Research of the method of pseudo-random number generation based on asynchronous cellular automata with several active cells

Stepan Bilan[1,*], *Mykola* Bilan[2], and *Sergii* Bilan[3]

[1] State Economy and Technology University of Transport, Kyiv, Lukeshevicha, str., 19, 03049, Ukraine
[2] The municipal educational institution Mayakskaya Secondary School, Mayak, Moldova
[3] Win-Interactive LLC, Vinnytsia, Ukraine

Abstract. To date, there are many tasks that are aimed at studying the dynamic changes in physical processes. These tasks do not give advance known result. The solution of such problems is based on the construction of a dynamic model of the object. Successful structural and functional implementation of the object model can give a positive result in time. This approach uses the task of constructing artificial biological objects. To solve such problems, pseudo-random number generators are used, which also find wide application for information protection tasks. Such generators should have good statistical properties and give a long repetition period of the generated pseudo-random bit sequence. This work is aimed at improving these characteristics. The paper considers the method of forming pseudo-random sequences of numbers on the basis of aperiodic cellular automata with two active cells. A pseudo-random number generator is proposed that generates three bit sequences. The first two bit sequences are formed by the corresponding two active cells in the cellular automaton. The third bit sequence is the result of executing the XOR function over the bits of the first two sequences and it has better characteristics compared to them. The use of cellular automata with two active cells allowed to improve the statistical properties of the formed bit sequence, as well as its repetition period. This is proved by using graphical tests for generators built based on cellular automata using the neighborhoods of von Neumann and Moore. The tests showed high efficiency of the generator based on an asynchronous cellular automaton with the neighborhood of Moore. The proposed pseudo-random number generators have good statistical properties, which makes it possible to use them in information security systems, as well as for simulation tasks of various dynamic processes.

1 Introduction

To date, the problem of creating sources of pseudo-random numbers great attention is given [1 - 7]. A large number of different pseudo-random number generators (PRNG) have already been created, which form high-quality pseudo-random bit sequences [1 - 7]. However, modern means of information processing and protection, as well as data transmission systems require improvement of such parameters as speed, length of the repetition period of the pseudo-random sequence of numbers, and unpredictability of each element of the bit sequence. A lot of attention is paid to PRNG, which are implemented on cellular automata (CA) [8-13]. For the implementation of PRNG, CA with various forms of organization are used (one-dimensional CA, two-dimensional CA, synchronous CA, asynchronous CA, hybrid CA, etc.). The PRNG based on asynchronous CA (ACA) high quality was shown in papers [9, 14]. They were investigated using statistical tests of ENT, NIST [4, 15, 16], as well as graphical tests [4]. Such studies allowed the analysis of ACA with one active cell. However, in fact, ACA with several active cells has not been investigated. Also hybrid CA (HCA) with different forms of neighborhood organization for heterogeneous cells have not been fully investigated.

2 PRNG based on the ACA with one active cell

In their previous papers, the authors considered the PRNG based on the ACA, in which only one cell changes its state at each time point [9, 14]. The various types of neighborhoods of cells (von Neumann neighborhood and Moore neighborhood are investigated). At the initial moment of time all the cells of the ACA are set to logical "0" and "1" states, and an active cell is chosen. Each cell of the ACA is in the main informative state and can be in an additional active state (active cell).

In each time step, only the active cell can change its state in accordance with the local transition function, which it implements. After changing its state in the next time step, each active cell transmits the active signal of

[*] Corresponding author: bstepan@ukr.net

one of the cells in the neighborhood of the active cell. That cell of the neighborhood of the active cell to which the active signal was transmitted becomes active in the next time step of the PRNG functioning. To select the active cell in the next time step, the active cell realizes a local function, the arguments of which are the signal values at the outputs of the neighborhood cells at the current time. The result of this function is the signal on one of the active outputs of the active cell at the present time. This output is connected to the active input of one of the cells in the neighborhood of the active cell. The additional active cell performs a constant change in the general condition of the ACA in comparison with the use of one active cell. This situation reduces the number of states that lead to the formation of signal generation cycles.

In the previous papers [9, 14], the following local functions were used, which were performed by each active cell. To change the basic information state of the active cell, the XOR function is used. In this case, the arguments of such a function are the values of the own state signal. To transmit the active signal to one of the neighborhood cells, a function is used which, at an odd time step from the neighborhood cells in the logical "1" state, determines the cell with the largest number of enumeration. In addition, the local activation function determines the neighborhood cell with the largest number among the neighborhood cells that are in the logical "0" state in the odd time step.

At each time step, the active cell state signal is read. In addition, in the local function of the active cell, an additional bit is used. This bit is a signal of the state of one of the cells of the ACA at each time step of the PRNG. A cell that forms an additional bit at any time can be selected according to any previously described law. An example of the functioning of a PRNG with one active cell of the ACA on Fig. 1 is shown.

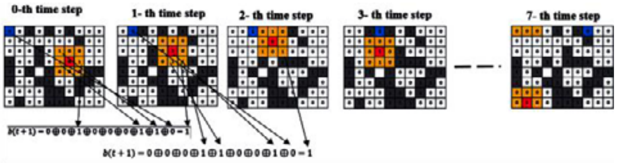


Fig. 1. An example of the functioning of a PRNG with one active cell.

In this example, the red cell is an active cell; the blue cell forms an additional bit. Condition of the active cell changes based on cells by neighborhood Moore. A red (active) cell forms a bit of a pseudo-random sequence at each time step. The sequence of bits formed after seven time steps corresponds to 0101010. The numbering of the neighborhood cells begins from the middle upper cell and increases clockwise.

The use of an additional bit as an additional argument of the function makes it possible to increase the length of the repetition period of the PRNG based on the ACA. The main characteristics that affect the quality of the PRNG on the basis of ACA with one active cell are: the dimension of the ACA, the shape of the neighborhood, the number of cells of the ACA in the initial state of the logical "1", the location of the cells in the logical "1" state on the ACA field and of the initial active cell, the local function of states of active cells and the local function of active cell transitions.

The hardware implementation of PRNG with one active cell is based on the implementation of one cell of the ACA. The cell of the ACA consists of two parts that realize the local function of states and the local function of the active signal transmission of one of the cells in the neighborhood of the active cell. In addition, the PRNG uses a switching circuit in its structure that implements the connection of the output of the active cell to the output of the generator at each instant of time.

In the papers [9, 14], the results of a test analysis of a PRNG based on ACA was described. As tests, ENT, NIST, and graphical tests were used. The obtained results confirmed the high quality of the operation of the PRNG based on the ACA with one active cell. It was determined how the performance of the PRNG affects such characteristics as the size of the ACA and the number of cells that have an initial state of logical "1". In addition, the influence of the shape of the neighborhood of ACA is been determined. In these papers, recommendations were given for the selection of high quality PRNG. It was shown that the small dimension of ACA with one active cell does not give high quality of the formed bit sequence and does not allow to form a pseudo-random bit sequence with a long repetition period.

In this regard, studies are underway to increase the length of the repetition period of the pseudo-random bit sequence based on the use of various variants of the organization ACA. Other forms of neighborhoods and other local functions of transitions to the active state are considered, and the possibility of increasing additional active cells.

3 PRNG on the basis of ACA with two active cells

PRNG based on ACA with one active cell at small dimensions have a number of shortcomings. With a small number of cells with initial states of logical "1", short cycles of bit sequences appear, and also the of single trajectories of motion of active cells are been appeared.

To eliminate such deficiencies, the ACA with two active cells are used.

The structure of PRNG based on ACA with two active cells is similar to a generator with one active cell. Only ACA is organized somewhat differently. The cell of such an ACA has a different structure since it can work in three modes.

- Standby mode,
- The mode of the first active cell,
- Mode of the second active cell.

The standby mode is characterized by the fact that the cell is set to the information state of the logical "1" or "0". In this state, the cell is located until it becomes active. In the active state, the cell can change its information state, or it may not change its own state.

This depends on the local function and on the values of the arguments for the local function of the active cell.

In the second mode, the cell is active, and it functions as well as the active cell, as described in the previous section.

If the cell is in the active state of the second active cell, then it performs the same functions as the first active cell. The only difference is that at an odd time step it performs a local function similar to that performed by the first active cell at the paired time step and vice versa. This separation of active cells in even and odd time steps is carried out in order that in the case of coincidences of the two active cells, one cell does not "disappear".

The following model describes the information state of the active cell of the ACA.

$$b_i(t+1)=\begin{cases} f\left[b^i_{N_j}(t)\right], & if \quad \exists b^{i,act1}_{N_j}(t)=1 \quad or \quad \exists b^{i,act2}_{N_j}(t)=1 \\ b_i(t), & in \quad other \quad case \end{cases} \qquad (1)$$

where $b^i_{N_j}(t)$ - signals on the information outputs of the cells that constitute the cell neighborhood of i-th cell at time t;

$b^{i,actl}_{N_j}(t)$ - signal at the j-th activation input of i-th cell in i-th activity mode and this signal comes from activation output of the cell that belongs to the cell neighborhood of i-th cell at time t $\left(j=\overline{1,N}\right)$;

N – the amount of neighbor cells, that makes the neighborhood of the i-th cell.

In accordance with this model, active cells change their state regardless of the mode of functioning of the active cell. However, the transmission of the active signal of one of the neighborhood cells for the second and third modes is different. In Fig. 2 the numbering of Moore neighborhoods for an active cell is shows.

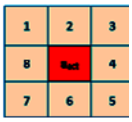


Fig. 2. The numbering of cells of the Moore neighborhood for an active cell.

The numbering of neighborhood cells and the local transition function can be chosen arbitrarily. To select an effective numbering and local transition function, it is necessary to carry out additional studies of the generator.

In Fig. 3 an example of active signal transmission by active cells in odd time step is shown.

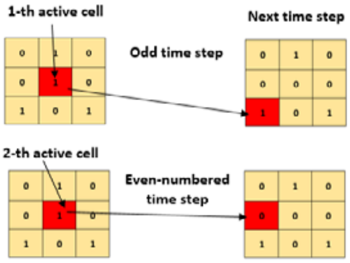


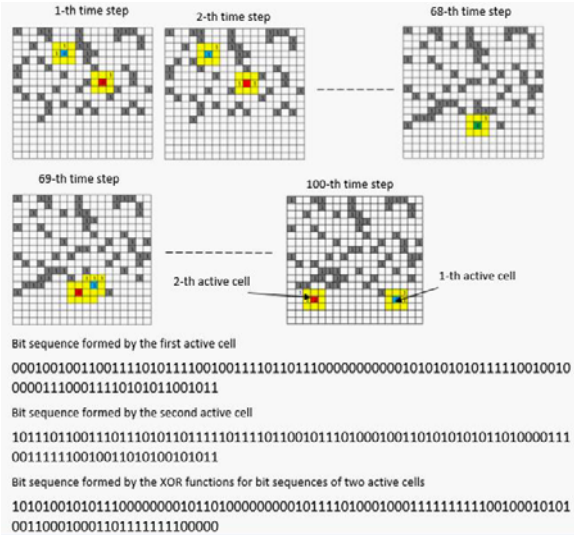
Fig. 3. An example of the transmission of an active signal by the first and second active cells in the neighborhood of Moore.

The use of two active cells avoids possible short cycles that can occur when only one active cell is used. In addition, the cell can change the direction of transmission of the active signal.

The second active cell disrupts the cycle in which the first active cell has stopped. An example of the operation of a PRNG based on ACA with two active cells on Fig. 4 is presented.

In this mode of operation of the PRNG, the active cells can coincide on one cell of the ACA. Therefore, the functions are chosen so that this coincidence does not affect the further operation.

On the example (Fig.4), it is evident that at 68 time step, two active cells converge into one active cell and at the next time step they form two active cells from one active cell. Such a work of PRNG is achieved by separating the function on even and odd time steps for each active cell.



Bit sequence formed by the first active cell

```
0001001001100111101011110010011110110111000000000000101010101011111001001000001110001111010101011001011
```

Bit sequence formed by the second active cell

```
1011101100111011101011011111011110110010111010001001101010101011010000111001111110010011010100101011
```

Bit sequence formed by the XOR functions for bit sequences of two active cells

```
1010100101011100000000010110100000000001011110100010001111111111001000101010011000100011011111111100000
```

Fig. 4. An example of the functioning of PRNG based on ACA with two active cells using the Moore neighborhood.

The value of the next bit of the generated sequence at the output of the PRNG can be the state of one of the active cells of the ACA. The PRNG can also generate two pseudo-random bit sequences. In addition, such a generator can generate a pseudo-random bit sequence in which each formed bit is the result of applying the XOR function to bits of two bit of sequences that are generated by the active cells.

Thus, using the PRNG on the basis of ACA with two active cells, it is possible to form three bit sequences. The third resulting bit sequence may have a longer repetition period than the first two cells.

The hardware implementation of such a PRNG has a more complex structure, since each cell of the ACA operates in three modes. The cell of such an ACA has a different circuit realization of the active state and a scheme for transferring the active signal to the cells of the neighborhood. There are in the asynchronous cellular automata two active cells that realize different functions of the active signal transmission at each time step. In addition, the presence of two active cells complicates the switching system, which connects both active cells to the two outputs of the PRNG at the same time. In addition, there is a need to use an additional XOR gate to form a third bit sequence. However, the use of two active cells does not reduce the performance of PRNG since active cells function simultaneously.

4 Analysis of the quality of the PRNG based on ACA with two active cells

The evaluation of the quality of such generators was performed using the statistical tests ENT and NIST, as well as using graphic tests [4, 15, 16].

The analysis was carried out in the following order. First, the initial settings of the generator were set, which were described earlier. Then, two bit sequences Q_1 and Q_2 were formed by the first and second active cells. Also a third bit sequence is been generated $Q_3 = Q_1 \oplus Q_2$, Which is the result of the bitwise addition modulo 2 of the first two bit sequences. Bit sequences were formed under different initial conditions and different lengths. ACA with dimension 10×10 and 15×15 are used. An additional bit for each active cell was formed by the ACA matrix itself. After scanning all the cells of the ACA, a matrix was used whose cell states were obtained through a number of time steps that are equal to the number of cells of the ACA. As neighborhoods, the von Neumann and Moore neighborhoods were chosen for all dimensions of the ACA.

The number of initial cells equal to 53 cells for ACA with the dimension 10×10 was used and 10, 50 and 100 of cells for ACA with 15×15 dimension. The location of cells with initial states of logical "1", as well as the initial locations of active cells that were used in testing on Fig. 5 are presented.

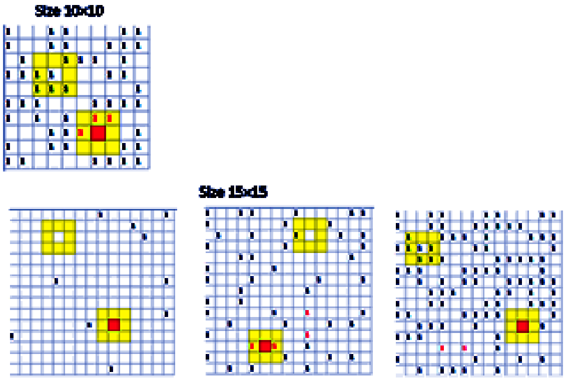


Fig. 5. The initial installation of the ACA for performance testing of the PRNG.

For each initial setup, bit sequences of length 100, 1000, 100000, 1,000,000 and 2,000,000 bits were generated, which were represented by bit files. With the help of the developed software, graphic tests were carried out, which implemented two tests:

- The histogram of distribution of the elements of sequence,
- The point’s distribution on the plane.

The results of testing the bit sequences generated using the von Neumann neighborhood on Fig. 6 are presented. The sequence length corresponds to 2000000 bits.

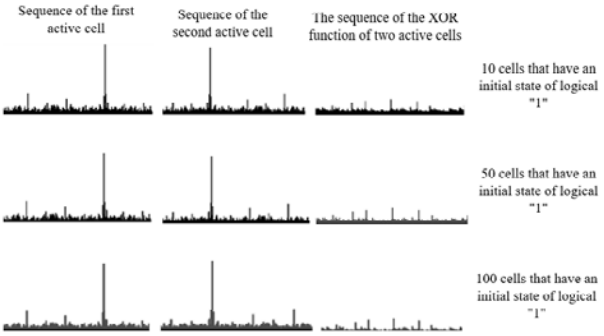


Fig. 6. The histogram of distribution of the elements of sequence for bit sequences formed using a von Neumann neighborhood.

The use of the von Neumann neighborhood does not give the desired results for small dimensions of the ACA, regardless of the number of cells in the logical “1” state. The ACA dimensions 15 × 15 also do not give good results.

The results of testing the bit sequences generated using the Moore neighborhood and have length the 2,000,000 bit on Fig. 7 are presented.

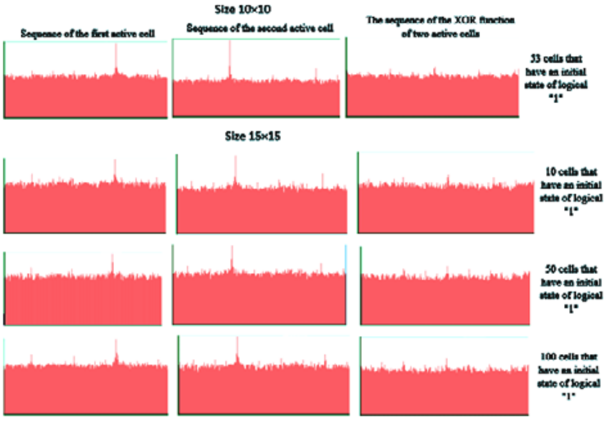


Fig. 7. The histogram of distribution of the elements of sequence for bit sequences formed using the Moore neighborhood.

The obtained histograms showed good results of the first test for the accepted sizes of ACA. It is shown that the size of the ACA 15 × 15 does not reduce the quality of the generator. It is important to note that the introduction of an additional XOR function removes defects in the bit sequences of each individual active cell. The forms of the obtained diagrams clearly shows good distribution of numbers.

The second test was carried out for sequences of 100,000, 1,000,000, 2,000,000 bits in length for the neighborhoods of von Neumann and Moore. The results of the second test for the PRNG based on the ACA with the von Neumann neighborhood on Fig. 8 are presented for a sequence with length of 1,000,000 bits.

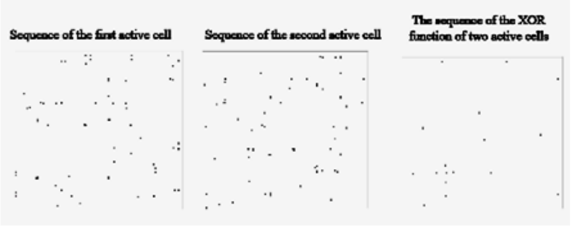


Fig. 8. Diagrams of the distribution of numbers on the plane for bit sequences formed using the von Neumann neighborhood and the length of the sequence of 1000000 bits.

Diagrams show unsatisfactory results for a sequence of 1,000,000 bits. The points are grouped in certain places on the plane, which indicates significant defects in the operation of the generator based on the von Neumann neighborhood. The results of the second test for the 2,000,000 bit sequences using the Moore neighborhood on Fig. 9 are shown. Tests were also carried out for bit sequences of shorter length (100,000 and 1,000,000 bits), which yielded positive results.

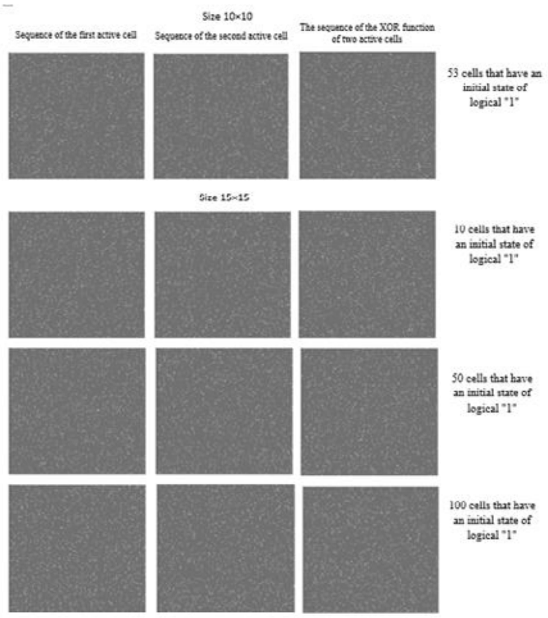


Fig. 9. Diagrams of the distribution of points in the plane for bit sequences formed using the Moore neighborhood for a sequence of length of 2,000,000 bits.

The test results showed a good distribution for the bit sequences formed by the active cells and using the XOR function.

4 Conclusion

The use of two active cells in the organization of ACA makes it possible to improve the properties of the generated pseudorandom bit sequences. Graphic tests have shown that the most effective is the neighborhood Moore. It gives a positive result for small size ACA when using graphical tests. The use of XOR functions for bit sequences formed by two active cells gives better results, which in graphical tests is proved. In addition, the length of the repetition period of the pseudo-random bit sequence is increased.

References

1. B. Schneier, Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C, Wiley Computer Publishing, John Wiley & Sons, Inc,. 784 (1996)
2. G. Marsaglia, Random number generators. Journal of Modern Applied Statistical Methods. **2**, 2-13 (2003)
3. W. Hörmann, J. Leydold, G. Derflinger, Automatic Nonuniform Random Veriate Generation. *Spr.-Verl., New York,* (2004)
4. E.V. Chugunkov, Methods and tools to evaluate the quality of pseudo-random sequence generators, focused on solving problems of information security: Textbook/M.: NEYAU MIFI, 236 (2012)
5. M. Matsumoto, T. Nishimura, M. Hadita, M. Saito. Cryptographic Mersenne Twister and Fubuki Stream/Block Cipher. (2005)
6. A. Tanvir, R. Md. Mahbubur. The Hybrid Pseudo Random Nimber Generator. Inter. Jour. of Hybr. Inform. Tech. **3**(1), 299-312 (2016)
7. A. Fog. Pseudo-Random Number Generators for vector Processor and Multicore Processors. Journ. of Mod. Appl. Stat. Methods. **14**(1), 308-334 (2015)
8. S. Wolfram, Cryptography with cellular automata. Lect. Not. in Comp. Scien.. **218**, p. 429-432 (1986)
9. S. Bilan, M. Bilan, S. Bilan, Novel pseudo-random sequence of numbers generator based cellular automata. Inf. Techn. and Sec. **3**, № 1, 38-50 (2015)
10. C. Fraile Ruboi, L. Hernandez Encinas, S. Hoya White, A. Martin del Rey, Rodrigues Sancher, The use of Linear Hybrid Cellular Automata as Pseudorandom bit Generators in Cryptography. Neu. Par. & Scien. Comp. **12**(2), p. 175-192 (2004)
11. K. Bhattachrjee, D. Paul, S. Das. Pseudorandom Pattern Generation Using 3-State Cellular Automata. In: EI Yacoubi S., Was J., Bandini S. (eds). Cellular Automatar. ACRI 2016. Lect. Not. in Comp. Scien. **9863**, 3-13 (2016)
12. G. Sh. Sirakoulis. Parallel Application of Hybrid DNA Cellular Automata for Pseudorandom Number Generation. JCA. **11**(1), 63-89 (2016)
13. B. Martin, P. Sole, Pseudo-random Sequences Generated by Cellular Automata". International Conference on Ralations, Orders and Graphs: Interaction with Computer Scince, May 2008, Mandia, Tunisia, Nouha editions, p. 401-410 (2008)
14. S. Bilan, M. Bilan, R. Motornyuk, A. Bilan, S. Bilan, Research and Analysis of the Pseudorandom Number Generators Implemented on Cellular Automata, WSEAS TRANS. on SYS., **15**, p. 275 - 281. (2016)

15. J. Walker, ENT. A Pseudorandom Number Sequence Test Program.- [electronic resource]. January 28th, 2008. http://www.fourmilab.ch/random
16. NIST.- National institute of standarts and technology. Computer security division. Computer security resource center.- Download Documentation and Software.: http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html