Analysis of Linear Group $GF(2^p)$ Cellular Automata*

Un-Sook Choi[1], Sung-Jin Cho[2,**], Yoon-Hee Hwang[3], and Han-Doo Kim[4]

[1] Department of Multimedia Engineering, Tongmyong University
Busan 626-847, Korea
choies@tu.ac.kr
[2] Division of Mathematical Sciences, Pukyong National University
Busan 608-737, Korea
sjcho@pknu.ac.kr
[3] Department of Information Security, Graduate School, Pukyong National University, Busan 608-737, Korea
yhhwang@pknu.ac.kr
[4] School of Computer Aided Science, Institute of Basic Science
Inje University, Gimhae 621-749, Korea
mathkhd@inje.ac.kr

Abstract. Cellular Automata(CA) has been used as modeling and computing paradigm for a long time. And CA has been used to model many physical systems. While studying the models of such systems, it is seen that as the complexity of the physical system increase, the CA based model becomes very complex and difficult to track analytically. Also such models fail to recognize the presence of inherent hierarchical nature of a physical system. In this paper we give the characterization of linear group $GF(2^p)$ CA. Especially we analyze the relationship between characteristic polynomial and transition rule of linear group $GF(2^p)$ CA.

1 Introduction

Cellular Automata(CA) was first introduced by Von Neumann [1] for modeling biological self-reproduction. Wolfram [2] pioneered the investigation of CA as mathematical models for self-organizing statistical systems and suggested the use of a simple two-state, three-neighborhood CA with cells arranged linearly in one dimension. Das et al. ([3] $\sim$ [5]) developed a matrix algebraic tool capable of characterizing CA. Cho et al. [6] proposed a new method for the synthesis of one-dimensional 90/150 linear hybrid group CA for CA-polynomials. And Cho et al. ([3] $\sim$ [9]) and many researchers ([6], [10] $\sim$ [12]) analyzed CA to study hash function, data storage, cryptography and so on.

* This work was supported by the Korea Research Foundation Grant funded by the Korean Government(MOEHRD)(KRF-2006-331-D00458).

** Author to whom all correspondence should be addressed.

H. Umeo et al. (Eds): ACRI 2008, LNCS 5191, pp. 136–143, 2008.

CA has been used as modeling and computing paradigm for a long time. And CA has been used to model many physical systems. While studying the models of such systems, it is seen that as the complexity of the physical system increase, the CA based model becomes very complex and difficult to track analytically. Also such models fail to recognize the presence of inherent hierarchical nature of a physical system.

To overcome these problems Sikdar et al. [12] and Cho et al. [13] studied $GF(2^p)$ CA.

In this paper, by using the results in [6] we give the characterization of linear group $GF(2^p)$ CA. Especially we analyze the relationship between characteristic polynomial and transition rule of linear group $GF(2^p)$ CA.

2 Linear $GF(2^p)$ CA Preliminaries

A $GF(2^p)$ CA can be viewed as an extension of $GF(2)$ CA. It consists of an array of cells, spartially interconnected in a regular manner, each cell being capable of storing an element of $GF(2^p)$.

Under three neighborhood restriction, the next state of the ith cell is given by a function of the weighted combination of the present states of the $(i-1)$th, ith and $(i+1)$th cells, the weights being elements of $GF(2^p)$. Thus if $q_i(t)$ is the state of the ith cell at the tth instant, then

$$q_i(t+1) = \phi(w_{i-1}q_{i-1}(t), w_i q_i(t), w_{i+1}q_{i+1}(t))$$

where ϕ denotes the local transition function of the ith cell and w_{i-1}, w_i and $w_{i+1} \in GF(2^p)$ specify the weights of interconnections.

The transition rule for a three neighborhood $GF(2^p)$ CA cell is represented by a vector of length 3, $< w_{i-1}, w_i, w_{i+1} >$. Here w_{i-1} indicates the weight of dependence of the cell on its left neighborhood, while w_i and w_{i+1} indicate the weighted dependency on itself and its right neighborhood respectively. If the same transition rule vector is applied to all the cells of a $GF(2^p)$ CA, the CA is called an *uniform* $GF(2^p)$ CA, otherwise it is called a *hybrid* $GF(2^p)$ CA.

An n cell $GF(2^p)$ CA can be characterized by an $n \times n$ state transition matrix $T = (t_{ij})$ as follows:

$$t_{ij} = \begin{cases} w_{ij}, & \text{if the next state of the } i\text{th cell depends on the present} \\ & \text{state of the } j\text{th cell by a weight } w_{ij} \in GF(2^p), \\ 0, & \text{otherwise.} \end{cases}$$

For example, let the state transition matrix of a 3-cell $GF(2^2)$ CA be the following:

$$T = \begin{pmatrix} 0 & \alpha^2 & 0 \\ \alpha^2 & \alpha & \alpha^2 \\ 0 & \alpha^2 & 1 \end{pmatrix}$$

where α is a generator of $GF(2^2) = \{0, 1, \alpha, \alpha^2\}$. α is a solution of the generator polynomial $g(x) = x^2 + x + 1$ and the generating matrix M is as the following form:

$$M = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

The next state X' of the present state X of an n-cell $GF(2^p)$ CA with state transition matrix T is given by $X' = TX$. Here T is an $n \times n$ matrix and X and X' are $n \times 1$ vectors.

For the vectors X and X' we need a vector representation of each α^i. Each of the vectors X and X' consists of a string of elements $\alpha^i \in GF(2^p)$. Therefore we need a binary representation of each of these α^i. The last column vector of M^i is used as the vector representation of α^i.

The addition and multiplication operations follow the additive and multiplicative rules of the underlying $GF(2^2)$ as noted in Table 1.

Table 1. Multiplication and addition over $GF(2^2)$

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

$+$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

In the above example M^i $(i = 2, 3)$ and α^i $(i = 1, 2, 3)$ are as the following form:

$$M^2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad M^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\alpha =< 10 >= 2, \alpha^2 =< 11 >= 3, \alpha^3 =< 01 >= 1$$

The *characteristic polynomial* $\Delta(x)$ of the state transition matrix T of a $GF(2^p)$ CA is $\Delta(x) = |T + xI|$. In the above example the characteristic polynomial of T is $\Delta(x) = x^3 + 2x^2 + 3x + 3$. This polynomial is a primitive polynomial on $GF(2^2)$ and thus its period is 63.

Let $\mathbf{C}$ be a $GF(2^p)$ CA whose state transition matrix is T. If $\det(T) \neq 0$, then $\mathbf{C}$ is called a *group* $GF(2^p)$ CA, otherwise it is called a *nongroup* $GF(2^p)$ CA.

3 Characterization of Linear Group $GF(2^p)$ CA

In the state transition matrix T_n of an n-cell $GF(2^p)$ CA $\mathbf{C}$ let the weight of the right state and the weight of the left state be the same. Then this $GF(2^p)$ CA is the natural extension of 90/150 $GF(2)$ CA. Therefore the T_n is as the following:

$$T_n = \begin{pmatrix} d_1 & i & 0 & \cdots & 0 & 0 \\ i & d_2 & i & \cdots & 0 & 0 \\ 0 & i & d_3 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & i & d_n \end{pmatrix}$$

where $i \in \{0, 1, 2, \cdots, 2^p - 1\}$ is the weight.

Remark. We denote T_n by $T_n =< d_1, d_2, \cdots, d_j, \cdots, d_n >_i$, where $d_j \in GF(2^p)$.

The following lemma can be proved by mathematical induction.

Lemma 3.1. Let $T_n =< d_1, d_2, \cdots, d_n >_i$. Then we obtain the following equation.

$$|T_{-1}| = 0,\ |T_0| = 1,\ |T_n| = d_n|T_{n-1}| + i^2|T_{n-2}|,$$

where $|T|$ is the determinant of T.

Following two theorems give conditions for the uniform group $GF(2^p)$ CA.

Theorem 3.2. Let $\mathbf{C}$ be an n-cell uniform $GF(2^p)$ CA with the state transition matrix $T_n =< 0, \cdots, 0 >_i$. If n is even (resp. odd), then $\mathbf{C}$ is a group(resp. nongroup) $GF(2^p)$ CA.

Proof. Since $d_j = d = 0$ for $j = 1, 2, \cdots, n$, $|T_n| = i^2|T_{n-2}|$ by Lemma 3.1. Since $|T_2| = i^2|T_0| = i^2, |T_n| = i^2|T_{n-2}| = i^n$ where n is even. Therefore for even n, $\mathbf{C}$ is a group $GF(2^p)$ CA. Since $|T_1| = i^2|T_{-1}| = 0, |T_n| = i^2|T_{n-2}| = 0$ where n is odd. Therefore for odd n, $\mathbf{C}$ is a nongroup $GF(2^p)$ CA.

Theorem 3.3. Let $\mathbf{C}$ be an n-cell uniform $GF(2^p)$ CA with the state transition matrix $T_n =< i, \cdots, i >_i$. If $n(mod 3) \neq 2$ (resp. $n(mod 3) = 2$), then $\mathbf{C}$ is a group(resp. nongroup) $GF(2^p)$ CA.

Proof. By Lemma 3.1 $|T_0| = 1, |T_1| = i$ and $|T_2| = 0$. Since

$$\begin{aligned} |T_{3k+2}| &= i|T_{3k+1}| + i^2|T_{3k}| \\ &= i(i|T_{3k}| + i^2|T_{3k-1}|) + i^2|T_{3k}| \\ &= i^3|T_{3k-1}| = i^3|T_{3(k-1)+2}|, \end{aligned}$$

$$|T_n| = \begin{cases} (i^3)^k|T_0|, & n = 3k \\ (i^3)^k|T_1|, & n = 3k+1 \\ (i^3)^k|T_2|, & n = 3k+2 \end{cases}$$

Hence $\mathbf{C}$ is a group $GF(2^p)$ CA for $n(mod 3) \neq 2$.

Following two theorems give conditions for the hybrid group $GF(2^p)$ CA.

Theorem 3.4. Let $\mathbf{C}$ be an n-cell hybrid $GF(2^p)$ CA with the state transition matrix $T_n =< 0, d, 0, d, \cdots >_i$. If n is even(resp. odd), then $\mathbf{C}$ is a group(resp. nongroup) $GF(2^p)$ CA.

Proof. i) $n = 2m + 1$:
Since $|T_{2m+1}| = 0 \cdot |T_{2m}| + i^2|T_{2m-1}| = i^2|T_{2(m-1)+1}|$ by Lemma 3.1, $|T_{2m+1}| = (i^2)^m|T_1| = 0$.
ii) $n = 2m$:
Since $|T_{2m}| = d \cdot |T_{2m-1}| + i^2|T_{2m-2}|$ by Lemma 3.1 and $|T_{2m-1}| = 0$ by i), $|T_{2m}| = i^2|T_{2m-2}|$. Therefore $|T_{2m}| = (i^2)^m|T_0| = i^{2m}$. Hence $\mathbf{C}$ is a group(resp. nongroup) $GF(2^p)$ CA for even(resp. odd) n.

Theorem 3.5. Let $\mathbf{C}$ be an n-cell hybrid $GF(2^p)$ CA with the state transition matrix $T_n =< d, 0, d, 0, \cdots >_i$. If $n(mod4) \neq 3$ (resp. $n(mod4) = 3$), then $\mathbf{C}$ is a group(resp. nongroup) $GF(2^p)$ CA.

Proof. Sine $|T_0| = 1$ and $|T_3| = 0$ by Lemma 3.1, we obtain the following equations.

$$\begin{aligned} |T_{4k+3}| &= d \cdot |T_{4k+2}| + i^2|T_{4k+1}| \\ &= d \cdot \{0 \cdot |T_{4k+1}| + i^2|T_{4k}|\} + i^2\{d \cdot |T_{4k}| + i^2|T_{4k-1}|\} \\ &= i^4|T_{4k-1}| = i^4|T_{4(k-1)+3}| \\ &= (i^4)^k|T_3| = 0 \end{aligned} \tag{3.1}$$

$$\begin{aligned} |T_{2m}| &= 0 \cdot |T_{2m-1}| + i^2|T_{2m-2}| = i^2|T_{2(m-1)}| \\ &= (i^2)^m|T_0| = i^{2m} \end{aligned} \tag{3.2}$$

By (3.1) and (3.2),

$$\begin{aligned} |T_{4k+1}| &= d \cdot |T_{4k}| + i^2|T_{4k-1}| \\ &= d \cdot i^{4k} + i^2|T_{4(k-1)+3}| \\ &= d \cdot i^{4k}. \end{aligned}$$

This completes the proof.

4 The Relationship between Characteristic Polynomial and Transition Rule of Linear $GF(2^p)$ CA

In this section we analyze the relationship between characteristic polynomial and transition rule of linear $GF(2^p)$ CA. The following theorem can be proved by mathematical induction.

Theorem 4.1. Let $\mathbf{C}$ be an n-cell $GF(2^p)$ CA with the state transition matrix $T =< d_1, d_2, \cdots, d_n >_i$ and with the characteristic polynomial Δ_n. Then we obtain the following equation.

$$\begin{aligned} \Delta_{-1} &= 0 \\ \Delta_0 &= 1 \\ \Delta_k &= (x + d_k)\Delta_{k-1} + i^2\Delta_{k-2} \end{aligned} \tag{4.1}$$

where Δ_k is the characteristic polynomial of $< d_1, d_2, \cdots, d_k >_i, k = 1, 2, \cdots, n$.

Theorem 4.1 provides an efficient algorithm to compute the characteristic polynomial of a $GF(2^p)$ CA. Initially, Δ_{-1} and Δ_0 are set to zero and one, respectively. Equation (4.1) is applied to obtain Δ_1. It is then reapplied to Δ_0 and Δ_1 to calculate Δ_2. Continuing, the polynomials $\Delta_3, \Delta_4, \cdots, \Delta_n$ are computed. Since Δ_n is the characteristic polynomial of T, the calculation of the characteristic polynomial is completed.

The following is an example of the calculation of the characteristic polynomial of the $GF(2^p)$ CA with the rule vector $< 0, 1, 2, 1 >_2$.

Example 4.2. Let $\mathbf{C}$ be a $GF(2^2)$ CA with the rule vector $< 0, 1, 2, 1 >_2$.

$$\begin{aligned}
\Delta_{-1} &= 0 \\
\Delta_0 &= 1 \\
\Delta_1 &= (x + d_1)\Delta_0 + 2^2\Delta_{-1} \\
&= (x + 0) \cdot 1 + 2^2 \cdot 0 \\
&= x \\
\Delta_2 &= (x + d_2)\Delta_1 + 2^2\Delta_0 \\
&= (x + 1) \cdot x + 2^2 \cdot 1 \\
&= x^2 + x + 3 \\
\Delta_3 &= (x + d_3)\Delta_2 + 2^2\Delta_1 \\
&= (x + 2) \cdot (x^2 + x + 3) + 2^2 \cdot x \\
&= x^3 + 3x^2 + 2x + 1 \\
\Delta_4 &= (x + d_4)\Delta_3 + 3^2\Delta_2 \\
&= (x + 1) \cdot (x^3 + 3x^2 + 2x + 1) + 2^2 \cdot (x^2 + x + 3) \\
&= x^4 + 2x^3 + 2x^2 + 3
\end{aligned} \tag{4.2}$$

This recurrence relation forms the basis for the synthesis of $GF(2^p)$ CA. Initially, we show how recurrence (4.1) satisfies the division algorithm for polynomials. Then we demonstrate that the repeated application of the recurrence relation is a reverse GCD computation.

We now show that repeated application of the division algorithm reverses the computation of the characteristic polynomial of a $GF(2^p)$ CA. Suppose that Δ_n and Δ_{n-1} are known. By the division algorithm, $x + d_n$ and Δ_{n-2} are uniquely determined and easily calculated. If the division algorithm is then applied to Δ_{n-1} and Δ_{n-2}, it will calculate $x + d_{n-1}$ and Δ_{n-3}. We may continue this process until we have computed $x + d_1$ and $\Delta_{-1} = 0$.

Example 4.3. Let $\mathbf{C}$ be a 4-cell $GF(2^2)$ CA with $\Delta_4 = x^4 + 2x^3 + 2x^2 + 3$ and $\Delta_3 = x^3 + 3x^2 + 2x + 1$.

dividend	*divisor*	*quotient*	*remainder*	$GF(2^2)$ *CA byte*
Δ_4	Δ_3	$x + 1$	$2^2(x^2 + x + 3)$	1
Δ_3	$x^2 + x + 3$	$x + 2$	$2^2 x$	2
$x^2 + x + 3$	x	$x + 1$	$2^2 \cdot 1$	1
x	1	$x + 0$	$2^2 \cdot 0$	0

(4.3)

From the calculation, we see that the divisor column is the same as the dividend column shifted up one position and the remainder column is a shift of the i^2 times with the divisor column. Comparing (4.2) to (4.3), we see that the sequence of polynomial in (4.3) is the reverse of the sequence of intermediate polynomials in

the characteristic polynomial calculation. Furthermore, (4.3) yields the sequence of quotients

$$[x+0, x+1, x+2, x+1]$$

By taking the constant terms of these quotients and reversing, we obtain the rule vector $< 0, 1, 2, 1 >_2$.

In Example 4.3 let $\Delta_3 = x^3+3$. Then we obtain the rule vector $< 3, 1, 2, 2 >_3$. Also let $\Delta_3 = x^3$. Then we obtain the rule vector $< 0, 0, 0, 2 >_3$.

If $\mathbf{C}$ is an n-cell $GF(2)$ 90/150 CA with the primitive polynomial as the characteristic polynomial, then there exist two Δ_{n-1}. But the Δ_{n-1} are several in the Example 4.3.

By Theorem 4.1 we can obtain a $GF(2^p)$ CA with Δ_n and Δ_{n-1}. But the method for finding Δ_{n-1} does not exist until now.

Theorem 4.4. Let $\mathbf{C}$ be an n-cell $GF(2^p)$ CA with the state transition matrix $T =< d_1, d_2, \cdots, d_n >_i$. And let $p(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ be the primitive polynomial which is the characteristic polynomial of T. For the nonsingular upper tridiagonal matrix U and for the companion matrix C of $p(x)$, let U and C be as the following:

$$U = (u_{ij}) = \begin{cases} u_i,\ i = j \\ a_i,\ i = j-1 \\ 0,\ i > j \\ x_{ij} \in GF(2^p),\ otherwise \end{cases} \qquad C = (s_{ij}) = \begin{cases} 1,\ i = j+1\ (j < n) \\ c_{i-1},\ j = n \\ 0,\ otherwise, \end{cases}$$

where c_i is the coefficient of $p(x)$. Then we obtain the following equation.

$$\begin{cases} d_1 = u_1^{-1} a_1 \\ d_k = u_{k-1}^{-1} a_{k-1} + u_k^{-1} a_k\ (1 < k < n) \\ d_n = u_{n-1}^{-1} a_{n-1} + c_{n-1} \end{cases} \tag{4.4}$$

Proof. Since the characteristic polynomials and the minimal polynomials of T and C are the same, T and C are similar. So $TU = UC$. Then we obtain the following:

$$\begin{cases} a_1 = u_1 d_1 \\ a_k = i a_{k-1} + u_k d_k\ (1 < k < n) \\ c_{n-1} u_n = i a_{n-1} + u_n d_n \\ u_{i+1} = i u_i \end{cases} \tag{4.5}$$

Since $i = u_{k-1}^{-1} u_k$, we obtain the following required result

$$\begin{cases} d_1 = u^{-1} a_1 \\ d_k = u_{k-1}^{-1} a_{k-1} + u_k^{-1} a_k\ (1 < k < n) \\ d_n = u_{n-1}^{-1} a_{n-1} + c_{n-1} \end{cases} \tag{4.6}$$

5 Conclusion

In this paper we analyzed linear $GF(2^p)$ CA. Especially, we proposed transition rules of linear group $GF(2^p)$ CA. Also we analyzed the characterization of linear

group $GF(2^p)$ CA. Especially we analyzed the relationship between characteristic polynomial and transition rule of linear group $GF(2^p)$ CA. Our results and Cho et al.'s results [6] will be helpful for the development of the synthesis of linear $GF(2^p)$ CA.

References

1. Von Neumann, J.: The Theory of Self-Reproducing Automata. In: Burks, A.W. (ed.), University of Illinois Press, Urbana (1966)
2. Wolfram, S.: Statistical Mechanics of Cellular Automata. Rev. Mod. Phys. 55, 601–644 (1983)
3. Das, A.K.: Additive Cellular Automata: Theory and Applications as a Built-In Self-Test Structure, Ph.D Thesis, I.I.T. Kharagpur, India (1990)
4. Das, A.K., Chaudhuri, P.P.: Vector space theoretic analysis of additive cellular automata and its application for pseudo-exhaustive test pattern generation. IEEE Trans. Comput. 42, 340–352 (1993)
5. Das, A.K., Chaudhuri, P.P.: Efficient characterization of cellular automata. Proc. IEE(Part E) 137(1), 81–87 (1990)
6. Cho, S.J., Choi, U.S., Hwang, Y. H., Kim, H.D., Kim, J.G., Heo, S.H.: New synthesis of one-dimensional 90/150 linear hybrid group cellular automata. IEEE Trans. Comput.-Aided Design Integr. Circuits Syst. 26(9), 1720–1724 (2007)
7. Cho, S.J., Choi, U.S., Hwang, Y.H., Pyo, Y.S., Kim, H.D., Heo, S.H.: Computing Phase Shifts of Maximum-Length 90/150 Cellular Automata Sequences. In: Sloot, P.M.A., Chopard, B., Hoekstra, A.G. (eds.) ACRI 2004. LNCS, vol. 3305, pp. 31–39. Springer, Heidelberg (2004)
8. Cho, S.J., Choi, U.S., Kim, H.D.: Analysis of complemented CA derived from a linear TPMACA. Computers Math. Applic. 45, 689–698 (2003)
9. Cho, S.J., Choi, U.S., Kim, H.D.: Behavior of complemented CA whose complement vector is acyclic in a linear TPMACA. Mathl. Comput. Modelling 36, 979–986 (2002)
10. Nandi, S., Kar, B.K., Chaudhuri, P.P.: Theory and applications of cellular automata in cryptography. IEEE Trans. Computers 43, 1346–1357 (1994)
11. Paul, K.: Theory and application of GF(2^p) Cellular automata, Ph.D Thesis, Departmen of Computer Science and Technology, Bengal Engineering College (A Deemed University) (2002)
12. Sikdar, B.K., Majumder, P., Mukherjee, M., Ganguly, N., Das, D.K., Chaudhuri, P.P.: Hierarchical Cellular automata as an on-chip test pattern generator. In: VLSI Design, Fourteenth International Conference on 2001, pp. 403–408 (2001)
13. Cho, S.J., Choi, U.S., Hwang, Y.H., Kim, H.D., Choi, H.H.: Behaviors of single attractor cellular automata over Galois field $GF(2^p)$. In: El Yacoubi, S., Chopard, B., Bandini, S. (eds.) ACRI 2006. LNCS, vol. 4173, pp. 232–237. Springer, Heidelberg (2006)