Annals of Pure and Applied Mathematics
Vol. 11, No. 1, 2016, 85-92
ISSN: 2279-087X (P), 2279-0888(online)
Published on 11 January 2016
www.researchmathsci.org

Annals of
Pure and Applied
Mathematics

Properties of a Class of Linear Non-Group Cellular Automata

Sukhendu Kuila[1]***, Dipanwita Roy Chowdhury***[2] **and *Madhumangal Pal***[1]

[1]*Department of Applied Mathematics, Vidyasagar University, India,*
E-mail: {babu.sukhendu, mmpalvu}@gmail.com

[2]*Department of Computer Science & Engineering, Kharagpur, India*
E-mail: drc@cse.iitkgp.ernet.in

Received 20 December 2015; accepted 8 January 2016

Abstract. We study on a special class of one dimensional, three neighborhood, two state, linear non-group Cellular Automata called LNGCA. We find property related to state transition diagram of this particular class of CA. The results have been verified with computer experiments.

Keywords: Cellular Automata, Properties of linear non-group Cellular Automata, Cryptography.

AMS Mathematics Subject Classification (2010): 37B15

1. Introduction

Recent technological advancement demands fast transaction, minimal power consumption, less time consuming devices. To cope with these fast communicative applications, any cryptographic construction taking arbitrary length message should have the capability in very fast computation besides providing security. Minimizing the number of operations in computation and employing easily computable functions makes a system efficient. A simple modular, cascadable, reusable component is needed to generate complex function (1) using relatively simple functions. One such component is Cellular Automaton (2) which runs in affordable speed. Parallel processing for even faster computation is it's another advantage. Because of its parallel execution and bit-wise operations, CA are one of the most recommended components (3), (4) as far as hardware implementation is concerned. To get these sorts of advantages, Cellular Automata are vastly used in Biological science, Physics, Mathematics, Computer Science, Commerce etc. Depending on its vast applicability, characterization of properties of cellular automata have been done in a series of research papers (5), (6), (7), (8) etc. Specifically, a large number of cryptographic constructions (4), (9), (3), (10), (11) have been made utilizing Cellular Automata properties. Finding out new elementary properties of Cellular Automata, keeping in mind its ever increasing usability in its vast application spectrum, have always been of great demand (1). In this paper, we study on a special class of one dimensional, three neighborhood, two state, linear Cellular Automata called LNGCA. The state-transition graph of LNGCA consists of a set of disjoint trees rooted at some cyclic states. Here we develop some new interesting theoretical properties regarding state transition diagram of LNGCA. Computer experiments have been conducted to verify the results.

The rest of the paper is organized as follows. In section 2, we state some preliminaries of Cellular automata. Then we report new properties of CA in section 3. Computer experimentation to validate the proposed property of newly defined CA is given in section 4 while concluding remarks have been made in section 5.

2. Preliminaries of Cellular Automata

We recall the concept of Cellular Automata (12). Cellular Automata are discrete lattice of cells with a particular geometry. Each cell consists of a memory element (Flip-Flop) and a combinatorial logic. Cells can assume values from a finite set Q. At each clock pulse, the cells are updated simultaneously. For k number of neighborhoods, $f : Q^k \rightarrow Q$ is the local transition rule depending on which the cell values are updated. The transition function totally depends on local neighborhood of cells. If the next state function of a cell is expressed in the form of a truth table, then the decimal equivalent of the output is conventionally called the rule number for the cell (13). e.g. for 3-neighborhood CA i-th cell at t-th clock cycle evolves as follows:

$$\mathrm{S}_\mathrm{i}^{\mathrm{t+1}} = \mathrm{f}(\mathrm{S}_{\mathrm{i-1}}^\mathrm{t}, \mathrm{S}_\mathrm{i}^\mathrm{t}, \mathrm{S}_{\mathrm{i+1}}^\mathrm{t})$$

To be more explicit, the combinational logic of rule-90 and rule-150 are given by

$$Rule-90\text{:}\ \mathrm{S}_\mathrm{i}^{\mathrm{t+1}} = \mathrm{S}_{\mathrm{i-1}}^\mathrm{t} \oplus \mathrm{S}_{\mathrm{i+1}}^\mathrm{t}$$
$$Rule-150\text{:}\ \mathrm{S}_\mathrm{i}^{\mathrm{t+1}} = \mathrm{S}_{\mathrm{i-1}}^\mathrm{t} \oplus \mathrm{S}_\mathrm{i}^\mathrm{t} \oplus \mathrm{S}_{\mathrm{i+1}}^\mathrm{t}$$

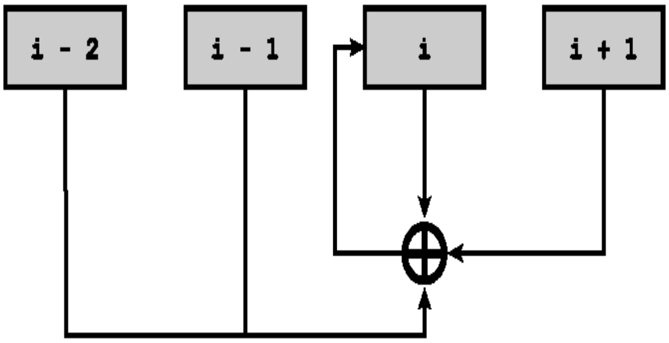

Figure 1: A four neighborhood CA

If in a CA, the values of next state of all the cells are calculated only by XOR operations of the present values of neighboring cells of the cell, then the CA is called linear CA. The operations depending on which cell values are updated is known as rule set. If n cells are connected and rules for each cell be placed one under another, then the matrix formed his way is called characteristic matrix of the CA. If a CA involves at least one nonlinear rule, then it is called non-linear CA.

A CA is called group CA if its transformation is invertible in the sense that the CA will always return to its initial state. In this CA if we draw state transition graph, all the states must be in one cycle. In matrix notation, the determinant of the characteristic matrix of group CA becomes non-zero. On the other hand, if in matrix representation, the determinant of the characteristic matrix (T) is zero, then the CA configuration is called non-group CA. The next state of the automation is computed as

$$X(t+1) = T \times X(t)$$

In state transition diagram, for non-group CA, it is impossible to include all the states in one cycle. In a non-group CA, the cycles in the state transition diagram are called attractors. In Fig:2, cyclic states are {1,2,3} and {0}. If the length of the cycle in an attractor is 1, then the state is called graveyard. Graveyard is a state with self-loop. So the 0 state always forms a graveyard. The set of all states rooted at a cyclic state α is called α-basin. A state is called non-reachable (leaf) if the state cannot be reached, whatever may the number of clock pulses be, starting from any other state. In other words, non-reachable states have no predecessor. In Figure 2, the states {5; 10; 4; 11; 7; 8; 6; 9} are non-reachable. The depth of a CA is defined to be the minimum number of clock cycles required to reach the nearest cyclic state from any non-reachable state in the state transition diagram of the CA. The diagram has depth 2. Also if n, r are order and rank of the characteristic matrix, the number of predecessors for each reachable state is 2^{n-r}. For the matrix T, the number of predecessors becomes 2^{4-3}. Now we define LNGCA as follows.

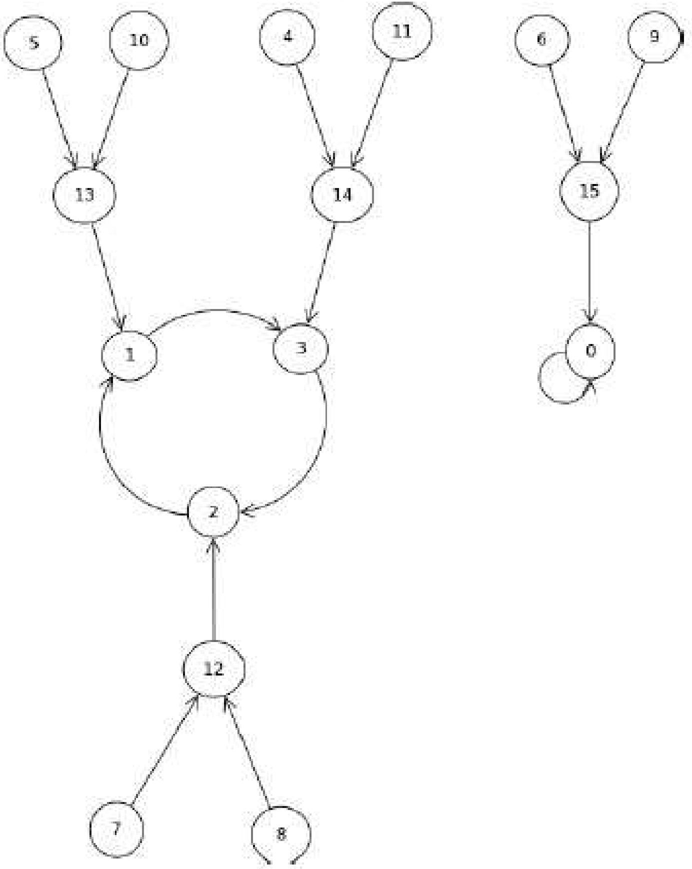

Figure 2: State Transition Diagram

Definition 1(LNGCA). *A linear non-group Cellular Automata characterized by matrix T is called LNGCA if it satisfies*

$$T^{\eta+1}(\alpha) = T^{\eta}(\alpha) \qquad \forall i \geq 1$$

$$\textit{and}$$

$$T^{\eta-1}(\alpha) \neq T^{\eta}(\alpha)$$

where α is any non-reachable state and η is the depth of the CA.

Computer experiments have been conducted in support of the existence of this particular type of CA. Small classes of experimental results are reported in Table-1. The next section reports some properties of the newly defined Cellular Automata. Here the conditions in LNGCA state that all non reachable states in the state transition diagram have equal length.

3. Properties of LNGCA

A linear non-group CA contains several non-reachable states, some reachable states and one or several cycles. The rule structure of an n cell CA can be characterized by an n × n matrix T whose ith row represents the updating rule of i-th cell. If the present state values of the cells are represented by a column vector α, then T(α), the matrix multiplication of T and α with XOR addition, is the next state value of the CA. In general, T^{i}(α) is the i-th time applications of T on α i.e., i consecutive clock pulses are given to the linear CA taking α as seed. Following results provide some new interesting properties of LNGCA.

Property 1. *If θ_1; θ_2 be any attractors of an LNGCA characterized by the matrix T, then $\theta_1 \oplus \theta_2$ must also be an attractor.*

Proof: Let us assume that η be the depth of the LNGCA. Then ∃ non-reachable statesα_1, α_2 such that

$$T^{\eta}(\alpha_1) = \theta_1 \text{ and } T^{\eta}(\alpha_2) = \theta_2$$

$$\text{with } T^{\eta-i}(\alpha_1) \neq \theta_1 \text{ and } T^{\eta-i}(\alpha_2) \neq \theta_2 \qquad \eta > i > 1$$

$$\begin{aligned} \text{Now} \quad \theta_1 \oplus \theta_2 &= T^{\eta}(\alpha_1) \oplus T^{\eta}(\alpha_2) \\ &= T^{\eta}(\alpha_1 \oplus \alpha_2) \\ &= \theta, \text{ an attractor} \qquad \text{[as depth of CA is } \eta] \end{aligned}$$

Property 2. *In an LNGCA characterized by the matrix T, if α is a non reachable state, then $\alpha \oplus T(\beta)$ is also non reachable, β being any state of the CA.*

Proof: Since T is a linear map, the image space of T must be a subspace of co-domain of T.

Now α is non-reachable ⇒ α ∉ Image space

Image space being closed, α ⊕ T(β) ∉ Image space of T for any β.

Hence α ⊕ T(β) is non-reachable.

The proof does not require the specific property of LNGCA. So, the property remains valid not only for LNGCA but also for any linear non-group CA.

Example 1. In Figure-1, the state 6 is non-reachable while 14 is reachable. Now 6 ⊕ 14 makes 8 which is also non-reachable as can be seen in that state transition diagram.

Extending the previously stated property, we give a more general property of linear non-group CA as follows.

Property 3. *If $\alpha; \beta$ be any two non-reachable states of an LNGCA characterized by the matrix T, then depth((α) $\oplus$ (β)) = min{depth(α); depth(β)} i.e., $\forall\, j \geq i$, the relation $T^i(\alpha) \oplus T^j(\beta) = T^i(\mu)$ holds; where μ is a non-reachable state.*

Proof: Since T is a linear map, T^j becomes a subspace of the vector space $T^i \quad \forall\, j \geq i$.

$\Rightarrow T^i(\alpha), T^j(\beta) \in$ Image space of T^i for non-reachable states α, β.

$\Rightarrow T^i(\alpha) \oplus T^j(\beta) \in$ Image space of T^i

Then the element $T^i(\alpha) \oplus T^j(\beta)$ can be written as

$$T^i(\alpha) \oplus T^j(\beta) = T^k(\mu) \text{ for k} \geq \text{i.}$$

There may arise three cases depending on the value of i

Case-1: *i = 0*

Here the result comes directly from Property-2.

Case-2: *0 < i < η*

Our intension is to show k = i and we prove it by contradiction

Let us consider k > i.

Then we have $T^i(\alpha) \oplus T^j(\beta) = T^k(\mu)$

$$\Rightarrow T^i(\alpha) \oplus T^j(\beta) \oplus T^j(\beta) = T^k(\mu) \oplus T^j(\beta)$$

i.e., $T^i(\alpha) = T^k(\mu) \oplus T^j(\beta)$

$$\Rightarrow T^i(\alpha) = \begin{cases} T^k\big(\mu \oplus T^{j-k}(\beta)\big), & j > k \\ T^j\big(\beta \oplus T^{k-j}(\mu)\big), & otherwise \end{cases}$$

$$\Rightarrow T^i(\alpha) = \begin{cases} T^k(\delta_1), & j > k \\ T^j(\delta_2), & otherwise \end{cases}$$

where $\delta_1 = \mu \oplus T^{j-k}(\beta)$ is a leaf element as μ is so and $\delta_2 = \beta \oplus T^{k-j}(\mu)$ is also a leaf element as β is so.

Therefore, in general, $T^i(\alpha) = T^{i+t}(\delta)$ for some t. [as k > i; j > i and δ being a leaf element].

$\Rightarrow$ i ≥ η

But here in this case, i < η which is a contradiction and hence i ≥ k.

The only remaining possibility is k = i.

Case-3: i ≥ η

Here $T^i(\alpha) = \theta_1$ and $T^j(\beta) = \theta_2$ for attractors θ_1 and θ_2.

Then from Property 1, we have $T^i(\alpha) \oplus T^j(\beta) = T^i(\mu)$.

Combining all the cases, we conclude that $T^i(\alpha) \oplus T^j(\beta) = T^i(\mu) \quad \forall\, j \geq i$.

Example 2. The states 15 and 1 are at depth 1 and at depth 2 respectively and 15 ⊕ 1 = 14. The state 14 is at depth 1 as shown in the Figure-1.

The proposition of Property-3 have been verified with computer experiment and the result for a particular rule-set is given in *Table-2,3*

4. Instances of LNGCA

In support of the existence of the special class of CA (LNGCA), computer generated experiments have been conducted. Some of these results are given in the following tables.

Rule set	**Level-0**	**Level-1**	**Level-2**	**Level-3**	**Level-4**	**Level-5**	**Level-6**	**Level-7**	**Cycle**	**Non-reachable**
<90,90,90,90,90,90,90>	0	85	34, 119	20, 54, 65, 99	8, 28, 42, 62, 73, 93, 107, 127	5, 13, 17, 25, 39, 47, 51, 59, 68, 76, 80, 88, 102, 110, 114, 122	2,7, 10, 15,19, 22,27, 30,32, 37,40, 45,49, 52,57, 60,67, 70,75, 78,82, 87,90, 95,97, 100, 105, 108, 112, 117, 120, 125	1,3,4,6, 9,11,12,14, 16, 18,21, 23,24, 26,29, 31,33, 35,36, 38,41, 43,44, 46,48, 50,53, 55,56, 58,61, 63,64, 66,69, 71, 72,74, 77,79, 81,83, 84,86, 89,91, 92,94, 96,98, 101,103, 104,106, 109,111, 113,115, 116,118, 121,123, 124,126	-	1,3,4,6, 9,11,12, 14,16, 18,21, 23,24, 26,29, 31,33, 35,36, 38,41, 43,44, 46,48, 50,53, 55,56, 58,61, 63,64, 66,69, 71,72, 74,77, 79,81, 83,84, 86,89, 91,92, 94,96, 98,101, 103, 104,106, 109,111, 113,115, 116,118, 121,123, 124, 126
<102,102,102,102,102,102,102>	0,64	32, 96		8, 16, 24, 40, 48, 56,					Remaining Sta	8,16,24, 40,48, 56,72, 80,89, 104,112, 120

				72, 80, 89, 104, 112, 120					tes	

Table 1: LNGCA for n = 7

4.1. Result in support of Property-3

The following experimental results given in *Table-2* show that for any (level-1) state α and any (level-2) state β, α ⊕ β ∈ {x : x is a level-2 state}.

Rule-set	α	Level-2	α ⊕ Level-2
<90,0,90,0,90,0>	2	1,3,4,5,6,7,9,11,12,13,14,15,16,17, 18,19,20,21,22,23,24,25,26,27,28, 29,30,31,33,35,36,37,38,39,41,43, 44,45,46,47,48,49,50,51,52,53,54, 55,56,57,58,59,60,61,62,63	3,1,6,7,4,5,11,9,14,15,12,13, 18,19,16,17,22,23,20,21,26, 27,24,25,30,31,28,29,35,33, 38,39,36,37,43,41,46,47,44, 45,50,51,48,49,54,55,52,53, 58,59,56,57,62,63,60,61
<90,0,90,0,90,0>	8	1,3,4,5,6,7,9,11,12,13,14,15,16,17, 18,19,20,21,22,23,24,25,26,27,28, 29,30,31,33,35,36,37,38,39,41,43, 44,45,46,47,48,49,50,51,52,53,54, 55,56,57,58,59,60,61,62,63	9,11,12,13,14,15,1,3,4,5,6,7, 24,25,26,27,28,29,30,31,16, 17,18,19,20,21,22,23,41,43, 44,45,46,47,33,35,36,37,38, 39,56,57,58,59,60,61,62,63, 48,49,50,51,52,53,54,55
<90,0,90,0,90,0>	10	1,3,4,5,6,7,9,11,12,13,14,15,16,17, 18,19,20,21,22,23,24,25,26,27,28, 29,30,31,33,35,36,37,38,39,41,43, 44,45,46,47,48,49,50,51,52,53,54, 55,56,57,58,59,60,61,62,63	11,9,14,15,12,13,3,1,6,7,4,5, 26,27,24,25,30,31,28,29,18, 19,16,17,22,23,20,21,43,41, 46,47,44,45,35,33,38,39,36, 37,58,59,56,57,62,63,60,61, 50,51,48,49,54,55,52,53
<90,0,90,0,90,0>	32	1,3,4,5,6,7,9,11,12,13,14,15,16,17, 18,19,20,21,22,23,24,25,26,27,28, 29,30,31,33,35,36,37,38,39,41,43, 44,45,46,47,48,49,50,51,52,53,54, 55,56,57,58,59,60,61,62,63	33,35,36,37,38,39,41,43,44, 45,46,47,48,49,50,51,52,53, 54,55,56,57,58,59,60,61,62, 63,1,3,4,5,6,7,9,11,12,13,14, 15,16,17,18,19,20,21,22,23, 24,25,26,27,28,29,30,31

Table 2: Experimental results in support of Property-3. (Level -1) states are α ∈ {2, 8, 10, 32}.

5. Conclusion

Some new properties of a class of Linear Non-Group Cellular Automata have been reported and the results have been verified in computer experimentation. The properties should have some applications to any field in the application spectrum of Cellular Automata. Research is still going on to improve existing CA models, combine CA systems with other mathematical and conceptual models, and better understand the implications and nature of CA in general.

REFERENCES

1. P.Caballero-Gil and A.Fster-Sabater, Using linear hybrid cellular automata to attack the shrinking generator, *IEICE Transactions* 89-A, 5 (2006),1166-1172.
2. D.R.Choudhury, S.Nandi and P.P.Chattopadhyay, Additive Cellular Automata Theory and Applications, *IEEE Computer Society Press*, 1997.
3. J.Daemen, R.Govaerts and J.Vandewalle, A framework for the design of one-way hash functions including cryptanalysis of damgrd's one-way function based on a cellular automaton. In *ASIACRYPT (1991)*, H. Imai, R. L. Rivest, and T. Matsumoto, Eds., vol. 739, *Lecture Notes in Computer Science, Springer*, pp. 82-96.
4. A.Das and P.P.Chaudhuri, Vector space theoretic analysis of additive cellular automata and its application for pseudoexhaustive test pattern generation, *IEEE Trans. Computers*, 42(3) (1993) 340-352.
5. S.Das, B.Sikdar and P.P.Chaudhuri, Characterization of reachable/nonreachable cellular automata states. In ACRI (2004), *P. M. A. Sloot, B. Chopard, and A. G. Hoekstra, Eds., vol. 3305 of Lecture Notes in Computer Science, Springer*, pp. 813-822.
6. N.Jamil, R.Mahmood, M.R.Z'aba, N.I.Udzir and Z.A.Zukarnaen, A new cryptographic hash function based on cellular automata rules 30, 134 and omega-ip network. *International Proceedings of Computer Science & Information Technology 27 (2012).*
7. J.Kari, Theory of cellular automata: A survey, *Theoretical Computer Science,* 334(13) (2005) 3 -33.
8. O.Lafe, Data compression and encryption using cellular automata transforms, *Engng. Applic. Artif. Intell.,* (1997).
9. O.Martin, A.Odlyzko and S.Wolfram, Algebraic properties of cellular automata. *Communications in Mathematical Physics,* 93(2) (1984) 219-258.
10. M.Mihaljevic, Y.Zheng and H.Imai, A family of fast dedicated one-way hash functions based on linear cellular automata over gf(q), 1999.
11. P.Pal Chaudhuri, D.R.Chowdhury and S.N.Chattopadhyay, *Additive cellular automata: theory and applications.*
12. S.Tripathy and S.Nandi, Lcase: Lightweight cellular automata-based symmetric-key encryption, *I. J. Network Security,* 8 (3) (2009) 243-252.
13. S.Wolfram, Random sequence generation by cellular automata, *Advances in Applied Mathematics,* 7(2) (1986), 123-169.
14. S.Kuila, D.Saha, M.Pal and D.Roy Chowdhury, CASH: Cellular automata based parameterized hash, In Security, Privacy, and Applied Cryptography Engineering, Vol. 8804 of the series *Lecture Notes in Computer Science*, pp. 59–75. Springer.
15. S.Kuila, D.Saha, M.Pal and D.Roy Chowdhury, Practical distinguishers against 6-round keccak-f exploiting self-symmetry, In Progress in Cryptology-AFRICACRYPT 2014, Marrakesh, Morocco, Springer, 2014, pp. 88-108.