Korean J. Math. **18** (2010), No. 4, pp. 357–368

# ON GROUP ORDERS OF SOME CELLULAR AUTOMATA

Jae-Gyeom Kim

Abstract. In this note, we will characterize group orders of hybrid CA configured with rules 60 and 195 and that configured with rules 102 and 153.

## 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 and group orders of group cellular automata have been studied [1-9]. In particular, group orders of uniform CA configured with rules 60, 102, 153 or 195 are characterized in [6, 9]. In this note, we will characterize group orders of hybrid CA configured with rules 60 and 195 and that configured with rules 102 and 153.

## 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 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: $x_i(t+1) =$

Received September 16, 2010. Revised November 8, 2010. Accepted November 11, 2010.
2000 Mathematics Subject Classification: 68Q80.
Key words and phrases: cellular automaton, group order.
This Research was supported by Kyungsung University Research Grants in 2010.

$f\{x_{i-1}(t), x_i(t), x_{i+1}(t)\}$, 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 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 $(i)$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 specified.

The logic functions for two complemented rules 195 and 163 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 | $x_i(t) \oplus x_{i+1}(t)$ |

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 rule which is applied to a group CA is referred to as a group rule. 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.*

Note that the least positive integer of such $m$'s is the group order of the group CA in Lemma 2.1.

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

LEMMA 2.3. ([3]) *If* $\overline{T}^m$ *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* $\ell$*-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 2.4. ([1]) *State transitions in all additive CA (noncomplemented, complemented, or hybrid) can be expressed by the relation noted in Lemma 2.3, 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 2.5. ([2]) *Let* $R$ *be a group rule. Then any additive CA with a rule vector which is a combination of* $R$ *and* $\overline{R}$ *is a group CA, where* $\overline{R}$ *denotes the complemented rule of* $R$.

THEOREM 2.6. ([6]) *A uniform CA of length* $\ell$ *configured with rule* 153 *or* 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* $2^a$.

## 3. Group orders of cellular automata

We will investigate group orders of hybrid CA configured with rules 60 and 195 at first. In the investigation, the matrices $[T^m]$ and $[I+T+\cdots+T^{m-1}]$ play important roles by virtue of Lemma 2.3 and 2.4, where $T$ is the characteristic matrix with respect to the rule 60.

So we begin with characterizations of such matrices. Let $T$ be the characteristic matrix of a CA configured with rule 60. Then, by mathematical induction, we can easily get $T^{2^a}$ where $a = 1, 2, \cdots$ as follows;

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

or

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

which is an explicit formular for Lemma 2.1 and 2.2 where rule 60 is applied. Thus we have the following lemma.

LEMMA 3.1. *Let $T$ be the characteristic matrix of a CA configured with rule* 60. *Then*

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

*where $a = 1, 2, \cdots$.*

Now we have a lemma of which proof is completely the same as the proof Lemma 3.3 in [6].

LEMMA 3.2. *Let $T$ be a matrix with modulo-2 logic. Then*

$$(I+T)^{2^a-1} = I + T + \cdots + T^{2^a-1}$$

*where* $a = 1, 2, \cdots$.

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 a CA configured with 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 the following lemma.

LEMMA 3.3. *Let $T$ be the characteristic matrix of a CA configured with rule* 60. *Then*

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

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

$$(I+T)^{\ell} = 0 \quad \textit{and} \quad (I+T)^{\ell-1} = \begin{pmatrix} 0 & & & \\ \vdots & & \mathit{0} & \\ 0 & & & \\ 1 & 0 & \cdots & 0 \end{pmatrix}$$

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

We are ready to deal with group orders of hybrid CA configured with rules 60 and 195. Note that such CA are group CA by Lemma 2.5.

THEOREM 3.4. *Let $H$ be a hybrid CA of length $2^a$ configured with rules* 60 *and* 195 *where* $a = 1, 2, \cdots$. *Suppose that the rule applied to the first cell of $H$ is* 195. *Then its transition diagram consists of equal cycles of length* $2^{a+1}$.

*Proof.* Let $T$ be the characteristic matrix of a CA of length $2^a$ configured with rule 60. And let $[F(x)]$ be the $2^a$-dimensional vector corresponding to $H$ as in Lemma 2.3. Then the first entry of $[F(x)]$ is 1 by Lemma 2.3. And let $(\widetilde{T})^m$ denote the application of the rule vector with respect to $H$ for $m$ successive cycles. Then we have

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

for all $f(x)$ by Lemma 2.3. And so we have

$$\begin{aligned}
&[(\widetilde{T})^{2^a}][f(x)] \\
&= [I + T + \cdots + T^{2^a-1}][F(x)] + [T^{2^a}][f(x)] \\
&= [(I+T)^{2^a-1}][F(x)] + [T^{2^a}][f(x)] \quad \text{by Lemma 3.2} \\
&= \begin{pmatrix} 0 & & & \\ \vdots & & 0 & \\ 0 & & & \\ 1 & 0 & \cdots & 0 \end{pmatrix} [F(x)] + [I][f(x)] \quad \text{by Lemma 3.1 and 3.3} \\
&= \begin{pmatrix} 0 & & & \\ \vdots & & 0 & \\ 0 & & & \\ 1 & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} 1 \\ c_2 \\ \vdots \\ c_{2^a} \end{pmatrix} + [f(x)] \quad \text{for some } c_i \\
&= \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} + [f(x)] \\
&\neq [f(x)]
\end{aligned}$$

for all $f(x)$. But we have

$$\begin{aligned}
&[(\widetilde{T})^{2^{a+1}}][f(x)] \\
&= [I + T + \cdots + T^{2^{a+1}-1}][F(x)] + [T^{2^{a+1}}][f(x)] \\
&= [(I+T)^{2^{a+1}-1}][F(x)] + [T^{2^{a+1}}][f(x)] \quad \text{by Lemma 3.2} \\
&= [0][F(x)] + [I][f(x)] \quad \text{by Lemma 3.1 and 3.3} \\
&= [f(x)]
\end{aligned}$$

for all $f(x)$. Therefore the cycle length of $f(x)$ is $2^{a+1}$ for all $f(x)$. Hence we have the conclusion. $\square$

To proceed more, we need another technical lemma.

LEMMA 3.5. *Let $T$ be the characteristic matrix of a CA of length $2^a$ configured with rule 60 where $a = 1, 2, \cdots$. Then we have*

$$[T^{2^{a-1}}][\mathbf{e}_i] = \begin{cases} [\mathbf{e}_i] + [\mathbf{e}_{i+2^{a-1}}], & \text{if } 1 \le i \le 2^{a-1}, \\ [\mathbf{e}_i], & \text{otherwise} \end{cases}$$

*where $\mathbf{e}_i$'s are the standard unit vectors of dimension $2^a$.*

*Proof.* It can be easily shown by Lemma 3.1. □

THEOREM 3.6. *Let $H$ be a hybrid CA of length $2^a$ configured with rules 60 and 195 where $a = 1, 2, \cdots$. Suppose that the rule applied to the first cell of $H$ is 60. Then the group order of $H$ is $2^a$.*

*Proof.* Let $T$, $[F(x)]$ and $(\widetilde{T})^m$ be as in the proof of Theorem 3.5. Then the first entry of $[F(x)]$ is 0 by Lemma 2.3 and we have

$$\begin{aligned}
&[(\widetilde{T})^{2^a}][f(x)] \\
&= [I + T + \cdots + T^{2^a-1}][F(x)] + [T^{2^a}][f(x)] \quad \text{by Lemma 2.3} \\
&= [(I+T)^{2^a-1}][F(x)] + [T^{2^a}][f(x)] \quad \text{by Lemma 3.2} \\
&= \begin{pmatrix} 0 & & & \\ \vdots & & \text{\Large 0} & \\ 0 & & & \\ 1 & 0 & \cdots & 0 \end{pmatrix} [F(x)] + [I][f(x)] \quad \text{by Lemma 3.1 and 3.3} \\
&= \begin{pmatrix} 0 & & & \\ \vdots & & \text{\Large 0} & \\ 0 & & & \\ 1 & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} 1 \\ c_2 \\ \vdots \\ c_{2^a} \end{pmatrix} + [f(x)] \quad \text{for some } c_i \\
&= [0] + [f(x)] \\
&= [f(x)]
\end{aligned}$$

for all $f(x)$. Thus the cycle length of $f(x)$ is a divisor of $2^a$ for any $f(x)$. Therefore the group order of $H$ is a divisor of $2^a$. Let $(k)$th entry of $[F(x)]$ be the first non-zero entry. Then we have $2 \le k \le 2^a$ by the assumption. If $2 \le k \le 2^{a-1}+1$, then

$$
\begin{aligned}
&[(\widetilde{T})^{2^{a-1}}][\mathbf{e}_k] \\
&= [I + T + \cdots + T^{2^{a-1}-1}][F(x)] + [T^{2^{a-1}}][\mathbf{e}_k] \quad \text{by Lemma 2.3} \\
&= [(I+T)^{2^{a-1}-1}][F(x)] + [T^{2^{a-1}}][\mathbf{e}_k] \quad \text{by Lemma 3.2} \\
&= [(I+T)^{2^{a-1}-1}] \begin{array}{c} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ c_{k+1} \\ \vdots \end{pmatrix} \end{array} \begin{array}{l} \\ \\ \\ \leftarrow (k)\text{th row} \\ \\ \\ \end{array} + [T^{2^{a-1}}][\mathbf{e}_k] \\
&= \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ c_{k+1} \\ \vdots \end{pmatrix} \begin{array}{l} \\ \\ \\ \leftarrow (k+2^{a-1}-1)\text{th row} \\ \\ \\ \end{array} + [T^{2^{a-1}}][\mathbf{e}_k] \quad \text{by Lemma 3.3} \\
&= \begin{cases} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ c_{k+1} \\ \vdots \end{pmatrix} \begin{array}{l} \\ \\ \\ \leftarrow (k+2^{a-1}-1)\text{th row} \\ \\ \\ \end{array} + [\mathbf{e}_k] + [\mathbf{e}_{k+2^{a-1}}], & \text{if } 2 \le k \le 2^{a-1} \\ \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ c_{k+1} \\ \vdots \end{pmatrix} \begin{array}{l} \\ \\ \\ \leftarrow (k+2^{a-1}-1)\text{th row} \\ \\ \\ \end{array} + [\mathbf{e}_k], & \text{if } k = 2^{a-1}+1 \end{cases} \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{by Lemma 3.5}
\end{aligned}
$$

$$
= \begin{array}{cl} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \\ 1 \\ \vdots \end{pmatrix} & \begin{array}{l} \\ \\ \\ \leftarrow (k)\text{th row} \\ \\ \\ \\ \leftarrow (k+2^{a-1}-1)\text{th row} \\ \\ \end{array} \end{array}
$$

$$
\neq \; [\mathbf{e}_k].
$$

And if $k > 2^{a-1}+1$, then

$$
\begin{aligned}
& [(\widetilde{T})^{2^{a-1}}][\mathbf{e}_1] \\
&= [(I+T)^{2^{a-1}-1}][F(x)] + [T^{2^{a-1}}][\mathbf{e}_1] \quad \text{by Lemma 2.3 and 3.2} \\
&= [(I+T)^{2^{a-1}-1}] \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ c_{k+1} \\ \vdots \end{pmatrix} \begin{array}{l} \\ \\ \\ \leftarrow (k)\text{th row} \\ \\ \\ \end{array} + [\mathbf{e}_1] + [\mathbf{e}_{2^{a-1}+1}] \quad \text{by Lemma 3.5} \\
&= [0] + [\mathbf{e}_1] + [\mathbf{e}_{2^{a-1}+1}] \quad \text{by Lemma 3.3 because } k + (2^{a-1}-1) > 2^a \\
&= [\mathbf{e}_1] + [\mathbf{e}_{2^{a-1}+1}] \\
&\neq [\mathbf{e}_1].
\end{aligned}
$$

Thus there exists a state $f(x)$ of which cycle length is greater than $2^{a-1}$ for any case of $F(x)$ in this theorem. Hence we have the proof. □

Now we have an interesting corollary by Lemma 2.2 and Theorem 2.5, 3.4 and 3.6.

COROLLARY 3.7. *Let $H$ be a uniform or hybrid CA of length $2^a$ configured with rules 60 or 195 where $a = 1, 2, \cdots$. If the rule applied to the first cell of $H$ is 60 [resp. 195], then the group order of $H$ is $2^a$ [resp. $2^{a+1}$].*

Now we will concern with CA of which length is not a power of 2.

THEOREM 3.8. *Let $H$ be a uniform or hybrid CA of length $\ell$ configured with rules* 60 *and* 195 *where $2^a < \ell < 2^{a+1}$ and $a = 1, 2, \cdots$. Then the group order of $H$ is $2^{a+1}$.*

*Proof.* Let $T$, $[F(x)]$ and $(\widetilde{T})^m$ be as in the proof of Theorem 3.5 except the sizes of $T$ and $[F(x)]$. Then we have

$$\begin{aligned}
&[(\widetilde{T})^{2^{a+1}}][f(x)]\\
&= [(I+T)^{2^{a+1}-1}][F(x)] + [T^{2^{a+1}}][f(x)] \quad \text{by Lemma 2.3 and 3.2}\\
&= [0][F(x)] + [T^{2^{a+1}}][f(x)] \quad \text{by Lemma 3.3 because } 2^{a+1}-1 \geq \ell\\
&= [0] + [T^{2^{a+1}}][f(x)]\\
&= [I][f(x)] \quad \text{by Lemma 3.1}\\
&= [f(x)]
\end{aligned}$$

for all $f(x)$. So the group order of $H$ is a divisor of $2^{a+1}$. But we have

$$\begin{aligned}
&[(\widetilde{T})^{2^a}][f(x)]\\
&= [(I+T)^{2^a-1}][F(x)] + [T^{2^a}][f(x)] \quad \text{by Lemma 2.3 and 3.2}\\
&= \begin{array}{r} \\ \\ \\ (2^a)\text{th row} \rightarrow \\ \\ \\ \\ \end{array}
\begin{pmatrix}
0 & 0 & & & & & \\
\vdots & \vdots & & & \mathbf{0} & & \\
0 & 0 & & & & & \\
1 & 0 & & & & & \\
0 & 1 & 0 & & & \cdots & 0\\
\vdots & & \ddots & & & & \\
0 & \cdots & 0 & 1 & 0 & \cdots & 0
\end{pmatrix}
\begin{pmatrix} c_1 \\ \\ \vdots \\ \\ c_\ell \end{pmatrix}\\
&\quad + \begin{array}{r} \\ \\ \\ \\ (2^a+1)\text{th row} \rightarrow \\ \\ \\ \\ \end{array}
\begin{pmatrix}
1 & 0 & & & & & & \\
0 & 1 & 0 & & & & & \\
\vdots & \vdots & \vdots & & & \mathbf{0} & & \\
0 & & & & \ddots & & & \\
1 & 0 & & & & & & \\
0 & 1 & 0 & \mathbf{0} & & & & \\
\vdots & \vdots & \ddots & & & & & \\
0 & \cdots & 0 & 1 & 0 & \cdots & 0 & 1
\end{pmatrix}
\begin{pmatrix} f(x)_1 \\ \\ \vdots \\ \\ f(x)_\ell \end{pmatrix}\\
&\qquad\qquad\qquad\qquad\qquad\qquad \text{by Lemma 3.1 and 3.3}
\end{aligned}$$

$$= (2^a)\text{th row} \rightarrow \begin{pmatrix} 0 \\ \vdots \\ 0 \\ c_1 \\ c_2 \\ \vdots \\ c_{\ell-2^a+1} \end{pmatrix} + \begin{pmatrix} f(x)_1 \\ \vdots \\ f(x)_{2^a-1} \\ f(x)_{2^a} \\ f(x)_{2^a+1} + f(x)_1 \\ \vdots \\ f(x)_\ell + f(x)_{\ell-2^a} \end{pmatrix}$$

$$= \begin{pmatrix} f(x)_1 \\ \vdots \\ f(x)_{2^a-1} \\ c_1 + f(x)_{2^a} \\ c_2 + f(x)_{2^a+1} + f(x)_1 \\ \vdots \\ c_{\ell-2^a+1} + f(x)_\ell + f(x)_{\ell-2^a} \end{pmatrix}$$

and we can always find $f(x)$ such that the first entry $f(x)_1$ of $[f(x)]$ is not equal to the second entry $c_2$ of $[F(x)]$ that means $f(x)_1 + c_2 = 1$. So there exists a state $f(x)$ of which cycle length is greater than $2^a$ for any $F(x)$. This completes the proof. $\square$

Finally we will give some results on uniform or hybrid CA configured with rules 102 or 153 which are parallel to Theorem 3.4 and 3.6, Corollary 3.7 and Theorem 3.8. 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.

THEOREM 3.9. *Let $H$ be a hybrid CA of length $2^a$ configured with rules* 102 *and* 153 *where $a = 1, 2, \cdots$. Suppose that the rule applied to the last cell of $H$ is* 153. *Then its transition diagram consists of equal cycles of length $2^{a+1}$.*

Theorem 3.10. *Let $H$ be a hybrid CA of length $2^a$ configured with rules* 102 *and* 153 *where $a = 1, 2, \cdots$. Suppose that the rule applied to the last cell of $H$ is* 102. *Then the group order of $H$ is $2^a$.*

Corollary 3.11. *Let $H$ be a uniform or hybrid CA of length $2^a$ configured with rules* 102 *or* 153 *where $a = 1, 2, \cdots$. If the rule applied to the last cell of $H$ is* 102 *[resp.* 153*], then the group order of $H$ is $2^a$ [resp. $2^{a+1}$].*

Theorem 3.12. *Let $H$ be a uniform or hybrid CA of length $\ell$ configured with rules* 102 *and* 153 *where $2^a < \ell < 2^{a+1}$ and $a = 1, 2, \cdots$. Then the group order of $H$ is $2^{a+1}$.*

## 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**(1)(1990), 81–87.

[4] B. Elspas, *The theory of autonomous linear sequential networks*, IRE Trans. Circuit Theory **CT-6**(1)(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**(4)(2009), 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. Comput. **43**(12)(1994), 1346–1357.

[9] W. Pries, A. Thanailakis and H.C. Card, *Group properties of cellular automata and VLSI applications*, IEEE Trans. Comput. **C-35**(12)(1986), 1013–1024.



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