid CA configured with rules* 51, 153 *and* 195 *is a group CA, then its state transition diagram consists of equal cycles of even length.*

Proof. From Lemma 2.5, it can be seen that group CA, under different configurations of rules 51, 153, and 195, generate cycles of even length m (positive integral power of 2). Now we have to prove that factors of m can not be a cycle lengths. Assume that the group CA has a cycle of length m_i [where m_i is a factor of m]. Then it must satisfy the following equations:

$$I+T+T^2+\cdots+T^{m_i-1}=0 \quad \text{and} \quad [\overline{T}^{m_i}][f(x)] = [T^{m_i}][f(x)] = f(x).$$

This implies that m_i is the group order of all cycle lengths of the group CA, suggesting that m_i is equal to m, i.e., all cycles are equal in length. Hence, the theorem. □

Lemma 2.5 and Theorem 2.6 were proved first in [4]. And the proofs of Lemma 2.5 and Theorem 2.6 in [1] are quite similar with the proofs in [4].

3. State transition diagrams of CA

Logical errors in the proofs of Lemma 2.5 and Theorem 2.6 were pointed out and a new proof of Lemma 2.5 was given in [3]. And the following proposition, which is contained in the proof of Lemma 2.5, was reproved in the new proof of Lemma 2.5 [3].

Proposition 3.1. *If a uniform CA of length ℓ configured with rule* 60*,* 102 *or* 204 *has group order n, then the corresponding complemented uniform CA of length ℓ configured with rule* 195*,* 153 *or* 51 *has group order n or $2n$.*

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

$$(T^{2^a})_{ij} = \begin{cases} 1 & i = j, \\ 1, & i = j + 2^a, \\ 0, & \text{otherwise}, \end{cases} \tag{7}$$

or

$$T^{2^a} = \left(\begin{array}{cccccccccccc}
1 & 0 & 0 & & & & & & & & & 0 \\
0 & 1 & 0 & & & & & & & & & 0 \\
0 & 0 & 1 & & & & & & & & & 0 \\
0 & 0 & 0 & 1 & & & & & \text{\Large 0} & & & 0 \\
\vdots & \vdots & \vdots & \cdots & \ddots & & & & & & & \vdots \\
0 & 0 & 0 & \cdots & 0 & 1 & 0 & & & & & 0 \\
1 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 & & & & 0 \\
0 & 1 & 0 & \cdots & 0 & 0 & 0 & 1 & 0 & & & 0 \\
0 & 0 & 1 & \cdots & 0 & 0 & 0 & 0 & 1 & 0 & & 0 \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 & 1 & \cdots & 0 \\
\vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & 0 & \cdots & 0 & 1 & 0 & 0 & \cdots & \cdots & \cdots & 1
\end{array}\right)
\begin{array}{l}
\\ \\ \\ \\ \\
\leftarrow (2^a)\text{th row} \\
\\ \\ \\ \\ \\ \\
\end{array} \tag{8}$$

So we have an easy lemma which is a part of Lemma 2.4.

Lemma 3.2. *Let T be the characteristic matrix with size $\ell \times \ell$ of CA rule* 60*. Then the order of T is 2^a where $2^{a-1} < \ell \le 2^a$.*

Note that $(A + B)^{2^a} = A^{2^a} + B^{2^a}$ in modulo-2 logic where A and B are matrices. Now we consider the matrix $I + T$ where T is the characteristic matrix of CA rule 60. The entries of $I + T$ are as follows;

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

So, in matrix multiplication $(I+T)A = B$, $I+T$ pull down every row one step and make the first row zero, or

$$B_{ij} = \begin{cases} 0 & i = 1, \\ A_{(i-1)j}, & \text{otherwise.} \end{cases}$$

Thus we have

$$((I+T)^t)_{ij} = \begin{cases} 1 & i = j+t, \\ 0, & \text{otherwise} \end{cases} \tag{9}$$

where $t = 1, 2, \cdots$, in particular,

$$(I+T)^\ell = 0 \ \text{ and } \ (I+T)^{\ell-1} = \begin{pmatrix} 0 & & & \\ \vdots & & 0 & \\ 0 & & & \\ 1 & 0 & \cdots & 0 \end{pmatrix} \tag{10}$$

where $\ell \times \ell$ is the size of T.

Lemma 3.3. *Let T be the characteristic matrix of CA rule* 60*. Then $(I+T)^{2^a-1} = I + T + \cdots + T^{2^a-1}$ where $a = 1, 2, \cdots$.*

Proof. We will use mathematical induction on a. If $a = 1$, then it is obvious. Let $a > 1$. Then we have

$$\begin{aligned} & I + T + \cdots + T^{2^a-1} \\ &= I + T + \cdots + T^{2^{a-1}-1} + T^{2^{a-1}} + T^{2^{a-1}+1} + \cdots + T^{2^a-1} \\ &= (I + T + \cdots + T^{2^{a-1}-1}) + T^{2^{a-1}}(I + T + \cdots + T^{2^{a-1}-1}) \\ &= (I + T^{2^{a-1}})(I + T + \cdots + T^{2^{a-1}-1}) \\ &= (I + T^{2^{a-1}})(I+T)^{2^{a-1}-1} \ \text{ by induction hypothesis} \\ &= (I+T)^{2^{a-1}}(I+T)^{2^{a-1}-1} \\ &= (I+T)^{2^a-1}. \end{aligned}$$

So we have the conclusion. □

Theorem 3.4. *A null boundary uniform CA of length ℓ configured with rule* 195 *has group order 2^a where $2^{a-1} \leq \ell < 2^a$. And its state transition diagram consists of equal cycles of length 2^a.*

Proof. Let T be the characteristic matrix of CA rule 60. At first, suppose that $\ell = 2^{a-1}$. Then we have

$$
\begin{aligned}
&[\overline{T}^{\ell}][f(x)]\\
&= [I+T+\cdots+T^{\ell-1}][F]+[T^{\ell}][f(x)] \quad \text{by Lemma 2.2}\\
&= [(I+T)^{\ell-1}][F]+[T^{\ell}][f(x)] \quad \text{by Lemma 3.3}\\
&= \begin{pmatrix} 0 & & & \\ \vdots & & \text{\Large 0} & \\ 0 & & & \\ 1 & 0 & \cdots & 0\end{pmatrix}\begin{pmatrix}1\\ \vdots\\ 1\end{pmatrix} + [I][f(x)] \quad \text{by (10) and Lemma 3.2}\\
&= \begin{pmatrix}0\\ \vdots\\ 0\\ 1\end{pmatrix} + [f(x)]\\
&\neq [f(x)]
\end{aligned}
$$

for all $f(x)$. And $[\overline{T}^{2^{a}}][f(x)] = [f(x)]$ for all $f(x)$ by Proposition 3.1 and Lemma 3.2. Now let $2^{a-1} < \ell < 2^{a}$. Then we have

$$
\begin{aligned}
&[\overline{T}^{2^{a-1}}][f(x)]\\
&= [(I+T)^{2^{a-1}-1}][F]+[T^{2^{a-1}}][f(x)] \qquad \text{by Lemma 2.2 and Lemma 3.3}\\
&= \begin{array}{r} \\ \\ (2^{a-1})\text{th row} \rightarrow \\ \\ \\ \end{array}\begin{pmatrix} 0&0&& \\ \vdots&\vdots&&\text{\Large 0}\\ 1&0&&\\ 0&1&0&\\ \vdots&\vdots&\ddots& \end{pmatrix}\begin{pmatrix}1\\ \\ \vdots\\ \\ 1\end{pmatrix}\\
&\quad + \begin{array}{r} \\ \\ \\ \\ \\ (2^{a-1}+1)\text{th row} \rightarrow \\ \\ \\ \end{array}\begin{pmatrix} 1&0&&&&\\ 0&1&0&&&\\ 0&0&1&0&&\text{\Large 0}\\ \vdots&\vdots&\vdots&&&\\ 0&&&&\ddots&\\ 1&0&&&&\\ 0&1&0&&\text{\Large 0}&\\ \vdots&\vdots&\ddots&&&1 \end{pmatrix}\begin{pmatrix}f(x)_1\\ \\ \\ \vdots\\ \\ \\ f(x)_{\ell}\end{pmatrix}\\
&\qquad\qquad \text{by (7), (8) and (9)}
\end{aligned}
$$

$$
\begin{aligned}
&= (2^{a-1})\text{th row} \rightarrow \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ \vdots \\ \\ 1 \end{pmatrix} + \begin{pmatrix} f(x)_1 \\ \\ \vdots \\ f(x)_{2^{a-1}} \\ f(x)_{2^{a-1}+1} + f(x)_1 \\ \vdots \\ f(x)_\ell + f(x)_{\ell - 2^{a-1}} \end{pmatrix} \\
&= \begin{pmatrix} \vdots \\ 1 + f(x)_{2^{a-1}} \\ \vdots \end{pmatrix} \\
&\neq [f(x)]
\end{aligned}
$$

for all $f(x)$. Hence we have the conclusion. □

Since the characteristic matrices of CA rules 60 and 102 are the transposes of each other, the discussion on some properties related to CA rule 60 and the complemented CA rule 195 in this section is parallel to that on the properties related to CA rule 102 and the complemented CA rule 153. So all of the results on CA rule 60 and the complemented CA rule 195 that was discussed in this section is still valid for CA rule 102 and the complemented CA rule 153. In particular, we can have the following theorem which is parallel to Theorem 3.4.

Theorem 3.5. *A null boundary uniform CA of length ℓ configured with rule 153 has group order 2^a where $2^{a-1} \leq \ell < 2^a$. And its state transition diagram consists of equal cycles of length 2^a.*

Note that a null boundary uniform CA configured with rule 51 has group order 2 obviously. And its state transition diagram consists of equal cycles of length 2 clearly.

References

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

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

[3] J. G. Kim, *S*ome properties of cellular automata, J. Chungcheong Math. Soc. **21** (2008), no. 4, 447–454.

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

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

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