Improved Method of Formation of an Increased Number of Binary Quasi-Orthogonal Code Sequence Systems with the Required Statistical and Correlation Characteristics

Aleksandr P. Zhuk
Department of Organization and Technology of Information Protection
North-Caucasus Federal University
Stavropol, Russia
alekszhuk@mail.ru

Dmitrii V. Orel
Department of Organization and Technology of Information Protection
North-Caucasus Federal University
Stavropol, Russia
kde.def@gmail.com

Igor A. Kalmykov
Department of Information Protection
North-Caucasus Federal University
Stavropol, Russia
kia762@yandex.ru

Andrey V. Studenikin
Department of Organization and Technology of Information Protection
North-Caucasus Federal University
Stavropol, Russia
studentstavropol@mail.ru

***Abstract*—The article offers the use of a class of special signals for information security in telecommunication systems with code division of channels. By varying the parameters of the random number generator, the type of initial distribution laws and the law of transformation, it is possible to form an unlimited number of systems of pseudo-random sequences with specified properties. This approach is an improved method of forming an increased number of binary quasi-orthogonal systems of code sequences with the required statistical and correlation characteristics. The proposed method of formation of an increased number of binary quasi-orthogonal code sequence systems with the required statistical and correlation characteristics can be used to obtain expanding codes in satellite communication systems.**

Keywords—wireless, telecommunication, multiple access, code sequence systems, quasi-orthogonality, correlation, spectrum

I. Introduction

Modern wireless telecommunications systems are used for transmission of noise-like information signals (NLS), which due to the unique structure of the code can be transmitted in a common frequency band and effectively separated at the receiving side. Technology multiple access CDMA communication enables stable complex under conditions of interference and achieving confidentiality when exchanging information [1, 2].

Ensuring the confidentiality of messages transmitted true recently for mobile robotic systems, wireless security systems, and in other areas [4, 5]. Transmission of confidential communications over wireless channels can be achieved by providing energy and structural secrecy signals - information carriers and information secrecy of the message itself. [6].

Estimate of the energy stealth communication system NLS indicates [7, 8] that the analysis in the detector is greater than a wider range of NLS and above the required value of the signal / noise ratio at the output of the detector, i.e. the most radical means increasing energy secrecy is to expand the spectrum NLS [6].

Structure (warning) signal for this secrecy is ensured by know their statistical characteristics to the natural background, as identification signs determinism may be crucial [9]. To ensure secrecy signal NLS sequences are particularly important issues synthesis length N, having a high complexity of structure and solving a sufficiently representative amount of the system L sequences, followed by subjecting them to an automatic changer for a particular algorithm with acceptable complexity of the apparatus.

II. Analysis of the Question

Signals system NLS largest volume L are divided into three types:

- small ($L = \sqrt{\beta} << \beta$);
- normal ($L = \beta$);
- great ($L << \beta$),

wherein for the pseudorandom sequences (PRS) process gain $B = N$, where N - PRS length [2].

For the PRS to meet the following basic requirements [11]:

- high resolution sequences systems formed on a single algorithmic basis;
- balance sequences structure (ratio of the number of "1" and "0" in the sequence);
- optimality of autocorrelation function (ACF) and cross correlation function (CCF) of sequences in the system.

By systems PRS imposed usual requirements required of the spread spectrum signals and code division, i.e., the presence of "good" correlation properties.

By the form of the algorithm formation PRS are divided into two classes: linear and nonlinear. Linear PRS does not provide structural secrecy NLS because of easy predictability.

Nonlinear PRS have higher unpredictability, but have several drawbacks:

- they belong to sequences forming assemblies with small volume;
- small length sequences;
- systems with increasing volume correlation properties PRS begin to deteriorate rapidly [4].

In recent years, a number of publications exploring the chaotic nature of the movement in some types of nonlinear dynamical systems. For a description of a nonlinear dynamical system at discrete instants of time generally used state equation of the form [4]:

$$x_{k+1} = F(x_k),\ k = 0, 1, 2, \ldots,$$

where $x_{k+1,}$ x_k - state of the system in the current and previous times; $F(\text{-})$ - usually its transition from a state x_k to a state x_{k+1}.

The choice of initial conditions xo and transition rules $F(\text{-})$. It determines the dynamic behaviour of the system in which it has a non-periodic character.

Investigation of models of nonlinear dynamic systems indicates a greater sensitivity of the system to small changes in initial conditions. This property is crucial because it allows you to form large systems of signals [12, 13].

By varying the initial conditions, the rules of the transition and the so-called parameter bifurcation [3] can be synthesized fairly large number of different sequences, spreading the spectrum of the information signal and change shape NLS from symbol to symbol.

The analysis shows that the side peaks of the normalized cross correlation functions (CCF) of such signals does not exceed the largest side peaks of normalized autocorrelation functions (ACF) of the same sequences and reach the level of 0.2 that is close to the level of random sequences (of the same order with side peaks MCF M-sequences), but at a predetermined code length *N* system *L* volume significantly exceeds the volume of the system M-sequences.

This leads to the conclusion about the applicability of this class of PRS for use in telecommunication systems CDMA.

III. Statement of the task

This leads to the conclusion about the applicability of this class of PRS for use in telecommunication systems CDMA.

Using the random and chaotic sequences as PRS generators and treating them with single system positions possible, taking into account the Kolmogorov entropy [6], which gives random sequences unpredictable. According to the authors, these two independent areas of random processes are not the only ones using them as PRS generators.

Consider a continuous random variable x, a given distribution law $f(x)$. Another random variable y is related to its functional relationship $y = \varphi(x)$.

The resulting distribution function of y transforms the initial random process in a new class of random functions, which in the formal description are beginning to show some of the specific properties of a class of chaotic functions - properties of self-similarity.

In this paper we propose to consider three classes of dependencies [14, 15]:

1) Stochastic processes described by classical methods.

2) Chaotic processes described equations states of a nonlinear dynamical system solutions which are strange attractor.

3) Singular (special) processes which are described by classical methods of the theory of random functions, but possess certain specific properties similar to the appearance of chaotic processes.

According to the authors, the third class is the link between the first and second classes and named special.

IV. Solution of the task

As currently told, there are two approaches to the description of random signals. First, the traditional approach is based on the idea that the subject description and studying the signal is random, unpredictable algorithmically. This approach is based on well-studied and developed the mathematical apparatus that combines the theory of probability and mathematical statistics. Such processes are called stochastic.

If there are many implementations of *N* random process $\xi(t)$ evolving in time t, then for sufficient duration *T* implementations, the concept of the cumulative distribution function:

$$F(x_1,t_1) = P\ \{\xi(t_1) \le x_1\}$$

those, the probability that at $t = t_1$ random function $\xi(t)$ is lower than x_1.

If $F\ (x_1,\ t_1)$ is the partial derivative of x_1, then

$$\frac{\partial \mathrm{F}(x_1 t_1)}{\partial x_1} = \mathrm{f}\,(x_1 t_1)$$

is called probability density of a random process $\xi(t)$.

To describe stochastic processes using numerical characteristics obtained by averaging these processes in a predetermined time (moment functions).

In the second approach, believed to complex the processes studied, but deterministic, implemented with a predetermined algorithm. In this case, the dynamic system, which behaviour is predetermined in time (described by a system of equations with predetermined initial conditions). However, the solution of these equations shows properties characteristic of random, unpredictable processes. The decisions may be no periodicity with limited motion in the phase space, but there is a significant dependence on initial conditions. In the simulation of the system, showing the chaotic behaviour, the accuracy of the result can only be guaranteed on a certain number of steps. The set of solutions in which there is the chaotic motion depending on the system parameters and initial conditions called strange attractor [6]. Kolmogorov showing the degree of chaos dynamic system. It is interpreted as the average rate of loss of information about the system. The magnitude of the Kolmogorov entropy can be judged potentially possible time predicting trajectory. This value is associated with the dimensionality of the system and with the features of nonlinearities, responsible for the conversion.

A third approach developed in this article is associated with the transformation of random argument function [5].

There is a random variable X with the density distribution $f(x)$. Another random value Y related to it functional relationship:

$$y = \varphi(x) \tag{1}$$

It is necessary to determine the density distribution of the value of Y.

We consider the axis of a portion of the x (a, b) on which lie all possible values of X. That is,

$$P\ (\mathrm{a} < x < \mathrm{b}) = 1.$$

In the particular case where the range of possible values of x is not limited to

$$\mathrm{a} = -\infty;\ \mathrm{b} = +\infty.$$

Consider the case where the function (1) on a plot (a, b) - increases monotonically (Fig. 1).

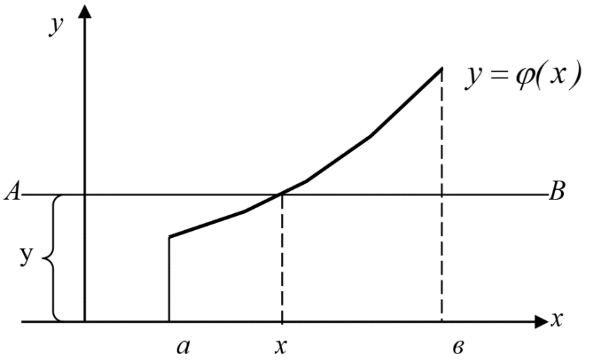


Fig. 1. Monotonically increasing function *y*

When the quantity X takes different values in the interval (a, b) random point (X, Y) always moves along the curve $y = \varphi(x)$. That is, the ordinate of the random point is defined by its abscissa.

Let $g(y)$ have a density distribution value y. In order to determine $g(y)$, we find the distribution function of the variable Y

$$G(y) = P(Y < y).$$

Draw a straight line AB which is parallel to the horizontal axis at a distance from y it (Fig. 1). To satisfy the condition of $Y < y$, random point (X, Y) must fall on the curve portion, which lies below line AB. For this purpose it is necessary and sufficient that the random variable X penetrated the portion of the abscissa of a to x, where x - the abscissa of the intersection point of the curve (1) and the line AB.

Consequently

$$G(y) \ = \ P(Y < y) = P(a \ < X < x) = \int_a^x f(x)dx.$$

We express the upper limit of the integral expressed in terms of y x

$$x = \psi(y) = \varphi^{-1}(y),$$

where ψ - the inverse function of y, then

$$G(y) = \int_a^{\psi(y)} f(x)dx. \tag{2}$$

Differentiating (2) the variable y entering the upper limit, we obtain

$$\mathrm{g(y)} = G'(y) = f[\psi(\mathrm{y})]\cdot\psi'(y), \tag{3}$$

where the prime hereinafter denotes differentiation with respect to y. Easy to show that for monotonically decreasing (1)

$$g(y) = G'(y) = -f[\psi(y)]\cdot\psi'(y).$$

Features (3) and (4) may be combined into one

$$\mathrm{g(y)} = |\psi'(y)|\cdot \mathrm{f}[\psi(\mathrm{y})]. \tag{4}$$

since the minus sign for decreasing function disappears due minus obtained as a result of its differentiation.

In the general case, when the function is not monotonic

$$\mathrm{G(y)} = \sum_{\mathrm{i}} \int_{\Delta_i(\mathrm{y})} \mathrm{f(x)dx},$$

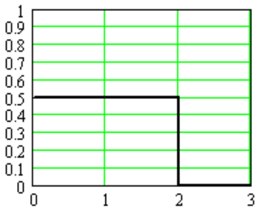
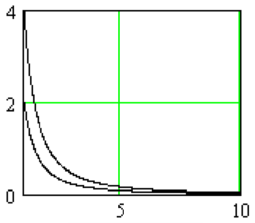
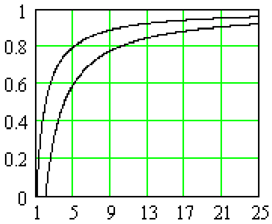
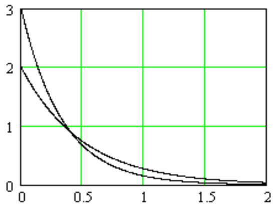
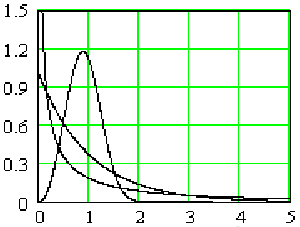
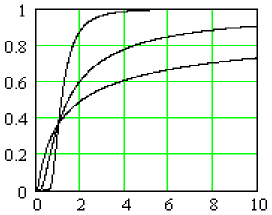
where Δ_i (y) - plot, which gets a random variable x.

The boundaries of the intervals where Δ_i (y) depend on y and given concrete form function (1) can be expressed explicitly.

In this paper we consider the case when the initial probability density $f(x)$ describes the distribution of instantaneous values of a random process $\xi(t)$.

The random variable Y, the associated functional dependence (1), determines the nature of the transformation. Consider the case where the result of the transformation is to obtain a sequence of characters, the random variable $y = \tau$ where τ - the time interval between symbols, which is a random variable, and the distribution law quantity τ fully

TABLE I. TWO INITIAL DISTRIBUTION LAWS: UNIFORM AND EXPONENTIAL

Source law distribution	Func. pre-obmation	Distribution law interval	Interval distribution function	The value of the interval between pilot symbols
Uniform	$\psi(\tau)$	Pareto	Pareto	
 $f(x)=\begin{vmatrix}1, \rho<x<1\\ 0, x<0, x>1\end{vmatrix}$	$\left(\frac{k}{\tau}\right)^{\alpha}$	 $g(\tau)=\frac{\alpha\cdot k^{\alpha}}{\tau^{\alpha+1}}$	 $G(\tau)=1-\left(\frac{k}{\tau}\right)^{\alpha}$	$\tau_n=\frac{k}{(1-rnd)^{\frac{1}{\alpha}}}$
Exponential	$\psi(\tau)$	Weibull	Weibull	
 $f(x)=\alpha e^{-\alpha x}, x>0$	τ^{β}	 $g(\tau)=\alpha\cdot\beta\tau^{\beta-1}e^{-\alpha\tau^{\beta}}$	 $G(\tau)=1-e^{-\alpha\cdot\tau^{\beta}}$	$\tau_w=\left[\frac{1}{\alpha}\ln\left(\frac{1}{1-rnd}\right)\right]^{\frac{1}{\beta}}$

describes the statistical properties of the sequence of symbols in the signal, so that

$$y = \tau = \varphi(x) \qquad (5)$$

In view of this clarification, the connection between the instantaneous values of a random process and a time interval between the signal thus formed symbols can be rewritten in the following form:

$$G(\tau)=\int_{a}^{\psi(\tau)} f(x)dx, \qquad (6)$$

$$q(\tau)=G'(\tau)=|\psi'(\tau)|\cdot f[\psi(\tau)]. \qquad (7)$$

The expression (6) in the general form is based on using the Fundamental Theorem of expression:

$$\int_{x_1}^{x_2} f\,(x)dx = F(x_2)-F(x_1).$$

Thus, we have:

$$G(\tau) = F[\psi(\tau)] - F(\alpha).$$

From where we find

$$F[\psi(\tau)] = G(\tau) - F(\alpha).$$

We define the random variable τ:

$$\tau = \psi^{-1}\{F^{-1}[G(y) - F(\alpha)]\}.$$

Given that $\psi^{-1} = \varphi$

$$\tau = \varphi\{F^{-1}[G(y) - F(\alpha)]\}.$$

The value of a is found from the normalization condition

$$\int_{a}^{\psi(\tau)} g(\tau)d\tau = 1$$

Switching flow intervals between incoming pulses distributed according to (8) may be obtained by nonlinear transformation of random variable. In other words (6) for generating a random variable with distribution function , it is necessary to construct a deterministic function $\tau = g^{-1}(y)$ and receive the required random numbers as values of the argument of the function defined by the number, is a random variable with uniform distribution law in the interval (0,1). Rewrite the formula (8) with these

$$\tau = \varphi\{rnd - F(\alpha)]\}, \qquad (9)$$

where *rnd* - random variable uniformly distributed in the interval (0,1).

For example, consider the conversion from (9) two initial distribution laws: uniform and exponential (Table 1).

As the transformation functions in the first case taken inverse power function, and in the second - the power function as shown in the second column of Table 1.

The selection of such conversion functions for said distribution laws dictated by the possibility of obtaining distribution interval duration between packets in the form of distributions with known heavy tails: Pareto and Weibull (Tab. 1, third col.). In the fourth and fifth col. of Tab. 1 lists the corresponding value of the distribution function $G(\tau)$ and she sought value τ (Fig. 2).

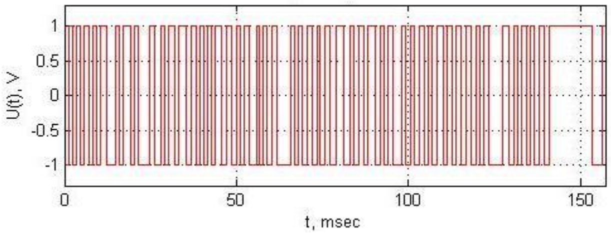


Fig. 2. The timing diagram for Pareto distribution (α = 3)

Type of ACF and CCF signals used determines the comparison of ACF and CCF functions study was conducted with the ACF and CCF of M-sequences and Gauss random sequences having ACF close in form to the δ-function having side autocorrelation functions emissions not exceeding levels 1/√*N*.

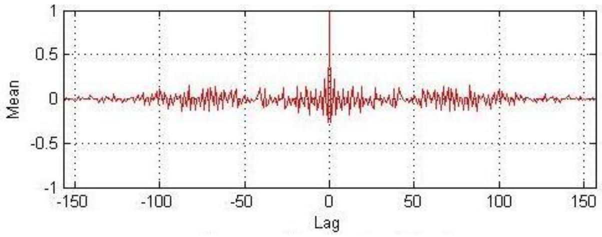


Fig. 3. ACF sequence Pareto (α = 3)

Typical view normalized aperiodic autocorrelation function is shown in Fig. 3, for Pareto distribution with shape parameter (α = 3).

Cross correlation function of two fragments of finite length signal obtained using Pareto distribution shown in Fig. 4.

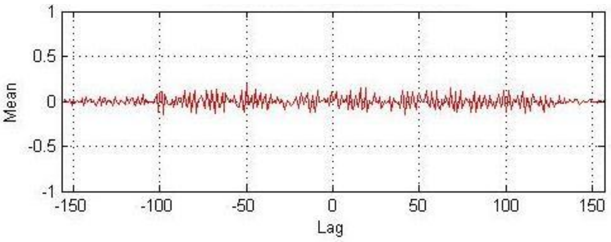


Fig. 4. CCF two fragments finite length signal obtained using Pareto (α=3)

As can be seen from the figure, the side normalized CCF peaks do not exceed the magnitude of the peaks of the normalized autocorrelation function of the same sequences.

Analysis of the results leads to the conclusion that the ACF and CCF singular sequences close to the correlation properties of random sequences.

Maximal side peaks of the same order with side peaks CCF M-sequences, but for a given length code system amount substantially exceeds the amount of system M-sequences.

There are a number of algorithms for pseudo-random numbers, for example, the deduction method. If you specify a seed γ_0 in the shape of irreducible fraction $\gamma_0 = m_0 / M$. Where m_0 and M – are integers and M is relatively prime number with some integer q, then all the subsequent numbers γ_k are irreducible fractions $\gamma_k = m_k / M$ where m_k is defined by the numerator

$$m_{k+1} = q \cdot \mathrm{m}_k -]\frac{q \cdot m_k}{M}[\cdot M, \tag{10}$$

and inverse square brackets mean that takes the greatest integer that does not exceed the result of the implementation of actions in brackets.

Expression (10) is a recurrent and allows to obtain a sequence of pseudorandom integers uniformly distributed in the interval (1, *M*, -1). The resulting sequences are cyclic, because after a certain amount of numbers begin to repeat the steps. Satisfactory sequence of integers is obtained when $q = 5^{17}$, $M = 2^{40}$, the length of the non-repeating sequence of $2.75 \cdot 10^{11}$ numbers.

V. Conclusion

Analysis of the results suggests a class of singular sequences suitable for use in telecommunication CDMA systems due to the rather "good" correlation properties.

In addition, singular sequences allow signals to form large systems which volume ($L >> B$) can significantly exceed the base signal resolution. By varying the parameters of the random number generator (10) views the initial distribution laws $f(x)$, the parameters of which are limited only by the normalization condition, and the selected transformation rule (1) can generate an unlimited number of systems of pseudorandom sequences with desired properties.

Acknowledgment

This work was supported by the Russian Foundation for Basic Research, project No. 18-07-01020.

References

[1] Varakin L. E. “Theory of signals systems”. Moscow, Soviet radio, 1978 (in Russian).

[2] Zalogin N.N., Kislov V.V. “Broadband chaotic processes in radio engineering and information systems”. Moscow, Radio Engineering, 2006 (in Russian).

[3] “System-wide issues of information security”. Collective monography. Edited by E. M. Sukharev. – Book 1. Moscow, Radiotechnics, 2003 (in Russian).

[4] Pashintsev, V.P., Peskov, M.V., Kalmykov, I.A., Zhuk, A.P., Senokosov, M.A. “Method for the evaluation of ionospheric diffractive and dispersive properties impact on the interference immunity of satellite communication systems” International Journal of Civil Engineering and Technology. 2018; 9(13), pp. 44-61.

[5] 5. Aleksandr Zhuk, Dmitrii Orel. “Improved Method for Estimating Noise Immunity of Global Navigation Satellite Systems”. Advances in Intelligent Systems Research. 2019; volume 166, pp. 303-308.

[6] Ventzel E. S. “Probability theory”. Moscow, Academy, 2003 (in Russian).

[7] Tebueva, F., Kopytov, V., Petrenko, V., Kharechkin, P., Sidorchuk, A. “Method for detecting and eliminating data time series outlier in high-speed process data sensors” International Journal on Communications Antenna and Propagation. 2017; 7(7), pp. 603-612.

[8] Zhuk, A.P., Ryabtsev, S.S., Khachkizov, R.A., (...), Dzhamiev, N.D., Sherbakov, D.A. “Analysis of the information protection methods in telecommunication systems with channels split by code”. In: CEUR Workshop Proceedings, 2254, pp. 303-310.

[9] Gavrishev, A.A., Zhuk, A.P., Osipov, D.L. “An analysis of technologies to protect a radio channel of fire alarm systems against unauthorized access”. In: SPIIRAS Proceedings. 2016.

[10] Orel, D., Zhuk, A., Zhuk, E., Luganskaia, L. “A method of forming code sets for CDMA in communication, navigation and control systems”. In: CEUR Workshop Proceedings. 2017.

[11] Tebueva, F.B., Kopytov, V.V., Petrenko, V.I., Shulgin, A.O., Demirtchev, N.G. “The identification of data anomalies from information sensors based on the estimation of the correlation dimension of the time series attractor in situational management systems” Journal of Theoretical and Applied Information Technology. 2018; 96(8), pp. 2197-2207.

[12] 12. Pashintsev, V.P., Kalmykov, I.A., Zhuk, A.P., Kalmykov, M.I., Rezenkov, D.N. “Application of spoof resistant authentication protocol of spacecraft in low earth orbit systems of satellite communication” International Journal of Mechanical Engineering and Technology. 2018; 9(5), pp. 958-965.

[13] Kopytov, V.V., Petrenko, V.I., Tebueva, F.B., Streblianskaia, N.V. “An improved Brown's method applying fractal dimension to forecast the load in a computing cluster for short time series”. Indian Journal of Science and Technology. 2016; 9(19): Article# 93909.

[14] D.L. Osipov, A.P. Zhuk and A.A. Gavrishev, “Apparatus for protection against imitation of controlled objects with high structural security of carrier signals”. Patent RF no. 2560824, pp. 15, 2015 (In Russian).

[15] A.A. Gavrishev and A.P. Zhuk, “Application of Methods of Nonlinear Dynamics to Study the Chaotic State of the Carrier Signals of Secure Communication Systems Based on Dynamic Chaos”. Vestnik NSU. Series: Information Technologies. No. 2018; 16(1), pp. 50-60 (in Russian).