East Asian Math. J.
Vol. 31 (2015), No. 1, pp. 019–025
http://dx.doi.org/10.7858/eamj.2015.002

# PERIODICITIES OF SOME ADDITIVE CELLULAR AUTOMATA

Jae-Gyeom Kim

Abstract. We investigate periodicities of some additive cellular automata with 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 [1-8].

In this note, we will investigate periodicities of some additive cellular automata with 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 state of its $k$ neighbors for a $k$-neighborhood CA. For a 2-state 3-neighborhood CA, the evolution of the $i^{\text{th}}$ cell can be represented as a function of the present states of $(i-1)^{\text{th}}$, $i^{\text{th}}$, and $(i+1)^{\text{th}}$ 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.

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 state, each mapping representing a CA rule. The CA, characterized by a rule known as rule 60, specifies an evolution from neighborhood

Received May 28, 2014; Accepted October 22, 2014.
2010 *Mathematics Subject Classification.* 68Q80.
*Key words and phrases.* additive cellular automaton, null boundary condition.
This Research was supported by Kyungsung University Research Grants in 2014.


(pISSN 1226-6973, eISSN 2287-2833)

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 given by

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

that is, the next state of $i^{\text{th}}$ 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 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 noncomplemented 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. And the number of cells of a CA is called the *length* of a 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.*

**Lemma 2.2.** [3] *If* $(\widetilde{T})^m$ *denote the application of the complemented rule* $\widetilde{T}$ *for* $m$ *successive cycles, then*

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

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

**Lemma 2.3.** [1] *State transitions in all additive CA's (noncomplemented, complemented, or hybrid) can be expressed by the relation noted in Lemma 2.2, where* $[F(x)]$ *contains nonzero entries for the cell positions with complemented rule. In the case of a CA where only noncomplemented rules are applied throughout its length,* $[F(x)]$ *turns out to be a null vector.*

**Lemma 2.4.** [8] *CA rules* 60, 102 *and* 204 *form groups for all lengths* $\ell$ *with group order* $n = 2^a$ *where* $a$ *is a nonnegative integer. And if the CA rule is* 60 *or* 102 *then* $\frac{n}{2} < \ell \leq n$.

**Theorem 2.5.** [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.*

**Theorem 2.6.** [5] *Let* $H$ *be a hybrid CA of length* $\ell$ *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* $m \geq 1$, $n \geq 1$ *and* $\ell = m + n$. *If* $a$ *is a non-negative integer so that* $max\{m, n\} \leq 2^a + 1$, *then* $T^{2+2^a} = T^2$ *where* $T$ *is the characteristic matrix of* $H$.

## 3. Periodicities of additive cellular automata

Let $R = \langle \cdots, R_i, \cdots \rangle$ be the rule vector of a noncomplemented CA of length $\ell$. And let $[F(x)]$ be a vector of length $\ell$ with entries 0 or 1. Then $R_{[F(x)]}$ will denote the rule vector of the hybrid CA of length $\ell$ where $i^{\text{th}}$ rule of $R_{[F(x)]}$ is the complemented rule $\overline{R}_i$ of $i^{\text{th}}$ rule $R_i$ of $R$ if $i^{\text{th}}$ entry of $[F(x)]$ is 1, otherwise $i^{\text{th}}$ rule of $R_{[F(x)]}$ is just $i^{\text{th}}$ rule $R_i$ of $R$.

**Lemma 3.1.** *Let* $H$ *be an additive CA and* $T$ *the characteristic matrix of the noncomplemented CA corresponding to the complemented CA* $H$. *And let* $\widetilde{T}$ *denote the application of* $H$. *If* $T^{s+t} = T^s$ *for some positive integers* $s$ *and* $t$, *then* $(\widetilde{T})^{s+2t} = (\widetilde{T})^s$.

*Proof.* Let $[F(x)]$ be the vector with entries 0 or 1 so that $R_{[F(x)]}$ is the rule vector of $H$ where $R$ is the rule vector of the noncomplemented CA corresponding to $H$. Let $T^{s+t} = T^s$ for some positive integers $s$ and $t$, then we have

$$[(\widetilde{T})^{s+2t}][f(x)]$$

$$= [I + T + T^2 + \cdots + T^{s+2t-1})][F(x)] + [T^{s+2t}][f(x)]$$
(by Lemma 2.2 and Lemma 2.3)
$$= [(I + T + \cdots + T^{s-1}) + (T^s + \cdots + T^{s+t-1}) + (T^{s+t} + \cdots + T^{s+2t-1})][F(x)] + [T^{s+2t}][f(x)]$$
$$= [(I + T + \cdots + T^{s-1}) + (T^s + \cdots + T^{s+t-1}) + (T^s + \cdots + T^{s+t-1})][F(x)] + [T^s][f(x)]$$
(because $T^{s+t} = T^s$)
$$= [I + T + \cdots + T^{s-1}][F(x)] + [T^s][f(x)]$$
(because modulo-2 summation is involved)
$$= [(\widetilde{T})^s][f(x)] \qquad \text{(by Lemma 2.2 and Lemma 2.3)}$$

for all $f(x)$, this means that $(\widetilde{T})^{s+2t} = (\widetilde{T})^s$. This completes the proof. □

Lemma 3.1 suggests not the period of $\widetilde{T}$ but an upper bound of the period of $\widetilde{T}$. Let $H_1$ be the additive CA of length 5 with rule vector $\langle 153, 153, 153, 153, 60\rangle$ and $H_2$ the additive CA of length 6 with rule vector $\langle 153, 153, 153, 153, 153, 60\rangle$. Then the periodicities of $T_1$ and $T_2$ are the same, but the periodicities of $\widetilde{T_1}$ and $\widetilde{T_2}$ are different, where $T_1$ and $T_2$ are the characteristic matrices of the noncomplemented CA corresponding to the complemented CA $H_1$ and $H_2$, respectively, and where $\widetilde{T_1}$ and $\widetilde{T_2}$ denote the applications of the complemented CA $H_1$ and $H_2$, respectively. In fact, we can find that $(T_1)^{2+4} = (T_1)^2$ and $(T_2)^{2+4} = (T_2)^2$, but we have $(\widetilde{T_1})^{2+4} = (\widetilde{T_1})^2$, $(\widetilde{T_2})^{2+4} \neq (\widetilde{T_2})^2$ and $(\widetilde{T_2})^{2+8} = (\widetilde{T_2})^2$.

**Corollary 3.2.** *Let $H$ be an additive hybrid CA of length $\ell$ configured with rules 60, 102, 153 or 195. Assume that the rule applied to the first $m$ cells and the rule applied to the second $n$ cells of the noncomplemented CA corresponding to $H$ are 102 and 60, respectively, with $m \geq 1$, $n \geq 1$ and $\ell = m + n$. If $a$ is a non-negative integer so that $max\{m, n\} \leq 2^a + 1$, then $(\widetilde{T})^{2+2^{a+1}} = (\widetilde{T})^2$ where $\widetilde{T}$ denotes the application of $H$.*

*Proof.* Let $a$ be a non-negative integer such that $max\{m, n\} \leq 2^a + 1$. Then $T^{2+2^a} = T^2$ by Theorem 2.6 where $T$ is the characteristic matrix of the noncomplemented CA corresponding to the complemented CA $H$. Hence we have the conclusion by Lemma 3.1. □

Let $H$ be an additive hybrid $CA$ of length $\ell$ configured with rules 51, 60, 102, 153, 195 or 204, $K$ the noncomplemented CA corresponding to the complemented CA $H$ and $R$ the rule vector of $K$. Then $K$ is a hybrid CA with rules 60, 102 or 204 and there are combined parts of different rules in the rule vector $R$. For each 102-60 combined part in $R$, i.e., for each part where rule 60 just follows rule 102, we can see there are interactions between the rules 102 and 60 in CA application. For any other combined part of different rules in $R$ other than 102-60 combined part, there is no interaction between the different rules [4]. Now let a maximal 102-60 combined part in $R$ denote $\langle 102, \cdots, 102, 60, \cdots, 60\rangle$ which could not be extended more in $R$ such a manner that rule 102's in a row then rule 60's in a row. And let a maximal uniform rule part in $R$ denote $\langle 60, \cdots, 60\rangle$, $\langle 102, \cdots, 102\rangle$ or $\langle 204, \cdots, 204\rangle$ which could not be extended more in $R$ as a uniform rule vector and could not be extended to a maximal 102-60 combined part in $R$. Then $R$ is a combination of maximal 102-60 combined parts and maximal uniform rule parts of which all the parts are completely independent of each other in CA application [4]. For the characteristic matrix $T_v$ of each maximal 120-60 combined part $R_v$ in $R$ with $m_v$ 102's and $n_v$ 60's, we have $(T_v)^{2+2^{a_v}} = (T_v)^2$ by Theorem 2.6 where $a_v$ is the least non-negative integer such that $max\{m_v, n_v\} \le 2^{a_v} + 1$. And for the characteristic matrix $T_u$ corresponding to each maximal uniform rule part $R_u$ in $R$, we have $(T_u)^{2^{a_u}} = I$ for some non-negative integer $a_u$ by Lemma 2.4, thus $(T_u)^{2+2^{a_u}} = (T_u)^2$. Now let $T$ be the characteristic matrix of $K$ and $a$ the least common multiple of $a_v$'s and $a_u$'s. Then we have $T^{2+2^a} = T^2$ because all the parts of maximal 102-60 combined parts and maximal uniform rule parts in $R$ are completely independent of each other in CA application. Hence, by Lemma 3.1, we have the following theorem.

**Theorem 3.3.** *Let $H$ be an additive hybrid CA configured with rules 51, 60, 102, 153, 195 or 204. Then $(\widetilde{T})^{2+2^{a+1}} = (\widetilde{T})^2$ where $\widetilde{T}$ denotes the application of $H$ and where $a$ is the least common multiple of $a_v$'s and $a_u$'s as was mentioned in the discussion above.*

## 4. Group cellular automata

In [4], group properties of additive hybrid CA's were discussed and Theorem 4.1 below was given. But, there was some omissions in the assumption of the theorem. In fact, the assumption that rule 60 does not just follow rule 153 and rule 195 does not just follow rule 102 in the rule vector of $H$ should be added. Nevertheless, the discussion and the proof for the theorem in [4] is still valid. For the sake of completeness, we will rediscuss about the assumption and the proof of the theorem.

**Theorem 4.1.** [4] *Let $H$ be an additive hybrid CA of length $\ell$ configured with rules 51, 60, 102, 153, 195 or 204. Assume that rule 60 does not just follow rule 102 and that rule 195 does not just follow rule 153 in the rule vector of $H$. Then $H$ is a group CA.*

At first, we give Theorem 4.2 which is a modified version of Theorem 4.1 as mentioned above. And we give the proof of Theorem 4.2 which is the same as the proof of Theorem 4.1 given in [4].

**Theorem 4.2.** *Let $H$ be an additive hybrid CA of length $\ell$ configured with rules 51, 60, 102, 153, 195 or 204. Assume that rule 60 does not just follow* *rule* 102 *in the rule vector of the noncomplemented CA corresponding to $H$. Then $H$ is a group $CA$.*

*Proof.* Let $R = \langle \cdots, R_i, \cdots \rangle$ be the rule vector of a noncomplemented CA of length $\ell$ and $[F(x)]$ the vector of length $\ell$ with entries 0 or 1 so that $R_{[F(x)]}$ is the rule vector of $H$ as was in section 3. And let $\widetilde{T}$ denote the application of the rule vector $R_{[F(x)]}$ where $T$ is the characteristic matrix corresponding to the rule vector $R$. Then we have

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

for all $f(x)$ by Lemma 2.2 and Lemma 2.3. And rule 60 does not just follow rule 102 in the rule vector $R$ by the assumption. So the noncomplemented CA with rule vector $R$ is a group CA by Theorem 2.5, and thus there exists a positive integer $t$ such that $T^t = I$ by Lemma 2.1. Therefore we have

$$\begin{aligned} & [(\widetilde{T})^{2t}][f(x)] \\ &= [I + T + T^2 + \cdots + T^{2t-1}][F(x)] + [T^{2t}][f(x)] \\ &= [(I + T + \cdots + T^{t-1}) + (T^t + \cdots + T^{2t-1})][F(x)] + [I][f(x)] \\ &= [(I + T + \cdots + T^{t-1}) + (I + T + \cdots + T^{t-1})][F(x)] + [f(x)] \\ &= [0][F(x)] + [f(x)] \quad \text{(since modulo-2 summation is involved)} \\ &= [f(x)] \end{aligned}$$

for all $f(x)$. This means that $(\widetilde{T})^{2t} = I$. Hence the additive hybrid CA $H$ with rule vector $R_{[F(x)]}$ is a group CA. This completes the proof. □

Finally, we deal with the assumption of Theorem 4.2. In fact, we will show that an additive hybrid $CA$ unsatisfying the assumption is not a group CA.

**Proposition 4.3.** *Let $H$ be an additive hybrid $CA$ of length $\ell$ configured with rules* 51, 60, 102, 153, 195 *or* 204. *Assume that rule* 60 *once follows rule* 102 *in the rule vector of the noncomplemented CA corresponding to $H$. Then $H$ is not a group $CA$.*

*Proof.* Let $R = \langle \cdots, R_i, R_{i+1}, \cdots \rangle$ be the rule vector of a noncomplemented CA of length $\ell$ with $R_i = 102$ and $R_{i+1} = 60$ and $[F(x)]$ the vector of length $\ell$ with entries 0 or 1 so that $R_{[F(x)]}$ is the rule vector of $H$ as was in section 3. And let $T$ be the characteristic matrix corresponding to the rule vector $R$ and $\widetilde{T}$ denote the application of $H$. Then we have

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

for all $f(x)$ and for all positive integers $s$ by Lemma 2.2 and Lemma 2.3. We can easily check that all the entries of $i^{\text{th}}$ and $(i+1)^{\text{th}}$ rows of $T^s$ are 0 for all integers $s \geq 2$. Thus the $i^{\text{th}}$ and $(i+1)^{\text{th}}$ values of $[(\widetilde{T})^s][f(x)]$ are independent of $f(x)$, and so $(\widetilde{T})^s$ could not be the identity operation for all integers $s \geq 2$. And both of the $i^{\text{th}}$ and $(i+1)^{\text{th}}$ values of $[T][f(x)]$ are the sum of the $i^{\text{th}}$

and $(i+1)^{\text{th}}$ values of $f(x)$, thus the $i^{\text{th}}$ and $(i+1)^{\text{th}}$ values of $[\widetilde{T}][f(x)]$ are dependent of the $(i+1)^{\text{th}}$ and $i^{\text{th}}$ values of $f(x)$, respectively, because $[\widetilde{T}][f(x)] = [F(x)] + [T][f(x)]$. And so $\widetilde{T}$ could not be the identity operation. In conclusion, $(\widetilde{T})^s$ could not be the identity operation for all positive integers $s$. Hence $H$ is not a group CA. □

## 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, *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] J. G. Kim, *Periodicities of some hybrid cellular automata with rules 102 and 60*, J. Chungcheong Math. Soc., 27 (2014), no. 4, 543–551.

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

[7] 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.

[8] 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.



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