UDC 621.396.2.018.424

NEW METHOD FOR GENERATION OF QUASI-ORTHOGONAL CHAOTIC SEQUENCES

K.A. LUKIN, V.Ye. SHCHERBAKOV AND D.V. SHCHERBAKOV

A new method for generation of quasi-orthogonal chaotic sequences for applications both in radars and communication systems has been suggested. The method is based upon a discrete chaotic map with two time delay parameters. The phase space structure of the suggested algorithm has been analyzed using computer simulation. The period spectrum of cyclic trajectories in the phase space for different values of the time delay parameters has been founded. The statistical and correlation characteristics of binary pseudorandom sequences, generated with the help of the suggested method have been studied in detail. It has been shown that for the properly chosen time delay parameters the suggested discrete chaotic algorithm generates binary pseudorandom sequences with a nearly uniform probability distribution. It has been shown that the correlation characteristics of binary pseudorandom sequences generated are rather similar to those of random process with a uniform probability distribution.

Keywords: quasi-orthogonal chaotic sequence, discrete chaotic algorithm, chaotic integer sequence, chaotic map, phase space, binary pseudorandom sequence, autocorrelation and cross-correlation function.

INTRODUCTION

One of the problems extant in design of radar and communication systems [1-5] lays in complexity of truly random sequences generation. The most appropriate generators of random sequences from the viewpoint of their quality are the generators, based on physical sources. However, they have number of drawbacks, such as: implementation difficulties of such generators in the required frequency band; complexity of their integration with other systems and subsystems, and also no possibility of random sequences reproducing using the same source.

That is why nowadays, pseudorandom sequences are widely used in various radars, communication and data transmission systems. A lot of algorithms for pseudorandom sequences (PR-sequences) generation are known to the date. Usually, recurrent algorithms are used for the PR-sequences generation. Binary PR-sequences on the basis of recurrent algorithms may be readily realized as a computer code or, otherwise, as a fast enough binary shift register. For example, so-called M-sequences generator may be implemented in this way. However, the main disadvantage of this approach consists in the absence of mathematical tool enabling derivation of algebraic polynomials for the arbitrary large power, generating the sequences of maximal period. In addition, their statistical properties, as a rule, are rather far from statistical properties of truly random signals.

The choice of proper binary PR-sequences is a very important stage of design and practical realization of both radars and communication systems. The chosen PR-sequence has to meet the requirements for both good auto (cross)-correlation properties and providing a large set for values of their lengths and, in particular, large number of sequences ensembles [2, 3, 5].

The known classes of both linear (M-sequences, Hadamard-sequences, Gold-sequences, Kasami-sequences and other) and nonlinear (Legendre-sequences, bent-sequences and other) PR-sequences do not meet some of the above requirements [5, 7].

Basic requirements to binary pseudorandom sequences (BPR-sequences), which can be used both in radar and communication systems are as follows [5, 7 and 10]:

1) binary sequence must be balanced, i.e. a number of «+1» differs from a number «-1» by no more than one unit;

2) occurrence probability of block from k identical symbols must be close to $p(k)=1/2^k$;

3) ensemble volume of binary sequences must be maximally large;

4) autocorrelation function of binary sequence must have one narrow peak and low side-lobes level;

5) it must be ensured a low level of cross-correlation between different binary sequences;

6) binary sequences must be reproduced on the receiving end of communication systems, i.e. it must be ensured a possibility for exact reiteration of the generated binary sequence for the same initial conditions;

7) it must be ensured an acceptable complexity of algorithm formula for its practical realization.

Nowadays, PR-sequences generated with a computer code are in a wide use both in radars and communication systems caused by resent advancing in digital electronics. In turn, development of computational mathematics methods resulted in elaboration of the special generation algorithms for so-called pseudorandom number sequences, in development of which a special role plays the methods for chaotic integer sequences generation in the limited interval of integers.

Basic requirements to *chaotic integer* sequences (CI-sequences) are as follows [6, 8]:

1) *high quality:* statistical properties of CI-sequence must be close to those of truly random process and it might have as long p|eriod as possible;

2) *efficiency:* algorithm for generation of CI-sequence must be quiet fast and occupy the minimal area in a computer memory;

3) *reproducibility:* the algorithm might generate exactly the same CI-sequence of any length for a chosen initial conditions, for arbitrary number of trials and minor changes in initial procedure must result in a generation of very different CI-sequences, still having a high-quality statistical properties;

4) *simplicity* – the algorithm formula must be as simple as possible in its realization and application.

In our opinion, random sequences generators based upon *multidimensional* chaotic systems may combine advantages of conventional random numbers generators used in computers and physical sources of noise signals.

In the paper we consider a new method for generation of quasi-orthogonal chaotic sequences, applicable in both radar and communication systems. Besides we investigate the period spectrum of binary pseudorandom sequences, generated according to the method suggested, and also study their statistical and correlation characteristics.

1. THE METHOD FOR GENERATION OF BINARY PSEUDORANDOM SEQUENCES BASED ON DISCRETE CHAOTIC ALGORITHM

On the basis of mathematical model of self-oscillatory modes in one-dimensional electromagnetic resonator with a nonlinear reflecting surface, the field dynamics in which obeys the system of functional-difference equations with *two* delays [9], the discrete chaotic algorithm for generating binary pseudorandom sequences has been developed and studied. This algorithm can be attributed to the class of recurrent parametric algorithms with two time delay parameters. The algorithms for PR-sequences generation using nonlinear difference equation with *one* delay have been derived in [11] from the model of nonlinear ring self-oscillatory system with filtration and delayed feedback.

The discrete chaotic algorithm suggested in our paper is based on the discrete nonlinear functional equation with two delay parameters, which in general case may be written as follows:

$$X_n = F\left(X_{n-q}, X_{n-Q}, q, Q, M\right), \qquad (1)$$

where X_n, X_{n-q} and X_{n-Q} are calculated and given terms of the generated chaotic integer sequence; n, q, Q, M are integer natural numbers; $M = 2,3,4...$; $Q = 2,3,4...$; $n \geq Q+1$; $1 \leq q < Q$; q and Q are the first and the second delay parameters, respectively.

$F(X)$ is the function describing nonlinear transformation (chaotic in general case) of initial values of the electromagnetic field either in the problem of self-oscillations in resonator with a nonlinear reflection [9] or in the time delay amplifying system [11], but with two delayed feedback channels.

For $q < Q$ the value of the delay parameter Q determines the number of terms in the integer sequence $X_{n-1}, X_{n-2} \dots X_{n-Q}$. Using these values a new value of variables X_n is iteratively calculated according to Eq.(1). That is why they might be used as initial conditions for the iterative process of the PR-sequence generation.

The authors has considered here the most simple nonlinearity in the discrete chaotic algorithm Eq.(1), namely linear dependence of the result on the linear combination of two variables with two different delays, but limited by modulus *M*:

$$X_n = \begin{cases} X_{n-q} + X_{n-Q} & if \quad X_{n-q} + X_{n-Q} \leq M \\ X_{n-q} + X_{n-Q} - M & otherwise \end{cases} \qquad (2)$$

The theory of functional difference equations implies the Eq.(2) with two delays is equivalently to the system of Q equations with a single delay. Thus a discrete algorithm (2) is defined on the bounded set M of integer natural numbers, which belong to the closed numerical interval $[1,\ M]$. For $q < Q$ the phase space of the dynamical system (2) has a dimension Q. A number of system states in the phase space of the system (2) that is defined on the bounded discrete set, is finite and equals M^Q.

From Eq. (2) one can see that the return operation $X_n \to X_n - M$ is applied to the values X_n exceeding M when generating chaotic integer sequence $\{X_n\}$, realizing thereby a nonlinear transformation of the variable X_n similar to the known algorithm of 1D Bernoulli shift. Therefore the map (2) can be classified as multidimensional (MD) Bernoulli shift, operating in *multidimensional phase space*.

It is clear that in our case the algorithm for generation of chaotic integer sequences is the more rich and more efficient in generation of many varieties of quasi-orthogonal sequences suitable for applications in both radar and communication systems.

Generation of *binary* pseudorandom sequence has been implemented via clipping procedure of the multilevel chaotic integer sequence with respect to some threshold equals to $M/2$ according to the following rule:

$$Y_n = \begin{cases} -1, & if \quad X_n \leq \dfrac{M}{2} \\ 1, & if \quad X_n > \dfrac{M}{2} \end{cases} \qquad (3)$$

Since every state for the self-oscillatory system is defined on the finite and limited set of integers, the system sooner or later returns back to its primary state and process will be repeated. It means that a binary sequence $\{Y_n\}$ formed by the system has a limited length, representing a segment for pseudorandom sequence of the above length. This implies that a value M^Q determines a maximal theoretical cycle, but therefore a maximum possible duration of non-periodic realization $L_{\max} = M^Q$, formed by the algorithm of the given dimension. Appearance of a period in the sequence $\{Y_n\}$ has been fixed when iteration started with the exact values of initial conditions $X_{n-1}, X_{n-2} \dots X_{n-Q}$.

2. RESULTS OF ALGORITHM STUDY

Phase space of the discrete dynamical system (2), consists of a set of isolated points with co-ordinates falling into the interval of integers $[1, M]$ and determine unambiguously the system state. Dynamics of the discrete dynamical system (2) may be described with the help of its representative point in the plane formed by the delayed coordinates which is, actually, an across-section of the phase space for the given parameters of the map (2). If to connect these points with solid lines we may get qualitative information on the CI-sequence length and chaotization rate of the system motion for each given set of the system parameters.

Two examples are shown in fig. 1 and 2 for different parameter sets of the map (2) .

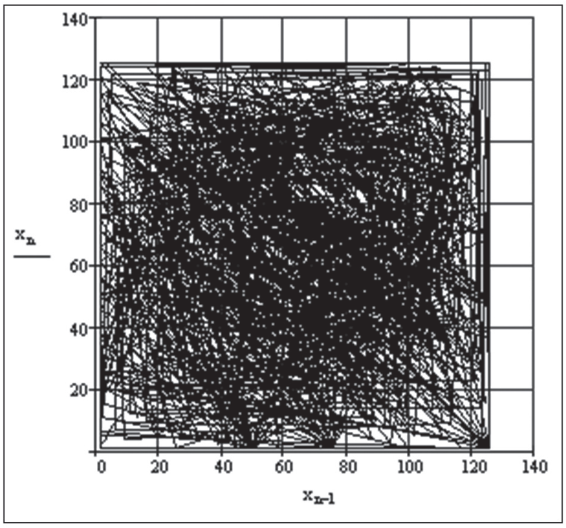

Fig. 1. Cross-section of the map (2) phase space in the delayed coordinates for the following parameter set of the map (2): M = 125, Q = 3, q = 1; and CI-sequence period = 775; representative points of the discrete dynamical system (2) are connected with solid lines at the neighboring instances of time

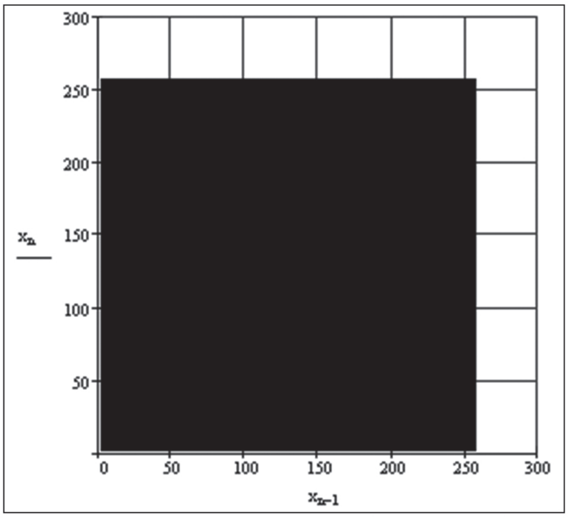

Fig. 2. Cross-section of the map (2) phase space in the delayed coordinates for the following parameter set of the map (2): $M = 125$, $Q = 3$, $q = 1$; $M = 257$, $Q = 3$, $q = 1$; and CI-sequence period = 66307; representative points of the discrete dynamical system (2) are connected with solid lines at the neighboring instances of time

One can see from these figures that the system path corresponds to the finite motion in the limited domain of the phase space. It is also seen, that the chaotization rate of any integer sequence strongly depends on the parameters M, Q, q. As a rule, with the increase of the parameters M and Q both the chaotiztion rate of the integer sequence and its period are increased.

Achievable values of the period of the binary pseudorandom sequences generated with the discrete chaotic algorithm (2) have been studied as functions of both the parameters q, Q, M and initial conditions.

Examples of the estimated period spectrum of binary pseudorandom sequences generated for various set of the parameters are represented in the Table 1.

The analysis of the above results has shown that there are some general laws in the periods estimations for the certain values of the M parameter. The most interesting cases take place for M parameter defined according to the following formulas:

a) $M = 2^k$, *where* $k = 1,2,3...$,

b) $M = 3^k$, *where* $k = 1,2,3...$,

c) $M = 5^k$, *where* $k = 1,2,3...$.

Rather simple analytical expressions for calculation of all periods of binary pseudorandom sequences have been obtained for the above cases, respectively:

$$\text{a) } Period_{q,Q}^{M=2^k} = 2^{k-1} Period_{q,Q}^{M=2}, \tag{4}$$

$$\text{b) } Period_{q,Q}^{M=3^k} = 3^{k-1} Period_{q,Q}^{M=3}, \tag{5}$$

$$\text{c) } Period_{q,Q}^{M=5^k} = 5^{k-1} Period_{q,Q}^{M=5}. \tag{6}$$

Generalizing these formulas we may derive the analytical expression for calculation of large enough periods of binary pseudorandom sequences generated by discrete chaotic map (2) depending on the q, Q, and M parameters:

$$Period_{q,Q}^{M=m^k} = m^{k-1} Period_{q,Q}^{M=m}, \tag{7}$$

where m is an integer natural number; $m = 2,3,4...$.

The period spectrums of binary pseudorandom sequences generated with algorithm (2) for the given values of the parameters q, Q, and M, and founded from the condition of exact reconstruction of the given initial conditions are presented in the Tables 2, 3 and 4.The periods obtained via simulation and calculated with formulas (4 - 6) have an absolutely exact coincidence. Increasing the values of the M, Q, and q parameters we may generate the binary pseudorandom sequences of the long enough length according to the Eq. (7).

In particular, certain laws have been found for the special case when M parameter equals to an *even number* and only parameters Q and q are varied. The related results of the period spectrums estimation for binary pseudorandom sequences for the above case are represented in the Table 5. Analyzing the Table 5 we may derive the followings laws:

1) The period spectrum of binary pseudorandom sequences, formed by the algorithm (2), is strictly symmetric with respect to the mean value of parameter q;

2) There are several different sequences with the same period in the phase space of the map (2).

Let denote as v the number of sequences with an identical period: $Period(v)_{Q,q}^{M}$. Then, for example, the writing $Period(2)_{4,q=1,3}^{256}=1920$ means that for $M=256$ and $Q=4$ there are two sequences with the period equal 1920. It follows from this consideration

Table 1

The period spectrum of binary pseudorandom sequences for the parameters set: $q=1$, $Q=2,3...12$ and $M=2,3...32$

	Period										
M/Q	2	3	4	5	6	7	8	9	10	11	12
2	3	7	15	21	63	127	63	73	889	1533	3255
3	4	8	40	26	364	728	3146	80	1640	8744	6560
4	6	14	30	42	126	254	126	146	1778	3066	6510
5	10	31	156	24	1562	19531	1116	390620	976562	487344	6781684
6	24	56	240	546	6552	92456	198198	5840	1457960	13404552	4270560
7	16	57	342	336	2400	48	1921600	2241867	1680600	4483734	117648
8	12	28	60	84	252	508	252	292	3556	6132	13020
9	12	24	120	78	1092	2184	9438	240	4920	26232	19680
10	60	217	1560	168	196812	2480437	15624	*	*	*	*
11	10	60	1330	120	118104	885775	*	590520	*	120	*
12	24	56	240	546	6552	92456	198198	5840	1457960	13404552	4270560
13	28	168	2196	366	371292	5198088	*	*	*	2613240	*
14	48	399	1710	336	50400	5096	*	*	*	*	*
15	40	248	3120	312	568568	14218568	3510936	1562480	*	*	*
16	24	56	120	168	504	1016	504	584	7112	12264	26040
17	36	288	96	288	88416	*	83520	*	*	*	*
18	24	168	240	546	6552	277368	198198	17520	4373880	13404552	4270560
19	18	381	14480	180	2476098	*	*	*	*	*	*
20	60	434	1560	168	196812	4960874	15624	*	*	*	*
21	16	456	13680	4368	218400	4368	*	*	*	*	*
22	30	420	3990	840	354312	*	*	*	*	61320	*
23	48	528	12166	1518	139920	6436342	*	*	*	*	*
24	24	56	240	1092	6552	92456	396396	5840	1457960	13404552	4270560
25	50	155	780	120	7810	97655	5580	1953100	4882810	2436720	33908420
26	84	168	10980	2562	7797132	*	*	*	*	*	*
27	36	72	360	234	3276	6552	28314	720	14760	78696	59040
28	48	798	1710	336	50400	6096	*	*	*	*	*
29	14	840	12194	5226	707280	731640	*	*	*	*	*
30	120	1736	3120	2184	5117112	*	*	*	*	*	*
31	30	920	61568	1986	476640	923520	*	*	*	*	*
32	48	112	240	336	1008	2032	1008	1168	14224	24528	52080

Note: * – more 16000000

Table 2

The period spectrum of binary pseudorandom sequences for the parameters set: $q=1$, $Q=2,3...15$ and $M=2^k$, *where* $k=1,2,3...11$

	Period										
Q/M	2	4	8	16	32	64	128	256	512	1024	2048
2	3	6	12	24	48	96	192	384	768	1536	3072
3	7	14	28	56	112	224	448	896	1792	3584	7168
4	15	30	60	120	240	480	960	1920	3840	7680	15360
5	21	42	84	168	336	672	1344	2688	5376	10752	21504
6	63	126	252	504	1008	2016	4032	8064	16128	32256	64512
7	127	254	508	1016	2032	4064	8128	16256	32512	65024	130048
8	63	126	252	504	1008	2016	4032	8064	16128	32256	64512
9	73	146	292	584	1168	2336	4672	9344	18688	37376	74752
10	889	1778	3556	7112	14224	28448	56896	113792	227584	455168	910336
11	1533	3066	6132	12264	24528	49056	98112	196224	392448	784896	1569792
12	3255	6510	13020	26040	52080	104160	208320	416640	833280	1666560	3333120
13	7905	15810	31620	63240	126480	252960	505920	1011840	2023680	4047360	8094720
14	11811	23622	47244	94488	188976	377952	755904	1511808	3023616	6047232	12094464
15	32767	65534	131068	262136	524272	1048544	2097088	4194176	8388352	16776704	33553408

Table 3

The period spectrum of binary pseudorandom sequences for the parameters set:

$q=1$, $Q=2,3...12$ and $M=3^k$, *where* $k=1,2,3...10$

	Period									
Q/M	3	9	27	81	243	729	2187	6561	19683	59049
2	4	12	36	108	324	972	2916	8748	26244	78732
3	8	24	72	216	648	1944	5832	17496	52488	157464
4	40	120	360	1080	3240	9720	29160	87480	262440	787320
5	26	78	234	702	2106	6318	18954	56862	170586	511758
6	364	1092	3276	9828	29484	88452	265356	796068	2388204	7164612
7	728	2184	6552	19656	58968	176904	530712	1592136	4776408	14329224
8	3146	9438	28314	84942	254826	764478	2293434	6880302	20640906	61922718
9	80	240	720	2160	6480	19440	58320	174960	524880	1574640
10	1640	4920	14760	44280	132840	398520	1195560	3586680	10760040	32280120
11	8744	26232	78696	236088	708264	2124792	6374376	19123128	57369384	172108152
12	6560	19680	59040	177120	531360	1594080	4782240	14346720	43040160	129120480

Table 4

The period spectrum of binary pseudorandom sequences for the parameters set:

$q=1$, $Q=2,3...12$ and $M=5^k$, *where* $k=1,2...5$

	Period				
Q/M	5	25	125	625	3125
2	10	50	250	1250	6250
3	31	155	775	3875	19375
4	156	780	3900	19500	97500
5	24	120	600	3000	15000
6	1562	7810	39050	195250	976250
7	19531	97655	488275	1441375	12206875
8	1116	5580	27900	139500	697500
9	390620	1953100	9765500	48827500	244137500
10	976562	4882810	24414050	122070250	610351250
11	487344	2436720	12183600	60918000	304590000
12	6781684	33908420	169542100	847710500	4238552500

that the Results of the Table 5 may be presented as follows:

$$Period(1)^{256}_{2,q=1}=384\ ,\ Period(4)^{256}_{11,q=1,4,7,10}=196224\ ,$$

$$Period(2)^{256}_{3,q=1,2}=896\ ,\ Period(4)^{256}_{7,q=1,3,4,6}=16256\ ,$$

$$Period(1)^{256}_{4,q=2}=768\ ,\ Period(2)^{256}_{4,q=1,3}=1920\ .$$

One can see that with growth of the parameter Q the number of different sequences with an identical period is growing as well.

3. STATISTICAL AND CORRELATION CHARACTERISTICS OF BINARY PSEUDORANDOM SEQUENCES

Probability distribution uniformity (or equiprobability) of integers over a given interval $[1,M]$ is a very important issue in the problem of the generation of chaotic integer sequences. From this point of view the suggested discrete chaotic algorithm (2) is not perfect. Nevertheless computer simulation carried out have shown, that for the properly chosen values of the M , Q , q parameters the algorithm (2) generates practically uncorrelated chaotic integer sequences with nearly uniform probability distribution: $p(x)=1/M$, provided the following condition is met:

Table 5

The period spectrum of binary pseudorandom sequences for the parameters set:

$M=256$, $Q=2,3...11$ и $q=1,2,3...10$

	Period									
Q/q	1	2	3	4	5	6	7	8	9	10
2	384									
3	896	896								
4	1920	768	1920							
5	2688	3968	3968	2688						
6	8064	1792	1152	1792	8064					
7	16256	11904	16256	16256	11904	16256				
8	8064	3840	27776	1536	27776	3840	8064			
9	9344	59520	2688	65408	65408	2688	59520	9344		
10	113792	5376	130944	7936	1920	7936	130944	5376	113792	
11	196224	262016	249984	196224	76160	76160	196224	249984	262016	196224

$$Period_{Q,q}^{M} (\mathrm{mod}\, M) = 0\ . \qquad (8)$$

Among the chaotic integer sequences generated by discrete chaotic algorithm (2) there are sequences for which condition (8) is met exactly, as in the below example:

$$Period_{9,1}^{5} = 390620/5 = 78124\ .$$

At the same time, there are many sequences for which condition (8) cannot be met exactly. Nevertheless, there are many sequences for which Eq. (8) is met approximately, and such sequences are also of a great practical interest. For example, chaotic integer sequences, generated with the suggested discrete algorithm (2), may be related to the sequences of that type:

$$Period_{7,1}^{125} = 488275/125 = 3906{,}2\ ;$$

$$Period_{3,1}^{257} = 66307/257 = 258{,}004\ .$$

The histograms of appearance frequency for generated integers in some chaotic integer sequences (CI-sequences) above mentioned are presented in fig. 3 and 4.

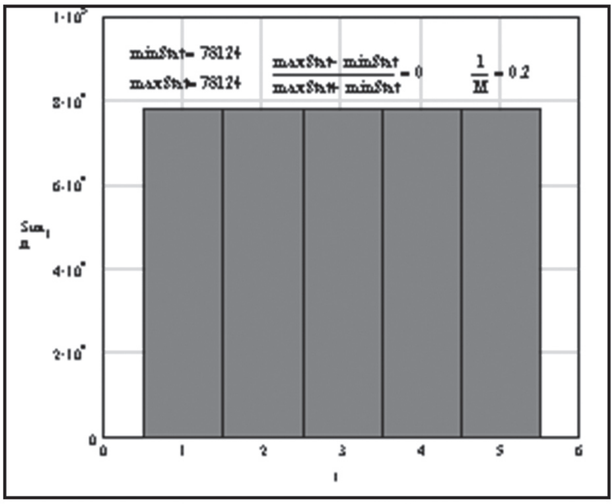

Fig. 3. Histogram of appearance frequency for different integers in CI-sequence for the following parameters: $M = 5$, $Q = 9$, $q = 1$; $Period = 390620$

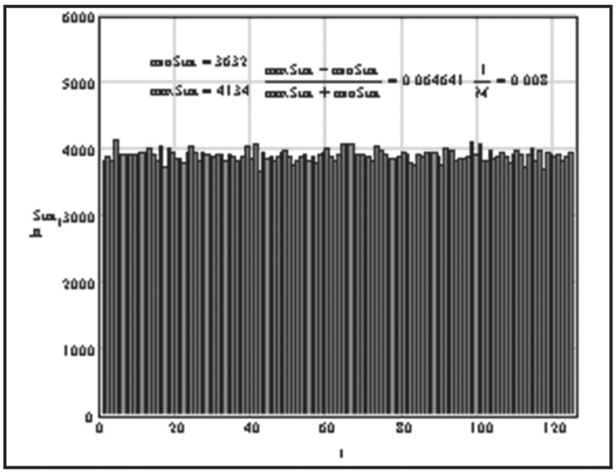

Fig. 4. Histogram of appearance frequency for different integers in CI-sequence for the following parameters: $M = 125$, $Q = 7$, $q = 1$; $Period = 488275$

We also analyzed the appearance frequency of the blocks of k identical characters in different realizations of binary pseudorandom (BPR) sequences generated via algorithm (2) and further application of the clipping operation (3). It is known that for ideal random process the appearance probability of blocks compound of k identical characters of binary process obeys the following probability distribution function $p(k) = 1/2^k$ [10]. Appearance frequencies of blocks of k identical characters in BPR-sequence obtained with the help of computer simulation using the algorithm (2) are presented in fig. 5 and 6.

Besides, estimations of correlation characteristics of BPR-sequences have been done for bulk enough BPR-sequences (a few hundred), generated via the algorithm (2) without any preferences in their balance characteristic.

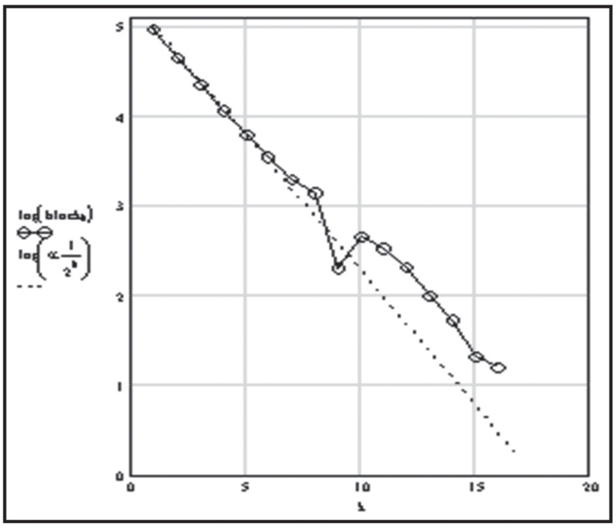

Fig. 5. Appearance frequency of blocks of k identical characters in BPR-sequence as function of parameter k; $M = 5$, $Q = 9$, $q = 1$; $Period = 390620$. Dashed line corresponds to the probability distribution $p(k) = 1/2^k$

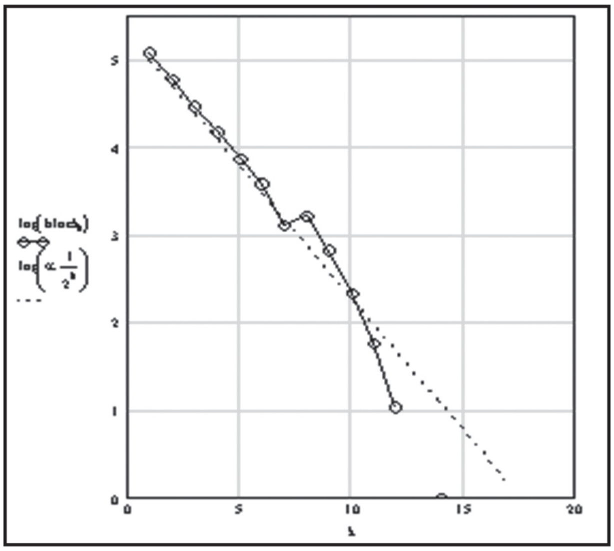

Fig. 6. Appearance frequency of blocks of k identical characters in BPR-sequence as function of parameter k; $M = 125$, $Q = 7$, $q = 1$; $Period = 488275$. Dashed line corresponds to the probability distribution $p(k) = 1/2^k$

Both autocorrelation and cross-correlation functions for the generated BPR-sequences of the length N equal to the period (*Period*) of the generated sequences according to the Tables 1...5, have been studied as well. Autocorrelation functions for two different realizations of BPR-sequences, generated via discrete chaotic algorithm (2) are presented in fig. 7 and 8. The maximal levels of the autocorrelation function side-lobes lay within the following range

$$R_{\max} = (2{,}4...4{,}6)/\sqrt{N}\ , \qquad (9)$$

where N is the length of the BPR-sequence.

The results obtained have shown that autocorrelation and cross-correlation functions of BPR-sequences generated via Eq.(2) are rather close to those of an ideal random process with the uniform distribution.

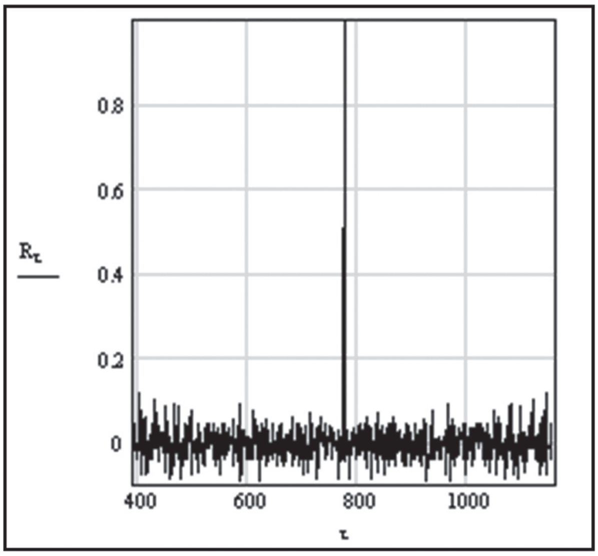

Fig. 7. Autocorrelation function of BPR-sequences for the following parameters: $M = 125$, $Q = 3$, $q = 1$; $Period = 775$

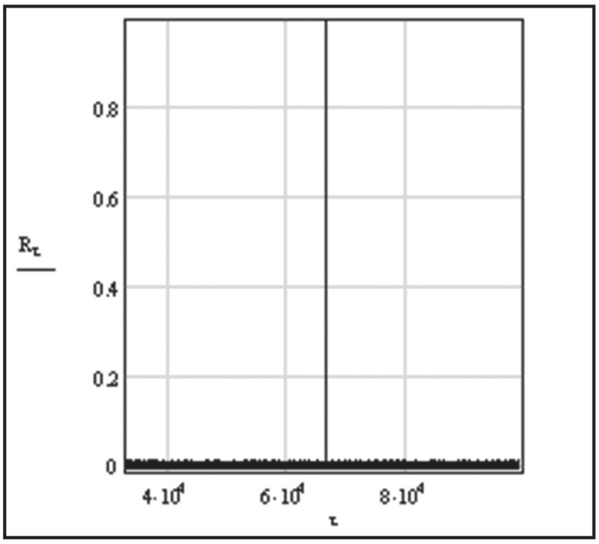

Fig. 8. Autocorrelation function of BPR-sequences for the following parameters: $M = 257$, $Q = 3$, $q = 1$; $Period = 66307$

The maximal outlier characteristics of the correlations are practically the same in all investigated auto- and cross-correlation functions and they are rather close to similar characteristics of the auto- and cross-correlations of random sequences with uniform probability distributions [7, 8 and 10].

CONCLUSIONS

1. A new method for generation of quasi-orthogonal chaotic sequences has been suggested for applications both in radars and communication systems. The method is based upon a discrete chaotic algorithm of a recurrent parametric type with two delay parameters. This algorithm allows generating a *rather wide* family of binary pseudorandom sequences.

2. Phase space structure of the suggested algorithm has been investigated and analyzed via computer simulation technique. The period spectrum of cyclic trajectories in phase space for different values of time delay parameters has been found. The analytical expression for calculation of rather long periods of BPR-sequences generated via discrete chaotic map with to delay parameters.

3. Statistical and correlation characteristics of BPR-sequences, generated according to the method suggested have been studied in detail. The computer simulation has shown that for the properly chosen values of the delay parameters the suggested discrete chaotic algorithm generates binary pseudorandom sequences with close to uniform probability distribution $p(x) = 1/M$. The correlation characteristics of BPR-sequences generated correspond to the correlation characteristics of the random process with uniform probability distribution.

4. It is shown that quasi-orthogonal binary sequences, generated according to the method suggested fulfill all the requirements to the signals used both in radars and communication systems.

References

[1] Konstantin Lukin, Valery Shcherbakov, Vladimyr Konovalov, Ryan Breed. Dedicated Short-Range Communication System for Vehicle-to-Vehicle Data Transmission on the Basis of Chaotic Waveform codes (DSRC-VVDT). // Proceedings of 16 International Conference on Microwaves, Radar and Wireless Communications – MIKON-2006, Krakow, Poland, May 22 – 24, 2006, Vol. 1, pp. 442 – 445.

[2] K.A. Lukin, V.Ye. Shcherbakov, V.M. Konovalov, D.S. Breed. Design Method of Self-Organizing Communication System for Vehicle-to-Vehicle Data Transmission on Highway. Radio-Electronic and Computer Systems, Kharkov «KhAI», 2007, №6 (25), pp. 238 – 244. (In Russian)

[3] K.A. Lukin, V.Ye. Shcherbakov, V.M. Konovalov, D.S. Breed. New Concept of Multiplex Broadband Wireless Communication for Vehicle-to-Vehicle Data Transmission on Highways. // Proceeding of the Sixth International Kharkov Symposium on Physics and Engineering of Microwaves, Millimeter and Submillimeter Waves – MSMW'07, Kharkov, Ukraine, June 25 – 30, 2007, Vol. 2, pp. 852 – 854.

[4] V.Ye. Shcherbakov, K.A. Lukin. The Modeling of System for Vehicle-to-Vehicle Data Transmission/Reception on Highway. Radio-Electronic and Computer Systems, Kharkov «KhAI», 2009, №7 (41), pp. 288 – 294. (In Russian)

[5] K.A. Lukin, V.Ye. Shcherbakov. A Forming Method of Quasi-Orthogonal Chaotical Codes for Data Transmission/Reception System between Vehicles on Highway. Applied Radio Electronics, 2012, Vol.11, №1, pp. 37 – 43. (In Russian)

[6] Knuth D.E. The Art of Computer Programming, vol.2, Seminumerical Algorithms. 2007. P. 832. (In Russian)

[7] Hayes Brian // American Scientists. 1999. V.87. №4. P. 296.

[8] Kahaner D., Moler C., Nash S. Numerical Methods and Software. 2001. P. 575.

[9] K.A. Lukin, Iu.L. Maistrenko, A.N. Sharkovskii, V.P. Shestopalov. Method of Difference Equations in a Resonator Problem with a Nonlinear Reflector. Reports of Academy of Sciences of the USSR, 1989, Vol. 309, pp. 327 – 331. (In Russian)

[10] Varakin L.Ye. Communication Systems with Noise-Like Signals. Moscow. Radio and Communication. 1985. (In Russian)

[11] Yu.V. Gulyaev, V.Ya. Kislov, V.V. Kislov, V.I. Kalinin, V.V. Kolesov, R.V. Belyaev, G.M. Vorontsov. Broadband Telecommunication Facilities with CDMA on the Basis of Chaotic Signals. Radiotekhnika, 2002, № 10, pp. 3 – 15. (In Russian)

Manuscript received December, 12, 2012

Konstantin A. Lukin, M. Sc. (1973), Ph. D. (1980), Doctor of Sc. in Physical Electronics (1989), Professor (2005), IEEE Fellow, a chief of Department for Nonlinear Dynamics of Electronic System, Institute for Radiophysics and Electronics of NAS of Ukraine. His current research interests are dynamical chaos, nonlinear microwave electronics, chaotic waveform generation, random signal processing, noise radar technology.

Valery Ye. Shcherbakov, M. Sc. (1976), a principal research engineer of Department for Nonlinear Dynamics of Electronic System, Institute for Radiophysics and Electronics of NAS of Ukraine. Current research interests: chaotic waveform generation, random and pseudo-random signal processing, short-range radar and spread spectrum communication system.

Dmytro V. Shcherbakov, M. Sc. (2003), M. Sc. (2005), Senior Software Engineer of Subsidiary Company «TOA Ukraine», TOA Technologies Inc., USA. Current research interests: Computer Science, Software Development, ICT Management, Business Intelligence, Business Administration.

УДК 621.396.2.018.424

Новый метод формирования квазиортогональных хаотических последовательностей / К.А. Лукин, В.Е. Щербаков, Д.В. Щербаков // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 1. – С. 17–24.

Предложен новый метод формирования квазиортогональных хаотических последовательностей для применения как в радарах, так и в связных системах. Метод разработан на базе дискретного хаотического отображения с двумя параметрами запаздывания. Компьютерным моделированием проанализирована структура фазового пространства предложенного алгоритма. Найден спектр периодов циклических траекторий в фазовом пространстве, различающихся параметрами запаздывания. Проведено исследование статистических и корреляционных характеристик бинарных псевдослучайных последовательностей, сформированных согласно методу. Моделирование показало, что при соответствующем выборе параметров запаздываний предложенный дискретный хаотический алгоритм формирует бинарные псевдослучайные последовательности с распределением вероятностей, близким к равномерному. Показано, что корреляционные характеристики бинарных псевдослучайных последовательностей, сформированных дискретным хаотическим алгоритмом, соответствуют корреляционным характеристикам случайного процесса с равномерным распределением вероятностей.

Ключевые слова: квазиортогональная хаотическая последовательность, дискретный хаотический алгоритм, хаотическая целочисленная последовательность, хаотическое отображение, фазовое пространство, бинарная псевдослучайная последовательность, автокорреляционная и взаимнокорреляционная функция.

Табл. 5. Рис. 8. Библиогр.: 11 наим..

УДК 621.396.2.018.424

Новий метод формування квазіортогональних хаотичних послідовностей / К.О. Лукін, В.Є. Щербаков, Д.В. Щербаков // Прикладна радіоелектроніка: наук.-техн. журнал. – 2013. – Том 12. – № 1. – С. 17–24.

Запропонований новий метод формування квазіортогональних хаотичних послідовностей для застосування як в радарах, так і в системах зв'язку. Метод розроблений на базі дискретного хаотичного відображення з двома параметрами запізнювання. Комп'ютерним моделюванням проаналізована структура фазового простору запропонованого алгоритму. Знайдений спектр періодів циклічних траєкторій у фазовому просторі, що розрізняються параметрами запізнювання. Проведено дослідження статистичних і кореляційних характеристик бінарних псевдовипадкових послідовностей, сформованих згідно з методом. Моделювання показало, що при відповідному виборі параметрів запізнювань запропонований дискретний хаотичний алгоритм формує бінарні псевдовипадкові послідовності з розподілом ймовірностей, близьким до рівномірного. Показано, що кореляційні характеристики бінарних псевдовипадкових послідовностей, сформованих дискретним хаотичним алгоритмом, відповідають кореляційним характеристикам випадкового процесу з рівномірним розподілом ймовірностей.

Ключові слова: квазіортогональна хаотична послідовність, дискретний хаотичний алгоритм, хаотична цілочисельна послідовність, хаотичне відображення, фазовий простір, бінарна псевдовипадкова послідовність, автокореляційна та взаємокореляційна функція.

Табл. 5. Іл. 8. Бібліогр.: 11 найм.