Original Research Article: full paper

(2020), «EUREKA: Physics and Engineering»
Number 3

ISOMORPHIC SIGNAL ENSEMBLES AND THEIR APPLICATION IN ASYNC-ADDRESS SYSTEMS

Vladimir Mikhaylov[1]
mihvj@yandex.ru

Roman Mazepa[1]
mrb402@mai.ru

[1]*Moscow Aviation Institute (National Research University)*
4 Volokolamskoe highway, Moscow, Russia, 125993

Abstract

The object of consideration is async-address systems using code division of subscribers. The subject of the analysis is quasi-orthogonal ensembles of signals based on code sequences that have normalized characteristics of cross-correlation functions (CCF) and provide reliable separation of subscribers (objects) when exposed to imitation and signal-like interference. The purpose of the analysis is to create a model and methodology for construction a set of the best code sequences ensembles having the ability to quickly change the instance of the set to counter imitation and signal-like interference. The solution is based on algebraic models of code sequences and their CCF representation.

The article proposes a comprehensive technique to construct signal ensembles set having normalized characteristics of the CCF. The quality of the primary ensemble of code sequences is ensured by the procedure for calculating the CCF optimized in the number of look over options. Optimization is based on the basic properties of the Galois field, in particular, on the Galois fields' isomorphism property. It provides a significant reduction in calculations when choosing the primary ensemble of code sequences with the specified properties of the CCF. The very choice of the best (largest in size) code sequences ensemble relies on the solution of one of the classical combinatorics problems – searching for maximal clique on a graph. The construction of signals ensembles set having normalized characteristics of the CCF is ensured by the use of special combinatorial procedures and algorithms based on the multiplicative properties of Galois fields. An analysis of the effectiveness of known and proven procedures searching for maximal clique is also performed in this article. The work results will be useful in the design of infocommunication systems using complex signals with a large base and variable structure to provide protection from signal structure research and the effects of imitation and signal-like interference.

Keywords: async-address systems, code division, signal ensembles, cross-correlation functions, imitation and signal-like interference.

DOI: 10.21303/2461-4262.2020.001223

1. Introduction

The task of the code sequences correlation properties analyzing to construct quasi-orthogonal ensembles as applied to async-address systems is well known. In particular, the papers [1–8] were devoted to this issue. A number of factors support the current interest in finding quasi-orthogonal ensembles. Firstly, the need for asynchronous-address systems that use code features for addressing channels and objects is increasing significantly. Secondly, the systems operation under conditions of imitation interference makes it difficult to signal-code constructions (SCC) and tactics of their application. In particular, the need for a dynamic change in some design parameters of the SCC is growing [9–11]. Thirdly, modern technical means are able to support the use of complex signals with a large base, ensuring compliance with the requirements for energy stealth of systems, high accuracy of measurement of motion parameters of highly dynamic objects, as well as high reliability and performance of their control systems. There are works (in particular [7]) that develop the direction of the search for signal classes with super-large ensembles.

The quality of quasi-orthogonal signal ensembles is estimated mainly by two parameters: the ensemble power and significant characteristics of the CCF of all signal pairs in the ensemble. An additional property of ensembles – the ability to quickly transform the ensemble sets structure – reflects the possibility of dynamically changing the code sequences composition in an ensemble in order to protect against signal structure research, the effects of imitation and signal-like interference, however, has been less studied.

The aim of research is to study the possibility of dynamically changing the code sequences composition in an ensemble and to create a methodology to create the sets of such ensembles.

The choice of CCF quality indicators determines the criterion to create the best of signals ensemble and, in this sense, is one of the most important steps in the ensembles design. Examples of common quality indicators are the maximum level of the CCF, the standard deviation of the CCF levels and the standard deviation of the CCF levels modules. Using the maximum level of CCF, choosing the best ensemble minimizes the upper limit of the probability of the code sequences detection-distinction. This criterion is most often used, although the requirements for an ensemble of code sequences are the most hard.

The desire to reduce the level of cross-correlation is understandable, however, the evaluation of the non-orthogonality chosen code sequences influence on the noise immunity of systems is not so obvious. Models of optimal receivers of complex signals corresponding to various uses of radio systems have been well studied. If at the input of the receiver there is one signal with an unknown code attribute from the set of possible ones, the following error probability estimate is valid [12]:

$$P_e\left(\frac{E}{N_0}, \rho_{ij}\right) \le P_e\left(\frac{E}{N_0}, \rho_{\max}\right) = P_e\left(\frac{E(1-\rho_{\max})}{N_0}, 0\right), \quad (1)$$

where $\rho_{\max}$ – maximum of the correlation coefficient value of distinguishable code sequences pair; E / N_0 – ratio of signal energy to noise power spectral density.

Evaluation makes it possible to bring a non-orthogonal signal system to an equivalent orthogonal signal with reduced signal energy (right-hand side of (1)). The degree of its reduction makes it possible to evaluate the quality of the designed signals ensemble. It is even more difficult to evaluate the quality of systems that perform code detection-distinction sequentially against the background of the effects of many signals with different structure.

In many design problems, the selection of this criterion is the "starting point" for designing of signals ensemble. The next step in the design of the ensemble is an exhaustive calculation of the CCF. Formalization of the problem of designing the best ensembles of code sequences.

2. Materials and methods

Design of the best ensembles of code sequences is based on the following formalization. Let's define the compatibility of codes pair (l, k) from original set in the form of a generalized inequality:

$$\theta_{l,k} \le \theta_{acc}, \quad (2)$$

where $\theta_{l,k}$ – selected measure of non-orthogonality of the codes pair (l, k) in the form of CCF characteristic, and θ_{acc} – acceptable level of non-orthogonality.

In particular, the maximum level of CCF $\rho_{l,k,\max}$ may be a measure of nonorthogonality.

If consider a graph where the set of vertices displays the set of codes, and the arcs (edges) – the compatibility of the corresponding codes pair in the original set, then it will look like a tree whose root is a reference code sequence (for example, with index l=1). Let's note that the indicated compatibility in terms of graph theory is usually represented as the adjacency matrix **A**, for which the element k of the row l is written as

$$a_{l,k} = \begin{cases} 1, \text{ for } \theta_{l,k} \le \theta_{acc}; \\ 0, \text{ for } \theta_{l,k} > \theta_{acc}. \end{cases} \quad (3)$$

To build a graph that displays the complete starting model for optimal ensemble constructing, it is necessary to add edges that show the compatibility of any codes pairs (i, j).

One of the basic properties of Galois fields – isomorphism – provides the fundamental possibility of obtaining such information without performing bulky calculations of CCF. The realization of this possibility is based on the number-theoretic representation of codes (more precisely,

the roots of the polynomials that generate them). Formally, the compatibility of a codes pair (i, j) is evaluated by the function

$$\theta_{i,j} = \theta_{1,k}, \tag{4}$$

where $j \equiv ik \pmod{N}$, and k defined as the result of dividing j by i in an integer Galois field.

The complete adjacency matrix A is constructed on the basis of (3) by copying the current row, starting from the number l=1, to the next row with a right cyclic shift of its elements. Such a matrix is called a circulant matrix, and the corresponding graph is called a circulant graph. Of course, this is possible only if a certain algebraic order of the graph vertices enumeration is performed.

The next section is devoted to constructing a mathematical model for listing the graph vertices. So, let's assume that the code compatibility graph (adjacency matrix) in the ensemble is known. Then the problem of constructing an optimal, in the sense of satisfying (2), maximal size ensemble is formulated in terms of graph theory as a maximal clique problem (maximal full subgraph).

3. Research results

The formalism introduced in (4) takes into account the regularities of vertex relations in a circulant graph. These regularities are the basis for constructing the code sequences ensembles that have identical properties of the CCF of any ensemble pairs. Let's call them "isomorphic ensembles". For their construction, it suffices to apply relations (4), however, the specified transformations, although routine, are rather bulky. These transformations can be greatly simplified and automated by ordering the sequential set of numbers k introduced in Section 2. Such an ordering is based on the concept and properties of the primitive root g modulo simple $N = 2^n - 1$, where n is the degree of the primitive polynomial generating nonzero elements of the Galois field. Since, by definition of the primitive root g, all its degrees run through the complete residue system modulo N it becomes possible to regularly list all the degrees of the primitive element $\alpha \in GF(2^n)$ of the corresponding Galois field. Such an enumeration, in turn, makes it possible to quickly construct isomorphic ensembles, since any of the degrees of the primitive root g, for example,

$$g^i \pmod{N}, \tag{5}$$

can be used as degree k of a primitive element α of the Galois field.

Corresponding item $\beta = \alpha^k$ can be used further to represent an isomorphic Galois field. Unfortunately, such a possibility exists only for prime numbers N – otherwise listing (5) will give an incomplete residue system modulo N. Another problem of listing (5) is that the constructed series includes numbers

$$k = 1, 2, 4, ..., 2^{n-1}, \tag{6}$$

as well as multiples of them, which leads to an enumeration of elements α^k – roots of the same polynomial, and this is unacceptable to solve the problem. Let's find such a minimum value of degree j in (5) at which the second element of the series (6) appears, i. e. number 2:

$$g^j \equiv 2 \pmod{N}. \tag{7}$$

By the definition of a primitive root, $g^{\varphi(N)} \equiv 1 \pmod{N}$, where $\varphi(N)$ – Euler function, for prime N equal $\varphi(N) = N - 1$. Raising both sides of the comparison (7) to the power of n, let's obtain $g^{jn} \equiv 1 \pmod{N}$, and, consequently, $j = \varphi(N)/n$. Let's note that this value determines the total number of primitive polynomials of degree n in the corresponding Galois field. It follows that the sequence of degrees

$$g^0 = 1, g^1, g^2, ..., g^{\frac{\varphi(N)}{n}-1} \tag{8}$$

enumerates all numbers k such that each α^k is the root of only its primitive polynomial of degree n defining any of the possible code sequences of a given length. Relation (8) allows to move from an enumeration of the roots to a more convenient and understandable enumeration of the degrees of the primitive root. Relation (4) should now be adjusted as follows:

$$\theta_{i,j} = \theta_{0,k}, \tag{9}$$

where i, j and k – degrees of primitive g, and $k = j - i$.

An ordered set of polynomials (or their roots) obtained by this rule is presented in the form of a graph in **Fig. 1**. The graph vertices are numbered according to the rule of degrees of the series (8). Thin arcs (graph edges) indicate the corresponding number-theoretic relations between the polynomials roots (corresponding codes). Thick arcs show, as an example, the compatibility relationships of these codes in the ensemble. They are also edges of the compatibility graph. The labels of the edges of the graph correspond to rule (9). Symmetry is observed in the graph: the left and right parts display the so-called mutual codes, as can be seen from the relation

$$g^{\frac{\varphi(N)}{2n}} \equiv -1 \,(\mathrm{mod}\, N).$$

Fig. 2 shows the basic properties of circulant graphs. The main one is the "property of chains". By "chain" let's mean a sequence of vertices of a graph having a pairwise compatibility relation and a compatibility relation of each vertex of the chain with **Fig. 2** the vertex "0". In **Fig. 2** such chains are combined by an oval. The base chain in **Fig. 2** is chain number 1.

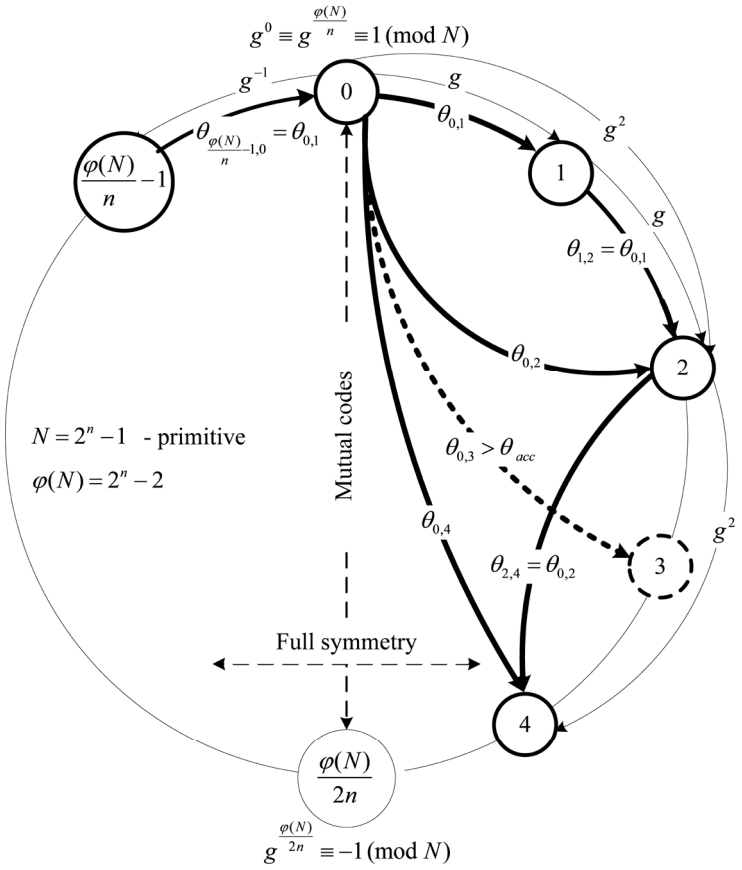

Fig. 1. Ordered polynomial roots set

Obviously, all the vertices in this chain form a clique, but it will not necessarily be maximal. It is also obvious that for some value of m the chain will break. **Fig. 2** demonstrates the situation of re-

newal of the compatibility relationship, starting from the top under the number m+1. But a new chain at number 2 will not increase the size of the clique if the length of this chain is less than the length of chain at number 1 (i. e. m). One of the most important properties of circulant graphs is that in chains with numbers higher than 1 and length m, only one vertex can be added to the base clique. Such a new vertex, capable of increasing the size of the base clique, has in **Fig. 2** number 2m and not shaded.

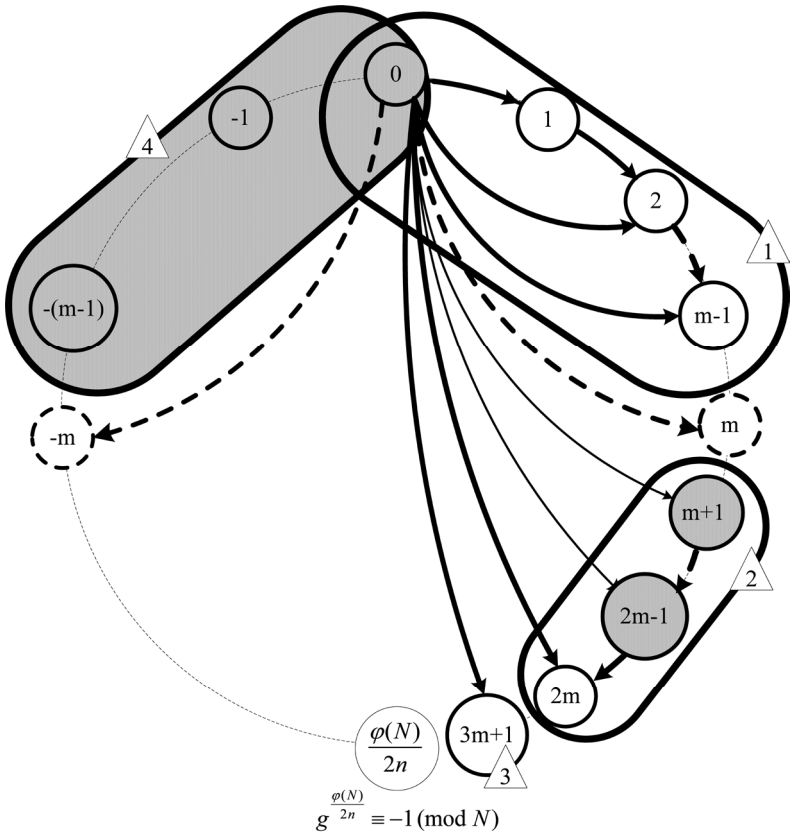

Fig. 2. Key properties of circulant graphs

Continuing the further construction of the model, it is possible to see that, at best, the next only vertex that extends the base clique is the vertex with the number 3m+1, which belongs to the chain with the number 3 and length m. This regularity is emphasized by the thickness of the arc edges of the graph. Another regularity follows from the symmetry property of circulant graphs, which manifests itself in the fact that at the same time chains numbered 1 and 4 can't be selected simultaneously for clique formation. Indeed, the vertex with the number – (m–1) in chain 4 can be selected together with the vertex 0, but the choice of chain 1 to form a clique immediately prevents this choice because it is impossible to attach the vertex with the number –m to the base clique.

The proposed model can be successfully used for a fairly accurate estimate of the maximal clique size (potentially achievable power of the ensemble of code sequences). According to the authors, at this time, there are no effective algorithms for finding the maximal clique on circulant graphs [13]. Nevertheless, the properties of graphs found in this section can contribute to the development of this direction. In any case, the introduced model and the properties of circulant graphs significantly simplify and accelerate the solution of the target problem — the creation of isomorphic signals ensembles set.

Unfortunately, the primitive g exists only for prime modules. For example, module values N=511; 1023; 2047 does not satisfy this requirement. Nevertheless, the analysis of numerical fields shows that in these situations it is possible to find a number g_1 with the best properties of enumerating the residue system for a given module. Finding a number is a relatively simple number-theoretic

task. When choosing such an ordered set of roots of polynomials, presented in **Fig. 1**, splits into two subsets: one is formed by degrees g_1 similarly to (8), but twice as short:

$$g_1^0 = 1, g_1^1, g_1^2, ... g_1^{\frac{\varphi(N)}{2n}-1}, \quad (10)$$

and the second maps the first subset into the space of roots of mutual polynomials:

$$-g_1^0 = -1, -g_1^1, -g_1^2, ... -g_1^{\frac{\varphi(N)}{2n}-1}. \quad (11)$$

In particular, for the values of the modules N=511; 1023; 2047 as g_1 numbers 5, 5, 3 can be chosen, respectively.

4. The discussion of the results

The problem is still reduced to the search for maximal clique, which belongs to the class of so-called NP-complex problems with polynomial complexity. All results obtained in the previous sections remain valid for this case.

By now, many methods and algorithms for solving this problem have been developed [14, 15]. The whole set of software tools designed to search for the maximal click or having such functionality consists of two subsets: universal and specialized tools. The first includes the MATLAB system (supplemented by the "maximalCliques.m" module [16]) and Wolfram Mathematica. The second subset is heterogeneous and contains executable programs, code sources and algorithms descriptions. Based on the analysis of the algorithms descriptions, two fairly trivial conclusions can be made:

– interest in the problem is high in different fields of research;

– theoretical basis of the algorithms is practically the same (the branch and bound method), and the differences in the algorithms are in the optimization of click search due to some (sometimes significant) decrease in accuracy or completeness of the result.

Each tool has its own characteristics, establishing areas and boundaries of their application.

Both products in the first subset of universal software have a single weakness: low speed. This flaw is most dawn in MATLAB. Most likely, this is due to the low productivity of the module "maximalCliques.m" (a fixable flaw) and the peculiarity of the implementation of parallel computing in MATLAB. The Wolfram Mathematica package is generally good, it is able to search for all clicks, but of a small dimension (the size of the adjacency matrix is up to 60×60) and not always accurate. In particular, at N=1023 and $\theta_{acc} = 2{,}5/\sqrt{N}$, an inaccurate solution was obtained on an ensemble of size 4.

The executable product "The Clique Algorithm" of Indian programmer Ashay Dharwadker [17] and the program "maxCliquePara" as a source of code [18] were selected from the second subset for comparative analysis. The first program has an average speed and, unfortunately, an inaccurate result. The second program, "maxCliquePara", after compiling it, demonstrated incomparably higher performance and accuracy of click search due to the use of parallel computing on all available computing resources of the processor (cores and threads). However, it finds only one maximal click.

Based on the performed analysis, an optimized method for solving the problem is proposed that effectively combines the functionality and power of the studied software.

The obtained results allow to construct a practical procedure for designing sets of the best quasi-orthogonal ensembles. The initial data for the construction is the result of calculating the CCF characteristics, presented as the first row of the adjacency matrix **A**, for which the element k of the row l (l=1) corresponds to (3). In this case, all elements of the string should be listed in accordance with (8)–(11).

1. Based on properties (3), (8), a circulant adjacency matrix **A** is constructed by copying the first row to the next row with a sequential cyclic right shift of the elements. For further operations

using the Wolfram Mathematica package, the adjacency matrix must have commas as element separators.

2. The “adj.cvs” adjacency matrix obtained in Section 1 is first converted in Wolfram Mathematica into a compatibility graph “graph” using the command

graph=AdjacencyGraph[Import[«adj.cvs»]],

and then exported to the DIMACS format using the command

Export[«file.col», graph, «DIMACS»].

In the next steps it is supposed to use the program “maxCliquePara”, which finds (although quickly) only one maximal click. To build the entire set of isomorphic ensembles, one can construct graphs set that include a given vertex – such a built-in command exists.

3. The “file.col” file obtained in the previous paragraph is passed as the first command-line parameter to the “maxCliquePara” program. If it is necessary to specify the exact amount of available computing resource, the second command line parameter is used in the form In the next steps it is supposed to use the program “maxCliquePara”, which finds (although quickly) only one maximal click. To build the entire set of isomorphic ensembles, one can construct graphs set that include a given vertex – such a built-in command exists.

4. The “file.col” file obtained in the previous paragraph is passed as the first command-line parameter to the “maxCliquePara” program. If it is necessary to specify the exact amount of available computing resource, the second command line parameter is used in the form $n = cores \times threads$, where “cores” and “threads” are the real number of cores and threads. For example, the command

maxCliquePara.exe file.col 8>result.txt

will start the search for the maximal click on the graph “file.col” on the processor with four cores in two threads and write the result to the file “result.txt”.

5. Since the program “maxCliquePara” renumbering the graph vertices, to correctly use the result, it is necessary to perform the inverse transformation using the original numbering used to obtain the file “file.col”.

6. To determine isomorphic ensembles based on the clique found in Section 3, one should use the cyclic shift procedure of the corresponding vertices of the graph shown in **Fig. 1.**

Let’s consider an example of constructing isomorphic sets of quasi-orthogonal ensembles. There are two possibilities to construct the isomorphic ensembles. The first is based on the cyclic shift of the rows of the compatibility matrix, which is equivalent to multiplying the degree k of the element α of the Galois field – the root of the corresponding polynomial – by g (or g_1). The second possibility to construct the isomorphic ensembles is related to the choice of g (or g_1) values. Of course, both of these approaches can be used together, but there is no way to guarantee that the results of the construction will not coincide.

For example, consider the first approach. Initial data: N=1023, $\theta_{acc} = 2{,}5/\sqrt{N}$, $g_1 = 5$. Under these conditions, the primary ensemble includes the following set of degrees k of a primitive element α of the Galois field (4): $k = \{1, 41, 205, 511, 367\}$. The other 29 sets for are as follows: $\{5, 205, 1, 383, 179\}$; $\{25, 1, 5, 223, 511\}$; $\{125, 5, 25, 23, 383\}$; … $\{205, 221, 41, 179, 89\}$.

Let’s note that, in particular, the first and second, second and third sets have two common elements – {1, 205}, {1, 5}, respectively – while the first and fourth sets of matching elements do not have. This can be significant when choosing isomorphic of code sequences ensembles sets in order to protect against active interference by dynamically changing the composition of code sequences in the ensemble. Let’s also note that the search for isomorphic ensembles that are optimal from the point of view of minimal “overlap” is a separate combinatorial task, but is not related to click search.

5. Conclusion

As a research result, the following results are obtained.

It is proved that the choice of the best code sequences ensembles consists of two completely different and computationally independent procedures, the first of which consists in the analysis of the CCF sequences, and the second in the search for the maximal click on a given compatibility graph. At the same time, the structure of code sequences is significant only at the stage of CCF calculation.

It is proved that the compatibility graph is circulant, which allows to construct it on the basis of one row of the adjacency matrix.

The relevance of developing an effective maximal click search algorithm that takes into account the circulant structure feature of the compatibility graph is established.

A detailed analysis and evaluation of existing software tools capable of searching for the maximal click, and, therefore, the best ensembles in the set of code sequences under consideration, is presented. Based on the analysis of software and experimental verification of their effectiveness, a methodology to construct a prototype of the best ensemble of code sequences has been created.

Regular methods to construct the isomorphic sets of code sequences ensembles based on found prototype are found. The method allows to dynamically change the composition of code sequences in the ensemble in order to protect async-address systems from signal structure research and the effects of imitation and signal-like interference.

The research results will be useful in the design of infocommunication systems using complex signals with a large base and variable structure to provide protection from signal structure research and the effects of imitation and signal-like interference.

References

[1] Gold, R. (1968). Maximal recursive sequences with 3-valued recursive cross-correlation functions (Corresp.). IEEE Transactions on Information Theory, 14 (1), 154–156. doi: https://doi.org/10.1109/tit.1968.1054106

[2] Sarwate, D. V., Pursley, M. B. (1980). Crosscorrelation properties of pseudorandom and related sequences. Proceedings of the IEEE, 68 (5), 593–619. doi: https://doi.org/10.1109/proc.1980.11697

[3] Gorgadze, S. F., Boikov, V. V. (2014). Test signals with multilevel subcarriers as applied to satellite radio-navigation systems. Journal of Communications Technology and Electronics, 59 (3), 245–258. doi: https://doi.org/10.1134/s1064226914020028

[4] Gorbenko, I. D., Zamula, A. A., Semenko, A. E., Morozov, V. L. (2017). Method for complex improvement of characteristics of orthogonal ensembles based on multiplicative combining of signals of different classes. Telecommunications and Radio Engineering, 76 (18), 1581–1594. doi: https://doi.org/10.1615/telecomradeng.v76.i18.10

[5] Golomb, S. W., Gong, G. (2005). Signal Design for Good Correlation. Cambridge University Press. doi: https://doi.org/10.1017/cbo9780511546907

[6] Stasev, Y., Kuznetsov, A., Karpenko, O., Sai, V. (2012). Discrete signals with multi-level correlation function. Telecommunications and Radio Engineering, 71 (1), 91–98. doi: https://doi.org/10.1615/telecomradeng.v71.i1.100

[7] Mazepa, R. B., Mikhaylov, V. Y. (2017). Performance characteristics of the isomorphic ensemble of signals for async-address systems. 2017 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SINKHROINFO). doi: https://doi.org/10.1109/sinkhroinfo.2017.7997539

[8] Vladimirov, S., Kognovitsky, O. (2019). Dual Basis Based Processing of Wideband Gordon–Mills–Welch Sequences Based on Two Linear Registers. Proceedings of Telecommunication Universities, 5 (2), 49–58. doi: https://doi.org/10.31854/1813-324x-2019-5-2-49-58

[9] Orel, D., Zhuk, A., Zhuk, E., Luganskaia, L. (2017). A method of forming code sets for CDMA in communication, navigation and control systems. CEUR Workshop Proceedings, 1837, 158–167.

[10] Sultanov, B. V., Rumyantseva, N. B., Zefirov, S. L. (2013). Analysis of the fast acquisition method in frequency hopping systems. Journal of Communications Technology and Electronics, 58 (6), 526–534. doi: https://doi.org/10.1134/s1064226913050094

[11] Kuzovnikov, A. V. (2014). Study of the methods for developing jamming-immune communications systems with the use of wavelet-modulated signals. Journal of Communications Technology and Electronics, 59 (1), 61–70. doi: https://doi.org/10.1134/s1064226914010069

[12] Viterbi, A. J. (1966). Principles of coherent communication. McGraw-Hill, 321.

[13] Monakhova, E. A. (2011). Structural and communicative properties of circulant networks. Prikladnaya Diskretnaya Matematika, 13, 92–115. doi: https://doi.org/10.17223/20710410/13/8

[14] Hou, B., Wang, Z., Chen, Q., Suo, B., Fang, C., Li, Z., Ives, Z. G. (2016). Efficient Maximal Clique Enumeration Over Graph Data. Data Science and Engineering, 1 (4), 219–230. doi: https://doi.org/10.1007/s41019-017-0033-5

[15] Utkina, I. (2018). Using Modular Decomposition Technique to Solve the Maximum Clique Problem. Springer Proceedings in Mathematics & Statistics, 121–131. doi: https://doi.org/10.1007/978-3-319-96247-4_8

[16] Wildman, J. (2020). Bron-Kerbosch maximal clique finding algorithm. MATLAB Central File Exchange. Available at: https://www.mathworks.com/matlabcentral/fileexchange/30413-bron-kerbosch-maximal-clique-finding-algorithm

[17] Dharwadker, A. The Clique Algorithm. Available at: http://www.dharwadker.org/clique/

[18] MaxCliquePara. Available at: http://commsys.ijs.si/~matjaz/maxclique/MaxCliquePara/

Received date 27.02.2020
Accepted date 15.04.2020
Published date 11.05.2020

MATHEMATICAL MODEL OF THE SYSTEM OF ACTIVE PROTECTION AGAINST EAVESDROPPING OF SPEECH INFORMATION ON THE SCRAMBLER GENERATOR

Volodymyr Blintsov
Department of Electrical Engineering of Ship and Robotic Complexes[2]
volodymyr.blintsov@nuos.edu.ua

Sergey Nuzhniy[1]
s.nuzhniy@gmail.com

Yurii Kasianov
Senior Lecturer[1]
yukas.nik.ua@gmail.com

Viktor Korytskyi[1]
vic.koritskiy@gmail.com

[1]*Department of Computer Technologies and Information Security*
[2]*Admiral Makarov National University of Shipbuilding*
9 Heroiv Ukrainy ave., Mykolayiv, Ukraine, 54025

Abstract

The development of reliable systems for protecting speech information that can protect it from being intercepted by cybercriminals is a fundamental task of the security service of organizations and firms. For these purposes, active jamming systems are used at the border of the controlled area. The main element of such systems is noise generators. However, in many cases, “white” noise and its clones are used as interference, which makes it possible for an attacker to gain unauthorized access. The structure and mathematical model of a speech information protection system based on a scrambler-type noise generator is proposed. The transition in such systems of protection of speech information to this structure allows to abandon the outdated, ineffective in modern conditions, energy noise of speech information and move on to a more productive method – information (linguistic) masking. An analysis of the destructive effect of this type of interference shows its high resistance to modern methods of mathematical processing of digital phonograms (wavelet transform, correlation-spectral analysis, etc.), filtering interference, and dividing the voices of speakers. Studies of the mathematical model in the environment of Matlab 15 R2015a/Simulink show the high efficiency of such a protection system and a decrease in the signal-to-noise ratio with a residual speech intelligibility of 0.1 by 6...9 dBA. This leads to a decrease in