JOURNAL OF THE CHUNGCHEONG MATHEMATICAL SOCIETY Volume 27, No. 4, November 2014 http://dx.doi.org/10.14403/jcms.2014.27.4.543

PERIODICITIES OF SOME HYBRID CELLULAR AUTOMATA WITH RULES 102 AND 60

JAE-GYEOM KIM*

ABSTRACT. We investigate periodicities of some hybrid cellular automata configured with rule 102 and 60 and null boundary condition.

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 researchers have studied on cellular automata configured with rules 51, 60, 102, 153, 195 or 204 [1-7].

In this note, we will investigate periodicities of some hybrid cellular automata configured with rule 102 and 60 and null boundary condition.

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 kneighbors for a k-neighborhood CA. For a 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 a CA, the modulo-2 logic is always applied.

Received May 12, 2014; Accepted October 20, 2014.

²⁰¹⁰ Mathematics Subject Classification: Primary 68Q80.

Key words and phrases: cellular automaton, null boundary condition.

This Research was supported by Kyungsung University Research Grants in 2014.

For a 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 states, each mapping representing a CA rule. The CA, characterized by a rule known as rule 102, specifies an evolution from the neighborhood configurations to the next states as:

The corresponding combinational logic of rule 102 is

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

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

And the CA, characterized by a rule known as rule 60, specifies an evolution from the neighborhood configurations to the next states as:

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.

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 noncomplemented 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.

544

THEOREM 2.2. [4] Let H be a hybrid CA configured with rules 60, 102 or 204. If rule 60 just follows rule 102 in the rule vector of H, then H is not a group CA. Otherwise, H is a group CA and can be regarded as a combination of independent uniform group CA's.

3. Periodicities of cellular automata

In this section, we deal with periodicities of some hybrid CA's with rules 102 and 60. We begin with observation of the square matrix S with sufficiently large size given by

where all the values of the blank entries are zero. From now on, all the values of the blank entries in matrix representation will always be zero unless otherwise specified.

We can easily get S^2 as follows;

$$(S^{2})_{i,j} = \begin{cases} 1, & \text{if } i = j \text{ and } j \ge 3, \\ 1, & \text{if } i = j + 2, \\ 0, & \text{otherwise,} \end{cases}$$

or

So the CA with characteristic matrix S is not a group CA by Lemma 2.1 and Theorem 2.2. For a matrix A and for a non-negative integer r, the entries $A_{i,(i+r)}$, $i = 1, 2, 3, \cdots$, will be called by the (r)th diagonal of A. And the entries which are not blank in the matrix representation of S^2 above will be called by the first 4 diagonals of S^2 .

We can also get S^6 and S^{10} as follows;

$$(S^6)_{i,j} = \begin{cases} 1, & \text{if } i = j \text{ and } j \ge 3, \\ 1, & \text{if } i = j + 2, \\ 1, & \text{if } i = j + 4 \text{ and } j \ge 3, \\ 1, & \text{if } i = j + 6, \\ 0, & \text{otherwise}, \end{cases}$$

or

546

and

$$(S^{10})_{i,j} = \begin{cases} 1, & \text{if } i = j \text{ and } j \ge 3, \\ 1, & \text{if } i = j + 2, \\ 1, & \text{if } i = j + 8 \text{ and } j \ge 3, \\ 1, & \text{if } i = j + 10, \\ 0, & \text{otherwise}, \end{cases}$$

or

We can find that $S^6 = S^4 S^2$ and $S^{10} = S^8 S^2$ are the results that copies of the first 4 diagonals of S^2 are shifted down 4 and 8 units, respectively, and then added to S^2 , respectively.

Furthermore, if S_t denotes the matrix that the first 4 diagonals of S^2 are shifted down t units for some positive integer t, or

$$(S_t)_{i,j} = \begin{cases} 1, & \text{if } i = j + t \text{ and } j \ge 3, \\ 1, & \text{if } i = j + 2 + t, \\ 0, & \text{otherwise,} \end{cases}$$

then we can similarly have that S^4S_t and S^8S_t are the results that all the entries of $S^6 = S^4S^2 = S^4S_0$ and $S^{10} = S^8S^2 = S^8S_0$ are shifted down t units, respectively, or

.

$$(S^4 S_t)_{i,j} = \begin{cases} 1, & \text{if } i = j + t \text{ and } j \ge 3, \\ 1, & \text{if } i = j + 2 + t, \\ 1, & \text{if } i = j + 4 + t \text{ and } j \ge 3, \\ 1, & \text{if } i = j + 6 + t, \\ 0, & \text{otherwise}, \end{cases}$$

and

$$(S^8 S_t)_{i,j} = \begin{cases} 1, & \text{if } i = j + t \text{ and } j \ge 3, \\ 1, & \text{if } i = j + 2 + t, \\ 1, & \text{if } i = j + 8 + t \text{ and } j \ge 3, \\ 1, & \text{if } i = j + 10 + t, \\ 0, & \text{otherwise.} \end{cases}$$

Now we are ready to get the following lemma.

LEMMA 3.1. Let S and S_t be the matrices as in the discussion above where t is a non-negative integer. Then, for each integer $a \ge 2$, $S^{2^a}S_t$ is the matrix given by

$$(S^{2^{a}}S_{t})_{i,j} = \begin{cases} 1, & \text{if } i = j + t \text{ and } j \ge 3, \\ 1, & \text{if } i = j + 2 + t, \\ 1, & \text{if } i = j + t + 2^{a} \text{ and } j \ge 3, \\ 1, & \text{if } i = j + 2 + t + 2^{a}, \\ 0, & \text{otherwise}, \end{cases}$$

in other words, $S^{2^a}S_t$ is the result that a copy of the sifted 4 diagonals of S_t is shifted down 2^a units and then added to S_t .

Proof. We will use an induction on a. For a = 2 and a = 3, we are done in the discussion above. Assume that the lemma is true for $a = 2, 3, \dots, n-1$ where n > 3. Then $(S^{2^2}(S^{2^3} \dots (S^{2^{a-2}}(S^{2^{a-1}}S_0)) \dots))$ is the matrix consisted of a - 2 consecutive downward iterations of the first 4 diagonals of $S_0 = S^2$. In other words, the matrix is the sum of $S_0, S_4, S_8, \dots, S_{(2^{(a-1)}-1)4}$. So if we denote this matrix by S', then we can have S', SS', S^2S', S^3S' and S^4S' one by one as follows;

$$(S')_{i,j} = \begin{cases} 1, & \text{if } i-j \equiv 0 \pmod{4}, \ 0 \leq i-j \leq 2^a - 4 \text{ and } j \geq 3, \\ 1, & \text{if } i-j \equiv 2 \pmod{4} \text{ and } 2 \leq i-j \leq 2^a - 2, \\ 0, & \text{otherwise}, \end{cases}$$
$$(SS')_{i,j} = \begin{cases} 1, & \text{if } i-j \equiv 0 \pmod{4}, \ 0 \leq i-j \leq 2^a - 4 \text{ and } j \geq 3 \\ 1, & \text{if } i-j \equiv 1 \pmod{4}, \ 1 \leq i-j \leq 2^a - 3 \text{ and } j \geq 3 \\ 1, & \text{if } i-j \equiv 2 \pmod{4} \text{ and } 2 \leq i-j \leq 2^a - 2, \\ 1, & \text{if } i-j \equiv 3 \pmod{4} \text{ and } 3 \leq i-j \leq 2^a - 1, \\ 0, & \text{otherwise}, \end{cases}$$

548

Periodicities of some hybrid cellular automata with rules 102 and 60 549

$$(S^{2}S')_{i,j} = \begin{cases} 1, & \text{if } i = j \text{ and } j \ge 3, \\ 1, & \text{if } i - j \text{ is even, } j \le 2 \text{ and } 2 \le i - j \le 2^{a} - 2, \\ 1, & \text{if } i = j \text{ and } i - j = 2^{a}, \\ 0, & \text{otherwise,} \end{cases}$$
$$(S^{3}S')_{i,j} = \begin{cases} 1, & \text{if } i = j \text{ and } j \ge 3, \\ 1, & \text{if } i = j + 1 \text{ and } j \ge 3, \\ 1, & \text{if } 2 \le i - j \le 2^{a} - 1 \text{ and } 1 \le j \le 2, \\ 1, & \text{if } 2^{a} \le i - j \le 2^{a} + 1, \\ 0, & \text{otherwise,} \end{cases}$$
$$(S^{4}S')_{i,j} = \begin{cases} 1, & \text{if } i = j \text{ and } j \ge 3, \\ 1, & \text{if } i = j + 2, \\ 1, & \text{if } i = j + 2, \\ 1, & \text{if } i = j + 2, \\ 1, & \text{if } i = j + 2 + 2^{a}, \\ 0, & \text{otherwise.} \end{cases}$$

And we have

$$S^{2^{a}}S_{0} = S^{(2^{2}+2^{2}+2^{3}+\ldots+2^{a-2}+2^{a-1})}S_{0}$$

= $S^{4}S^{(2^{2}+2^{3}+\ldots+2^{a-2}+2^{a-1})}S_{0}$
= $S^{4}(S^{2^{2}}(S^{2^{3}}\cdots(S^{2^{a-2}}(S^{2^{a-1}}S_{0}))\cdots))$
= $S^{4}S'$

So we have the conclusion in the case of t = 0. And the conclusions in other cases can be easily induced just by applying shift down to the conclusion in the case of t = 0.

By Lemma 3.1 we can easily have a lemma.

LEMMA 3.2. Let S be the matrix S in Lemma 3.1 and m the matrix size of S. If $m \ge 2$ and $m \le 2^a + 2$ for some non-negative integer a, then $S^{2+2^a} = S^2$.

Let S be the matrix S in Lemma 3.1 with size $m \ge 2$ and T another matrix S in Lemma 3.1 with size $n \ge 2$. And let S^* be the matrix of 180degree rotation of S. Then $(S^*)_{i,j} = S_{(m-i+1),(m-j+1)}$ for all i, j. And $(S^*)^k$ is the matrix of 180-degree rotation of S^k for all positive integers k. So the properties about periodicities of S^* and S are coincide. Now

let U be the square matrix of size m + n - 2 given by

$$U = \left(\begin{array}{cc} S^* & 0\\ 0 & T \end{array}\right)$$

in which $(S^*)_{(m-1),(m-1)}$, $(S^*)_{(m-1),m}$, $(S^*)_{m,(m-1)}$ and $(S^*)_{m,m}$ are overlapped with $T_{1,1}, T_{1,2}, T_{2,1}$ and $T_{2,2}$, respectively, or

Then, for all positive integers k, we can easily check that

$$U^k = \left(\begin{array}{cc} \left(S^*\right)^k & 0\\ 0 & T^k\end{array}\right)$$

with 4 entries overlap between $(S^*)^k$ and T^k as between S^* and T above. In fact, for all integers $k \ge 2$, all the overlapping entries between $(S^*)^k$ and T^k are zero and so there is no actual interaction between $(S^*)^k$ and T^k .

Now we are ready to have a result on periodicities of some hybrid CA's with rules 102 and 60.

THEOREM 3.3. Let H be a hybrid CA of length ℓ configured with rules 102 and 60. Assume that the rule applied to the first m cells of H is 102 and the rule applied to the second n cells of H is 60 with $m \ge 1, n \ge 1$ and $\ell = m + n$. If a is a non-negative integer so that $max\{m,n\} \le 2^a + 1$, then $U^{2+2^a} = U^2$ where U is the characteristic matrix of H.

Proof. If $\ell \leq 3$, it is obvious. So let $\ell > 3$. And let U be the characteristic matrix of H. Then U is of the form

$$U = \left(\begin{array}{cc} S^* & 0\\ 0 & T \end{array}\right)$$

550

just as in the discussion above where S^* and T are the matrices as in the discussion above of size m + 1 and n + 1, respectively. So we have

$$U^k = \left(\begin{array}{cc} (S^*)^k & 0\\ 0 & T^k \end{array}\right)$$

for all positive integers k. Hence we have the conclusion by Lemma 3.2 because the properties about periodicities of S^* and S are coincide and because $(S^*)^k$ and T^k are completely independent of each other for all integers $k \ge 2$.

References

- P. P. Chaudhuri, D. R. Chowdhury, S. Nandi, and S. Chattopadhyay, Additive celular automata theory and applications, Vol. 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] J. G. Kim, On hybrid group cellular automata, East Asian Math. J. 27 (2011), no. 1, 67-73.
- [5] S. Nandi, Additive cellular automata: Theory and application for testable circuit design and data encryption, PhD thesis, I.I.T., Kharagpur, India, 1994.
- [6] 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.
- [7] 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