DOI: 10.17725/rensit.2022.14.151

Information Technologies Based on Noise-like Signals: II. Statistical and Fractal Properties of Chaotic Algorithms

Vadim V. Kashin, Vladimir I. Grachev, Viktor I. Ryabenkov, Vladimir V. Kolesov

Kotelnikov Institute of Radioengineering and Electronics of RAS, http://www.cplire.ru/

Moscow 125009, Russian Federation

E-mail: vvkashin@cplire.ru, grachev@cplire.ru, ryabenkov.vi@list.ru, kvv@cplire.ru

Received June 11, 2022, peer-reviewed June 18, 2022, accepted June 25, 2022

Abstract: **Discrete chaotic signals with high information capacity have been developed and studied on the basis of nonlinear systems with dynamic chaos. The influence of the main parameters of the generating chaotic algorithm with a delay on the statistical, correlation, structural and fractal characteristics of non-periodic pseudorandom integer and binary sequences generated by the algorithm is analyzed by numerical methods. It is shown that non-periodic pseudorandom sequences (PRSs) formed by a chaotic algorithm with a delay, for all values of the main parameters, have good statistical, correlation, structural and fractal characteristics close to random sequences of independent tests. It is shown that these characteristics are provided on a long PRS cycle in a multidimensional phase space with all the basic parameters of the chaotic algorithm and an arbitrary choice of initial conditions. Such binary PRSs can be used quite effectively in telecommunication systems using stream coding of large blocks of information messages from the point of view of secrecy, noise immunity and cryptographic stability of the communication channel.**

Keywords: **information technology, chaotic dynamics, pseudorandom sequences, redundant codes, noise-like signals**

UDC 621.391

Acknowledgments: The work was carried out within the framework of the state task of the Kotelnikov IRE of RAS from the Ministry of Education and Science of the Russian Federation.

For citation: Vadim V. Kashin, Vladimir I. Grachev, Viktor I. Ryabenkov, Vladimir V. Kolesov. Information Technologies Based on Noise-like Signals: II. Statistical and Fractal Properties of Chaotic Algorithms. *RENSIT: Radioelectronics. Nanosystems. Information Technologies*, 2022, 14(2):151-164e. DOI: 10.17725/rensit.2022.14.151.

Contents

1. INTRODUCTION

At present, the most promising method for forming pseudorandom sequence (PRS) is the use of chaotic algorithms that describe the complex nonequilibrium behavior of nonlinear dynamic systems. For application in radio engineering systems, a new class of random sequences is proposed, which are formed on the basis of algorithms that describe the behavior of self-oscillating systems with delay, having dynamic chaos modes [1]. A feature of such systems is their non-linearity and non-periodicity of the time process generated by them. By changing the parameters of such a dynamic system and the initial conditions, it is possible to change the nature of its behavior over a wide range and thereby purposefully control the type and properties of the generated chaotic signal.

The proposed algorithms for generating a chaotic signal simulate the behavior of ring self-oscillatory systems with delayed feedback and strong amplitude-phase nonlinearity. When the signal circulates through the feedback circuit, the non-linearity of the system leads to an expansion of the signal spectrum. The width of this spectrum is limited by the filtering properties of the self-oscillating system. The relationship between these two competing factors—nonlinearity, which broadens the spectrum, and filtering, which narrows the spectrum—makes it possible to create a chaotic signal with a given spectrum width. The signals generated in this case belong to the class of broadband chaotic signals.

In nonlinear dynamical systems described by nonlinear equations with regular (nonrandom) coefficients and oscillating under the action of regular external forces, unpredictable or chaotic oscillations arise. In other words, the solutions to these equations are very sensitive to small changes in the initial conditions. Another important property of chaotic oscillations is the loss of information about the initial conditions: chaotic oscillations "forget" the initial state.

Despite the fact that random number generators have been known for a long time, recently, however, much attention has been paid to the study of a new method for obtaining pseudo-random sequences based on systems with dynamic chaos. Random number generators play an important role in the statistical modeling of systems. In this case, one of the main issues is the assessment of their stochasticity. The efficiency of statistical modeling of systems on a computer and the reliability of the results obtained significantly depend on the quality of the initial (basic) sequences of pseudo-random numbers, which are the basis for obtaining stochastic effects on the elements of the system being modeled. The number of random numbers used to obtain a statistically stable estimate of the characteristics of the system functioning process when implementing a modeling algorithm on a computer varies within a fairly wide range depending on the class of the simulation object, the type of estimated characteristics, the required accuracy and reliability of the simulation results.

All used random number generators undergo thorough preliminary testing, which is a set of checks on various statistical criteria, including as the main checks (tests) for equability, stochasticity and independence. Therefore, the availability of simple and economical methods for generating sequences of random numbers of the required quality largely determines the possibility of their practical use in machine statistical modeling of systems and when used in noise-immune information channels.

In information systems with redundant coding during information transmission, the problem of the possibility of absolutely accurate reproduction of the code sequence at

a known key for the numerical reproduction of a chaotic process of long duration remains relevant, which is rather problematic in dynamic systems with continuous time.

This problem can be largely solved by using chaotic random integer generators, the study of the statistical properties of which at a new level has become possible with the development of a new approach - dynamic chaos in discrete systems.

2. RESEARCHED ALGORITHM

In this paper, we consider the chaotic algorithm with delay proposed in [1], which forms a non-periodic pseudo-random sequence (PRS) of integer numbers $\{x_n\}$. Algorithm defined on a finite closed interval of the natural series [1, M], M > 1:

$$\begin{aligned}
&\tilde{x}_n = x_{n-1} + (-1)^{x_{n-Kz}} \cdot x_{n-Nz}, \\
&(Kz \in [2, \mathrm{Nz}-1],\ \ \mathrm{Nz} > \mathrm{Kz},\ \ \mathrm{x}_n \in [1, \mathrm{M}]), \\
&\mathrm{x}_n = \tilde{x}_n, \qquad \text{if}\ \ \tilde{\mathrm{x}}_n \in [1, \mathrm{M}], \\
&\mathrm{x}_n = \tilde{x}_n - \mathrm{M}, \ \ \text{if}\ \ \tilde{\mathrm{x}}_n > M, \\
&\mathrm{x}_n = \tilde{x}_n + \mathrm{M}, \ \ \text{if}\ \ \tilde{\mathrm{x}}_n < 1.
\end{aligned} \tag{1}$$

where Nz is the delay parameter that determines the dimension of the phase space (PS) of the algorithm, and the number Kz is selected from the interval of integer numbers [1, Nz] of the delayed members of the sequence, the parameter M determines the largest of the PRS numbers. It was shown in [1] that algorithm (1), with an appropriate choice of parameters, generates the PRS of integers, and after clipping, binary sequences with statistical and correlation properties close to those of random sequences. In this case, the length of a non-periodic segment of the sequence before the loop closes can be very large: $N = 10^{12}$ and more.

The phase space (PS) of the algorithm is a finite set of M^{Nz} points of states of a given discrete dynamic system (DS), which, in its movement in the PS, from the initial state with the corresponding radius vector $\vec{\mathbf{R}}_0(x_{-1}, x_{-2}, ..., x_{-Nz})$ passes discretely to another PS point with a radius vector $\vec{\mathbf{R}}$ according to the law determined by mapping (1). Due to the limited set of PS points, the movement of system (1) occurs along closed "trajectories" of one or several cycles, which, due to the uniqueness of the transformations used, do not have common points. All PS points belong only to one particular cycle, or to an isolated point with coordinates (M, M, ..., M). All cycles are nested one inside the other, covering all states of the DS.

Note that for Kz = Nz the behavior of the DS differs from the behavior of the system described by algorithm (1). With an appropriate choice of the values of the algorithm parameters and a sufficient number of points on the cycle, transitions in the PS, as a rule, are random in nature, and at the same time are completely determined, and the algorithm forms herewith a pseudo-random sequence before the cycle is closed. Such cycles we will call pseudo-random cycles (PRCs), i.e., "strange" regions [2] of a given conservative system that preserves the phase space. These cycles are isolated numerical sets, not connected by trajectories, which are not attracting regions, in contrast to the "strange attractor" of continuous time DS.

3. INFLUENCE OF THE DELAY PARAMETER

The main parameter of the algorithm (1) is the delay parameter Nz, which determines the main characteristic of the algorithm - the dimension of the PS and the total number of state points of a given DS in this space - M^{Nz}. To demonstrate the main results of the analysis, we confine our studies to small values of the algorithm parameters. For example, **Table 1** shows the number of PS points and the cycle spectra (i.e., the periods of cycles existing in

Table 1

Cycle spectrum of algorithm (1) for M = 5, Kz = 3

Nz	M^{Nz}	Number of DS state points on cycles
4	625	562, 27(2 cycles), 8, 1
5	3125	2291, 183, 170, 169, 1
6	15625	11687, 3223, 463, 110, 1
7	78125	56640, 9948, 2761, 1744, 1429, 420, 423, 339, 211, 150, 1
8	390625	252618, 106377, 10679, 10152, 2990, 1 (spectrum is not shown in full)

the PS and their number) of algorithm (1) with a change in the quantity delay and fixed values of the parameters Kz and M.

From Table 1 it can be seen that when the delay value changes, the spectrum of cycles changes completely. Herewith does not happen simple addition of new or repeating cycles.

On **Fig. 1** and **Fig. 2** shows the structure of PS of algorithm on the example of individual cycles from N_c = 118 points (Nz = 3, Kz = 2, M = 5) and N_c = 414 (Nz = 3, Kz = 2, M = 9). For clarity, the successive points of the state of the DS on the cycles are connected by straight lines.

It can be seen from the figures that the successive points of the states of this DS on the cycle are located randomly. These points correspond to the PRS formed by the given algorithm. In this case, the cycle occupies almost the entire volume of the PS.

4. FRACTAL PROPERTIES OF PSEUDORANDOM CYCLES

To assess the degree of chaotic state of the processes, generated by the algorithm before the cycles are closed, one can use the fractal properties of the PRCs.

In the classical dynamics of systems, three types of dynamic motion were known: equilibrium, periodic motion, or limit cycle, and quasi-periodic motion. These states are called attractors, since in the presence of damping the system is "attracted" to one of the listed states.

Chaotic oscillations represent a new class of motions that cannot be reduced to any of the above. This class of motions is often associated with a state called a strange attractor. Classical attractors correspond to classical geometric regions in phase space: a point, a closed curve, or a surface in three-dimensional phase space. The strange attractor, as it turned out, is associated with a new geometric object – a fractal. The concept of a fractal was first formulated by Benoit Mandelbrot [4]. The

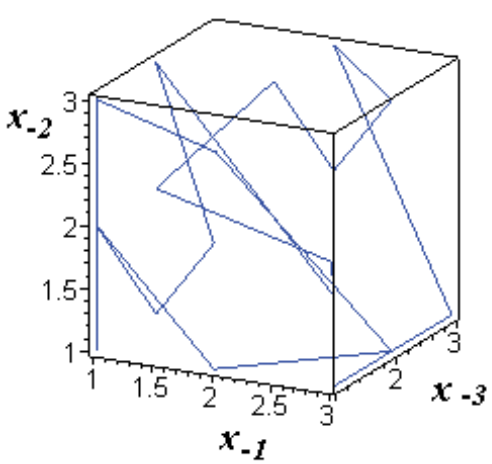

Fig. 1. *Phase portrait of algorithm (1) with parameters Nz = 3, Kz = 2, M = 5 (N = 51 cycle points N_c = 51 are shown). M^{Nz} = 125.*

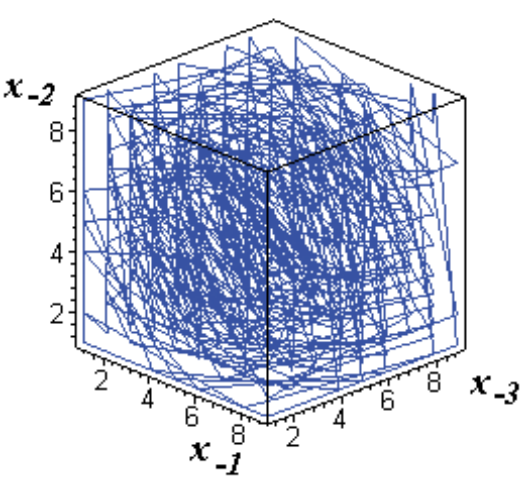

Fig. 2. *Phase portrait of algorithm (1) with parameters Nz = 3, Kz = 2, M = 9 (N_c = 414, N = 414). M^{Nz} = 729.*

main content of the theory of fractals is that, within the framework of this theory, objects are considered whose dimension is greater than their topological dimension and is a fractional value.

We study the change in the parameter of the correlation dimension of the cycles of algorithm (1) with a change in the value of the parameter Nz. We will determine the correlation dimension of the set of points on cycles based on the calculation of the correlation integral $C(l)$, determined by the number of pairs of points, the distance between which in the PS is less than l [3].

We will calculate the correlation integral for small values of all parameters of the algorithm: Nz, M, and Kz. The last two parameters M = 5 and Kz = 3 will be unchanged, and the delay parameter will be changed within Nz = 4÷7. The results obtained are shown in **Fig. 3** and **Fig. 4,** on which the dependences of the logarithm of the correlation integral on the logarithm l are plotted. The bases of the logarithms are 2.

First, it is necessary to analyze the dependence of the correlation dimension on the number of points at the cycle taken to calculate the correlation integral. Obviously, for a relatively short cycle length, all its points are taken. But as the cycle length increases, the counting time required to determine the distances between all possible pairs of numbers sharply increases, so only a part of the system state points is analyzed on long cycles.

On Fig. 3 plots $\log C(l)$ versus $\log l$ for cycles of algorithm (1) with parameters M = 5, Kz = 3 and Nz = 6, $\mathbf{R}_0$(4, 1, 4, 4, 4, 3). One curve in this figure corresponds to taking into account all points on a cycle with a small period N_c = 463. The total number of pairs of points introduced into consideration in this case is N_R = 104196. Three other dependencies are determined for another, longer cycle containing N_c = 3223 system state points, $\mathbf{R}_0$(3, 4, 1, 2, 4, 3). At the same time, the calculation of the correlation integral took into account not all points of the set, but only part of them: 500 for N_R = 122265, 1000 for N_R = 494515, or 2290 for $N_R = 2.6 \cdot 10^6$ cycle points. It can be seen from the graph that all four curves almost completely coincided. Consequently, the fractal dimension of the two studied

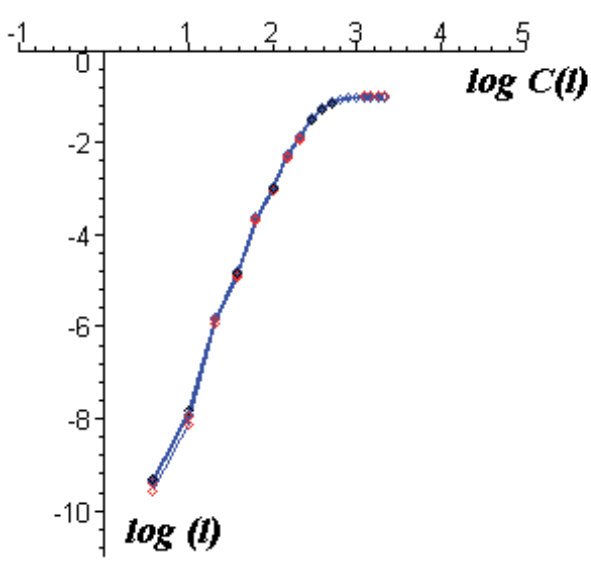

Fig. 3. *Dependence of the correlation integral logarithm on the logarithm l for four cycles of the algorithm (M = 5, Kz = 3, and Nz = 6).*

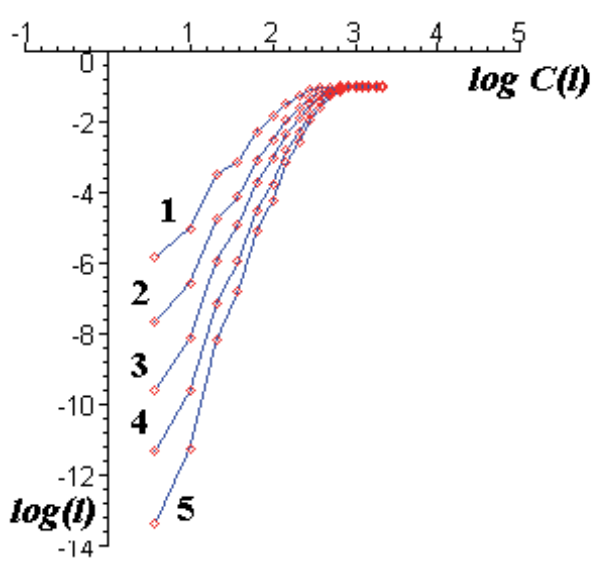

Fig. 4. *Dependence of the correlation integral logarithm on the logarithm l for different values of the parameter Nz (M = 5, Kz = 3).*

cycles of the algorithm (N_c = 463 and N_c = 3223) is the same and is completely determined only by the parameters of the algorithm, and not by the sizes of the cycles.

Graphs Fig. 3 and Fig. 4 do not have clearly defined linear segments, therefore, the exact determination of the fractal dimension of the cycles from the local angular slope of the graph curves gives a significant scatter, while the estimate of the correlation dimension gives the value D_2 ~ 4.8 with the geometric dimension of the PS equal to 6.

On Fig. 4 plots log$C(l)$ versus log$l$ for separate cycles of algorithm (1) with the same parameters M = 5, Kz = 3 and different delay values:

Nz = 4, N_c = 562, $\mathbf{R}_0$(3, 5, 3, 2), N = 561, N_R = 155396, D_2 ~ 3.0 (curve 1),

Nz = 5, N_c = 2291, $\mathbf{R}_0$(4, 3, 1, 4, 2), N = 1000, N_R = 495510, D_2 ~ 3.7 (curve 2),

Nz = 6, N_c = 3223, $\mathbf{R}_0$(3, 4, 1, 2, 4, 3), N = 2290, $N_R = 2.6\cdot10^6$, D_2 ~ 4.8 (curve 3),

Nz = 7, N_c = 1429, $\mathbf{R}_0$(2, 2, 1, 2, 3, 2, 4), N = 14228, $N_R = 1.06\cdot10^6$, D_2 ~ 5.2 (curve 4),

Nz = 8, N_c = 10152, $\mathbf{R}_0$(5, 3, 3, 4, 3, 2, 2, 4), N = 2000, $N_R = 2.0\cdot10^6$, D_2 ~ 6.5 (curve 5).

The results obtained show that as the delay parameter increases, the fractal dimension of pseudorandom cycles increases, which leads to better chaotization of processes in a discrete DS and, accordingly, to an improvement in the statistical characteristics of the formed PRS. At the same time, the observed difference between the correlation dimension and the geometric dimension of the PS indicates some inhomogeneity in filling the space with points of the pseudorandom cycle, at least for relatively small values of Nz, M.

The probability distributions of the generated numbers $p(x)$ for many cycles, especially long (N ~ N_c) cycles, are close to a uniform distribution ($p(x)$ = 1/M). The root-mean-square deviations from the uniform law for the PRS generated by the algorithm at M = 5, Kz = 3 and different delay values are shown in **Fig. 5**:

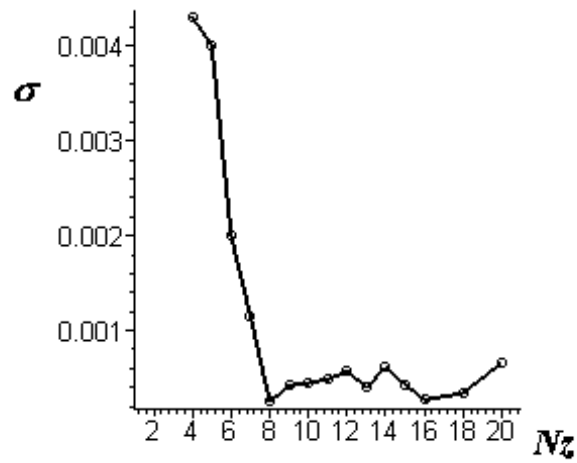

Fig. 5. *Root-mean-square deviation from the uniform distribution of pseudo-random sequences generated by the algorithm depending on the parameter Nz (M = 5, Kz = 3).*

The numerical values of σ obtained on this graph at Nz = 4÷10 refer to the longest of the set of cycles in the PS (see Table 1) with the corresponding initial conditions. In this case, the analyzed length of the sequence was equal to the length of the cycle: N = N_c. For delays Nz = 11÷20, at which the length of cycles exceeded N = 10^7, the initial conditions were taken to be unitary (1, 1, ..., 1), and the length of the analyzed PRS was N = 500000.

As the analysis showed, for all studied delay values, the algorithm generates a PRS with a probability distribution that is continuous over all generated numbers and is close to a uniform law. But, as follows from the data in Fig. 5, if at small delays the rms deviation is about 10^{-3}, then with an increase in the parameter Nz, the difference from the uniform distribution density $p(x)$ = 1/M decreases.

For practical purposes of encoding information, it is expedient to use a large

length PRS, and, consequently, large values of the parameters Nz, M are required. Similar conclusions for the distribution function will be valid in this case as well. So, when studying the dependence $\sigma = f(Nz)$ for pseudorandom cycles of algorithm (1) with the domain of definition [1, 255], i.e. M = 255, and with the same parameter Kz = 3, the following result was obtained: with an increase in the delay from Nz = 4 to Nz = 24 and the length of the analyzed implementations of the PRS from N = 210000 terms, the difference between the distribution density $p(x)$ and the uniform law is approximately the same, and is in the range from $\sigma = (1.3 \div 1.5) \cdot 10^{-4}$.

Thus, it is shown that the sequence generated by the algorithm has an almost uniform distribution law, which is actually independent of the delay quantity. It should be noted that the difference from the uniform distribution law decreases significantly with the expansion of the domain of definition of the algorithm [1, M].

5. GEOMETRIC STRUCTURE OF THE PRS

Let us analyze the behavior of the DS state points on a pseudo-random cycle using fractal geometry methods, considering a random sequence generated by algorithm (1) as an analogue of the geometric relief of a complex "coastline" with a digitized value of its heights and depths of depressions. Let us estimate the geometric structural complexity of such a relief by determining the probabilities of the modulus of equal distances between adjacent points of the geometric relief. In arithmetic representation, this is equivalent to the modulus of the same difference between neighboring numbers in the PRS.

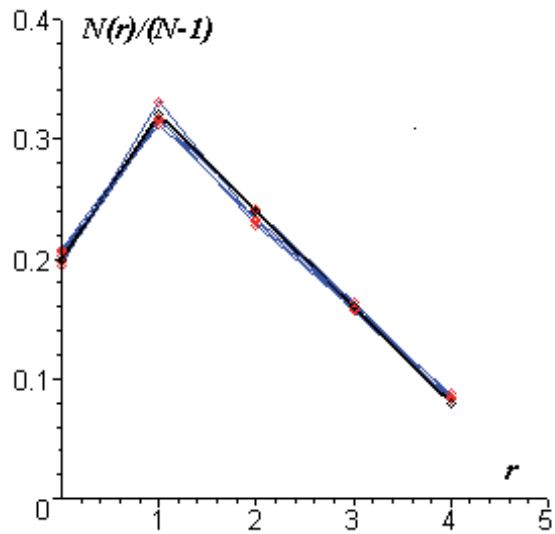

Fig. 6. *Probabilities $p(r) = N(r)/(N - 1)$ of differences between neighboring numbers $r = |x_n - x_{n+1}|$ in realizations of sequences with Kz = 3, M = 5.*

On **Fig. 6** plots the frequency dependences N(r)/(N – 1) of the occurrence of identical events: $|x_n - x_{n+1}| = r$, n = 1, …, (N – 1), r = 0, …, (M – 1) in a sequence of N members depending on the value of r for the same cycles as in Fig. 4.

On Fig. 6 plots the dependence of N(r)/(N – 1) on r for the same cycles as in Fig. 4 (Nz = 4÷8), as well as a reference (prototype) graph for a random process with a uniform distribution. The total value of the deviation modules of probabilities $p(r)$ from the reference values $p_{ref}(r)$: $s = \sum |p(r) - p_{ref}(r)|$ and the coefficient of geometric structural complexity of the sequence $\{x_n\}$ – S/(1 + s), are presented in **Table 2**.

From the data in Fig. 6 it can be seen that all points $p(r)$ for all the studied cycles with different delays Nz are very close to

Table 2

Nz	N_c	s	S
4	562	$1.15 \cdot 10^{-2}$	0.988
5	2291	$2.87 \cdot 10^{-2}$	0.972
6	3223	$2.93 \cdot 10^{-2}$	0.971
7	1429	$3.17 \cdot 10^{-2}$	0.969
8	10152	$1.49 \cdot 10^{-2}$	0.985

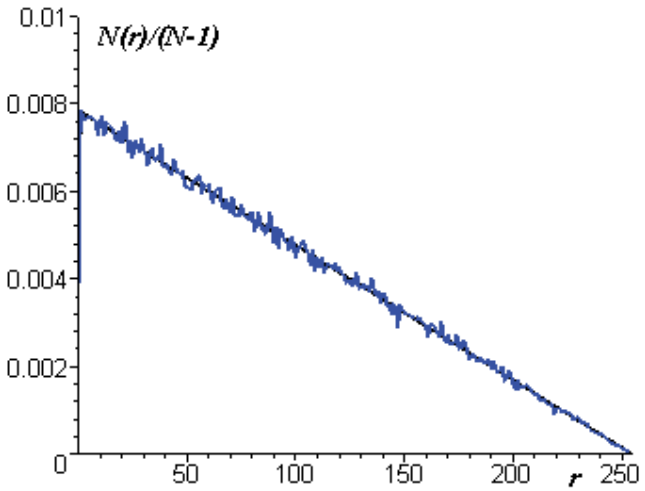

Fig. 7. *Probabilities $p(r) = N(r)/(N-1)$ of differences between neighboring numbers $r = |x_n - x_{n+1}|$ in realizations of sequences at $M = 255$.*

each other and to the reference values, and, accordingly, the coefficients of structural complexity of the generated PRSs are close to unity.

Similar results were obtained for the PRS of algorithm (1) with the domain of definition [1, 255], Kz = 3, unit initial conditions and implementation length N = 2100: when the parameter Nz changes from the value 4 to the value Nz = 24. The summary difference from the reference graph is within $(2.5 \div 3.2) \cdot 10^{-2}$, coefficient S is close to the value of 0.97. On **Fig. 7** plots the dependence $p(r)$ for the delay Nz = 24 ($s = 2.54 \cdot 10^{-2}$, S = 0.975) and the theoretical line $p(r)$. It can be seen from the figure that both graphs are close to each other.

Thus, for the studied values of the algorithm parameters, the fractal geometric structural complexity of the PRS formed by pseudo-random cycles, for fixed parameters M and Kz, any delay values Nz > 4, and a cycle length greater than at least 0.02 MNz, practically does not differ from the complexity of a random evenly distributed process.

6. BINARY SIGNAL

Estimation of the correlation characteristics of clipped (reduced to binary) segments of the generated sequences at different values of the delay parameter (Nz from 3 to 24) showed that the lateral outliers of aperiodic autocorrelation functions and cross-correlation functions for the analyzed values of Nz are practically within the same limits: $(1.3 \div 4.5)/\sqrt{N}$ for ACF of arbitrarily chosen 100 segments of length N = 128 symbols, and $(2.4 \div 5.0)/\sqrt{N}$ for ACF of arbitrarily chosen 50 segments of length N = 1024. The largest outliers of cross-correlation functions are approximately in the same range (**Table 3**).

The analysis was carried out for clipped PRSs formed by algorithm (1) with a domain of definition [1, 255] and unitary initial conditions. It follows from the results obtained that one of the most important statistical characteristics of the process being formed – the level of the highest correlation function outliers, is close to the corresponding characteristic of random sequences [5], somewhat yielding to it, and with a significant volume of PS, practically does not depend on the quantity of the feedback parameter.

The result obtained is possible only if the values taken by the sequence on all projections of the state vector in the PS are

Table 3

Statistical characteristics $R_{max}\sqrt{N}$ of clipped PRSs generated by algorithm (1) for different values of the delay parameter

Nz	ACF		CCF	
	N = 128	N = 1024	N = 128	N = 1024
3	1.3 - 4.5	2.6 - 4.6	1.7 - 4.2	2.4 - 5.0
5	1.5 - 3.8	2.7 - 4.9	1.6 - 4.1	2.8 - 4.5
7	1.5 - 4.0	2.7 - 4.2	1.5 - 4.0	2.5 - 4.3
9	1.7 - 4.4	2.4 - 4.4	1.6 - 3.5	2.5 - 4.2
12	1.7 - 3.8	2.6 - 5.0	1.6 - 4.1	2.4 - 4.5
16	1.3 - 3.6	2.5 - 4.7	1.5 - 4.0	2.3 - 4.4
24	1.5 - 3.8	2.5 - 4.3	1.5 - 3.8	2.7 - 4.2

statistically independent. At the same time, adding additional coordinates to the PS practically does not change the characteristics of the process in the case of finding the state vector on a chaotic trajectory. At the same time, by increasing the PS dimension, and, therefore, increasing the total number of admissible state vectors and reducing the proportion of short cycles, the possibilities of obtaining a non-periodic movement of a long duration increase significantly. The same conclusion is confirmed by the results of the analysis of the block structure of generated sequences after clipping and the selection of balanced codes with given correlation properties.

7. BLOCK STATISTICS IN PRS

The dependence of the block structure V(k) of clipped sequences on the value of the feedback parameter Nz is shown in **Fig. 8**. The number of blocks of the greatest length k_{max} recorded in the experiment and their number $V(k_{max})$ are presented in **Table 4**. Counting blocks of identical characters in sequences of N = 270000 members indicates that with Nz ≤ 5, the algorithm generates sequences with a block structure that has significant differences from the law $P(k) = 1/2^k$. Curve 1 in Fig. 8, corresponding to the feedback

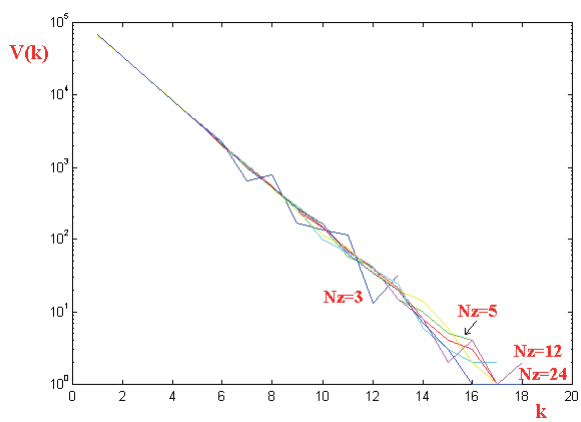

Fig. 8. *The number of blocks of identical symbols in the clipped PRS depending on the parameter Nz*

Table 4

Number of max blocks

Nz	$k_{макс}$	$V(k_{макс})$
3	13	32
5	16	4
7	17	1
9	19	1
12	18	2
16	19	1
24	18	1

parameter Nz = 3, deviates significantly from this law, starting from a block of size k = 7. At the same time, blocks with a size greater than k = 13 were not recorded over the analyzed sequence length.

As the delay increases from Nz = 3 to Nz = 9, the presence of ever longer blocks up to k = 19 is fixed in the generated sequence of a given length, and the statistics of the block structure noticeably improves. With a further increase in the delay to Nz = 24, the probabilities of the number of blocks P(k) as a function of their size k differ little from the ideal dependence $P(k) = 1/2^k$. The size of the largest block on the studied segment of the formed sequence of 270000 members practically does not change anymore, remaining at the level of k_{max} = 18÷19 symbols. At the same time, the presence of one or two such blocks over the length of the sequence is consistent with the expected probability of their occurrence.

Thus, the performed numerical experiment and the results obtained show that the block structure of the clipped sequence generated by algorithm (1) turns out to be close to the ideal distribution law $1/2^k$ with a delay Nz > 5, when the probability distribution of the numbers generated by the algorithm is almost uniform, and the initial conditions are chosen in such a way as to ensure their statistical independence. The distribution uniformity and statistical independence of the PRS values are

necessary conditions for the high quality of the statistical and correlation characteristics of the pseudo-random process generated by the algorithm.

8. SIGNAL SYSTEM VOLUME

Signals system volume generated by the algorithm when the value of the feedback parameter Nz was changed was estimated by selecting from the generated clipped sequence balanced (admissible imbalance no more than ±1) codes from $N_{code} = 128$ symbols with the following correlation properties:

- lateral outliers of the aperiodic autocorrelation function (ACF) do not exceed $R_{max} = 2.26/\sqrt{N}_{code} = 0.2$,
- outliers of aperiodic cross-correlation functions (CCFs) over the entire array of selected codes are less than or equal to $R_{max} = 3.39/\sqrt{N}_{code} = 0.3$.

Aperiodic correlation functions were calculated by the formula for balanced sequences $\{x_j\}$, $\{y_j\}$, $j = 1, 2, \ldots, N_{code}$ [5]:

$$R(\mathrm{m}) = \frac{1}{N_{code}} \sum_{j=m+1}^{N_{code}} x_j \cdot y_{j-m}, \quad m \geq 0.$$

The selection of sequences with given correlation properties was carried out on the same fixed length of the generated sequence of N = 60000 members. The number of signals V(codes) of balanced codes selected to the system in the numerical experiment, depending on the value of the feedback parameter of the algorithm, is given in **Table 5**:

Table 5

Number of selected codes with given correlation properties, $N_{code} = 128$

Feedback parameter Nz	Number of selected codes V(codes)
3	68
4	92
5	94
7	91
9	103
12	91
16	103
24	97

Thus, the numerical experiment showed that the number of selected balanced codes of size 128, generated by the algorithm when changing the delay parameter, depends to a small extent on the value of this parameter, remaining approximately at the level of 91÷103 codes with a fixed implementation length of 60,000 symbols. A significant decrease in the number of codes selected in the signals system was observed only at Nz = 3. It should be noted that the above results refer mainly to the selection of short segments of the sequence with the size $N_{code} = 128$. It is quite possible that in the formation of a system of long-duration code signals, the role of the delay parameter will be more significant.

9. INFLUENCE OF THE QUANTITY OF THE DEFINITION AREA OF ALGORITHM

When changing the value of the integer interval of the domain of definition of the algorithm [1, M], i.e. values of the parameter M, the number of independent coordinates of the phase space remains unchanged, but its volume M^{Nz}, the number of system state points, changes significantly. Significant changes are also observed in the PS pattern.

For odd values of M, all cycles, as a rule, have a different period, i.e. presented in the singular. For an even value of M, cycles of the same period occur many times. As an example, **Table 6** shows the spectra of cycles for fixed values Nz = 4, Kz = 2 (in parentheses the number of cycles in the PS at a multiplicity greater than one is indicated).

It can be seen from the data presented that, for even values of M, the cycles have a short period and, as a rule, are presented repeatedly. At odd values of M, simple regularities in the structure of the spectra of cycles are not observed, and all cycles, with rare exceptions, have different periods.

The influence of the parameter quantity M of the algorithm on the statistical properties

Table 6

Spectra of cycles in the PS of algorithm (1) for different values of the parameter M

M	Spectrum of cycles
2	1, 15
4	1, 15, 30 (8)
8	1, 15, 30 (8), 60 (64)
16	1, 15, 30(8), 60(64), 120(512)
6	1, 15(3), 30(3), 80, 90(12)
12	1, 15, 30(72), 80, 90(192), 240(5)
18	1, 15(6), 30(21), 80, 90(105), 240(27), 270(324)
10	1, 15(5), 30(10), 150(6), 312(2)
20	1, 15, 30(93), 150(918), 312(2), 1560(6)
14	1, 3(2), 15(7), 30(21), 210(168), 342(7)

M	Spectrum of cycles
3	1, 7, 29, 44
5	1, 8, 27 (2), 562
7	1, 9, 22, 427, 653, 1289
9	1, 7, 10, 20, 22, 24, 29, 44, 75, 134, 296, 767, 5132
11	1, 21, 24, 41, 101, 173, 250, 14030
13	1, 626, 2992, 3712, 5056, 7977, 8197
15	1, 27, 44, 176, 562, 828, 1637, 4702, 7764, 11405, 11484, 11881
17	1, 529, 2471, 2549, 3619, 73684
19	1, 4182, 4219, 5067, 5408, 5916, 28778, 75061
21	1, 1289, 2833, 5228, 5401, 25900, 58208, 88633

of the generated sequence was studied by numerical simulation for several odd values M = 127, 255, 511, 1023 with a delay parameter equal to Nz = 16. The odd values of M are chosen from the considerations of obtaining a non-periodic PRS of obviously large length with an initial vector in a PS with unit coordinates. For large values of the number of states in the PS of the algorithm $M^{Nz} > 127^{16} = 4.6 \cdot 10^{33}$, the probability of getting into a short cycle with non-periodic segments of the generated sequence of size N of the order of 300,000 members is quite small. Since algorithm (1) with an odd value of M = 255 was taken as the basis for numerical analysis, odd values of this parameter were also chosen for comparison.

9.1. Distribution function p(x)

As shown by numerical analysis, algorithm (1) generates a PRS with a probability distribution of generated numbers close to uniform for all selected values of the parameter M. The difference from the uniform law is characterized by the relative average and maximum difference between the histograms of the frequency of occurrence of numbers in the generated sequence by absolute value, as well as the RMS deviation (**Table 7**).

When calculating the distribution function, it is necessary to take into account the increase in the sample size with the growth of M in such a way that a proportionally equal number of possible values would fall into each discharge of the histogram. Therefore, Table 7 shows the results of determining $p(x)$ in the case of one implementation duration of N = 210,000 members (the first 4 rows), and in the case of an increase in the duration of N each time by a factor of two (the last 4 rows of the table).

For the same value of N, with increasing M, there is a slight increase of distribution difference from uniform one. In this case, the RMS deviation remains the same level. With an increase in the sample length (in proportion to the growth of M), the differences in the modulo distribution of $p(x)$ from the uniform law are the same. In this case, the RMS deviation decreases with increasing M.

Table 7

The difference between the distribution of the frequency of generating numbers from the uniform law when changing the length of the interval of the domain of definition

M	$\Delta p_{av.rel.}$	$\Delta p_{max.rel.}$	σ
127 (N = 210000)	$1.89 \cdot 10^{-2}$	$6.3 \cdot 10^{-2}$	$2.02 \cdot 10^{-3}$
255 (N = 210000)	$2.74 \cdot 10^{-2}$	$9.16 \cdot 10^{-2}$	$2.17 \cdot 10^{-3}$
511 (N = 210000)	$3.84 \cdot 10^{-2}$	$17.8 \cdot 10^{-2}$	$2.15 \cdot 10^{-3}$
1023 (N = 210000)	$5.70 \cdot 10^{-2}$	$22.1 \cdot 10^{-2}$	$2.24 \cdot 10^{-3}$
511 (N = 420000)	$2.72 \cdot 10^{-2}$	$11.43 \cdot 10^{-2}$	$1.53 \cdot 10^{-3}$
127 (N = 60000)	$3.70 \cdot 10^{-2}$	$13.4 \cdot 10^{-2}$	$4.14 \cdot 10^{-3}$
255 (N = 105000)	$4.01 \cdot 10^{-2}$	$13.3 \cdot 10^{-2}$	$3.10 \cdot 10^{-3}$
511 (N = 210000)	$3.84 \cdot 10^{-2}$	$17.8 \cdot 10^{-2}$	$2.15 \cdot 10^{-3}$
1023 (N = 420000)	$3.98 \cdot 10^{-2}$	$17.7 \cdot 10^{-2}$	$1.58 \cdot 10^{-3}$

From the data of Table 7 it can be seen that the distribution of generated numbers is almost uniform for all values of the parameter M and the deviation from this law is actually the same. The distribution of conditional probabilities also confirms the uniform distribution of points (x_{i+j}, x_i) over the entire area of the square [1, M, 1, M] in the transition tables (matrices) $x_j(n + s) = f(x_i(n))$ for algorithm with the corresponding values of the parameters M and Nz.

9.2. Correlation Properties

When selecting segments to the signal system, strictly balanced blocks of the clipped sequence with specified correlation properties $R_{max} \le \varepsilon = \alpha/\sqrt{N}_{code} = 0.2 \div 0.3$ were selected. In this numerical experiment, the amplitude of the autocorrelation functions (ACFs) and cross-correlation functions (CCFs) lateral surges was determined with respect to the level $1/\sqrt{N}_{code}$, i.e. value α. Thus, the obtained values show how many times the CF emissions exceed the level $1/\sqrt{N}_{code}$. The calculations were carried out for clipped segments of the implementation of the PRS with a length of 270,000 symbols. The results of calculations for 100 segments sequentially formed by the algorithm are shown in **Table 8**.

The results of Table 8 show that with an appropriate choice of a pseudo-random cycle, which is determined by the initial conditions,

Table 8

The magnitude of the largest outliers $R_{max}\sqrt{N}_{code}$ of the correlation functions of pseudorandom sequences generated by algorithm (1) for various values of the interval length [1, M].

M	Clipped sequence			
	ACF		CCF	
	N = 128	N = 1024	N = 128	N = 1024
127	1.5 - 3.8	2.4 - 4.1	1.8 - 3.8	2.4 - 4.1
255	1.3 - 3.6	2.5 - 4.7	1.5 - 4.0	2.3 - 4.4
511	1.3 - 3.7	2.5 - 4.7	1.3 - 4.3	2.3 - 4.4
1023	1.5 - 3.9	2.5 - 4.6	1.6 - 3.4	2.4 - 4.6

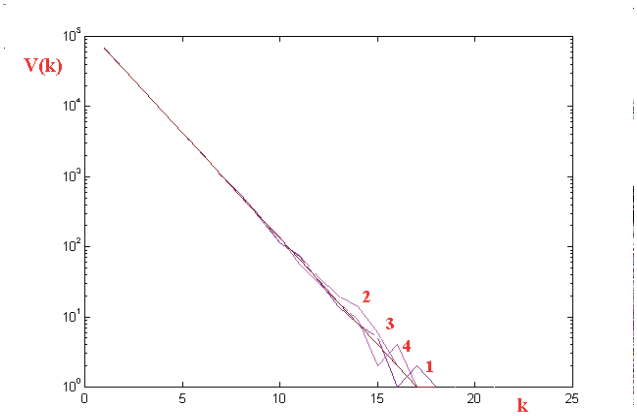

Fig. 9. *The number of blocks of identical symbols in the clipped pseudo-random sequence depending on the parameter M: M_2 = 127 (curve 1), M_2 = 255 (curve 2), M_2 = 511 (curve 3), M_2 = 1023 (curve 4).*

the correlation characteristics of the sequences generated by the algorithm (1) are practically independent of the size of the algorithm definition area and are at the same level as in the formation of code segments of 128 numbers, and in 1024 characters.

9.3. Block structure

The distribution of the block structure V(k) = func(k) of clipped sequences generated by the algorithm with areas of definition M = 127, 255, 511 and 1023 is shown in **Fig. 9**. The sizes of the largest blocks of identical symbols, fixed in the numerical experiment, are shown in **Table 9.** The length of the analyzed sequence in this case is also 270000 symbols.

As follows from the obtained results, the block structure of binary sequences exactly follows the ideal law $1/2^k$ up to blocks of size k = 14, regardless of the interval of the domain of definition of M. In practice, differences from

Table 9

The number and size of the maximum block, fixed in a numerical experiment

M	k_{max}	$V(k_{max})$
127	18	1
255	19	1
511	21	1
1023	1	1

this law for large k can be neglected, because For reliable fixation of rare large blocks of symbols, it is required to analyze the generated sequence over a much longer length. Thus, the data in Fig. 9 indicate the high statistical quality of the PRS generated by the algorithm for any domain of definition chosen for analysis area of definition [1, M].

9.4. Scope of signal system

To estimate the volume of the signal system, the selection of balanced codes of size N_{code} = 128 into the signal system with specified correlation properties $R_{max} \le 0.2$ for ACF and $R_{max} \le 0.3$ for CCF was carried out for all four values of the parameter M = 127, 255, 511 and 1023. The number of selected balanced codes with given correlation properties at a fixed length of the implementation of the sequence N is different for each case of choosing the value of the parameter M (**Fig. 10**). For some N, the difference in the number of selected codes reaches 1.5 times. At the same time, the selection rate in this case turned out to be the best for the algorithm with M = 255. However, with an increase in the implementation length, the number of selected code segments for all

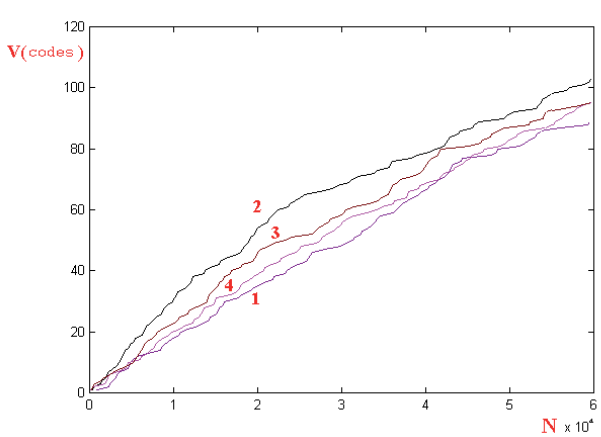

Fig. 10. *The number of selected codes (N_{code} = 128) with specified properties depending on the length of the implementation of the sequence N, generated by the algorithm (1) for different values of the parameter M: M_2 = 127 (curve 1), M_2 = 252 (curve 2), M_2 = 511 (curve 3), M_2 = 1023 (curve 4).*

M becomes close and in the interval N = 60000 this number is within 85÷103.

The data on the selection of codes with given correlation properties also confirm the actual independence of the quality of the pseudo-random sequences generated by the algorithm (1) on the size of the domain of definition – parameter M.

Thus, the analysis of the behavior of the dynamic system under consideration with a change in the parameter M has shown that the studied statistical characteristics of the formed PRSs, in fact, little depend on the value of this parameter. In this case, it should be taken into account that the full number of possible states MNz in the PS of the Nz dimension algorithm (the volume of the PS) depends on the value of M. Nevertheless, for practical purposes of encoding information, it is advisable to choose large values of the algorithm parameters Nz and M and a "long" (i.e., with a large number of DS state points) cycle in the PS, which provides good statistical and correlation properties and the required length of a continuous non-periodic coding sequence.

10. CONCLUSION

Based on a numerical experiment, it is shown in the work that non-periodic pseudo-random sequences (PRSs) generated by the analyzed chaotic algorithm with delay, for all values of its main parameters, have good statistical, correlation and fractal characteristics, close to random sequences of independent trials. It is shown that these characteristics are provided on a long PRS cycle in a multidimensional phase space for almost all the main parameters of the chaotic algorithm and an arbitrary choice of initial conditions. Such binary PRSs can be quite effectively used in telecommunication systems using streaming coding of large

blocks of information messages from the point of view of secrecy, noise immunity and cryptographic stability of the communication channel.

REFERENCES

1. Nikita A. Ageykin, Vladimir I. Grachev, Viktor I. Ryabenkov, Vladimir V. Kolesov. Information Technologies Based on Noise-like Signals: I. Discrete Chaotic Algorithms. *RENSIT: Radioelectronics. Nanosystems. Information Technologies,* 2022, 14(1):47-64. DOI: 10.17725/rensit.2022.14.047.
2. Schuster HG. *Deterministic Chaos: an Introduction*. Weinheim, Physik-Verlag, 1984, 220 p.
3. Francis C. Moon. *Chaotic and fractal dynamics: An introductions for applied scientists and engineers*. New York, J.Wiley&Sons, cop., 1992, 508 p.
4. Mandelbrot BB. *The Fractal Geometry of Nature*. N.Y., WH Freeman&Co, 1983.
5. Varakin LE. *Sistemy svyazi s shumopodobnymi signalami* (Systems with Noise-Like Signals). Moscow, Radio i Svyaz' Publ., 1979.