FEEDBACK SHIFT REGISTERS AS CELLULAR AUTOMATA BOUNDARY CONDITIONS

K. Salman

Middle Tennessee State University
Murfreesboro, TN 37132, USA
ksalman@mtsu.edu

ABSTRACT

We present a new design for random number generation. The outputs of linear feedback shift registers (LFSRs) act as continuous inputs to the two boundaries of a one-dimensional (1-D) Elementary Cellular Automata (ECA). The results show superior randomness features and the output string has passed the Diehard statistical battery of tests. The design is good candidate for parallel random number generation, has strong correlation immunity and it is inherently amenable for VLSI implementation.

KEYWORDS

Linear Feedback Shift Registers Cellular Automata Boundary Conditions Diehard

1. INTRODUCTION

Both LFSRs and CAs have been used extensively in a wide area of applications, particularly random number generation for Mont Carlo simulation, communications, cryptography and network security [1-8]. LFSRs, albeit simple in structure and design were proven to have comparatively weak statistical featured when utilized in the production of pseudo random numbers [2]. The weakness can be attributed to the linearity of the exclusive-or function used in the feedback network.. Additionally, non-linear feedback shift registers have their problems as well [1]. On the other hand, a uniform 1-D CA, where one rule is implemented throughout the spatiotemporal evolution of the CA, have shown unique and useful characteristics, and have been suggested by [3,4] and others for use in random number generation. A notable impediment however, is the input to the boundaries of the CA, where it is confined to a limited span. For example, a necessary condition for an unbounded (bi-infinite) 1-D ECA to produce a pseudo random contiguous string of length x Î ¥ is to have a span of $x + 2$ cells long. Hence, a relatively long string of output will render the CA overly unsuitable. However, a shorter span K Î ¥ implies a constant span length and therefore a fixed and limited number of cells. Hence, inputs are needed to feed the two extremities of the ECA. One approach attempted to solve this problem is to make the ECA evolve in a continuous loop (referred to as autonomous or *periodic*), in which case the peripheral cells (i.e. the last and the first extreme cells) are made adjacent to

Sundarapandian et al. (Eds) : CSE, CICS, DBDM, AIFL, SCOM - 2013
pp. 11–21, 2013. © CS & IT-CSCP 2013 DOI : 10.5121/csit.2013.3302

each other, as depicted in figure 1. An alternative technique used earlier in the literature is to feed the peripheral cells with fixed inputs. Figure 2 depicts the various boundaries from $GF(2)$ used.

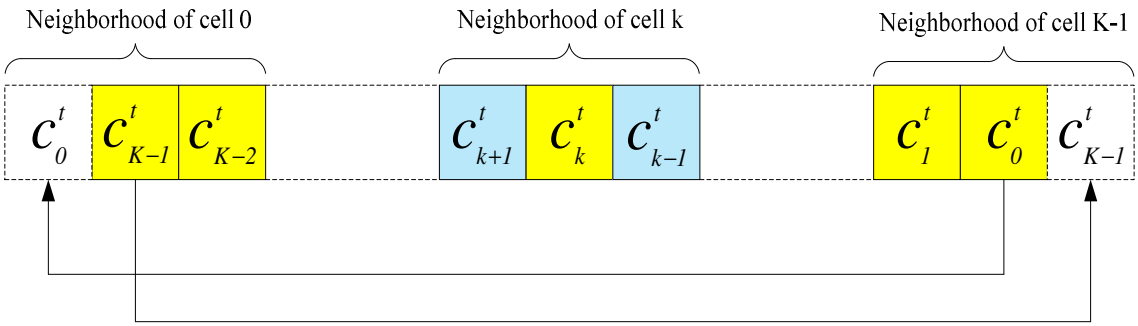

Figure 1, ECA *periodic* boundary configuration

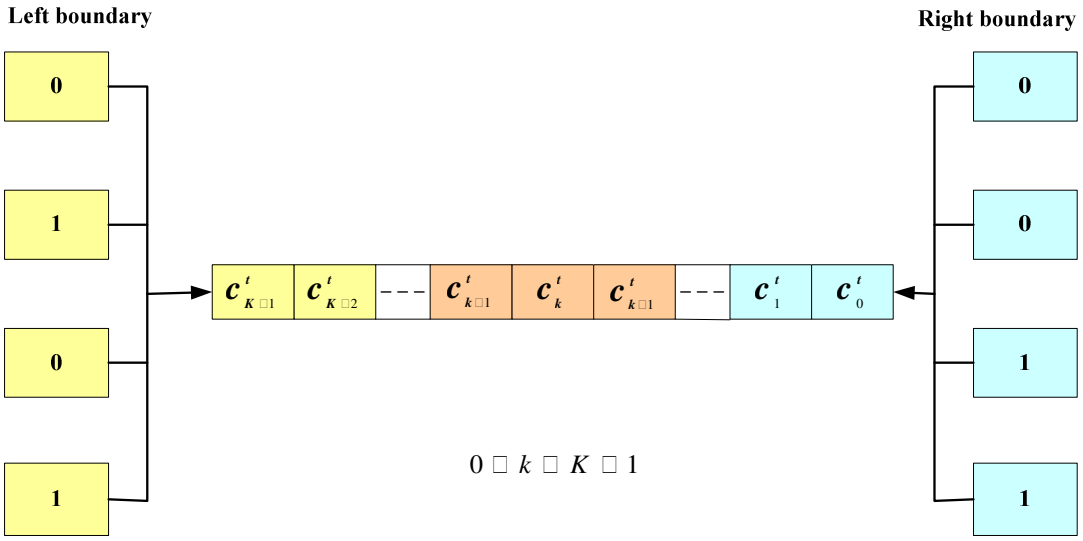

Figure 2. Common one dimensional cellular automaton fixed boundary conditions.

All these methods running under chaotic rule 30 on uniform one-dimensional ECAs have produced much shorter periods than the LFSR and drastically failed the well-established Diehard battery of tests [7]. This paper reports the findings of a new method whereby a pair of uncorrelated LFSRs are used to generate the two boundary conditions. With this design the output string of the center bit of the ECA evolving for time steps$T = 2^K$, where K is the span length, has passed the Diehard battery of tests and produced attractive parallelism and correlation properties. This paper is arranged such that the theoretical analysis and the proposed approach are included in the section called Preliminaries, while the results section discusses the improvement in the performance of the ECA. The conclusion finalizes the outcome of the paper.

2. PRELIMINARIES

For the purpose of this paper we will restrict our attention towards one dimensional cellular automaton. The cells are arranged on a linear finite lattice, with a symmetrical neighborhood of three cells and radius $r = 1$. Each cell takes its value from the set $G = \{0,1,\ldots,p\}$ and we let $p = 2$. All cells are updated synchronously and the cells are restricted to local neighborhood interaction with no global communication. The ECA will evolve according to one uniform neighborhood transition function, which is a local function (rule) $f : G^{2r+1} \to G$ where the ECA evolves after certain number of time steps *T*. Out of a total of $p^{p^{2r+1}}$ rules we use rule 30 as suggested by Wolfram and adopt his numbering scheme [3,4]. It follows that a 1-D ECA is a linear register of $K, K \in \infty$, memory cells. Each cell is represented by c_k^t, where $k = [1:K]$ and $t = [1,\infty)$, that describes the content of memory location k at time evolution step t. Since $p = 2$ the cell takes one of two states from $GF(2)$. This implies the applicability of Boolean algebra to the design over $GF(2)$. A minimum Boolean representation of chaotic Rule30 in terms of the relative neighborhood cells is:

$c_k^{t+1} = c_{k+1}^t \oplus (c_k^t + c_{k-1}^t)$ or $c_i^{t+1} = c_{k+1}^t + c_k^t + c_{k-1}^t + (c_k^t \times c_{k-1}^t) \bmod 2$, where $2 \le k \le K-2$, as depicted in figure 3.

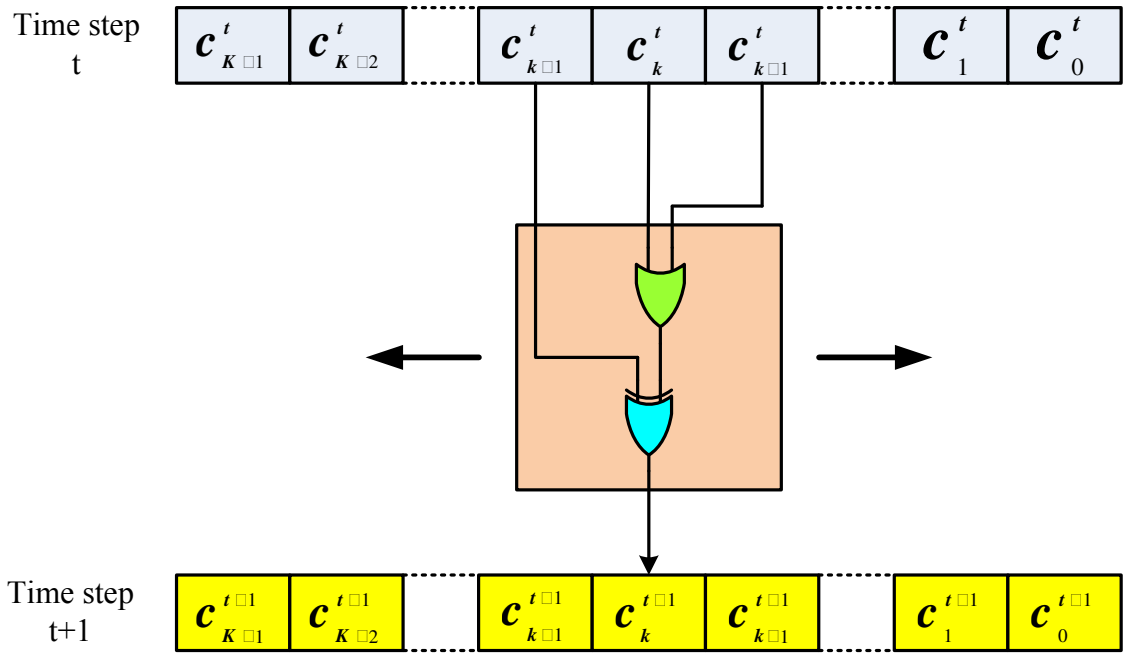

Figure 3. Illustration of Rule 30 operating on the present state of neighborhood of time step *t* to produce the next state cell of time step *t+1*.

Furthermore, since the ECA is actually a finite state machine then the present state of the neighborhood of cell c_k^t, $(c_{k+1}^t, c_k^t, c_{k-1}^t)$ at time step t and the next state c_k^{t+1} at time step $t+1$, can be analyzed by the *state transition table* and the *state diagram* depicted in figure 4.

Present State c_k^t	Neighborhood $c_{k+1}^t - c_{k-1}^t$			
	0-0	0-1	1-1	1-0
0	**0**	**1**	**0**	**1**
1	**1**	**1**	**0**	**0**

Next State

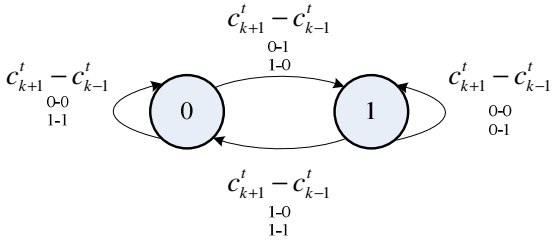

Figure 4, State machine analysis of Rule 30.

It can be seen from above that in order to evolve from the present time step t to the next time step $t+1$, each cell at lattice location k would require the present state of itself c_k^t as well as the present state of the other two cells in its neighborhood c_{k+1}^t and c_{k-1}^t. Therefore, if the ECA is allowed to expand freely, leftwise and rightwise the total number of cells at each time step $t+1$, say $K \in \mathbf{N}$ would need $K+2$ cells at time step t. For example to produce the string $T = 1101110$ from the evolution of the unbounded ECA of span length W= ¥ by the concatenation of the center cell would require a span of length W= $2T + 1$, i.e. 13 cells, as can be seen in figure 5. Hence, if the ECA is unbounded then for a string of *T-bits* would require the evolution of the ECA of span $2T + 1$ as illustrated in figure 5. This condition will eventually lead to an unpractical span of the ECA. Hence, it is imperative that the ECA has to be bounded. The open literature is rich with research on fixing the size of the ECA and provides data for the extreme cells of the bounded ECA. Figure 2 gives a brief account of some common fixed boundary conditions. Figure 6 categorizes the boundary conditions to include the new boundary condition proposed in this paper using LFSR as a new source for boundary conditions. The fixed boundary conditions are already illustrated in figure 1. The miscellaneous category includes either some ad hoc permutations of the fixed boundaries or some fixed sequence of inputs. The autonomous category, commonly referred to as *periodic*, make the extreme cells of the ECA adjacent, as illustrated in figure 2. The resultant ECA becomes circular as depicted in figure 8, and with time evolution it can be visualized as a cylinder. The expression for the extreme left and right cells at time step $t+1$ are, respectively

$c_{K-1}^{t+1} = c_0^t \oplus (c_{K-1}^t + c_{K-2}^t)$ and $c_0^{t+1} = c_{K-1}^t \oplus (c_1^t + c_0^t)$.

The published results of these different types of boundary conditions produced poor results when used as a source of generating random numbers. In this paper we are proposing a new source for the boundaries. We have used the well established LFSR as the source of inputs to the extreme cells of the fixed 1-D ECA, as shown in figure 9. A LFSR of span N memory cells can be described by the following simple recurrence equation,

$L_0^{t+1} = a_0 L_0^t \oplus a_1 L_1^t \oplus \cdots a_i L_i^t \oplus \cdots \oplus a_{N-1} L_{N-1}^t$ where $a_i \in GF(2)$.

The choice of a_i are exactly the coefficients of a *primitive polynomial* of degree N. The extreme cells of the new design at time step $t+1$ can now be described by

$c_{K-1}^{t+1} = c_{K-2}^{t} \text{ Å } (L_0^t + c_{K-1}^t)$ and $c_0^{t+1} = R_0^t \text{ Å } (c_0^t + c_1^t)$

0000001000000
0000111000 0
0011 00100
1101111
00100
111
0

Figure 5, Simple time evolution of an unbounded 1-D ECA under GF(2).

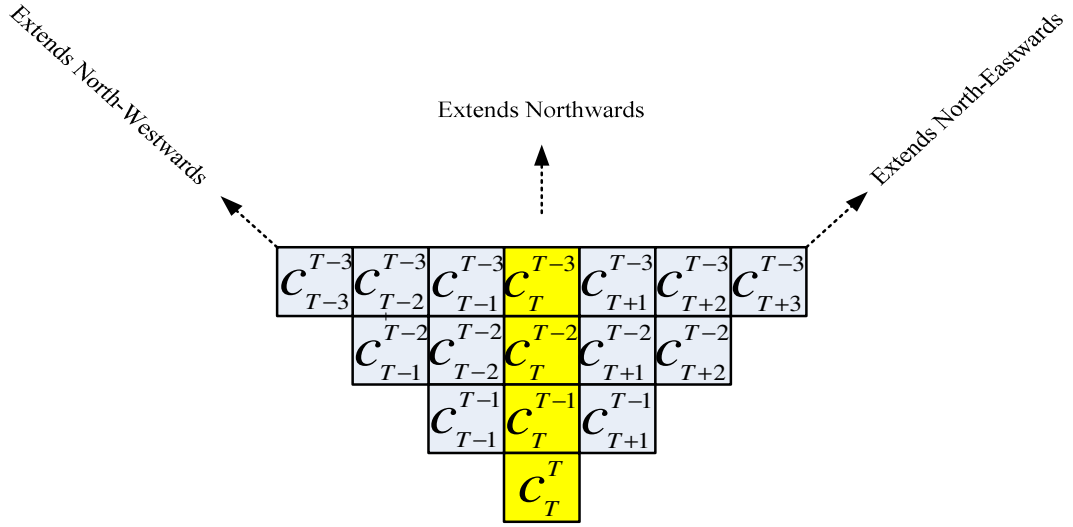

Figure 6, Illustration of time evolution of a bi-infinite 1-D ECA.

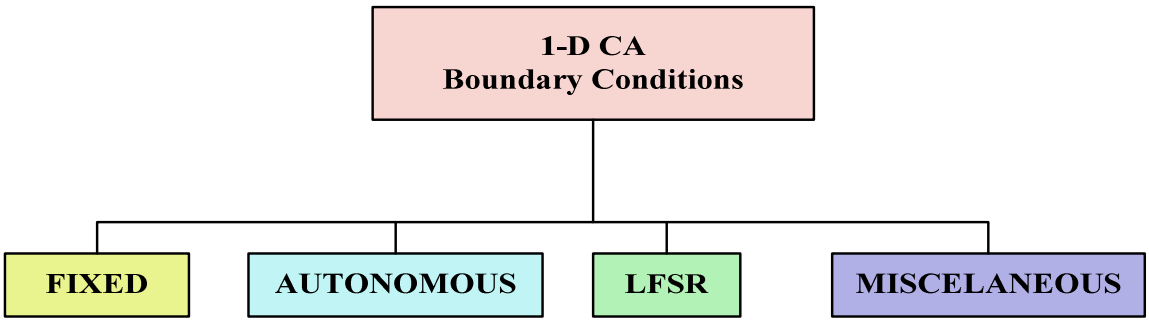

Figure 7, Categorization of a fixed span 1-D ECA boundary condition sources.

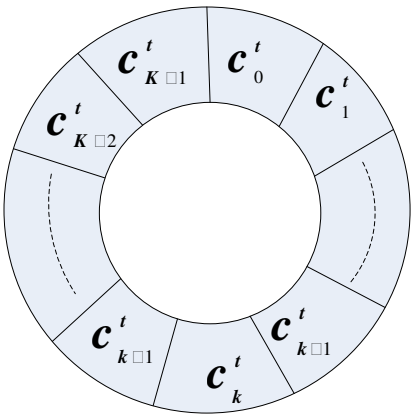

Figure 8, Another illustration of the autonomous (periodic) boundary conditions.

3. RESULTS

In order to test the statistical properties of the new proposed design, we developed a suite of programs emulating all known types of boundary conditions for wide range of spans for both the ECA and the LFSRs used as boundaries. We will include snapshots of results obtained for representative runs on the Diehard battery of tests [8], which has been adopted in this paper due to its well established stringent requirements on the statistical randomness of the output string. Due to the restrictions imposed by this test the ECA span K has to be at least 27-bit long evolving for a minimum of 2^K time steps. Table 1 shows the results of running the diehard tests on the *periodic* boundary conditions for spans 32, 33, up to 512. The ECA running in the *periodic* boundary mode has not been able to pass all the tests even for a span of 256-bits. The results of running the diehard tests on the fixed boundary conditions have totally failed and therefore not worth reporting here. The results of the diehard tests on the ECA using two LFSRs of span 3-bit each as the boundary conditions for various increasing spans of the ECA did not show any significant change and therefore it is not reported. It is clear that such boundary conditions will give slightly better results than fixed boundary conditions but do not show improvement over the *periodic* boundary condition. However, when the LFSR span increased to 15-bits for both registers some improvement were noticeable as shown by the results reported in table 2. Excellent results were obtained when the span of the LFSRs were increased to match the span of the ECA. The ECA has passed all tests with extremely superior p-values, as shown in table 3.

4. CONCLUSIONS

The string of contiguous stream data collected from the evolution of the 1-D ECA for the center cell of various boundary conditions were tested by the 15 Diehard battery of tests. The various fixed boundary conditions failed the diehard tests almost completely and were considered unworthy reporting. The autonomous boundary conditions have shown far better statistical properties than the fixed boundary conditions. However, it still falls far below the minimum requirements of the diehard tests for reliable considerations in producing dependable random numbers even for long spans of the ECA (512-bit). When the boundaries were fed from LFSRs results did not improve significantly until the span of the LFSRs were comparable to that of the ECA. The results steadily improved up to the upper bound when the two spans were comparable.

It can be concluded that the new approach can produce random numbers even at modest size of the ECA (i.e. 27-bit). More in depth study of the results show that the new approach produced superior p-values than the best of the autonomous results. Further assertion of the diehard results are also apparent from visual inspection of the spatiotemporal output as can be seen from figure 10. It is easy to expect that the fixed boundary conditions cause a ECA running under Rule 30, which is in group III (i.e. the chaotic class) to evolve into Group I or II (i.e. point attractors or limit cycles with extremely small periods), according to Wolfram's ECA classification [4-5]. Therefore, such boundary conditions preclude these ECAs from achieving strong random number generators. The autonomous (*periodic*) boundary conditions, on the other hand gave better results which is indicative of better distribution during ECA evolution. However, the periods of this type were far lower than the maximum length obtainable from LFSRs. The proposed design have an added favorable feature when considering the initial seeds. It is clear that all the possible 2^K *K-tuples* can be used as seeds including the all 0's and all 1's that usually yield quiescent states. This is not possible with any other known boundary conditions including the autonomous type. All the tests were performed using a single one as the initial seed. This is admittedly not the case in a practical situation. Some patterns were observed during the initial evolution of the ECA but did not persist. Although these initial patterns did not negatively impact the diehard tests it was found that avoiding the use of trinomials for the LFSRs and replace them with primitive polynomials of better distribution of the coefficients managed to remove these patterns. One salient feature of the design is the almost total destruction of the cross-correlation between different cells as shown in figure 11(a). This strong correlation is an inherent feature of LFSRs that can be observed as maximum and constant between any two cells of the LFSR and as linear patterns on the diagonal ridge between the outputs of the LFSR cells, figure 11(b). An immediate consequence is the ability to use the ECA as a parallel source of pseudo random numbers that can be considered a strong candidate for parallel data compaction (signature analysis) in VLSI testing [8]. This is justified since the structure as depicted in figure 9 presents a simple memory-based and inherently parallel design that is amenable to large scale integration. Inspection of rule 30 reveals that the function is surjective. Since reversibility implies bijection, it follows that the proposed system is not clear cut reversible. Hence analytical techniques may not be available to adequately and inversely describe the spatiotemporal data evolution in at most polynomial time. For a LFSR of span N , there are $(2^N - 1)$ *N*-tuple words as seeds. The two LFSRs are uncorrelated and running independently and synchronously, hence the effective input computational complexity from these registers to the ECA would be $(2^N - 1)^2$. The 1-D ECA of span *K* can be initialized with a total of 2^K *K*-tuple words as initial seeds. There are a total of 2^{2^3} rules, which is the rule space of a1-D ECA. Thus the computational asymptotic complexity of the system is

$O((2^N - 1)^2 \cdot 2^{2^3} \cdot 2^K) \approx O(2^{3K})$ for $K \sqsubset N$, as compared to 2*N* for the LFSR and $O(2^K)$ for a 1-D ECA with autonomous boundary conditions.

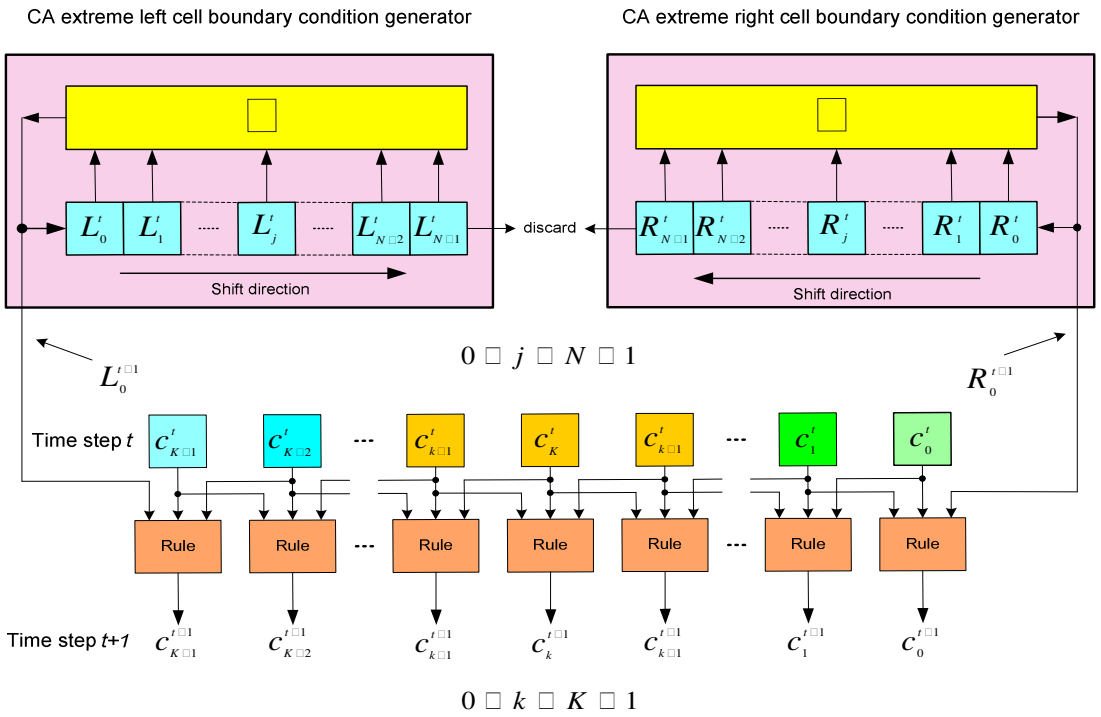

Figure 9, Block Diagram Representation of the Proposed ECA System, reversing the order of indexing, such that the most significant cell is the extreme left hand cell and vice versa for the extreme right hand cell which becomes the least significant cell.

Table 1, Diehard tests results for 1-D ECA of variable spans and with autonomous boundaries.

P_VALUES	S32	S33	S64	S128	S256	S512
T_1	0.4913	0.6089	0.4871	0.5683	0.5976	0.7166
T_2	1	1	1	1	1	1
T_3	0.759	0.7895	0.5035	0.4525	0.643	1
T_4	1	1	1	1	1	1
T_5	1	1	0.4973	0.5195	0.5777	0.7068
T_6	1	1	0.804	0.7769	0.4856	0.7756
T_7	1	1	0.999	1	1	1
T_8	1	1	1	1	1	1
T_9	1	1	0.6235	1	0.431	0.3777
T_10	1	1	0.4376	0.6587	0.489	0.5068
T_11	1	1	0.5549	0.5016	0.457	0.4066
T_12	1	1	1	0.019	1	1
T_13	0.3985	0.4106	0.337	1	0.2194	0.375
T_14	1	1	1	0.3576	1	1
T_15	1	0.8809	1	1	0.8697	0.8524
Summary	**3 pass 12 fail**	**4 pass 11 fail**	**8 pass 7 fail**	**8 pass 7 fail**	**9 pass 6 fail**	**8 pass 7 fail**

Table 2, Diehard tests results for 1-D ECA of variable spans and with two LFSRs as boundaries of span15-bit each.

	S27	S28	S29	S30	S64	S128	S256
T_1	0.8893	0.5869	0.6834	0.005	0.2502	0.5655	0.5638
T_2	1	1	1	1	1	1	1
T_3	0.402	0.2845	0.52	0.485	0.681	0.0795	0.144
T_4	0.997	1	1	1	1	1	1
T_5	1	1	1	1	0.4418	0.5753	0.4226
T_6	1	1	1	1	0.8211	0.6235	0.7855
T_7	1	1	1	1	0.8848	0.992	1
T_8	1	1	1	1	1	1	1
T_9	1	1	1	1	0.4273	0.0373	0.5168
T_10	1	1	1	1	0.2837	0.00035	0.0049
T_11	1	1	1	1	0.2291	0.1859	0.0362
T_12	1	1	1	1	1	1	1
T_13	1	0.0537	0.6473	0.4943	1	0.1131	0.0442
T_14	1	1	1	1	1	1	1
T_15	1	1	1	1	1	1	0.9056
Summary	3 pass 12 fail	3 pass 12 fail	3 pass 12 fail	3 pass 12 fail	8 pass 7 fail	9 pass 6 fail	10 pass 5 fail

P_VALUES

Table 3, Diehard tests results for ECA of variable spans and with 2LFSRs for boundaries of same as the ECA spans.

	S27	S28	S32	S64	S128
T_1	0.242	0.43	0.3046	0.2398	0.2695
T_2	0.0744	0.4376	0.1128	0.5284	0.2123
T_3	0.8442	0.6365	0.3417	0.3317	0.5543
T_4	0.4688	0.47	0.4323	0.2713	0.0628
T_5	0.52235	0.4697	0.5166	0.4421	0.5454
T_6	0.4755	0.32	0.5486	0.5584	0.4654
T_7	0.6092	0.485	0.3151	0.4642	0.6849
T_8	0.5581	0.5083	0.4601	0.5009	0.6135
T_9	0.2253	0.6181	0.6947	0.5722	0.5413
T_10	0.8818	0.2469	0.9452	0.728	0.0897
T_11	0.7111	0.3404	0.1944	0.7524	0.5147
T_12	0.456	0.423	0.9646	0.9847	0.1522
T_13	0.3026	0.1387	0.2413	0.1063	0.3202
T_14	0.2085	0.6276	0.1753	0.3521	0.4801
T_15	0.343	0.5539	0.7578	0.4428	0.4845
Summary	15 pass 0 fail	15 pass 0 fail	15 pass 0 fail	15 pass 0 fail	15 pass 0 fail

P_VALUES

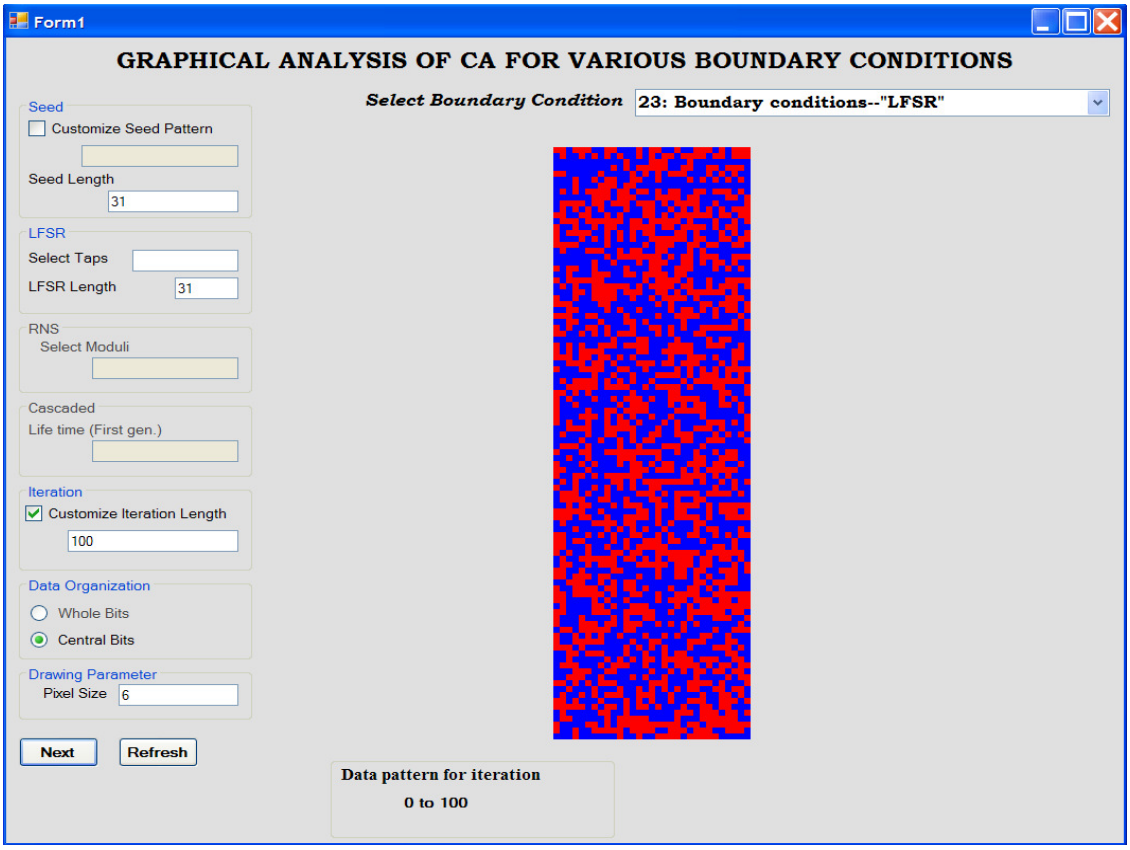

Figure 10, Spatiotemporal output of 1-D ECA span 31-bit with two LFSRs as boundary inputs source of the same span. One hundred time steps is shown.

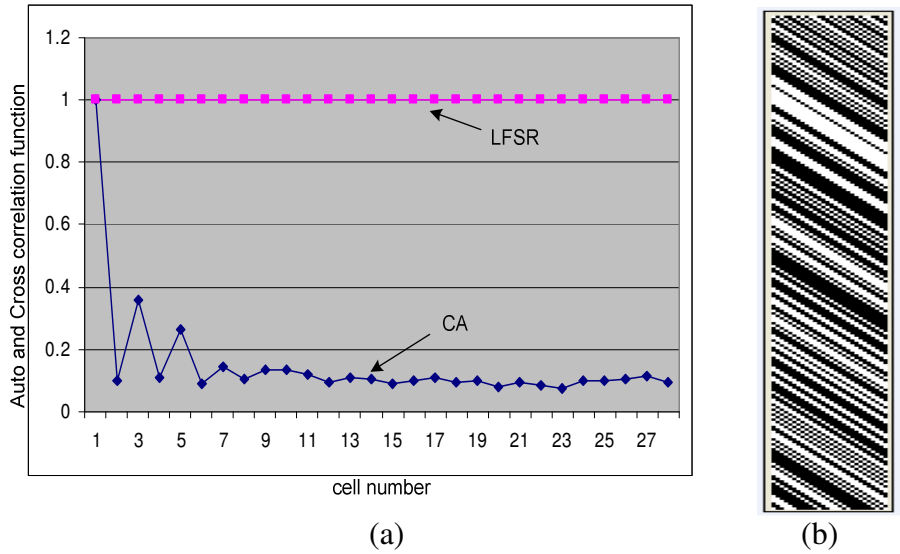

Figure 11, Spatiotemporal images of ECA28, LFSR28 and correlation properties.

REFERENCES

[1] SIEGENTHALER, T. : 'Correlation Immunity of Nonlinear Combining Functions for Cryptographic Applications', IEEE Transactions on Information Theory, Vol. IT-30, No. 5, September 1984, pp. 776-780.

[2] GUSTAVSON, F. G.: 'Analysis of the Berlekamp-Massey Linear Feedback Shift-Register Synthesis Algorithm.' IBM J. Res. Dev. 20, Number 3, pp. 204-212, 1976.

[3] WOLFRAM, S.: 'A New Kind of Science'. Champaign, IL: Wolfram Media, 2002.

[4] WOLFRAM, S.: 'Random Sequence Generation by Cellular Automata', Advances in Applied Mathematics. Volume 7, Issue 2, June 1986, Pages 123-169.

[5] SEREDYNSKI, FRANCISZEK, BOUVRY PASCAL, and ZOMAYA, ALBERT Y.: 'Cellular automata computations and secret key cryptography', Parallel Computing, Vol. 30, 2004, pp. 753-766.

[6] LLACHIINSKI, Andrew: 'Cellular Automata: A Discrete Universe', World Scientific, 2001, pp. 94.

[7] HORTENSIUS, P.D., McLEOD, and CARD, H.C.:'Parallel Random Number Generation for VLSI Systems Using Cellular Automata', IEEE Transactions on Computers, Vol. 38, Issue 10, October 1989, pp. 1466-1473.

[8] 'The Marsaglia Random Number CDROM including the Diehard Battery of Tests of Randomness', Florida State University, http://i.cs.hku.hk/~diehard/