East Asian Mathematical Journal
Vol. 27 (2011), No. 1, pp. 67–73

ON HYBRID GROUP CELLULAR AUTOMATA

Jae-Gyeom Kim

Abstract. We investigate some conditions for hybrid cellular automata to be group 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. And researchers have studied on cellular automata configured with rules 51, 60, 102, 153, 195 or 204 and whether such cellular automata are group cellular automata [1-6].

In this note, we will investigate some conditions for such cellular automata to be group cellular automata.

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 $(i-1)^{\text{th}}$, i^{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 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.

Received August 19, 2010; Accepted December 7, 2010.
2000 *Mathematics Subject Classification.* 68Q80.
Key words and phrases. Cellular automaton, group cellular automaton.
This Research was supported by Kyungsung University Research Grants in 2010.

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^{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		dependency	noncomplemented	
Rule	logic function		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.*

Theorem 2.2. [3] *A noncomplemented CA is a group CA if and only if the determinant* $\det T = 1$ *where* T *is the characteristic matrix for the CA.*

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 ℓ-dimensional vector (ℓ = 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 2.4. [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. [6] *CA rules* 60, 102 *and* 204 *form groups for all lengths ℓ with group order $n = 2^a$ where a is a nonnegative integer. And if the CA rule is* 60 *or* 102 *then* $\dfrac{n}{2} < \ell \leq n$.

3. Hybrid group cellular automata

We will concern with hybrid CA configured with rules 60, 102 or 204. A hybrid CA with rule vector $\langle \cdots, R_i, \cdots \rangle$ means the rule R_i applies to i^{th} cell for each i.

Now we will investigate whether such a hybrid CA of length ℓ is a group CA. Let $\langle \cdots, 60, 102, \cdots \rangle$ be the rule vector of a hybrid CA where rules 60 and 102 apply to i^{th} and $(i+1)^{\text{th}}$ cells, respectively. Then the corresponding characteristic matrix T of the CA is given by

$$\left(\begin{array}{cccc|c} & & & \vdots & \\ & & & & 0 \\ \cdots & 0 & 1 & 1 & \\ \hline & & & & \\ & 0 & & & 1 \quad 1 \quad 0 \quad \cdots \\ & & & & \vdots \end{array}\right).$$

So $\det T = \det A \cdot \det B$, where A and B are the submatrices of T given by

$$\begin{pmatrix} & & & \vdots \\ \cdots & 0 & 1 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 1 & 0 & \cdots \\ \vdots & & & \end{pmatrix}$$

of size i and $\ell - i$, respectively. And the states of the first i cells of the CA and the states of the latter $\ell - i$ cells of the CA are completely independent for all time steps. Thus the hybrid CA can be completely split into two CA's. One of them is a CA of length i with rule vector $\langle \cdots, 60 \rangle$ and the other one is a CA of length $\ell - i$ with rule vector $\langle 102, \cdots \rangle$. This means that whether the hybrid CA is a group CA which is completely determined by two split CA's, i.e., the hybrid CA is a group CA if both of two split CA are group CA.

Let $\langle \cdots, 60, 204, \cdots \rangle$ be the rule vector of a hybrid CA where rules 60 and 204 apply to i^{th} and $(i+1)^{\text{th}}$ cells, respectively. Then the corresponding characteristic matrix T of the CA is given by

$$\begin{pmatrix} & & \vdots & \\ \cdots & 0 & 1 & 1 \\ \hline & 0 & & \end{pmatrix} \quad \begin{pmatrix} & 0 & \\ \hline 1 & 0 & 0 & \cdots \\ \vdots & & & \end{pmatrix}.$$

So the remaining discussion is quite similar to the case in the above. Note that the rule vector $\langle \cdots, 60, 204, \cdots \rangle$ includes the rule vectors $\langle \cdots, 60, 204, 60, \cdots \rangle$, $\langle \cdots, 60,\ 204, 102 \cdots \rangle$ and $\langle \cdots, 60, 204, 204 \cdots \rangle$.

Let $\langle \cdots, 204, 102 \cdots \rangle$ be the rule vector of a hybrid CA where rules 204 and 102 apply to i^{th} and $(i+1)^{\text{th}}$ cells, respectively. Then the corresponding characteristric matrix T of the CA is

$$\begin{pmatrix} & & \vdots & \\ \cdots & 0 & 0 & 1 \\ \hline & 0 & & \end{pmatrix} \quad \begin{pmatrix} & 0 & \\ \hline 1 & 1 & 0 & \cdots \\ \vdots & & & \end{pmatrix}.$$

So the remaining discussion is quite similar to the first case. Note that the rule vector $\langle \cdots, 204, 102 \cdots \rangle$ includes the rule vectors $\langle \cdots, 60, 204, 102, \cdots \rangle$, $\langle \cdots, 102,\ 204, 102 \cdots \rangle$ and $\langle \cdots, 204, 204, 102 \cdots \rangle$.

Let $\langle \cdots, 204, 204 \cdots \rangle$ be the rule vector of a hybrid CA where rule 204 applies to i^{th} and $(i+1)^{\text{th}}$ cells. Then the corresponding characteristric matrix T of the CA is

$$\begin{pmatrix} & & \vdots & \\ \cdots & 0 & 0 & 1 \\ \hline & 0 & & \end{pmatrix} \quad \begin{pmatrix} & 0 & \\ \hline 1 & 0 & 0 & \cdots \\ \vdots & & & \end{pmatrix}.$$

So the remaining discussion is quite similar to the first case. Note that the rule vector $\langle \cdots, 204, 204 \cdots \rangle$ includes the rule vectors $\langle \cdots, 60, 204, 204, \cdots \rangle$, $\langle \cdots, 102,\ 204, 204 \cdots \rangle$ and $\langle \cdots, 204, 204, 60 \cdots \rangle$.

Now let $\langle \cdots, 102, 204, 60 \cdots \rangle$ be the rule vector of a hybrid CA where rules 102, 204 and 60 apply to $(i-1)^{\text{th}}$, i^{th} and $(i+1)^{\text{th}}$ cells, respectively. Then

the corresponding characteristic matrix T of the CA is given by

$$\left(\begin{array}{ccc:c:cccc} & & & \vdots & & & & \\ & & & & & 0 & & \\ \cdots & 0 & 1 & 1 & & & & \\ \hdashline \cdots & 0 & 0 & 1 & 0 & 0 & \cdots & \\ \hdashline & & & 1 & 1 & 0 & \cdots & \\ & 0 & & & & & & \\ & & & \vdots & & & & \end{array}\right).$$

So $\det T = \det A \cdot \det B$ where A and B are the submatrices of T given by

$$\begin{pmatrix} & & & \vdots \\ \cdots & 0 & 1 & 1 \\ \cdots & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 & \cdots \\ 1 & 1 & 0 & \cdots \\ \vdots & & & \end{pmatrix}$$

of size i and $\ell - i + 1$, respectively. And the states of the first i cells of the CA are not influenced at all by the states of the remaining $\ell - i$ cells of the CA. Similarly, the states of the latter $\ell - i + 1$ cells of the CA are not influenced at all by the states of the remaining $i - 1$ cells of the CA. Thus the hybrid CA can be completely split into two CA. One of them is a CA of length i with rule vector $\langle \cdots, 102, 204 \rangle$ and the other one is a CA of length $\ell - i + 1$ with rule vector $\langle 204, 60, \cdots \rangle$. And their corresponding characteristic matrices are A and B in the above, respectively.

Note that rule vectors $\langle \cdots, 102, 204 \rangle$ and $\langle 204, 60 \cdots \rangle$ can be regarded as rule vectors $\langle \cdots, 102, 102 \rangle$ and $\langle 60, 60 \cdots \rangle$ respectively, because we assume null boundary condition.

Finally, let $\langle \cdots, 102, 60, \cdots \rangle$ be the rule vector of a hybrid CA where rules 102 and 60 apply to i^{th} and $(i+1)^{\text{th}}$ cells, respectively. Then the corresponding characteristic matrix T of the CA is given by

$$\begin{pmatrix} & & \ddots & & & & & & & \\ & & a & 1 & b & & & & & \\ 0 & \cdots & 0 & 0 & 1 & 1 & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 1 & 1 & 0 & 0 & \cdots & 0 \\ & & & & & c & 1 & d & & \\ & & & & & & & \ddots & & \end{pmatrix}.$$

So $\det T = 0$ because i^{th} and $(i+1)^{\text{th}}$ rows of T are same. Thus the hybrid CA is not a group CA by Theorem 2.2.

From the discussion in the above, we have the following by Lemma 2.5.

Theorem 3.1. *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.

Now we will concern with additive hybrid CA configured with rules 51, 60, 102, 153, 195 or 204. Let $R = \langle \cdots, R_i, \cdots \rangle$ be the rule vector of a CA of length ℓ configured with noncomplemented rules 60, 102 or 204. Let $[F(x)]$ be a vector of length ℓ with entries 0 or 1. Then $R_{[F(x)]}$ will denote the rule vector of the hybrid CA of length ℓ where i^{th} rule of $R_{[F(x)]}$ is the complemented rule $\overline{R}_i$ of i^{th} rule R_i of R if i^{th} entry of $[F(x)]$ is 1, otherwise i^{th} rule of $R_{[F(x)]}$ is i^{th} rule R_i of R.

Theorem 3.2. *Let H be an additive hybrid CA of length ℓ configured with rules* 51, 60, 102, 153, 195 *or* 204. *Suppose 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.*

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

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

for all $f(x)$ by Lemma 2.4, where $\widetilde{T}^{m}$ denotes the application of the rule vector $R_{[F(x)]}$ for m successive cycles. 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 3.1, and thus there exist a positive integer r such that $T^r = I$ by Lemma 2.1. Therefore we have

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

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

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] S. Nandi, *Additive cellular automata: Theory and application for testable circuit design and data encryption*, PhD thesis, I.I.T., Kharagpur, India, 1994.
[5] 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.
[6] 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