JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **21**, No. 4, December 2008

SOME PROPERTIES OF CELLULAR AUTOMATA

Jae-Gyeom Kim*

Abstract. In this short note, we will point out and modify some logical errors in literatures about the theory 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, 3]. In fact, the errors in [3] have been repeated in [1].

In this short note, we will point out some of such errors and modify parts of them. For the purpose, we will use terminologies and notations just as in [3]. In section 2, we will give some terminologies and notations in [3] and quote some contents from [3].

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 k of its neighbors for a k-neighborhood CA. For 2-state 3-neighborhood CA, the evolution of the ith 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.

Received July 29, 2008; Accepted August 27, 2008.
2000 Mathematics Subject Classification: Primary 68Q80.
Key words and phrases: cellular automaton, group cellular automaton.
*This Reserch was supported by Kyungsung University Research Grants in 2005.

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 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 ith cell depends on the present states of its left and right 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 & 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.

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

Table 1. Logic funtions

complement			noncomplement	
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 iff $T^m = I$ where T is the chracteristic 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 (L = 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. *[4] CA rules 60, 102 and 204 form groups for all lengths (l) with group order $O(G) = n = 2^a$; $a = 0, 1, 2, \cdots$; $n \geq l > n/2$.*

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 and hybrid CA's with complemented rules 51, 153, and 195. The corresponding noncomplemented rules are 204, 102 and 60.

LEMMA 2.5. *[3] Complemented CA rules 195, 153 and 51 form groups for all lengths with group order $O(G) = m = 2^a$; ($a = 0, 1, 2, \cdots$).*

Proof. [3]. 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),

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

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

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

In the case of R, being any combination of rules 60, 102 and 204, it can be directly shown that $rank[T + I] < L$, 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

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

This is a contradiction and, hence, it follows that

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

$$\begin{aligned}&\Rightarrow \overline{T}^m[f(x)] = T^m[f(x)] = f(x) \\ &\Rightarrow T^m = I.\end{aligned} \tag{5}$$

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 in Section 2, 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. *[3] 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. [3]. 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 [3]. And the proofs of Lemma 2.5 and Theorem 2.6 in [1] are quite sinilar with the proofs in [3].

3. Pointing out and modification

At first, we will point out logical errors in the proof of Lemma 2.5.

At the beginning of the proof, R is assumed as a combination of the rules 60, 102 and 204. But such a hybrid CA is not a group CA generally. For example, the CA with $\langle 204, 102, 60\rangle$ is not a group CA by Theorem 2.6 of [2] because the determinant of the corresponding characteristic matrix is 0. So the rules of Lemma 2.5 should be restricted to uniform rules.

Equation (3) in the proof is obtained, by assuming $I + T + T^2 + \cdots + T^{m-1} \neq 0$, from the equation

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

If $I + T + T^2 + \cdots + T^{m-1}$ is invertible, the equation (3) holds. But nonzero matrix generally is not invertible. So equation (3) can not be

obtained directly from the assuming. And the rest of the proof is not satisfactory.

Now we will give a new proof the Lemma 2.5.

New proof of Lemma 2.5. Consider a CA with rule R and characteristic matrix T where R is a uniform rule of 60, 102 or 204. Then, by Lemma 4, R is a group rule with group order n for n as some integral power of 2 which means n is the least positive integer so that $T^n = I$. The corresponding complemented CA with characteristic matrix $\overline{T}$ is a group CA by Lemma 2.3. So we have

$$\overline{T}^m = I \tag{7}$$

for some positive integer m by Lemma 1 and may assume that m is the least positive integer with such property. And we have, by Lemma 2.2,

$$\overline{T}^m[f(x)] = [I + T + T^2 + \cdots + T^{m-1}][F(x)] + [T^m][f(x)] \tag{8}$$

for any state $f(x)$. From (7) and (8), we have

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

By transposition of the term $[T^m][f(x)]$, we have

$$[T^m + I][f(x)] = [I + T + T^2 + \cdots + T^{m-1}][F(x)]. \tag{9}$$

The right side of (9) is independent of the state $f(x)$. Thus, for any state $f(x)$ and $g(x)$, we have $[T^m + I][f(x)] = [T^m + I][g(x)]$ and so $[T^m + I][f(x) - g(x)] = 0$. It means $[T^m + I][h(x)] = 0$ for all state $h(x)$. Therefore we have $[T^m + I] = 0$ which means that $T^m = I$ because modulo 2 summation is involved. This says that n divides m because n is the group order of the CA with characteristic matrix T.

Now let $k = 2n$. Then, from (8), we have

$$\begin{aligned} \overline{T}^k[f(x)] &= [I + T + T^2 + \cdots + T^{2n-1}][f(x)] + [T^{2n}][f(x)] \\ &= [I + T + T^2 + \cdots + T^{2n-1}][f(x)] + [f(x)]. \end{aligned} \tag{10}$$

And we have

$$\begin{aligned}
&I + T + T^2 + \cdots + T^{2n-1} \\
&= (I + T + T^2 + \cdots + T^{n-1}) + (T^n + T^{n+1} + T^{n+2} + \cdots + T^{2n-1}) \\
&= (I + T + T^2 + \cdots + T^{n-1}) + (I + T + T^2 + \cdots + T^{n-1})T^n \\
&= (I + T + T^2 + \cdots + T^{n-1}) + (I + T + T^2 + \cdots + T^{n-1}) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{(because } T^n = I\text{)} \\
&= 0 \text{ (because modulo 2 summation involved).}
\end{aligned}$$

Thus we have $\overline{T}^k[f(x)] = [f(x)]$ for all $f(x)$ from (10). This means that m divides $k(= 2n)$ because m is the group order of the complemented CA with characteristic matrix $\overline{T}$.

Hence we have shown that $m = n$ or $m = 2n$ which means that m is a power of 2.

Finally, we will point out some errors of Theorem 2.6. The proof of Theorem 2.6 is started with the result of Lemma 2.5. But the proof of Lemma 2.5 is not valid in case of hybrid CA at all as was pointed out above. So the proof of Theorem 2.6 is not valid in case of hybrid CA. Furthermore, the proof of Theorem 2.6 depend on the equation (4). But we have pointed out above there is no logical basis for the equation. Thus the proof of Theorem 2.6 should be reconstructed.

References

[1] P. P. Chaudhuri, D.R. Chowdhury, S. Nandi and S. Chattopadhyay, Additive 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, Efficient characterization of cellular automata, Proc. IEE (Part E), 15 (1990), no. 1, 81–87.

[3] 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.

[4] 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