On the Selection of Cellular Automata based PRNG in Code Division Multiple Access Communications

Arnab MITRA

Adamas Institute of Technology,
Kolkata-700126, India.
mitra.arnab@gmail.com, arnab.mitra@etti.tuiasi.ro

Abstract: The main contribution of this article is to investigate the application suitability of Cellular Automata based pseudo-random noise generator in Code Division Multiple Access Communications. New dynamics in group Cellular Automata were explored. Extensive analysis for two classes of group Cellular Automata (maximum length Cellular Automata and equal length Cellular Automata) were carried out. The analysis and comparison results for these classes of group Cellular Automata demonstrate the advantages of equal length Cellular Automata over maximum length Cellular Automata in view of code division multiple access applications.

Keywords: Pseudo-Random Noise Generator, Linear Feed Back Shift Register, Coupled Map Lattice, Cellular Automata, Code Division Multiple Access.

1. Introduction

Pseudo-random noise generators (PRNGs) are used in engineering applications such as in built-in self-test (BIST) circuits applications and in the validation of design and manufacturing control. In data security, strength of the crypto-system depends on the quality of PRNGs. In communications, multiple equal length random keys are required in view of code division multiple access (CDMA), where the keys in CDMA should be independent (de-correlated) between them. Application specific requirements resulted in numerous approaches for PRNGs, for example, PRNG designs are available based on Coupled Mapped Lattices (CMLs) [42], Cellular Automata (CAs) [5, 27, 38], and Linear Feed Back Shift Register (LFSRs) [9, 12, 17]. CAs were suggested for potential uses in BISTs and data security applications with advantages of having low cost physical implementation and support for easy incorporation in very-large-scale integration (VLSI) architecture [5, 27].

CAs evolve in discrete space and time. Elementary CAs (ECAs) are 1-dimensional, 3-neighbourhood CAs with fixed or periodic boundary condition [38]. ECA evolutions are dependent on binary values of the CA cells and CA transition functions (total 256 rules, also known as Wolfram CA rules). The next state function (CA rule) of the i^{th} cell at time $t+1$ is $x_i^{t+1}=f\{x_{i-1}^t, x_i^t, x_{i+1}^t\}$ of the present states of $(i-1)^{th}$, i^{th} and $(i+1)^{th}$ cell at time *t* [27]. A CA rule is additive when it involves only XOR and XNOR logic.

A special class of ECAs always producing cycles is referred as group CA. Additive rules play an important role in generation of group CAs. Uses of group CAs as PRNGs were described in [27].

The main purpose of this article is to compare PRNGs based on CAs, LFSRs, and CMLs aiming CDMA applications and to show that a class of ECAs, Equal Length Cellular Automata (ELCAs) is well suited for CDMA applications.

The article is organized as follows: PRNGs based on LFSRs, CMLs, and CAs are compared in Section 2; Section 3 introduces the analysis of CA based PRNGs in all fixed boundary conditions; while properties related to CA based PRNGs are discoursed in Section 4. Discussion and conclusions are followed in Section 5 and Section 6 respectively.

2. Comparisons of Various Solutions for PRNGs

We review and compare several types of PRNGs based on CMLs along with fuzzy versions of CMLs, chaotic circuits, LFSRs, and CAs along with fuzzy versions of CAs (fuzzy-CAs (fCAs)).

PRNGs using CMLs were suggested for data security applications [4, 19, 31, 34, 41, 42]. CMLs were referred as real valued non-linear systems of coupled chaotic maps [42]. For example, the discretized CMLs consisting of skew tent maps were defined as [12],

$$z_{i,n+1}=(1-\varepsilon)v(z_{i,n})+ \\ +\frac{\varepsilon}{2}\left[v(z_{i-1,n})+v(z_{i+1,n})\right], \\ \forall i=0,1,\ldots,L-1 \quad (1)$$

where the number of sites is L, $z_{1,n}\in(0,1)$ present the state variable (real valued) for the site i at time n (=0,1,...), coupling constant is $\varepsilon\in(0,1)$ with skew tent map is as [42],

$$v(z)=\begin{cases}\frac{z}{p}, & 0\le z\le p\\ \frac{z-p}{1-p}, & p<z\le 1\end{cases} \quad (2)$$

where parameter $p\in(0,1)$.

Stream cipher generation using CMLs along with computation of largest linear correlations between consecutive key streams, which is below the safe bounds, were introduced in [42]. Equal length tent maps (ELTM) (with analogy to ELCAs) and binary tent maps (BTM) based BIST applications were presented in [34]. The BTM was defined as [34],

$$x_{n+1}=\begin{cases}2x_n, & x_n\le 127\\ (2^8-1)-2(x_n-128), & x_n\ge 128\end{cases} \quad (3)$$

Stability issues and enhanced pattern formation in CMLs using fuzzy nodes towards information security were put forward in [30]. CfMLs are efficient in processing of uncertainty in information. Necessary conditions for periodicity, conditions for the minimal number of iterations in simulations of CfMLs, and validation of results (for both of CMLs and CfMLs) were discussed in [21]. Chaos-based PRNGs were introduced in many papers, e.g., [8, 29]. The drawback for this class of PRNGs is the requirement for digitization for the uses in digital systems.

Many PRNGs for BISTs use LFSRs. Multiple-polynomial LFSRs (MP-LFSRs) based PRNGs for BISTs were established in [12]. LFSR-PRNGs aiming reduced circuitry in BISTs were demonstrated in [17]. In an another design, LFSR-PRNGs with self re-seeding capacity were shown to produce longer pseudo-random sequences with minimal logic [9]. An example of LFSR-based low-cost BIST architecture with low silicon area overhead was described in [20].

CAs (specifically group CAs) were suggested as PRNGs in data security and BISTs applications. [5, 7, 8, 13, 18, 27, 37]. A large number of research papers study the chaos dynamics in ECAs [2, 15, 22, 28, 39]. PRNG characteristics for the Maximum Length Group CAs (MaxCAs) were explored in details [5, 7, 8] and MaxCAs were suggested as PRNGs in BISTs [5, 13, 18] and data security applications [5, 27].

On the other hand, a novel fCA and fCA based PRNGs were recommended in [35] because, due to the continuous interval of the fuzzy output values, these behave as true random (chaotic) generators. Detailed investigations on the dynamics of fCAs were described in [1, 3, 10]. Notions of CAs and fuzzified principle of CAs including the state transitions, delay of transition and choice of a local transition function were investigated in [1]. Hierarchy for fCAs and the precise interclass relationships for the fCA-classes were described in [1]. Flocchini et al. explored system dynamics with fuzzy CA rule 90 [10]; using the fuzzified version of system dynamics they explained the reason for generation of complex patterns by crisp CA rule 90. H. Betel et al. thoroughly explored the relationship between crisp and fuzzy CAs in [3] and argued “a strong connection between them by focusing on two properties: density conservation and additivity” [3]. This is one of the reasons why we restricted the study in Section 3-5 to CAs only.

PRNGs based on the LFSRs and group CAs were compared in [18] in order to address the efficiency of the PRNGs. In [18], CAs attained higher speed and “reduced area occupancy in the silicon area” [18] compared to the LFSRs with identical characteristic polynomials. Summarized data on the PRNGs are given in Table 1.

Next, the CAs (group CAs) are explored. Combined cycles from equal lengths (nonmaximal length group CAs) and maximum length CA cycle (MaxCAs) were proposed for cryptographic uses [27]. An n-cell ECA at 3-neighborhood null boundary produces one cycle of length 1 and another cycle (MaxCA) with length of 2^n-1. Pseudo-random characteristics are observed in MaxCA cycle [5, 7, 8, 18, 27]. The cycles produced with MaxCAs at null boundary condition were comparable with the cycles produced with LFSRs [18].

Table 1. Comparison of selected features for PRNGs

Type	Coverage of the states	Speed of generation	Uses
LFSR	Maximum length cycle is 2^n-1	Slower than CA	BISTs, data security
CA	Maximum length cycle is similar to LFSR	Faster Than LFSR	BISTs, data security, image encryption
fCA	Properties are closely related to CA		
CML	Need digitization for uses in digital applications		
CfML	Properties are closely related to CML		

ELCAs are another variant of group CAs, where produced all cycles are of equal lengths. An n-cell ECA at 3-neighborhood null boundary set up produces 2^n number of equal length cycles of length 2^{n-m}, for $\forall n \geq 1$, and $\forall m=1,2,\ldots,(n-1)$ [23]. ELCAs were examined as an alternative ECA based PRNG in data security [24], and CDMA applications [25, 36]. In other researches, uses of cycles of length 8 were suggested for encryptions of gray scale images [6, 14, 40], thus potential uses of ELCAs of length 8 were argued for image encryption in [25]. In another research, Equal Length Cycle Cellular Automata (ELCCAs) were synthesized as a special case of invertible CAs and were suggested for uses in protein synthesis [11].

Additive rules were applied to the synthesis of group CAs (specifically ELCAs and MaxCAs) [23]. Dynamics of ELCAs at several fixed boundary conditions were thoroughly explored in [25] and cost efficiency associated with the design of ELCA chips were presented in [25, 36]. Hence, the dynamics of MaxCAs in fixed boundary conditions might uncover its potential in view of CDMA applications.

3. Analysis of MaxCAs at Several Fixed Boundaries

MaxCAs were examined in fixed boundary conditions. Simulation results for MaxCAs for automata size 4 are in Table 2. The notations used throughout the article are: c_i, for $i=1,2,\ldots,n$ represents CA cycle; arrow between two decimal number represent state transition in the cycle; r*(s)* represents correlation coefficient at some shift s; and c represents correlation coefficient.

Table 2. MaxCAs at several fixed boundaries scenarios for automata size 4

Rule	Fixed boundary conditions			
	0_0	***0_1***	***1_0***	***1_0***
90, 150, 90, 150	c_1 0→0 c_2 1→3→6 →11→2 →5→13 →9→7→ 8→4→14 → 15→12→ 10→1	c_1 0→1→2 →4→15 →13→8 →5→12 →11→3 →7→9→ 6→10→0 c_2 14→14	c_1 0→8→ 12→2→1 3→1→11 →10→9 →15→4 →6→3→ 14→7→0 c_2 5→5	c_1 0→9→ 14→6→2 →12→3 →15→5 →4→7→ 1→10→8 →13→0 c_2 11→11

A cycle of length 15 (MaxCA for automata size 4) was achieved at all fixed boundary conditions (refer Table 2). No identical cycles of length 15 were produced whenever the boundary conditions were changed. Only the maximum length cycle comparable to LFSRs were produced with the MaxCA cycle in 0_0 (null) boundary. Recall that the maximum length cycle from LFSRs does not include the state 0 in it (similar for maximum length cycles with MaxCAs at 0_0 boundary).

Simulations for MaxCAs with automata size 5, 6 and 7 at 0_0 boundary confirm that state 0 were not present in the maximum length cycles. Hence maximum length cycle from MaxCAs similar to LFSRs were found to be dependent on the boundary conditions (null boundary).

Auto-correlations for the non-identical MaxCAs from automata size 5 with all fixed boundaries are shown in Figure 1.

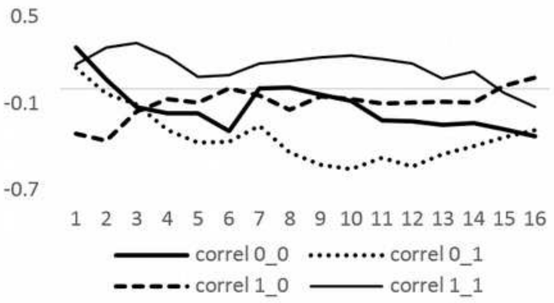


Figure 1. Correlation coefficients for MaxCAs at fixed boundaries, automata size 5

Absolute values of the maximum and the minimum correlations coefficients for the MaxCAs from Figure 1 are in Table 3.

Table 3. Correlation coefficients for MaxCAs with automata size 5

Absolute value of correlation coefficients	Fixed boundary conditions			
	0_0	***0_1***	***1_0***	***1_0***
Maximum	0.329	0.554	0.355	0.318
Minimum	0.008	0.029	0.006	0.024

For MaxCA at 0_0 boundary, the absolute value of the maximum correlation coefficient is 0.329 and the absolute value of the minimum correlation coefficient is 0.008 (see second column of Table 3). Both correlation coefficients at 0_0 boundary are low with comparison to the coefficient values of 0_1, 1_0 and 1_1 boundary in Table 3. Similar results were obtained for MaxCAs with automata size 6. Therefore, MaxCAs at 0_0 boundary is better suitable for PRNG type requirements than of MaxCAs at other fixed boundaries.

Further properties related to MaxCAs and ELCAs in view of CDMA applications are examined in Section 4.

4. Comparison of MaxCAs and ELCAs

MaxCAs and ELCAs for automata size 5 (odd size) and size 6 (even size) were analyzed through RUNs tests, followed by FFT spectrum and auto-correlation coefficient analysis. Hybrid ELCAs were used as they were suggested as better suitable for applications concerning randomness than of uniform ELCAs [25]. String of rules used for generating MaxCAs [5] and ELCAs are given in Table 4. RUNs tests results for MaxCAs and ELCAs are in Table 5.

Table 4. String of rules for generation of MaxCAs and ELCAs

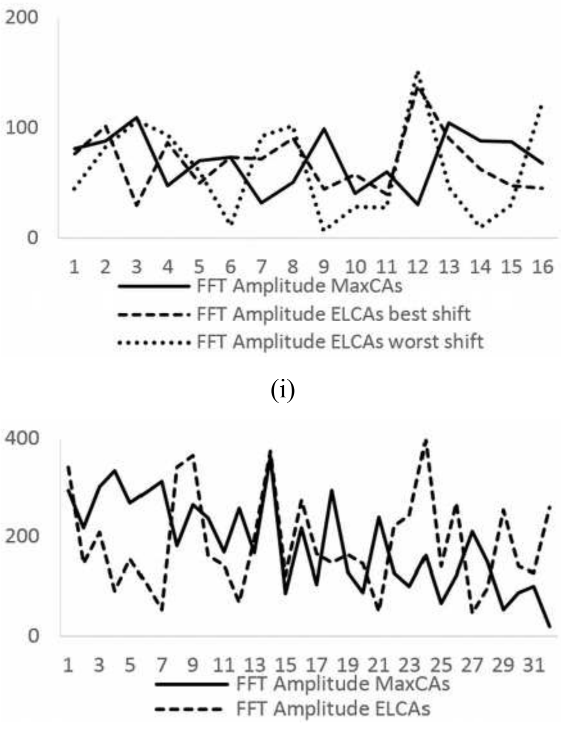
Automata Size	String of rules	
	MaxCAs	**Hybrid ELCAs**
5	150,150,90, 90,150	153,102,153,153,153
6	90,150,90, 150,90,150	153,102,153,153, 153,153

Table 5. Results obtained in RUNs tests [43]

Automata size	RUNs Tests results (*p*-values)	
	MaxCAs at 0_0	***Concatenated ELCAs at 0_0, no shift***
5	0.35965	0.5
6	0.40052	0.49686

The p-values in Table 5 were in the range, $0.025 < p < 0.975$, which failed to reject the null hypothesis of randomness that the data were not random [32, 43, 44].

As suggested in [36], appropriate shifting between cycles may result in the change for degree of independency of the ELCA cycles. Thus, appropriate shifting of the cycles for ELCAs were considered in FFT spectrum analysis. Changes in the auto-correationship were found for ELCAs for automata size 5, but no change was found for ELCAs for automata size 6. Fourier spectrums excluding the 0th frequency of FFT spectrum, both for MaxCAs and ELCAs, are given in Figure 2.



(i)

(ii)

Figure 2. FFT spectrum for ELCAs and MaxCAs. Notice in (ii) that the spectrum produced by the ELCA is closer to the white spectrum. The spectrum of the MacCA is close to 1/f noise

Only the FFT amplitude (power spectrum) was considered. Two are cases shown in Figure 2: i) The absolute value FFTs for ELCAs (the best shift and the worst shift are in dotted lines, while continuous line represents MaxCAs) for automata size 5; ii) The absolute-value FFTs for ELCAs with no shift (ELCAs are in dotted line and continuous line represents MaxCAs) for automata size 6. A reasonable amount of randomness was supported from FFT spectrums of ELCAs and MaxCAs.

The use of the Euclidean distance and cycle correlations between cycles were recommended in [36] to check the degree of independency (orthogonality) between cycles. The Euclidean distance d between two ELCA cycles was defined as the minimal distance between ELCA cycles when they are arbitrarily shifted one with respect to the other. Considering two cycles of equal length $C_{1L}=(C_{1,1}, C_{1,2}, \ldots, C_{1,h}, \ldots, C_{1,L})$ and $C_{2,L}=(C_{2,1}, C_{2,2}, \ldots, C_{2,h}, \ldots, C_{2,L})$; then [36],

$$d^2(C_{1L}, C_{2L})=min_k \sum_{h=1}^{L} (c_{1,h}-c_{2,h+k})^2 \quad (4)$$

where initial elements in C_{1L} and C_{2L} cycles are arbitrary chosen, k is shift, and by convention $C_{2,h+k}=C_{2,(h+k)} mod\, L$ (infinitely repeatable cycles) [36]. Also the (maximal) correlation of the cycles was employed for the similarity between the cycles. The maximal correlation was defined as [36],

$$C_{xy}=\frac{max_k \sum_{j=1}^{L} c_j c'_{j+k}}{\sqrt{\sum_{j=1}^{L} c_{j^2}} \sqrt{\sum_{j=1}^{L} (c'_j)^2}} \quad (5)$$

We applied the Equation 5 to ELCAs where the *max* is considered over all shifts. The correlation coefficient of Equation 5 for arbitrarily concatenated ELCAs (with shifts) and MaxCAs are in Figure 3. Arbitrary shifting of cycles for ELCAs were responsible in changes of correlations for automata size 5 at 0_0 boundary. String of rules used for generation of ELCAs and MaxCAs for Figure 3 were from Table 4.

For concatenated cycles $c1c2$ from MaxCAs, the best cases of the maximum absolute correlation coefficient is $r(1)=0.408$ and the minimum absolute correlation coefficient is $r(3)=0.054$. For ELCAs with concatenated cycles $c1c2c3c4$ with the best shift, the best cases of the maximum absolute correlation coefficient is $r(15)=0.204$ and the minimum absolute correlation coefficient is $r(5)=0.003$; for the worst shift, the best cases of the maximum absolute correlation coefficient is $r(5)=0.320$ and two minimum absolute correlation coefficients are $r(1 \text{ and } 2)\approx 0.02$. Correlation coefficients show that two shifts for ELCAs were present for automata size 5 such that, absolute value of the correlation coefficient (c) is less than 0.05, which is a low correlationship, whereas only one such low valued shift was found for MaxCAs.

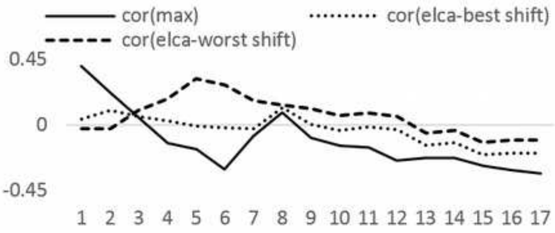


Figure 3. Auto-correlation of MaxCAs and ELCAs for automata size 5 at 0_0 boundary

Arbitrary shifting of cycles for ELCAs for automata size 6 were not responsible in changes in the correlations. Thus ELCA shifts were not considered in Figure 4. The CAs in Figure 4 use the sets of rules as in Table 4.

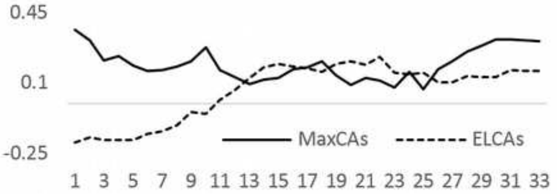


Figure 4. Auto-correlation of MaxCAs and ELCAs for automata size 6 at 0_0 boundary

For concatenated cycles $c1c2$ from MaxCAs, the best case of the maximum absolute correlation coefficient is $r(1)=0.366$ and minimum absolute correlation coefficient is $r(25)=0.073$. For ELCAs with concatenated cycles $c1c2c3c4c5c6c7c8$, the best case of the maximum absolute correlation coefficient is $r(22)=0.230$ and minimum absolute correlation coefficient is $r(11)=0.018$. One shift for ELCAs produces the absolute value of the correlation coefficient (c) less than 0.05, which is a low correlation value, whereas no such low value was found for MaxCAs.

Correlation analysis confirms that ELCAs have lower correlations and more number of shifts that produce correlation values ≈0 compared to the MaxCAs. As argued in [25, 36], the number of shifts lead to correlation values close to 0 imply the number of choices as independent keys in CDMA and thus a PRNG. Therefore, ELCAs may be used as PRNG and CDMA application.

5. Discussion

Simulations and correlation analysis with MaxCAs approve that MaxCAs at 0_0 boundary is more suitable to serve as PRNG compared to the MaxCAs achieved with 0_1, 1_0 and 1_1 boundaries; MaxCAs at 0_0 boundary is only comparable to LFSRs (see Table 2 and Section 3). This result is similar to the result found in [18] who compared CA-PRNG with LFSR-PRNG.

MaxCAs in all fixed boundary conditions demonstrated that a cycle of length $2^n - 1$ is realized irrespective of the boundary conditions. Hence there is no need to consider the boundary conditions for MaxCAs whenever the aim is only a cycle of length $2^n - 1$, not the degree of randomness of the cycle. No identical MaxCA cycles were achieved with 0_0, 0_1, 1_0 and 1_1 boundary conditions (refer Table 2).

ELCAs with same rule produced identical ELCA cycles irrespective of the boundary conditions [25, 26, 36]. Generation of identical cycles irrespective of the boundary conditions were not found for the MaxCAs (see Table 2, Annex). Hence, there is no concern for the boundary values while designing ELCA chips [25, 36] and also there is no need for assigning program memory for the software implementations of ELCAs. Therefore, ELCAs are better choice over MaxCAs for a cost efficient software and hardware design [25, 36].

Low correlation values were found for the concatenated ELCAs with reference to MaxCAs. A larger number of shifts with correlation value |c|≈0 were present in ELCAs than of MaxCAs. Moreover, ELCAs generated a larger number of independent cycles (keys) than of MaxCAs. Hence, more number of choices as independent key in CDMA applications may be found with ELCAs with reference to MaxCAs. Thus, the achieved results with ELCAs are beneficial for CDMA type applications compared to the MaxCAs.

6. Conclusions

The detailed investigation of PRNGs, specifically of PRNGs based on group CAs was carried out. It clarified aspects in the dynamics of MaxCAs and ELCAs. Analytical results found that ELCAs may be used as PRNG and are beneficial for uses in CDMA with respect to MaxCAs. Furthermore, ELCA-PRNGs may be used in BISTs, data security, and image cryptography. Concluding, further studies on group CAs may investigate the scopes in design of low cost and fast image processing applications in embedded systems as discussed in [16].

Acknowledgements

Research was carried out at “Gheorghe Asachi” Technical University of Iasi, Romania with ‘cLINK’ (EU ERASMUS MUNDUS) grant (Grant Agreement No: 212-26451001-001-EM Action 2 Partnerships). I thank to H.-N. Teodorescu who proposed the research topic, corrected and revised several versions of this paper.

REFERENCES

1. ADAMATZKY, A. I., **Hierarchy of Fuzzy Cellular Automata**, Fuzzy Sets and Systems, vol. 62, no. 2, 1994, pp. 167-174.

2. ADAMATZKY, A., C. J. MARTINEZ, **On Generative Morphological Diversity of Elementary Cellular Automata**, Kybernetes, Emerald Group Publishing, vol. 39, no. 1, 2010, pp. 72-82.

3. BETEL, H., P. FLOCCHINI, **On the Relationship Between Boolean and Fuzzy Cellular Automata**, Journal of Electronic Notes in Theoretical Computer Science (ENTCS), vol. 252, 2009, pp. 5-21.

4. CECCONI, F., R. LIVI, A. POLITI, **Fuzzy Transition Region in a One-dimensional Coupled-stable-map Lattice**, Physical Review E, vol. 57(3), 1998, pp. 2703-2712.

5. CHAUDHURI, P. P., D. R. CHOWDHURY, S. NANDI, S.

CHATTOPADHYAY, **Additive Cellular Automata: Theory and Applications**, vol. 1, Wiley-IEEE Computer Society, 1997.

6. CHEN, R.-J., J.-L. LAI, **Image Security System using Recursive Cellular Automata Substitution**, Pattern Recognition, vol. 40, 2007, pp. 1621-1631.

7. CHO, S.-J., et al., **Computing Phase Shifts of Maximum-length 90/150 Cellular Automata Sequences**, Cellular Automata, Springer, 2004, pp. 31-39.

8. COMPAGNER, A., A. HOOGLAND, **Maximum-length Sequences, Cellular Automata, and Random Numbers**, Journal of Computational Physics, vol. 71, no. 2, 1987, pp. 391-428.

9. CROUCH, A. L., D. P. MATTHEW, **Self Re-seeding Linear Feedback Shift Register (LFSR) Data Processing System for Generating a Pseudo-random Test Bit Stream and Method of Operation**, U.S. Patent No. 5, 383, 143, 17 Jan., 1995.

10. FLOCCHINI, P., F. GEURTS, A. MINGARELLI, N. SANTORO, **Convergence and Aperiodicity in Fuzzy Cellular Automata: Revisiting Rule 90**, Physica D: Nonlinear Phenomena, vol. 142, no.1-2, 2000, pp. 20-28.

11. GHOSH, S., T. BACCHAR, N. S. MAITI, I. MITRA, P. P. CHAUDHURI, **Theory and Application of Equal Length Cycle Cellular Automata (ELCCA) for Enzyme Classification**, 9th International Conference Cellular Automata for Research and Industry (ACRI 2010), Italy, Sep 21-24, 2010, pp. 45-57.

12. HELLEBRAND, S., J. RAJSKI, S. TARNICK, S. VENKATARAMAN, B. COURTOIS, **Built-in Test for Circuits with Scan Based on Reseeding of Multiple-polynomial Linear Feedback Shift Registers**, IEEE Trans. Computers, vol. 44, no. 2, 1995, pp. 223-233.

13. HORTENSIUS, P. D., R. D. MCLEOD, W. PRIES, D. M. MILLER, H. C. CARD, **Cellular Automata-based Pseudorandom Number Generators for Built-in Self-test**, IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems, vol. 8, no.8, 1989, pp. 842-859.

14. JIN, J., **An Image Encryption based on Elementary Cellular Automata**, Optics and Leasers in Engineering, vol. 50, 2012, pp. 1836-1843.

15. KARI, J., **Theory of Cellular Automata: A Survey**, Theoretical Computer Science, vol. 334, 2005, pp. 3-33.

16. KHALID BUKHARI, S. U., R. BRAD, C. BĂLĂ–ZAMFIRESCU, **Fast Edge Detection Algorithm for Embedded Systems**, Studies in Informatics and Control, vol. 23, no. 2, 2014, pp. 163-170.

17. KIM, H.-C., **Linear Feedback Shift Register, Multiple Input Signature Register, and Built-in Self-test Circuit using Such Registers**, U.S. Patent No. 5,938,784, 17 Aug, 1999.

18. KOKOLAKIS, I., I. ANDREADIS, P. TSALIDES, **Comparison between Cellular Automata and Linear Feedback Shift Registers based Pseudo-random Number Generators**, Microprocessors and Microsystems, vol. 20, no. 10, 1997, pp. 643-658.

19. KONISHI, T., K. KUNIHIKO, **Clustered Motion in Symplectic Coupled Map Systems**, Journal of Physics A: Mathematical and General, vol. 25, no. 23, 1992, pp. 6283-6296.

20. KRASNIEWSKI, A., P. SLAWOMIR, **Circular Self-test Path: A Low-cost BIST Technique for VLSI Circuits**, IEEE Trans. Computer-Aided Design of Integrated Circuits and Systems, vol. 8, no. 1, 1989, pp. 46-55.

21. LI, C.-Y., J.-S. CHEN, T.-Y. CHANG, **A Chaos-based Pseudo Random Number Generator using Timing-based Reseeding Method**, IEEE Int. Symp. Circuits and Systems (ISCAS 2006), Greece, May 21-24, 2006, pp. 1-4.

22. MARTINEZ, G. J., **A Note on Elementary Cellular Automata Classification, J. Cellular Automata, vol. 8, no. 3-4,** 2013, **pp. 233-259.**

23. MITRA, A., A. KUNDU, M. CHATTOPADHYAY, S. CHOTTOPADHYAY, **An Analysis of Equal Length Cellular Automata (ELCA) generating Linear Rules for Applications in Distributed Computing,** J. Cellular Automata, vol. 10, no. 1-2, 2015, pp. 95-117.

24. MITRA, A., A. KUNDU, **Analysis of Sequences Generated by ELCA-type Cellular Automata targeting Noise Generation**, 19th International Conference on System Theory, Control and Computing (ICSTCC 2015), Romania, Oct 14-16, 2015, pp. 883-888.

25. MITRA, A., H.-N. TEODORESCU, **Detailed Analysis of Equal Length Cellular Automata with Fixed Boundaries**, Journal of Cellular Automata, Old City Publishing, 2016, accepted.

26. MITRA, A., H.-N. TEODORESCU, **Detailed Analysis of CAs with Fixed Boundaries** (Submitted), pp. 1-74, http://iit.academiaromana-is.ro/papers/iit_art16.html (accessed on 24.02.2016).

27. NANDI, S., B. K. KAR, P. P. CHAUDHURI, **Theory and Application of Cellular Automata in Cryptography**, IEEE Trans. Computers, vol. 43, no. 12, 1994, pp. 1346-1357.

28. SUTNER, K., **Classification of Cellular Automata**, Encyclopedia of Complexity and Systems Science, Springer, 2009, pp. 755-768.

29. TANG, K. W., W. K. TANG, K. F. MAN, **A Chaos-based Pseudo-random Number Generator and Its Application in Voice Communications**, International Journal Bifurcation and Chaos, vol. 17, no. 3, 2007, pp. 923-933.

30. TEODORESCU, H.-N., **Self-organizing Uncertainty-based Networks**, In: Systematic Organisation of Information in Fuzzy Systems. Computer and Systems Science, NATO Science Series, vol. 184, 2003, pp. 131-159.

31. TEODORESCU, H.-N., **Pattern Formation and Stability Issues in Coupled Fuzzy Map Lattices**, Studies in Informatics and Control, vol. 20, no. 4, 2011, pp. 345-354.

32. TEODORESCU, H.-N., **Characterization of Nonlinear Dynamic Systems for Engineering Purposes - A Partial Review**, International Journal of General Systems, vol. 41, no. 8, 2012, pp. 805-825.

33. TEODORESCU, H.-N., **Iterated Maps with Exponential Slopes for Nonlinear Dynamics Generation**, 2014 IEEE International Conference on Applied Electronics (AE 2014), Pilsen, Sep 9-10, 2014, pp. 293-296.

34. TEODORESCU, H.-N., **Generalized Binary Tent-maps for Built-in Self-test for Wearable Medical Devices**, 5th IEEE E-Health and Bioengineering Conf. (EHB 2015), Romania, Nov 19-21, 2015, pp. 1-4.

35. TEODORESCU, H.-N., **Type-D Fuzzy CAs for Medical and Social Sciences**, 5th IEEE E-Health and Bioengineering Conf. (EHB 2015), Iasi, Romania, Nov 19-21, 2015, pp. 1-4.

36. TEODORESCU, H.-N., **On the Regularities and Randomness of the Dynamics of Simple and Composed CAs with Applications**, Romanian Journal of Information Science and Technology, Romanian Academy, vol. 18, no. 2, 2015, pp. 166-181.

37. TOFFOLI, T., **Cellular Automata as an Alternative to (rather than an approximation of) Differential Equations in Modeling Physics**, Physica D, vol. 10, no. 1, 1984, pp. 117-127.

38. WOLFRAM, S., **Theory and Applications of Cellular Automata**, World Scientific Press, 1986.

39. WUENSCHE, A., M. LESSER, **The Global Dynamics of Cellular Automata**, Addison-Wesley, 1992.

40. XIAOYANG, Y., S. YANG, Y., YANG, Y. SHUCHUN, C. HAO, G. YANXIA, **An Encryption Method for QR Code Image Based on ECA**, Int. J. Security and Its Applications, Science & Engineering Research Support Society, vol. 7, no. 5, 2013, pp. 397-406.

41. YE, R., W. ZHOU. **A Chaos-based Image Encryption Scheme using 3D Skew Tent Map and Coupled Map Lattice**, Int. J. Computer Network and Information Security, vol. 20, no. 4, 2012, pp. 38-44.

42. YIN, R., J. YUAN, Q. YANG, X. SHAN, X., WANG, **Gemstone: A New Stream Cipher using Coupled Map Lattice**, 5th Int. Conf. Information Security and Cryptology (Inscrypt 2009), China, Dec 12-15, 2009, pp. 198-214.

43. https://home.ubalt.edu/ntsbarsh/business-stat/otherapplets/Randomness.htm (accessed on 26.02.2016).

44. http://www.real-statistics.com/non-parametric-tests/one-sample-runs-test/ (accessed on 26.02.2016)

ANNEX

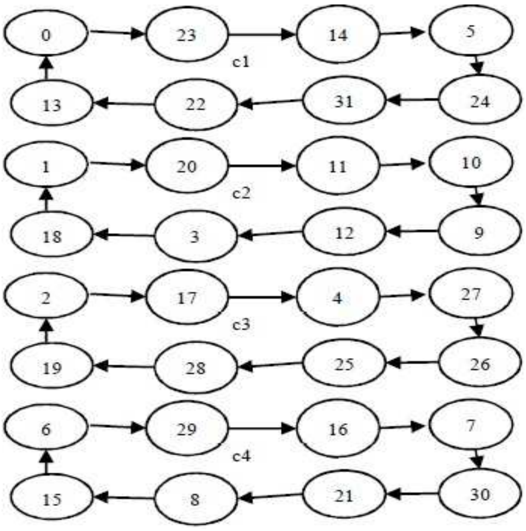


Figure A1. ELCAs at 0_0 and 1_0 boundary, automata size 5 with rule 153,102,153,153,153

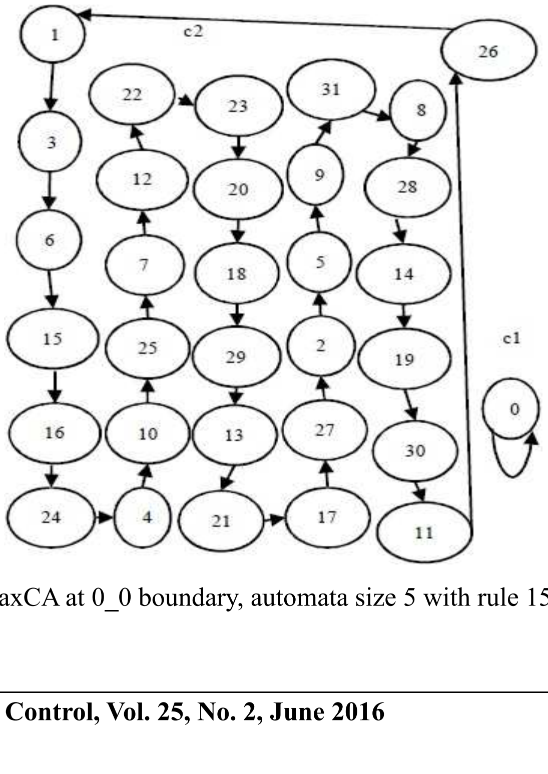


Figure A2. MaxCA at 0_0 boundary, automata size 5 with rule 150,150,90,90,150

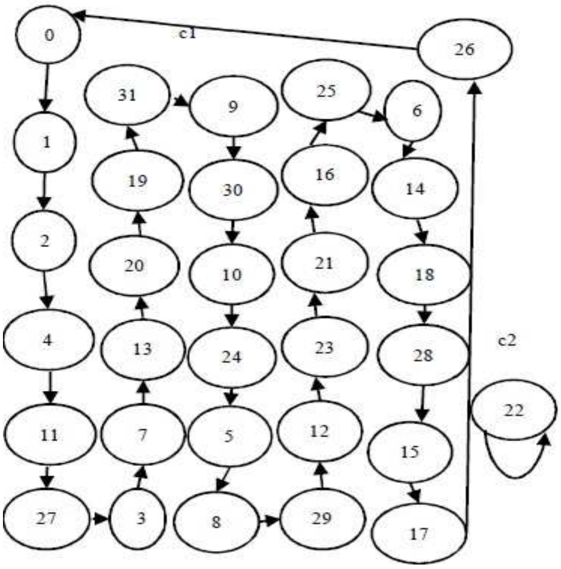


Figure A3. MaxCA at 0_1 boundary, automata size 5 with rule 150,150,90,90,150

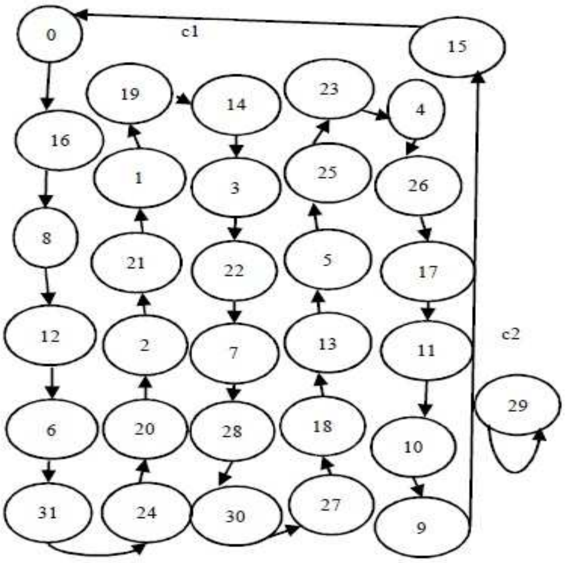


Figure A4. MaxCA at 1_0 boundary, automata size 5 with rule 150,150,90,90,150

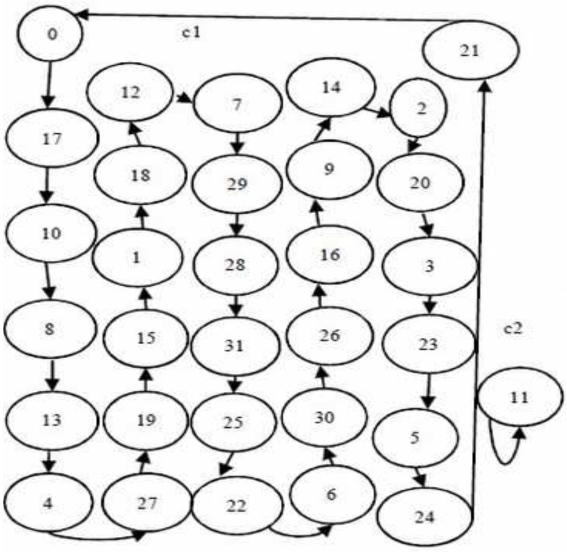


Figure A5. MaxCA at 1_1 boundary, automata size 5 with rule 150,150,90,90,150