A Method of Forming Code Sets for CDMA in Communication, Navigation and Control Systems

Dmitrii Orel
North-Caucasus Federal University
Russian Federation
kde.def@gmail.com

Aleksandr Zhuk
North-Caucasus Federal University
Russian Federation
alekszhuk@mail.ru

Elena Zhuk
North-Caucasus Federal University
Russian Federation
a1jona@yandex.ru

Liudmila Luganskaia
North-Caucasus Federal University
Russian Federation
lyuda_st87@mail.ru

Abstract

The method of forming code sets for communication, navigation and control systems with CDMA is proposed. The method allows forming code sets of various desired dimension: any length of codes and any number of codes in set. The formed binary codes have required statistic and correlation properties for using in wireless systems with CDMA. Quantity of sets allows increasing the structural secrecy of wireless systems to increase integrity, availability, reliance and secrecy of transmitted data.

1 Introduction

Code division multiple access technology (CDMA) has been used actively in wireless communication, navigation and control systems.

Radio channels are used actively in projects that implement the Smart City technology [Boc12] [Zai13-2] [Sam14], such as developing intelligent transport systems and Wireless Metropolitan Area Network (WMAN). Such network may be a data channel for sensors, communication and control devices in other solutions for Smart city: safety, transport, urban infrastructure management, location-based services (LBS).

Security systems are also actively moving to wireless links. At present, the promising for such systems is technology with noise-like signals based on the ultra-wide band (UWB) with the choice of time-frequency position by pseudorandom. To detect / reduce the incidence of false positives more reliable and modern communication protocols are being introduced: 4G and LTE. Autonomous security and fire detectors with GSM-modules and cameras are being evolving. For fire systems, a reliable way to transmit notifications about fire is two-way radio channel transmission system on the allocated frequencies [Zai13-2].

In addition, the trend is increasing usage of global navigation satellite systems (GNSS) signals in various technical infrastructure. Synchronization of power network, public communications networks [Zhu12-1], cable television broadcasting networks [Kuk03], of cellular mobile networks IMT-450 [Ore11-1], banking and exchange systems, as well as other radio networks [Ore11-1] based on GNSS. It should be noted that it is planned to

In: S. Hölldobler, A. Malikov, C. Wernhard (eds.): *YSIP2 – Proceedings of the Second Young Scientist's International Workshop on Trends in Information Processing, Dombai, Russian Federation, May 16–20, 2017*, published at http://ceur-ws.org.

significantly expand the use of unmanned aircraft, unmanned vehicles and other modes of transport in coming decade. Controlling these objects in most cases is carried out by wireless channel.

Such increase in the use of wireless technology, in turn, increases interest of different kinds of intruders to disrupt the wireless data transmission channels in these systems. Jamming and spoofing radio signals can lead to disruption of integrity, availability, reliance and secrecy of transmitted data. One of the possible ways to counteract the influence to wireless data transmission channel is to increase the noise immunity of a wireless system. As a key step for jamming and spoofing the radio signal is a radio intelligence, the most important component of the noise immunity increase is to increase the secrecy - the system's ability to resist radio intelligence (monitoring). According to radio intelligence stages here are the following kinds of secrecy:

1. Energy secrecy: counter signal detection in noise.
2. Structure secrecy: resistance to definition of signals structure.
3. Information secrecy: counter disclosure of information.

Most mentioned communication, navigation and control systems use or have a tendency to introduce the principle of CDMA. High interest in the technology of wideband multiple access with CDMA is caused by it largely superior to other access methods. CDMA signals have sufficiently high energy secrecy - for each communication channel is used a wideband signal, and the energy of signals is generally below the natural level of noise. Information secrecy can be implemented by cryptographic methods. Their use in a number of cases will allow to resist against the threats to secrecy and reliance of the information but would be ineffective against the threats to integrity and availability.

Structural secrecy of CDMA signals can be achieved by using a large number of orthogonal and quasi-orthogonal code sets, which are replaced at intervals. The smaller change period used for code sets and the greater number of sets to be used, the higher structural secrecy of wireless system will be achieved. The ideal case would be a one-time used code set with its change without repeating.

In most modern communication, navigation and control systems are used binary code sets (BCS) with the base $N \geq 256$ and the number of codes in set $K \geq 30$. BCS is a number of binary codes with equal length (base), which are orthogonal or quasi-orthogonal to each other. Each binary code is used in one radio channel, and the orthogonality or quasi-orthogonality allows dividing channels in receiver. However, existing methods of forming code sets allow them to receive them in an amount effective to change them without repeating for a limited period of time, measured from a few hours to several months [Ore14]. It is necessary to have a method of forming code sets, allowing maintain a high level of structural secrecy of the signal for the life-time of the wireless system. In this regard, the purpose of this article is to provide a method of forming BCSs for wireless systems with CDMA, which allows their amount sufficient to increase the structural secrecy of radio signal for a period of 10 years or more. Such period is chosen as a minimum life-cycle time of communication technology.

2 Methods

It should be noted that the entire set of requirements to BSC imposed necessary for use them in wireless systems with CDMA. For CDMA wireless systems, codes with good correlation properties are most suitable. For BSC with good correlation properties is necessary codes to have signs of randomness, have the following properties [Gol67]:

1. Balance Property: in each period of binary code the number of "1" is different from the number of "0" not more than one unit.
2. Series Property: a half of binary code series "1" and "0" has a length 1, one-quarter - 2, one eighth - 3 etc. as long as it still makes sense.
3. Autocorrelation Property: if binary code compared with any cyclic shift during the same period, the number of hits different from the number of mismatches must be not more than one unit. The result of the summation modulo 2 of binary code with its cyclic shift should also be balanced binary code.

In case of using BCS duding 1 ms, the number of sets must be $A_r = 3.1536 \cdot 10^{11}$ to change them for a period of 10 years without repeating. As is quite big, it must be proved, that the number of BCS with required properties exists. As it is known, common number of codes with base N is $A = 2^N$.

It is needed to estimate the number of sets convenient to the Balance Property. The number of "1" code bits is , the number of "0" code bits is . Then the number of codes with Balance Property can be found as the number of combinations of $n_1 = (N+2)/1$ in N, or the number of combinations of $n_0 = (N+2)/1$ in N. It can be proved, that these numbers are equal:

$$C_N^{n_0} = \frac{N!}{n_0!(N-n_0)!} = \frac{N!}{(\frac{N-1}{2})!(\frac{N+1}{2})!}, \qquad (1)$$

$$C_N^{n_1} = \frac{N!}{n_1!(N-n_1)!} = \frac{N!}{(\frac{N+1}{2})!(\frac{N-1}{2})!}. \qquad (2)$$

As the expressions (1) and (2) differ only in the order of the factors in the denominator, then $C_N^{n_0} = C_N^{n_1}$. Then the common number of codes with Balance Property can be found with the next expression:

$$K(n_1) = C_N^{n_1} = C_N^{(N+1)/2}. \qquad (3)$$

To keep the Series Property [Var78], the common number of series in the code bust be approximately equal to the half of the code length:

$$\mu_0 \approx 0.5(N+1), \qquad (4)$$

where N - code length. The expression to find the number of codes with required series number [Kuk03] is:

$$A_\mu = 2C_{N-1}^{\mu-1} = 2\frac{(N-1)!}{(\mu-1)!(N-\mu)!}, \qquad (5)$$

where μ - the number of series in code, N - code length.

In addition, codes in BCS must have small peaks of the shifted correlation functions. The common number of codes with required Autocorrelation Property is limited and is estimated with the next expression [Kan06]:

$$A_{cf} = \sqrt{2/(\pi N)} \cdot 2^N. \qquad (6)$$

Table 1 shows the numbers of codes for length 4095, 8191 and 10230 [Pch08] convenient for different requirement as an example.

Table 1: Number of binary codes satisfying various requirements

Number of binary codes	N		
	4095	8191	10230
Common number of binary codes A	$5.22 \cdot 10^{1232}$	$5.45 \cdot 10^{2465}$	$3.43 \cdot 10^{3079}$
Number of binary codes with Balance Property A_b	$6.5 \cdot 10^{1230}$	$4.8 \cdot 10^{2463}$	$1.35 \cdot 10^{3077}$
Number of binary codes with Series Property A_μ	$6.5 \cdot 10^{1230}$	$4.8 \cdot 10^{2463}$	$1.35 \cdot 10^{3077}$
Number of binary codes with Autocorrelation Property A_{cf}	$6.5 \cdot 10^{1230}$	$4.8 \cdot 10^{2461}$	$1.35 \cdot 10^{3075}$

In [Var78] it is concluded that the larger the probability of high side peaks of the autocorrelation function (ACF) is reduced by the number of series tends to the optimal value μ_0. Codes with optimal number of series at the same time are convenient to the Series Property. Than it can be concluded, that there is exits the number of codes, that are required all mentioned properties: $A_{b\ \mu cf} = A_b \cap A_\mu \cap A_{cf}$. At the same time, the number of codes, that are required all mentioned properties, is approximately equal to the number of codes, that are required Autocorrelation Property: $A_{b\ \mu cf} \approx A_{cf}$.

Based on the above, and considering that $A_r \ll A_{b\ \mu cf}$, it can be assumed that there is a theoretical number of codes with the necessary properties.

According to [Gol67], it is considered that the binary codes with the base [±1] have good correlation properties when the averaged value of the aperiodic autocorrelation function (AACF) side peaks modules close to the value $1/\sqrt{N}$ for all time shifts. However, a more rigorous assessment of the correlation properties of the binary code is the maximum value of the side peak AACF R_A modulus. It is known that the maximum AACF side peak can not be less marked border $R_A \geq 1/\sqrt{N}$, where N - binary code length. The correlation properties of the binary code as better as lower the value of the maximum side peak AACF modulus. In BCS along with ACF are important cross correlation functions (CCF) of each pair of binary codes included in BCS. For maximum peaks aperiodic cross correlation functions (ACCF) there is also a lower limit of values, called the Welch bound [Ipa92] [Lev99]. The lower limit of the side peaks ACCF maximum values modulus of the binary codes with the base [±1] is:

$$R_C \geq \frac{\sqrt{N - [\frac{\pi N}{\sqrt{8M}}]}}{N},\ M \geq 5, \qquad (7)$$

where M - the number of binary codes in BCS; N code length; [] - rounding to greater.

Table 2 presents lower bounds of AACF and ACCF maximum side peaks modules for BCS containing $M = 50$ codes of length N 4095, 8191 and 10230 bits.

Table 2: The lower bounds of the maximum values of the AACF and ACCF maximum side peaks modules for BCS of 50 codes

Code length N	Lower bound of AACF maximum side peak modulus R_A	Lower bound of ACCF maximum side peak modulus R_C
4095	0.016	0.016
8191	0.011	0.011
10230	0.010	0.010

As it can be seen from Table 2, the lower bounds AACF maximum side peaks and ACCF maximum peaks modules are close in their values and decrease with increasing code length.

In [Var78] noted that to reduce the RMS CCF should be reduced RMS ACF. Thus, having a plurality of codes with small maximum AACF side peaks of them can be formed BCS with small ACCF peaks.

The given theoretical calculations should be compared with the actual BCS characteristics obtained as a result of a computational experiment.

In this paper, we propose a method of forming BCS, allowing get the required amount of them to ensure a high level of structural secrecy of radio signal for 10 years.

The functional transformation method includes the following main stages:

1. Formation of the original series of pseudo-random numbers $RND = \{rnd_1,\ rnd_2, ...,\ rnd_i\}$ with uniform distribution law.

2. Functional transformation of pseudo-random numbers using the selected function:

$$\tau_i = G^{-1}(rnd_i). \qquad (8)$$

In the method of functional changes as a function is used the expression that characterizes the probability density of interest.

3. Sampling values τ_i of the selected step d:

$$t_i =]\tau_i/d[. \qquad (9)$$

Obtained on the basis of this method a number of pseudo-random numbers $T = \{t_1,\ t_2, ...,\ t_i\}$ has the probability density function G. Thus, changing the form of the function G_{-1} can be obtained numerical series, obeying different distribution laws. Thus it is possible to simulate different processes.

Described modeling method can be supplemented by steps, allowing to model binary codes with properties, which are determined by the choice of the function G_{-1} [Ore13].

The above-described modeling method improved for modeling binary codes with an arbitrary distribution of bits series [?]. To this end, the three above stages have been added to the following:

4. Preparation of bits series of the future binary code by multiplying the series of ones with length t_i at -1 degree t_i:

$$a_i = (-1)^{t_i} \cdot \underbrace{(11...1)}_{t_i}. \qquad (10)$$

5. Preparation of the binary code by building in a single sequence all the series obtained in step 4:

$$n = \{a_1,\ a_2, ...,\ a_i\}. \qquad (11)$$

6. Perform steps 1-5 for the forming the next binary code. In this series of random numbers on j-th and (j+1)-th steps should not overlap either partially or completely.

A feature of this method is the use of simulation BCS resulting functional conversion of pseudorandom numbers t_i ($T = \{t_1,\ t_2, ...,\ t_i\}$) as a parameter, which determines the length of the binary series of the same sign in binary code [Ore13]. The described transformation is graphically represented in Figure 1.

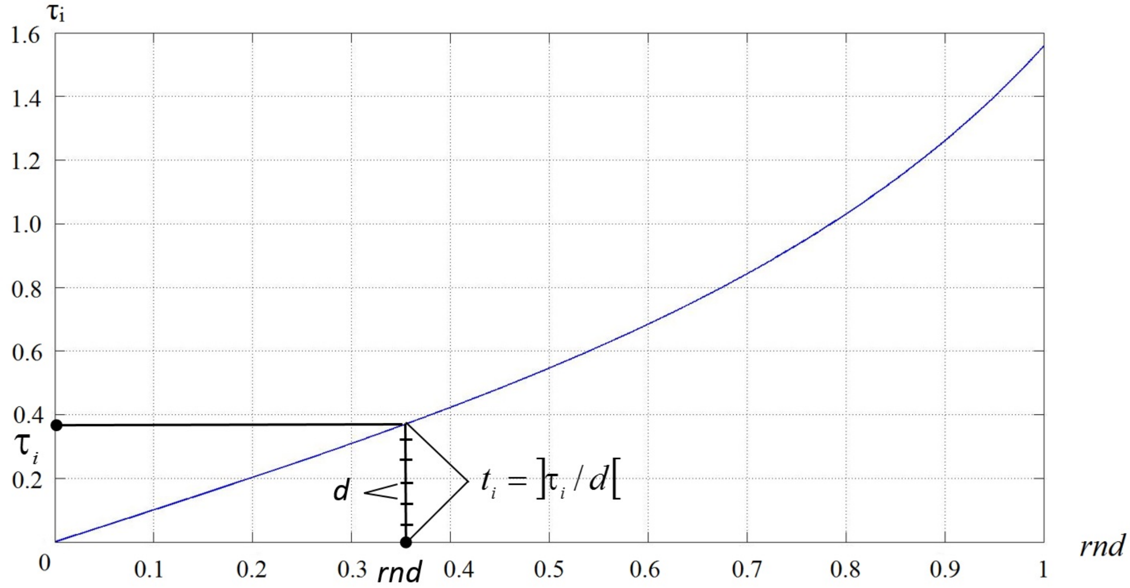

Figure 1: Converting the values of bits in the length of series τ_i

Actual values of the function τ_i being replaced by natural values of the bits series lengths $t_i =]\tau_i/d[$ in formed binary codes.

The proposed BCS modeling method is variable enough: the properties of BCS are significantly influenced by selecting the pseudo-random number generator (PRNG), the choice of the function itself, as well as the steps and the sampling method of rounding. Using various combinations of the designated parameter BCS can be obtained with the desired properties [Zhu10].

Since the choice of the function has a decisive importance to the law of the distribution of the bits series lengths, it can be concluded that the function G^{-1} is an important parameter that determines the properties of the resulting BCS. In the present analysis, it was found that in order to provide the required correlation characteristics in the code the Series Property must be observed: the number of series of length n should be equal $k = 1/2^n$ as long as it makes sense. The maximum length of a bits series at their optimal distribution is $l = \log_2 N$ where N - the code length.

In the proposed method of forming BCS, function values are used as a bits series length of the BCS. This used function allows to set the law of distribution of values obtained, and therefore, the law of distribution of the bits series lengths. For getting pseudo-random numbers distributed according to the law, describes the function G, it must be used the function G^{-1}. It follows that for the binary code series with the distribution of obeying the law, describes the function $G = k = 1/2^n$, it is necessary to use the reverse function $G^{-1} = \tau = log_2(1/rnd)$ [Ore11-2] in the proposed method of modeling BCS where - pseudorandom numbers produced using a PRNG.

3 Results

Computational experiment was conducted to confirm the theoretical hypotheses. For the computational experiment on the BCS formation on the basis of the proposed method in the paper in Matlab environment of computer simulation and engineering calculations the software package has been developed [Zhu12-2]. Results of computational experiment for obtaining a binary codes based on the function in question are listed in Table 3 and in Figures 2-4.

Table 3: Characteristics of the resulting binary codes

Number of codes	100
Code length	10230
Proposed number of series	5116
AACF maximum side peak	0.0467
ACCF maximum peak	0.0567
Actual number of series	5116

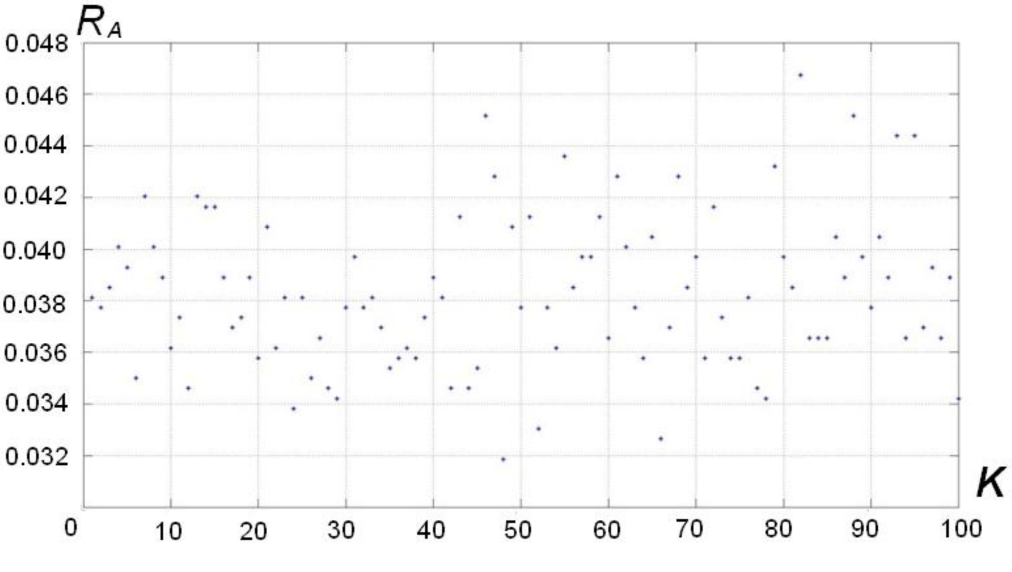

Figure 2: Maximum AACF side peaks of randomly chosen 100 formed codes

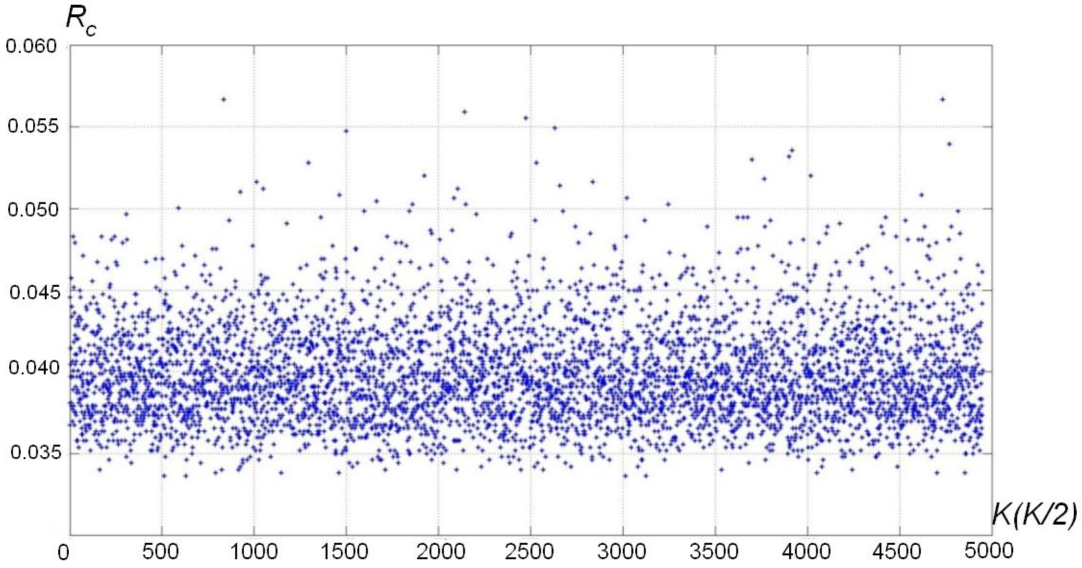

Figure 3: Maximum ACCF peaks of combinations of randomly chosen 100 codes

4 Discussion

Results of computational experiments allow to confirm following theoretical hypotheses that have been put forward earlier:

1. The proposed method of the formation of BCS is based on inverse functional changes with pseudo-random arguments allows to create binary codes predetermined length and shape them into BCS.
2. The use in the proposed method of forming BCS the function $\tau = \log_2 (1/rnd)$ provides k-distributed of series in code and close to optimal correlation properties.
3. The received codes based on said function have Balance Property: number of bits equal to "1" is different from the number of bits equal to "0", not more than one.
4. The resulting codes based on said function have Series Property: a half code period series "1" and "0" has a length 1, one-quarter - 2, one eighth - 3 etc. as long as it still makes sense.
5. Obtained binary codes based on said function have Autocorrelation Property: if code elementwise is being compared with its any cyclic shift during the same code period, the number of hits will be different from the number of mismatches not more than one unit. The highest peaks of the aperiodic correlation functions have similar values to the designated Welch bound (Table 2) and are generally comparable with those values BCS, currently used in wireless systems with CDMA.
6. The highest peaks of the cross-correlation function of the obtained codes does not exceed the maximum side peaks of the autocorrelation function.
7. Proposed BCS forming method by functional transformations pseudorandom arguments can be used to generate codes of any length N and code number in the set K. It should be noted, that Series Property, k-distribution of series, is well satisfied for $N = 2^m - 1$.
8. The number of unique codes obtained on the basis of the proposed forming method is determined with the pseudo-random number generator period used as the source data. When using the pseudo-random number generator with a long period, for example MT13997, may get a number of BCS exceeding A_r.

The stated purpose of the article on the development of a method of forming sets of binary codes (BCS) for wireless systems with CDMA, which allows form them in an amount sufficient to enhance the structural secrecy

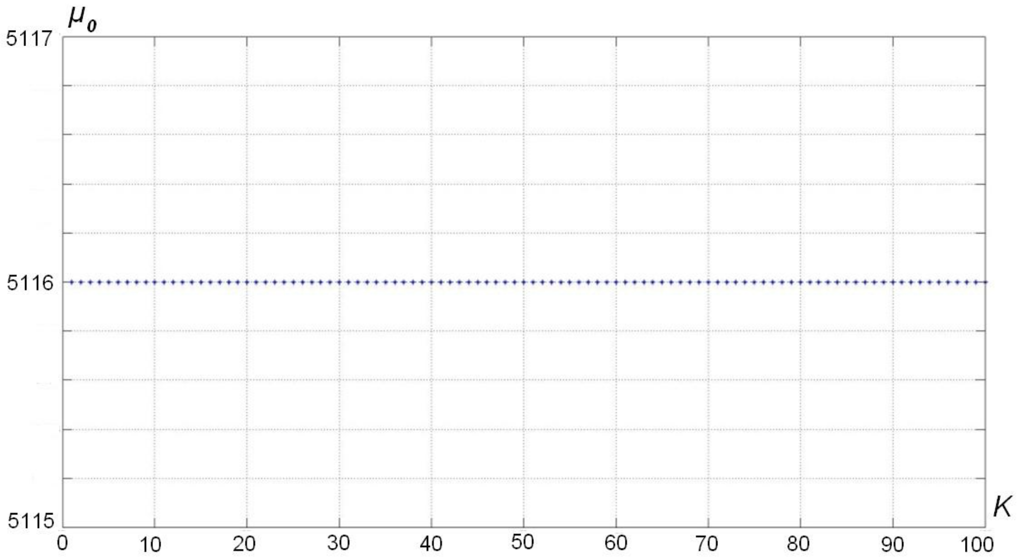

Figure 4: Number of bits series in formed binary codes

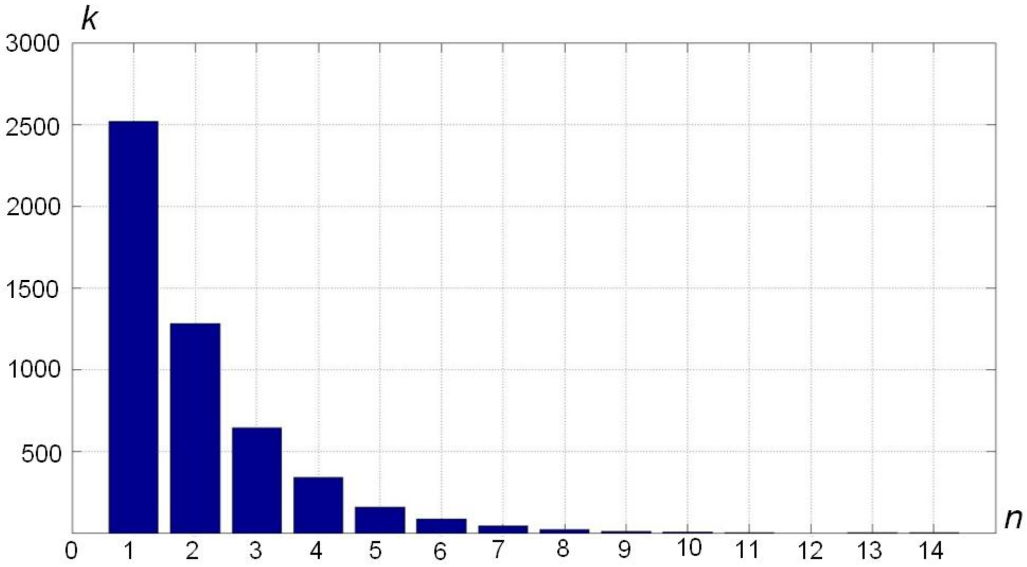

Figure 5: Distribution of a bits series of different lengths in randomly chosen binary code

of radio signal for a period of 10 years or more is achieved. Based on the proposed in the article method of forming the BCS based on the functional transformation of pseudo-random arguments it is possible to obtain the codes corresponding to all their requirements for use in wireless systems with CDMA. Proposed method of forming BCS can be used in the apparatus of forming the code sequences of different CDMA wireless systems to improve their structural secrecy, and as a result, the noise immunity.

5 Acknowledgments

We would like to thank Vladimir Petrovich Pashintsev for many fruitful discussions

References

[Boc12] P. Bocharov. Communication technologies for security systems: the types and features of application. *Security Systems*, - 2012. - No. 1. - Pp. 100-103.

[Gol67] S Golomb. *Shift Register Sequences.* San Francisco, Holden-Day, 1967.

[Ipa92] V.P. Ipatov. *Periodic discrete signals with optimum correlation properties.* - Moscow: Radio and Communications, 1992. - 152 p.

[Kan06] Z.M. Kanevsky, V.P. Litvinenko, G.V. Makarov, D.A. Maksimov. Ed. Z.M. Kanevsky. *The Basics stealth theory: Textbook.* - Voronezh: Publishing house of the Voronezh State University, 2006. - 197 p.

[Kuk03] K.I. Kukk. Digital satellite earth stations broadcasting distribution network. *Proceedings NIIR*, - Moscow: 2003.

[Lev99] V.I. Levenshtein. New Lower Bounds on Aperiodic Crosscorrelation of Binary Codes. *IEEE Transactions on Information Theory*, - No. 45. - Jan 1999. Pp. 284-288.

[Ore11-1] D.V. Orel. Analysis of equipment functioning threats for civilian users of global satellite navigation systems. *Proceedings of the North Caucasian branch of the Moscow Technical University of Communications and Informatics*, - Rostov-on-Don: HRC "University", 2011. - Pp. 44-48.

[Ore11-2] D.V. Orel. Simulation of stochastic systems quasiorthogonal signals for secure global satellite navigation system. *Bulletin of the Stavropol State University - Scientific journal "Vestnik of SSU."*, - No. 75 (4). - 2011. - Pp. 111-116.

[Ore13] D.V. Orel. Development of systems modeling method binary quasi-orthogonal code sequences for global navigation satellite systems. *Herald of the North Caucasus Federal University*, - No. 3 (36). - 2013. - Pp. 26-30.

[Ore14] D.V. Orel, A.P. Zhuk. A method for increasing noise immunity of navigation signal of satellite radio navigation system. *Proceedings of the Moscow Physical-Technical Institute*, - No. 4 (24) - Vol. 6, 2014. - Pp 119-125.

[Pch08] A.P. Pchelintcev. The new GLONASS signals. *Electronic Journal "Integrated Satellite Navigation Systems"*, - No. 2, 2008. - Pp. 4-6.

[Sam14] E. Samyshkina, S. Klimova, V. Kurdimanov, M. Kanzafarova. New standards in the field of technical equipment safety and anti-criminal protection. *Security Algorithms.*, - 2014. - No. 3. - Pp. 12-14.

[Var78] L.E. Varakin. *The theory of signal systems.* - Moscow: Soviet Radio, 1978. - 304 p.

[Zai13-1] A. Zaitsev. Select communication channel for fire monitoring organization. *Security Algorithms*, - 2013. - No. 4. - Pp. 18-22.

[Zai13-2] A. Zaitsev. Areas of technical equipment and security systems in modern conditions. *Security Algorithms*, - 2013. - No. 3. - Pp. 6-10.

[Zhu10] A.P. Zhuk, L.A. Fomin, D.V. Romanko, D.V. Orel. Using a special class of information signals for transmission in radio CDMA. *Neurocomputers: development, use*, No. 1, 2010. - Pp. 40-45.

[Zhu12-1] A.P. Zhuk, D.V. Orel. Estimation of noise immunity of satellite radio navigation systems. *Information and Communication Technologies*, - No. 2, 2012. - Pp. 83-88.

[Zhu12-2] A.P. Zhuk, D.V. Orel, Z.V. Chernyak. The program complex "Quasi-orthogonal code sequences generator based on the functional transformation of pseudo-random arguments". *Certificate of state registration of the computer program (Russia)*, No. 2012612605 on 31 May 2012.