Network of Locally Coupled Cellular Automata with Random Memory Models

Emre Göncü and Müştak E. Yalçın

Department of Electronics and Communication Engineering,
Istanbul Technical University
egoncu@itu.edu.tr, mustak.yalcin@itu.edu.tr

Abstract

Cellular Automata with Random Memory (CARM) is a new Cellular Automata model which has been recently inroduced. In this model, instead of memories, delay lines are used. Therefore, how much previous times to be considered is a random process. Implementation of CARM model is not required any special hardware since delay in discrete time systems can be easily generated from a random delay characteristics of wires and transistors in programmable logic devices. In this paper, a network of locally coupled CARM model has been studied. Each CARM model is thought to be a random number generator and here we will present that these generators can synchronise with local coupling keeping random behaviour of each cells in the network.

1. Introduction

Cellular Automata (CA) are discrete dynamical systems used in many kinds of applications like modelling, image processing, random number generating *etc*.

The next states of the cells depend on only the current states of the cells, in a standard CA. However, in a Cellular Automata with Memory (CAM), the next states of the cells rely on the previous states, in addition to current states of the cells. The first known CAM is the model proposed by Edward Fredkin [1]. In addition, many kinds of CAM models have been proposed, so far [2][3][4][5].

Cellular Automata with Random Memory (CARM) is a new CA model which has been recently proposed [6]. Considering the dynamics of a CARM, the next states of the cells depend on randomly chosen previous or current states, instead of specified previous or current states of the cells in the CAM manner.

In this paper, outputs of two CARMs with the same parameters except the probabilistic parameters which are the random delay values are tried to distinguish. For this manner, the well-known statistical test named Poker Test is chosen as a merit function to distinguish the random outputs of CARMs. The experiments show that the new method is very useful to distinguish CARM with different probabilistic parameters. Furthermore, locally coupled CARM networks are analysed in this paper. Interestingly, experiments show that after local coupling, two CARMs are synchronized such that they are generates outputs with the similar statistical characteristic.

The paper is organised as follows. In Section II, and III abstract form of CA and CAM models have been given. In Section IV, definitions of a CARM and the sub-models of it have been given. In Section V, the statistical characteristics of an CARM have been extracted using Poker Test. Furthermore, ,in Section VI, locally coupled CARMs have been proposed and analysed by their results of the Poker Tests. Finally, Section VII concludes the paper with a short summary.

2. Cellular Automata (CA)

A d-dimensional Cellular Automaton (CA) can be defined with a cellular space $\mathbb{Z}^d$, a set of state Q, a neighbourhood V and a local rule f. The neighbourhood V is defined as follows,

$$V = (i_1, i_2, \ldots, i_s),\ i_1, \ldots, i_s \in \mathbb{Z}^d.$$

The states of the cells are determined for every time step according to the local rule, f, such that $f : Q^s \to Q$, where s denotes the number of elements in neighbourhood V. Hence the dynamics of an CA is given as follows

$$\alpha_i(n+1) = f(\alpha_{i+i_1}(n), \alpha_{i+i_1}(n), \ldots, \alpha_{i+i_s}(n)) \quad (1)$$

where $\alpha_i(n)$ denotes the state of cell sited at point $i \in \mathbb{Z}^d$ for time step n.

An Elementary Cellular Automata (ECA)[7] is defined by $\mathbb{Z}$, set of states $Q = \{0, 1\}$, neighbourhood $V = (-1, 0, 1)$ and a elementary local rule $f : Q^3 \to Q$. Therefore the dynamics of an ECA is given by

$$\alpha_i(n+1) = f(\alpha_{i-1}(n), \alpha_i(n), \alpha_{i+1}(n)). \quad (2)$$

An example of an elementary local rule, named Rule 150 is given in Fig. 1 (black boxes denotes 1, white boxes denotes 2). Each triple value at the upper row of the figure determine the all combinations of the states $\alpha_{i-1}(n)$, $\alpha_i(n)$ and $\alpha_{i+1}(n)$, from left to right. $\alpha_i(n+1)$ values assigning to the each above triple are given at the lower row of the Fig. 1. Notice that the decimal value of the lower row is 150 .

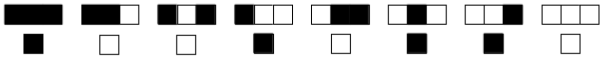

Figure 1. Wolfram notation of Rule 150. (Black squares denote state 1, white squares denote state 0)

Behaviour of an ECA can be seen by its evolution figure. In Fig. 2, evolution of an ECA composed of 15 cells with Rule 30 for 15 time steps.

3. Cellular Automata with Memory (CAM)

The next states of the cells depend on the previous states, in addition to current states of the cells, in a CAM.

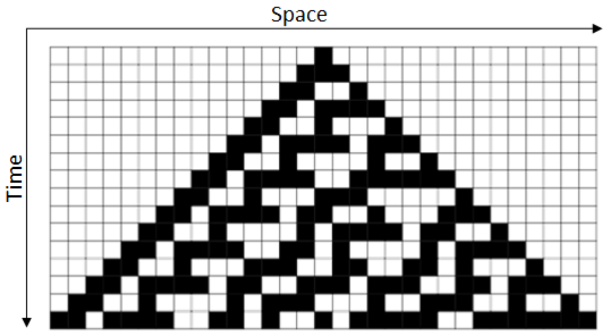

Figure 2. Evolution of an ECA composed of 31 cells with Rule 30 for 15 time steps.

The dynamics of the Fredkin's CAM model for elementary manner can be given by

$$\alpha_i(n+1) = f(\alpha_{i-1}(n), \alpha_i(n), \alpha_{i+1}(n), \alpha_i(n-1)). \quad (3)$$

Notice that, here f is not an elementary local rule ($f : Q^3 \to Q$) since its domain is Q^4 because of the term, $\alpha_i(n-1)$.

There are also different of CAM models [2][3][4]. One of the CAM models has been suggested in our previous work[5]. The dynamics of that CAM model for elementary manner has been given as follows

$$\alpha_i(n+1) = f(\alpha_{i-1}(n-x), \alpha_i(n-y), \alpha_{i+1}(n-z)) \quad (4)$$

where x, y and z are non-negative integers.

4. Cellular Automata with Random Memory (CARM)

CARM is a new CA model which has been recently proposed [6]. In a CARM model, the next states of the cells depend on randomly chosen previous states, instead of specified previous states in the manner of CAM models.

A d-dimensional CARM can be defined with $\mathbb{Z}^d$, Q,

$$V = (i_1, i_2, \ldots, i_s),\ i_1, \ldots, i_s \in \mathbb{Z}^d$$

and $f : Q^s \to Q$. Hence the dynamics can be given by

$$\alpha_i(n+1) = f\Big(\alpha_{i+i_1}(n - \tau_{i+i_1}(n)), \alpha_{i+i_2}(n - \tau_{i+i_2}(n)), \ldots, \alpha_{i+i_s}(n - \tau_{i+i_s}(n))\Big) \quad (5)$$

where $\tau_{i+i_1}(n), \tau_{i+i_2}(n), \ldots, \tau_{i+i_s}(n)$ are random integers which are elements of set $\{0, 1, \ldots, N\}$, $N < \infty$ for the time step n. Equation 5 is valid for $n \geq N$. For $n < N$, the system works like a standard CA given in equation (1).

An elementary CARM (ECARM) can be defined with cellular space $\mathbb{Z}$, set of states $Q = \{0, 1\}$, neighbourhood $V = (-1, 0, 1)$, and a function $f : Q^3 \to Q$. Hence the dynamics of an ECARM is given as follows

$$\alpha_i(n+1) = f\Big(\alpha_{i-1}(n - \tau_{i-1}(n)), \alpha_i(n - \tau_i(n)), \alpha_{i+1}(n - \tau_{i+1}(n))\Big) \quad (6)$$

For an ECARM, let the N be 1 and the number of cells in the ECARM be M. Therefore, τ_m for $m = 0, 1, \ldots, M-1$ can be considered as random variables with Bernoulli distribution. Each random variable τ_m can be 1 and 0 with probabilities p_m and $1 - p_m$, respectively. Hence that special ECARM is called, Elementary CARM with minimal memory (ECARMM).

In Figs 3 and 4,evolutions of two ECARMMs composed of 128 cells with same initial conditions and Rule 150 for 64 time steps are given. Figure 3 illustrates the evolution of the ECARMM with parameter $p_m = 0.1,\ m = 0, 1, \ldots, 127$. Figure 4 illustrates the evolution of the ECARMM with parameter $p_m = 0.3,\ m = 0, 1, \ldots, 127$.

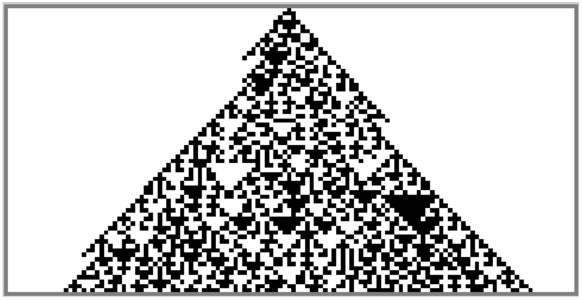

Figure 3. Evolution of the ECARMM composed of 128 cells with parameter $p_m = 0.1,\ m = 0, 1, \ldots, 127$ and Rule 150 for 64 time steps.

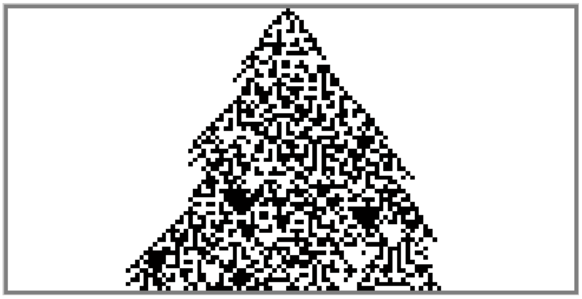

Figure 4. Evolution of the ECARMM composed of 128 cells with parameter $p_m = 0.1,\ m = 0, 1, \ldots, 127$ and Rule 150 for 64 time steps.

5. Statistical Characteristics of an ECARMM

FIPS-140-2[8] tests are using to verify the randomness of random numbers. Poker test is one of the FIPS-140-2 tests that measure the frequency of the certain 4-digits in the random sequences. To pass the poker test, frequency of the 16 possible 4-digits are closed to each other, namely uniform.

To apply the Poker test, there must be exist a sequence 20000 bits. The test divide the sequence to 5000 4-digit sub-sequences, consecutively. Then, the frequency of the 16 possible 4-digit sub-sequence is calculated from the 5000 sub-sequences. Let $f(i),\ i = 0, 1, \ldots, 15$ denotes the frequency of the decimal number i corresponding a possible 4-digit. Hence the Poker test quality is calculated from below equation

$$X = \frac{16}{5000}\sum_{i=0}^{15} f(i)^2 - 5000 \tag{7}$$

To pass the Poker Test for the sequence, X should be $2.16 < X < 46.17$.

In this paper, to distinguish ECARMMs constructed with different Bernoulli distribution, the Poker test quality measure X is exploited. Let be defined two ECARMMs composed of M cells with same initial conditions such that first ECARMM has $p_m = P_1$, and second ECARMM has $p_m = P_2$ for $m = 0, 1, \dots, M-1$. Assume that the two ECARMMs evolves for 20000 time steps. Therefore for any cell a sequence composed of 20000 bits can be obtained. If the poker test is applied that sequence, a X value will be obtained. Obviously for every evolution starting from same initial conditions, the X values are different even for the same cell of a same ECARMM. However, experiments show that average of the X values, obtained from many evolutions for the same cell of same ECARMM converges to a value, denoted by X_{avr1} and X_{avr2} for the first and the second ECARMM, respectively. Furthermore, experiments show that the average values X_{avr1} and X_{avr2} are different for different P_1 and P_2 values. Hence, exploiting the average values, ECARMM constructed with different distribution can be distinguished even if they have same initial conditions.

In Fig. 5, two Gaussian distributions fitting the X values obtained from the 50 trials of evolutions with same initial conditions for two ECARMMS with Rule 150 and values $P_1 = 0.1$ and $P_2 = 0.3$ are given. In every trial, ECARMMs are evaluated from same initial conditions along 500000 time steps. Hence, the X values are obtained by applying Poker test to last 20000 states of 8th cells of the two ECARMMS. Considering the Fig. 5, fitting curves can be easily distinguished.

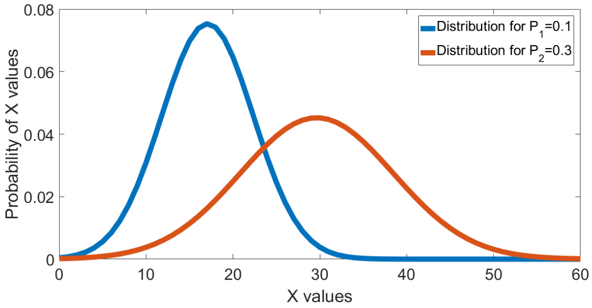

Figure 5. The two Gaussian distributions fitting the X values obtained from the 50 trials of evolutions with same initial conditions for two ECARMMS with Rule 150 and values $P_1 = 0.1$ and $P_2 = 0.3$

6. Locally Coupled ECARMMs

In this paper, statistically behaviours of locally coupled ECARMMs are analysed. For the easiest case, firstly, two locally coupled ECARMMs are considered. Figure 6 illustrates the used coupling scheme.

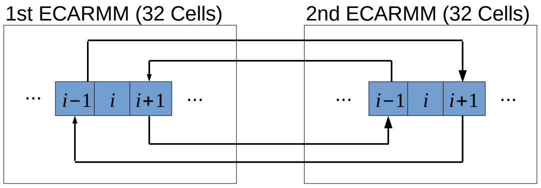

Figure 6. Locally coupling scheme

More formally, the dynamics of 1st ECARMM and 2nd ECARMM is given the following equations, respectively,

$$\alpha_i^1(n+1) = f(\alpha_{i+1}^2(n), \alpha_i^1(n-\tau_i(n)), \alpha_{i-1}^2(n)) \tag{8}$$

$$\alpha_i^2(n+1) = f(\alpha_{i+1}^1(n), \alpha_i^2(n-\tau_i(n)), \alpha_{i-1}^1(n)) \tag{9}$$

where $\alpha_i^1(n)$ and $\alpha_i^2(n)$ denote the states of the cells sited at i in 1th ECARMM and 2nd ECARMM, respectively, for time step n.

The same tests mentioned for the two non-coupled ECARMMs (Fig. 5) are applied to the two local coupled ECARMMs with parameters $P_1 = 0.1$ and $P_2 = 0.3$. Figure 7 illustrates the Gaussian distributions fitting the X values for the two ECARMMs. Considering the figures, the local coupling causes the closer distributions than the non-coupling manner. In fact, the two distributions are almost synchronized.

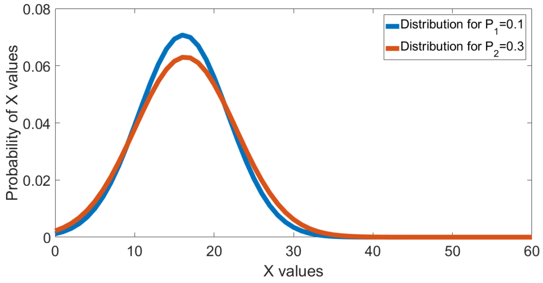

Figure 7. The Gaussian distributions fitting the X values for the two locally coupled ECARMMs.

In Figs. 8 and 9, non-coupled and locally-coupled 9 ECARMMs are given, respectively. The dynamics of locally coupled ECARMMs are given in the following equations,

$$\alpha_i^1(n+1) = f(\alpha_{i+1}^9(n), \alpha_i^1(n-\tau_i(n)), \alpha_{i-1}^9(n)) \tag{10}$$

$$\alpha_i^2(n+1) = f(\alpha_{i+1}^1(n), \alpha_i^2(n-\tau_i(n)), \alpha_{i-1}^1(n)) \tag{11}$$

$$\alpha_i^3(n+1) = f(\alpha_{i+1}^2(n), \alpha_i^3(n-\tau_i(n)), \alpha_{i-1}^2(n)) \tag{12}$$

$$\vdots$$

$$\alpha_i^9(n+1) = f(\alpha_{i+1}^8(n), \alpha_i^9(n-\tau_i(n)), \alpha_{i-1}^8(n)). \tag{13}$$

Hence, considering the Figs. 8 and 9, locally coupling causes the closer distributions than the non-coupling manner, as well.

7. Conclusion

ECARMMs are easily hardware implementable and very good candidates for TRBGs. In this paper, statistical characteristics of ECARMMs with same parameters (initial conditions, number of cells, rules, etc.) except probabilistic parameters $(P_1, P_2, \dots)$ have been analysed. Furthermore, the ECARMMs with different probabilistic parameters have been tried to distinguish. To distinguish the ECARMMs, well known statistical test, Poker test has been used. The experiments show that the Gauss distributions of fitting the X values obtaining from applied Poker tests to a specified cell (8th cell)of the ECARMMs are very useful candidates to distinguish the ECARMMs.

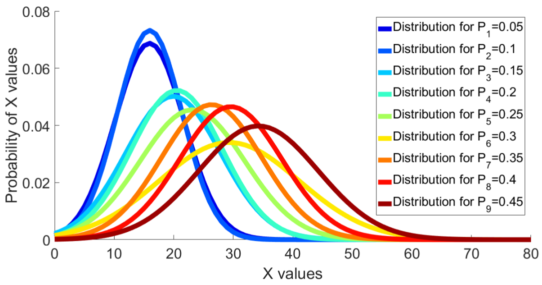

Figure 8. Nine Gaussian distributions fitting the X values obtained for non-coupled nine ECARMMs.

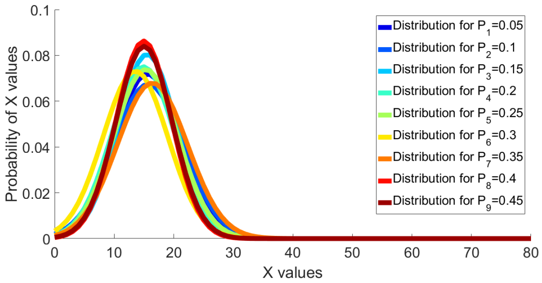

Figure 9. Nine Gaussian distributions fitting the X values obtained for locally coupled nine ECARMMs.

Additionally, statistical characteristics of the ECARMMs after locally coupling have been analysed. The experiments show that locally coupling causes the closer distributions than the non-coupling manner.

8. References

[1] T. Toffoli and N. H. Margolus, “Invertible cellular automata: A review,” *Physica D: Nonlinear Phenomena*, vol. 45, no. 1-3, pp. 229 – 253, 1990.

[2] R. Alonso-Sanz and M. Martín, “One-dimensional cellular automata with memory: Patterns from a single site seed,” *International Journal of Bifurcation and Chaos*, vol. 12, no. 01, pp. 205–226, 2002.

[3] R. Alonso-Sanz and M. Martín, “Cellular automata with memory,” *AIP Conference Proceedings*, vol. 661, no. 1, 2003.

[4] P. Letourneau, *Statistical Mechanics of Cellular Automata with Memory*, ser. Canadian theses. University of Calgary (Canada), 2006. [Online]. Available: http://books.google.com.au/books?id=0wqZIxcBmh4C

[5] E. Göncü and M. E. Yalçın, “A new cellular automata model with memory and its fpga implementation,” in *Cellular Nanoscale Networks and their Applications (CNNA), 2014 14th International Workshop on*, July 2014, pp. 1–2.

[6] E. Göncü and M. E. Yalçın, “Cellular automata with random memory and its implementations,” *to appear in International Journal of Bifurcation and Chaos*, vol. 27, no. 5, 2017.

[7] S. Wolfram, “Statistical mechanics of cellular automata,” *Rev. Mod. Phys.*, vol. 55, pp. 601–644, Jul 1983. [Online]. Available: http://link.aps.org/doi/10.1103/RevModPhys.55.601

[8] “Fips pub 140-2, security requirements for cryptographic modules,” 2002, u.S.Department of Commerce/National Institute of Standards and Technology.