— described the methods of building barker-like codes with high capabilities for detecting and correcting multiple errors, which are based on the use of combinatorial configurations with a ring structure of the type of ideal ring bundle. The methods make it possible to create coding systems with improved quality indicators in terms of power and immunity to interference.

— the corrective efficiency of barker-like codes built on the basis of multi-element IRBs with optimized parameters reaches the value of 0.5 with an arbitrarily large number of bits of code sequences. At the same time, the maximum possible number of corrected errors is 25% of the total number of code bits;

— research results can find practical application for the development of information technologies and systems with improved technical characteristics according to such indicators as ensuring the reliability of information, increasing the reliability, functional safety and survivability of information and information-management systems.

References:

1. Ahmad J., Akula A., Mulaveesala R., Sardana H.K. Barker-Coded Thermal Wave Imaging for Non-Destructive Testing and Evaluation of Steel Materials. *IEEE Sensors Journal*. 2019. Vol.19, No.2, pp.735-742. doi: 10.1109/JSEN.2018.2877726.
2. Aljalai A.M.N., Feng C., Leung V.C.M., Ward R., Improving the energy efficiency of dft-s-ofdm in uplink massive mimo with barker codes: in 2020 International Conference on Computing, Networking and Communications (ICNC), 2020, pp. 731-735. doi: 10.1109/ICNC47757.2020.9049829.
3. Fu J., Ning G., Barker coded excitation using pseudo chirp carrier with pulse compression filter for ultrasound imaging. *BIBE 2018: International Conference on Biological Information and Biomedical Engineering*. 2018, Shanghai, China, pp.1-5.
4. Lakshmi R., Trivikramarao D., Subhani S., Ghali V.S., Barker coded thermal wave imaging for anomaly detection: in 2018 Conference on Signal Processing And Communication Engineering Systems (SPACES), 2018, pp.198-201. doi:10.1109/SPACES.2018.8316345.
5. Riznyk O., Povshuk O., Y. Kynash Y., Yurchak I. Composing method of anti-interference codes based on non-equidistant structures: in 2017 XIIIth International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH), Lviv, 2017, pp.15-17. doi:10.1109/MEMSTECH.2017.7937522.
6. Riznyk V., Riznyk O., B. Balych B., Parubchak V. Information Encoding Method of Combinatorial Optimization. 2006 International Conference – Modern Problems of Radio Engineering, Telecommunications, and Computer Science, Lviv-Slavsko, 2006, pp.357-357. doi:10.1109/TCSET.2006.4404550.
7. Tsmots I., Riznyk O., Rabyk V., Kynash Y., Kustra N., Logoida M. Implementation of fpga-based barker's-like codes: in Lytvynenko, V., Babichev, S., Wo´jcik , W., Vynokurova, O., Vyshemyrskaya, S., Radetskaya, S. (eds.) Lecture Notes in Computational Intelligence and Decision Making, 2020, pp.203-214. Springer International Publishing, Cham. doi:10.1007/978-3-030-26474-115.

METHODS FOR INFORMATION CODING IN MOBILE SYSTEMS

DOI: https://doi.org/10.30525/978-9934-26-300-2-17

Oleg RIZNYK
candidate of technical sciences, associate professor,
Lviv Polytechnic National University
e-mail: oleh.y.riznyk@lpnu.ua
Olga MYAUS
candidate of technical sciences, associate professor,
Lviv Polytechnic National University
e-mail: olha.m.miaus@lpnu.ua
Evgeny SAVELOV
postgraduate,
Lviv Polytechnic National University
e-mail: Yevhenii.E.Savelov@edu.lpnu.ua

Introduction. Naturally, there is a need to protect information from unauthorized access, theft, destruction, distortion and other criminal acts. The concept of information vulnerability is introduced, which describes the effectiveness of selected methods for information protection. With the development and complication of methods and forms of automation of information processing processes, its vulnerability increases.

The spectrum of problems expands significantly when the user starts working with wireless networks, because errors may occur during data transmission over these communication channels. Their reasons may be different, but the result is the same – the data is distorted and cannot be used on the receiving side for further processing.

As a rule, the possibility of twisting a bit in the stream of transmitted data at the level of a physical wireless channel is within $10^{-2}\ldots10^{-6}$. At the same time, users and many application processes often demand that the possibility of errors in received data is no worse $10^{-6}\ldots10^{-12}$. The fight against emerging errors is conducted at different levels [1, 2].

Many different methods, both hardware and software, are known to deal with emerging errors. Each of these methods has its advantages and disadvantages, in particular, it is believed that the first are more reliable and faster to use, because they are performed at a low hardware level, and the second are able to provide more flexible and comprehensive protection.

In one method, on the transmitting side, the transmitted data is encoded with one of the known error-correcting codes. On the receiving side, accordingly, the received information is decoded and errors detected are corrected. The capability of the applied error-correcting code depends on the number of redundant bits generated by the encoder. If the redundancy introduced is small, that is, there is a danger that the received data will contain undetected errors, this can lead to errors in the operation of the application process. If you use a code with a high correction ability, it leads to a low data transfer rate. Thus, it is necessary to determine the optimal parameters of the interference-resistant code depending on the task [3].

Issues of development of mathematical models and optimization methods of coding systems for information protection are becoming important. In this regard, the research of information encoding methods using mathematical models formed on combinatorial configurations and the application of a complex approach to the study of various classes of combinatorial structures is an urgent problem. The focus of the modern theory of combinatorial structures is not only classical algebraic or combinatorial constructions, such as groups, block diagrams, cutting sets, but also objects of a new nature, in which algebraic operations are somehow related to the combinatorial properties of the basic set [4].

Thus, the following specific tasks emerge from the general task of the research:

— to investigate the combinatorial properties of ideal ring bundle and the possibilities of their practical application;

— to investigate the method of encoding and decoding data based on the sequence of numbers forming the ideal ring bundle (IRB);

— compare the effectiveness and performance of this coding method with the best similar coding systems;

— to analyze the technical feasibility of using the coding method based on IRB and compare the results to determine the advantages and disadvantages of the chosen method.

The importance of studying combinatorial configurations is particularly evident in the theory of coding during the synthesis of codes with high immunity to interference. However, traditional methods of encoding information and converting signals, as well as methods that use classical combinatorial configurations, do not always make it possible to fully reveal the capabilities of coding systems. Therefore, an important and urgent problem is the research and use of new effective models to improve information coding systems according to such indicators as, for example, the speed of message transmission, code immunity, ease of detecting and correcting errors. Such models include knitwear – combinatorial constructions, the elements of which can be ordered integers or integer tuples, and the combinatorial properties of these constructions are determined both by the values of their elements and by the values of the sums of any number of these elements, taking into account their ordering [5].

The practical value of this project directly derives from the modern needs of information technology, information technology and related branches of science, which are related to the research of information coding methods on a combinatorial basis for information protection [6].

So, the software and hardware methods of data protection, the concepts and main properties of ideal ring bundles were considered, the advantages and disadvantages of the developed coding system based on this mathematical model were studied, and the technical feasibility of the practical use of such a system was analyzed.

Requirements for interference-resistant coding. The development of an effective interference-resistant system, which could detect and correct distorted positions in the data array, is extremely important due to the need to limit access to important information and ensure safe file transfer over a wireless network, in which errors that lead to information content distortion are possible.

In order to fulfill this task, that is, to build an interference-resistant system, we need to consider the theory of interference-resistant coding as a basis for building any interference-resistant system and the ideal ring bundle, on the basis of which it is possible to build a better interference-resistant system than the existing ones.

Interference-resistant codes are one of the most effective means of ensuring high fidelity both when storing and transmitting discrete information. A special theory of interference-resistant coding, which has been developing rapidly recently, has been created. K. Shannon formulated a theorem for the case of transmission of discrete information from a channel with interference, which states that the probability of erroneous decoding of received signals can be ensured as arbitrarily small by choosing the appropriate method of encoding signals.

Interference-resistant codes are codes that allow detecting or detecting and correcting errors that occur as a result of the influence of interference. Immunity of coding is ensured by introducing redundancy into code combinations, i. e. by the fact that not all symbols in code combinations are used to transmit information.

The minimum code distance for a pair of code combinations is determined for all pairs of code combinations of the code under consideration. The minimum code distance for a code is the smallest code distance value among all code distance values defined for all pairs of code combinations of the code. This parameter characterizes the ability of the code to detect and correct errors. Each code combination corresponds to its own digital signal implementation. Mathematically, the problem of determining the minimum code distance is solved using addition modulo 2.

This parameter is related to the corrective properties of the code. They include the properties of detecting errors, correcting errors and correcting errors of lower frequency and detecting errors of higher frequency. In this context, the following points can be highlighted:

— the larger the minimum code distance of the code, the better its ability to detect errors;

— it is necessary to distinguish between the concepts of «minimum code distance for a pair of code combinations» and «minimum code distance for a code».

The connection between the minimum code distance and the corrective properties of the code is very valuable for the optimal parameters of the interference-resistant code, depending on the task:

$$t_d = d_{\min} - 1, \tag{1}$$

$$t_c = \frac{d_{\min} - 1}{2}. \tag{2}$$

With the increase of the minimum distance, along with the growth of the corrective properties, the redundancy of the code increases. Therefore, in this situation, the optimal choice of corrective properties of the code is extremely important.

Development of the theory of barker-like coding using combinatorial configurations. By an optimal combinatorial system, we mean a system whose structure determines the optimal ratio of incidence between elements. This ensures the achievement of maximum combinatorial diversity with established restrictions on the rules of interaction of elements and functioning of the entire system as a whole.

The solution to the problem of synthesis of optimal combinatorial systems is based on methods of structural optimization, which derives from the general principle of optimal structural relations (principle of OSV), which is based on the provisions of combinatorial analysis (theory of cyclic difference sets), the theory of Galois numbers and fields.

Technical devices and systems in which the principle of optimal structural relations is implemented have a number of advantages compared to systems created by traditional methods. The maximum diversity of the system is achieved without disrupting its internal connections due to the peculiarities of the structure. The high reliability of optimal combinatorial systems is ensured by the stability of connections.

Let be the given set of $M_n = \{x_i\}$, $i = \overline{1, N}$ elements and specify the multiplication operation performed on the elements of this set. Then N -a knit by the operation of multiplication is an ordered set of N elements, on the set of M_N which a set of new elements is formed M_s as a result of the specified operation between all ordered pairs, triplets, etc., that is, sets of sequentially placed elements of this set. Therefore, it can be assumed that $n-$ bundle generates a set $M = M_N \cup M_s$, the basic elements of which belong to the set M_N, and the newly formed elements belong to the set M_s.

Each of the $x_i \in M_N$ bundle elements has at least two poles, which are its conditional inputs and outputs and indicate the direction of sequential operations. Any bundle can be characterized by three parameters: order N, multiplicity R and sum of all elements S_N.

The order of bundle N is the number of basic elements included in its composition. Multiplicity R - the number of repetitions of each of the elements. The number of newly formed elements of bundle is determined by its order and structure, and the sum of all elements is determined by the formula:

$$S_N = N(N-1)/R+1 \qquad (3)$$

One-dimensional bundle is formed on an ordered collection of elements that are one-dimensional mathematical objects (numbers, segments, etc.).

A one-dimensional ideal numerical string is a string on which the set of all numbers generated by it exhausts the values proportional to the elements of the natural series with a given number of repetitions of each of the elements. In the context of the problem of designing a cryptographic system for the protection of graphic images, we are interested in one-dimensional ideal circular meshes due to the construction of jam-resistant codes with the lowest degree of redundancy. When choosing other types of bundle, we get interference-resistant codes with much lower correction capabilities.

Algorithms for the construction of ideal ring bundles for the synthesis of Barker-like codes. During the construction of simple perfect bundle, it turned out that not all values n have an ideal ring bundle (IRB). For example, all attempts to construct IKB for $N=7$ and $N=11$ have failed, although for the rest of the values n within the first ten simple perfect rings exist. A similar picture is observed when considering multiple perfect bundles. In particular, it follows from the definition of the concept of a multiple ideal ring bundle that is $S_N - 1 = \dfrac{N(N-1)}{R}$ an integer, from which one of the necessary conditions for the existence R of -multiple IRBs is determined:

$$N(N-1) \equiv 0 \pmod{R} \qquad (4)$$

The existence, construction and list of combinatorial objects of type 1KB is, in fact, a problem, the solution of which is the subject of studying combinatorial analysis as the theoretical basis of discrete mathematics. Therefore, the necessary and sufficient conditions for the existence of IRB should be established on the basis of the provisions of combinatorial analysis.

There are a lot of algorithms for constructing IRBs, namely: classical methods of construction based on difference sets, an algorithm based on Galois fields, however, algorithms of selective branching and asymmetric movements have become more common for constructing IRBs on a computer.

The algorithm is based on the use of the combinatorial properties of the IRB and implements the principle of growing bundles of natural numbers according to certain rules. Its essence is to compile a sequence of numbers chosen in the order of increasing their values while meeting the necessary conditions that satisfy the formation of ideal bundle with given parameters. The conditions for the formation of knits follow directly from the combinatorial properties of these sequences.

Step 1. According to the data N, R the sum of the numbers S_N of the IRB is calculated.

Step 2. An array of N cells numbered in ascending order.

Step 3. Ones are written $(R+1)$ in the first cells of the array, R twos are written in the first cells, and zeros are entered in the rest.

Step 4. For the first time, a number A is defined as the largest number of the shortest sequence of numbers, formed by the set of sums found on all separate sequences belonging to the array, increased by one. Next time, a number A with the same value is defined as the next largest number of the shortest sequence of numbers increased by one. If there are free cells of the array, the number A is written in the free cell with the lowest serial number.

Step 5. The new value of the sum of the elements of the IRB array is calculated. If there are free cells in the array, all sums on all sequences are found, and in their absence – all linear sums on a single sequence:

a) if each of the found sums occurs no more than R once and there are free cells, then the transition is made to step 4. If there are no free cells and if the condition that the new value of the sum is not greater than the previous one is met, the IRB variant is obtained, after which step 7 is performed. Otherwise, step 6 is performed;

b) if at least one of the found sums appears more than R once, step 6 is performed.

Step 6. The largest number is found B, then it is determined whether there is a free cell number with a number greater than the one where the number is located B; if such a cell exists, then the number is transferred from the cell with a lower number B to a free cell with a higher number, after which step 5 is performed; otherwise, step 7 is performed.

Step 7. The cell with the number is freed and step 6 is performed. The appearance of a unit in the cell B provided that it is not present in the previous cells for odd values n and similarly in the cell $\frac{N+2}{2}$ for even values, n serves as a sign of the end of the calculations when building a complete family of IRBs $\frac{N+3}{2}$.

Asymmetric branching algorithm makes it possible to generate sets of complete families of IKB, the order N of which acquires all the values of numbers within the given limits from $n_{\min}$ to $n_{\max}$. It is based on performing one of two types of operations at each step:

- combining two sequences of numbers into a single sequence (forward movement);
- separation of the sequence of numbers into two separate sequences (backtracking).

When moving forward, a number is defined A as the largest number of the shortest natural series, formed by the set of sums of numbers found on individual sequences of the array, increased by one. Then a pair of numbers is selected from the set of all the first and last numbers belonging to two different sequences so that the sum of the given number pair is equal to A, and the two sequences found are combined into one.

When going backwards on the set of all sequences, a number is searched for B as the maximum sum of two adjacent numbers and these two numbers are separated, forming two separate sequences.

Preparatory operations of the algorithm:

- using values N ($n_{\min} \le N \le n_{\max}$) and R calculate the table $S_N = f(N)$ according to formula (4);
- select an array $n_{\max} \times n_{\max}$, each line of which is intended for entering one of the numerical sequences;
- enter R the number in the first cells of the first row of the array 1, and in the cell $(R+1)$ – as 2.

Step 1. Check whether the following requirements are met:

- the total number of all N numbers entered in the array is not $n_{\max}$;
- the sum of all numbers $\sum_{i=1}^{N} r_i$ entered in the array does not exceed $S_N = f(N)$;
- the sum of all the numbers $\sum_{i=1}^{N} r_i$ entered in the array, $S_N = f(N)$;
- all sums on the set of all sequences of numbers do not occur more than R times;
- all N the numbers entered in the array occupy one line, that is, they form a single sequence.

If all the listed requirements are satisfied, then the resulting sequence is one of the IRB variants, and after printing the numbers of the found bundle, you should proceed to step 2. If requirement 5 is not fulfilled, provided that all other requirements are satisfied, or requirement 3 is provided, that requirements 1 and 2 are satisfied, step 1 must be performed. When at least one of requirements 1, 2, or 3 is not satisfied, it is necessary to go back (step 3).

Step 2. Determine the direction of further calculations, for which you should:

- find the number A, and if $N > 4$, as follows from step 1, clause 5, it is enough to limit yourself to the calculation of all sums whose numerical values do not exceed $\frac{1}{2}\sum_{i=1}^{N} r_i$;
- find out whether it is possible to move forward – from the set of pairs of the first and last numbers belonging to different sequences, find a pair of numbers whose sum is equal to A, excluding the pairs that are already taken into account on the given set of sequences. If the mentioned pair is found, perform point 3;
- make a move forward – combine both sequences so that in the new sequence the numbers of the found pair are next to each other, and if there are several such pairs, choose the one in which the difference in numbers is the largest, then perform step 1. If a pair of such numbers is not found, then perform item 4;
- check whether the total number of numbers entered in the array is equal to $n_{\max}$. If $N < n_{\max}$, then go to point 5;
- enter a sequence that includes a single element whose numerical value is equal to, in a free line of the array A, then perform step 1; otherwise, switch to reverse gear (step 3).

Step 3. Make a move back, for which you need:

- on the set of all sequences, find a number B as the maximum sum of two adjacent numbers and disconnect the sequence containing these numbers so that they belong to different sequences, and if there are

several pairs of adjacent numbers whose sums are equal to, B disconnect the pair formed by the last of the previous moves forward. From the sequences, each of which contains a single element, exclude those that are equal to or exceed the number B;

— check whether the termination conditions of the calculations are satisfied. The sign of completion is the appearance in the array of R series of natural numbers from 1 to N, where $N = ent\frac{2n_{\max}+5}{3}$ at $R=1$; $n_{\max} > 8$; at $R>1$ $N = ent\frac{n_{\max}}{R}$.

If the specified requirements are met, the calculation is complete, otherwise, go to step 2.

Considering the complexity of the second algorithm, this work uses the selective branching algorithm as it is theoretically simpler and less resource-intensive.

In order to implement the algorithm of selective movements, it is necessary to build a table of ring sums, according to which we determine the possibility of the existence of families of IRBs and, as a result, the direction of execution of the algorithm. The following formulas are used to calculate the elements of the circular sum table:

$$\begin{aligned} S(l,\, i+1) &= S(l,\, i) + k_{i+1},\ i \neq N,\ l \neq i+1 \\ S(l,\, 1) &= S(l,\, N) + k_i,\ l \neq 1 \end{aligned} \qquad (5)$$

On the main diagonal should be placed elements of IRB. We will give an example of calculating ring sums for IRB (1, 1, 1, 2, 2, 1, 3, 4) with parameters $N=8$ and $R=4$:

1	2	3	5	7	8	11	15
15	1	2	4	6	7	10	14
14	15	1	3	5	6	9	13
13	14	15	2	4	5	8	12
11	12	13	15	2	3	6	10
9	10	11	13	15	1	4	8
8	9	10	12	14	15	3	7
7	6	7	9	11	12	15	4

The advantages and convenience of using perfect ring bundles, which are a partial example of the set of numerical bundles, are vividly illustrated when constructing a table of circular sums, which demonstrates whether a given sequence is a bundle. This is exactly the case where the elements of the table are the weighting coefficients of the system. And therefore it is quite easy to check the fulfillment or non-fulfillment of the conditions, with minimal expenditure of resources and to take appropriate actions. For this interference-resistant system, the issue of redundancy becomes important in terms of determining the efficiency of the entire system. And that is why the issue of choosing the optimal IC, capable of providing the best indicators of redundancy and corrective ability, is of great importance. It is clear that it is necessary to achieve the highest possible correction ability of the code with minimal redundancy. It is also worth remembering an additional «side» effect: the use of ideal ring bundles (IRB) for data encoding is a technical novelty, and therefore no one will know on which of the IRB sets our system is built on, and therefore it can be used not only as a means of protection against physical obstacles, but as a reliable tool to protect against unauthorized access to valuable information [7].

Methods of synthesis of interference-resistant barker-like codes. It is necessary to build an interference-resistant system capable of providing protection in two main directions:

— from interference – the system must have the highest possible correction ability for successful data transmission over a wireless network, where, as is known, various types of interference may occur;

— from unauthorized access – the algorithm on the basis of which this system is built must be sufficiently complex and non-obvious to make it impossible to decode the data in some way.

Therefore, before proceeding with the software implementation, it is necessary to assess the technical feasibility of implementing an interference-resistant system based on IRB, and for that it is necessary to compare it with the best similar systems known today. Most experts consider this a system based on Bose – Choudhury – Hockingham (BCH) codes. During the comparison, such indicators as the speed of the encoding-

decoding process, degree of redundancy, correction ability, algorithmic complexity, etc. are taken into account.

Knits make it possible to ensure a sufficiently high correction ability of such a system due to its unique combinatorial properties, and the dissimilarity of the encoding-decoding process compared to existing cryptographic methods that use the properties of polynomials makes the protection even stronger.

The basis of the construction of interference-resistant codes, as is known, is the principle of introducing redundancy, which makes it possible to detect and correct errors by imposing additional requirements on the transmitted signals, followed by their verification [8].

The synthesis of interference-resistant codes on the basis of IRB became possible due to the fact that an ideal ring with parameters N and R corresponds to a cyclic BIB scheme on a set of elements $\{b_j\} = \{j\},\ j = \overline{1,\ 2,\ \ldots,\ S_N}$, which is one of the main types of block diagrams.

A block diagram is the arrangement of elements of a set $\{b_i\} = \{i\},\ i = \overline{1,\ 2,\ \ldots,\ v}$ in a subsets $B_j,\ j = \overline{1,\ 2,\ \ldots,\ a}$, called blocks, with the same number of elements $k_j = k,\ A_j = 1,\ 2,\ \ldots,\ a$ in each block, and the element b_i belongs to r_i different blocks, and each $p-$ and every pair of different elements $(b_i, b_j),\ i \neq j,\ p = 1,\ 2,\ \ldots,\ \frac{v(v-1)}{2}$ is repeated in λ_p the blocks.

The main type of block diagrams include balanced incomplete block diagrams (balanced incomplete block design) or BIB schemes. BIB schemes are formed on the basis of a set of v different elements $(i \neq j \Rightarrow b_i \neq b_j)$ with the number of elements $k < v$ in each block, and the placement of elements in blocks is characterized by the fact that:

- all elements of one block are different;
- each element appears in r different blocks $(r_i = r),\ i = 1,\ 2,\ \ldots,\ v$;
- each $p-$ and every pair of different elements $(b_i,\ b_j),\ p = 1,\ 2,\ \ldots,\ \frac{v(v-1)}{2}$ appears in λ different blocks $\lambda_p = \lambda$.

Between the parameters v, a, k, r, λ of the BIB scheme, which are expressed by known ratios:

$$ak = vr \tag{6}$$

$$r(k-1) = \lambda(v-1) \tag{7}$$

A BIB scheme is called symmetric if:

$$v = a \tag{8}$$

Therefore, according to (8):

$$k = r \tag{9}$$

According to (7) and (9), the ratio is valid for a symmetric BIB scheme:

$$k(k-1) = \lambda(v-1) \tag{10}$$

In the partial case when $\lambda = 1$, the symmetric BIB scheme is called a finite projective plane $(k-1)-$ th of the order.

A symmetric BIB scheme is called cyclic when there is a cyclic automorphism for it α, which consists in the fact that the change of the index $j \to j+1 \pmod v$ for all k elements $j-$ th of the block of the BIB scheme leads to the formation of a set of elements $(j+1 \pmod v)-$ th of the block of the same BIB scheme, so that the set of elements of a separate block is completely defines the entire BIB scheme.

Now, $(k_1,\ k_2,\ \ldots,\ k_n)$ let's match the sequences of numbers that form the IRB to the following $S_N = \frac{N(N-1)}{R} + 1$ sequences:

$$\begin{aligned} B^{(1)} &= (b_1^{(1)}, b_2^{(1)}, \ldots, b_N^{(1)}) \\ B^{(2)} &= (b_1^{(2)}, b_2^{(2)}, \ldots, b_N^{(2)}) \\ &\ldots \\ B^{(S_n)} &= (b_1^{(S_N)}, b_2^{(S_N)}, \ldots, b_N^{(S_N)}) \end{aligned} \tag{11}$$

the elements of which are determined by the formula:

$$x_j - 1 \equiv \sum_{i=1}^{j} k_i \pmod{S_N},\ j = 1, 2, \ldots, N, \qquad (12)$$

To build a cyclic code on the basis of the IRB, we select a row of S_N cells of a one-dimensional array numbered in ascending order and fill the cells with information «units», the numbers of which coincide with the numbers determined from the IRB according to formula (12). Enter «zeros» in the cells that remain unfilled. The resulting sequence of ones and zeros is S_N a bit code combination, the cyclic shift of which can be used to obtain all the last allowed combinations for this cyclic code.Based n the above, let's build a table of code combinations of a Barker-like code based on IRB (1, 1, 1, 2, 2, 1, 3, 4) with parameters $N = 8$ and $R = 4$ (and respectively $S_N = 15$). According to formula (12), we get:

$$\begin{aligned} x_1 &= \sum_{i=1}^{1} k_i \pmod{S_N} + 1 = 2 \\ x_2 &= \sum_{i=1}^{2} k_i \pmod{S_N} + 1 = 3 \\ &\ldots \\ x_8 &= \sum_{i=1}^{8} k_i \pmod{S_N} + 1 = 1 \end{aligned} \qquad (13)$$

However, this table of code combinations will not be complete without a «zero» combination. Thus, we get $S_N + 1 = 16$ code combinations. The complete table of code combinations of the barker-like sequence based on IRB (1, 1, 1, 2, 2, 1, 3, 4) is displayed in the Tab 1.

Table 1

Representation of numbers by combinations of barker-like codes on the basis of IRB

Numeric	Code
0000	000000000000000
0001	000100110101111
0010	001001101011110
0010	010011010111100
0011	100110101111000
0100	001101011110001
0101	011010111100010
0110	110101111000100
0111	101011110001001
1000	010111100010011
1001	101111000100110
1011	011110001001101
1100	111100010011010
1101	111000100110101
1110	110001001101011
1111	100010011010111

Cyclic IRB code is a block code, that is, the number of bits in one block is a constant value. How many bits can be encoded in one block: $n = \log_2(S_N + 1) = \log_2 16 = 4$. After constructing the code combinations, let's find out the possibilities of this code, namely determine the minimum code distance, correction and correction ability. It is easy to find that each of S_N $(S_N - 1)/2$ of different pairs of code combinations contains exactly R single N symbols in digits of the same name, which follows from the properties of the IRB. The remaining $N - R$ symbols of the same and as many other code combinations differ from the symbols contained in the digits of the same name. Therefore, the minimum code distance for this code is defined as:

$$d_{\min} = 2(N - R) \qquad (14)$$

The number of errors that can be detected t_d and the number of errors that can be corrected t_c using the correction code are related to the minimum code distance by dependencies, and are, respectively:

$$t_d \le d_{\min} - 1 \tag{15}$$

$$t_c \le \frac{d_{\min} - 1}{2} \tag{16}$$

In the considered example, the values $N = 8$ and $R = 4$ were not chosen by chance, and there is an explanation for this. So let's consider the possibility of establishing a relationship between N and R, in which the code in question acquires additional advantages. As we can see from formulas (14), (15) and (16), the correcting ability of the code increases with the increase of the minimum code distance and, in fact, this problem is reduced to providing the largest minimum code distance with the smallest possible value $d_{\min}$ of S_N.

Let's try to express the above mathematically. The corrective capacity of the code increases with the increase of the difference $\sigma = N - R$. After substitution $R = \sigma - N$ in (14), we obtain the following equation relative to σ:

$$\sigma = N - \frac{N \times (N-1)}{S_N - 1} \tag{17}$$

After simple mathematical manipulations, we get:

$$S_N = 2N \tag{18}$$

After mutual substitution and solving the equation in integers, we find the ratio between N and R, at which the code acquires the ability to detect and correct the maximum possible number of errors, namely:

$$R = \begin{cases} \frac{N}{2}, \ \textit{for even values } N \\ \frac{N-1}{2}, \ \textit{for odd values } N \end{cases} \tag{19}$$

The ratio we found is extremely important for solving the problem of building an optimal cyclic IRB code, which essentially boils down to choosing an IRB with the necessary parameters.

To illustrate, let's consider an example of calculating the corrective capacity of interference-resistant codes built on the basis of IRB with parameters:

- $N = 6, \ R = 1;$
- $N = 15, \ R = (N-1)/2;$
- $N = 16, \ R = N/2.$

The length of the allowed code combinations for all three codes is the same: $S_N = 31$. The maximum number of errors that can be detected or corrected by the first of the specified codes is and 4, respectively 9, while each of the other two codes allows to detect 15 and correct up to 7 errors. In principle, any IRB can become the basis for the synthesis of an interference-resistant code. However, it should be noted that the most effective interference-resistant codes can be built with the help of ICs, the parameters of which are related by this relationship. And also continuing to describe the use of the IRB base (1, 1, 1, 2, 2, 1, 3, 4), we determine the minimum code distance and the correcting ability of the code:

$$\begin{aligned} d_{\min} &= 2 \cdot (8-4) = 8 \\ t_d &= 8 - 1 = 7 \\ t_c &= \frac{8-1}{2} = 3 \end{aligned} \tag{20}$$

The interference-resistant system of barker-like sequences based on IRB is able to encode 4 the bits of the data array into a sequence of length 15 and at the same time correct to 3 the positions of the sequence (or 20%), while the cryptographic system based on BCH codes with the same length of the sequence and the number of information bits allows editing to the 4 positions of (or $26,67\%$). In terms of corrective ability, BCH codes show better results, although globally 3 or 4 per block length 15 is not critical, because for most software the threshold of correctability is 10%. For greater clarity, the data will be displayed in the Tab. 2.

Table 2

Comparative characteristics of interference-resistant codes

Indicator	Numerical value (points)	
	Codes based on IRB	Codes based on BCH
Code redundancy	11	11
Corrective ability	3	4
Code power	16	16
Data encoding speed, MB/s	2,015	1,936
Data decoding speed, MB/s	0.608	1,316
Resource consumption of the system, MB	80	120
Security, (1-10)	9	4

The second most important parameter that determines the feasibility of implementing a particular development is the speed of the encoding and decoding process. It was experimentally established that both coding systems give approximately the same results when encoding a data array, however, the process of decoding data using IRB is performed more than twice as fast as BCH [9]. The resource consumption also adds «pluses» to codes based on IRB. During the experimental encoding and decoding of 10 megabytes of data, BCH codes take up $120\ Mb$ computer memory, while IRB codes take up only $80\ Mb$. The next parameter, unfortunately, does not have a clear numerical expression and subjective assessments have to be used to determine it – we are talking about data security.

Conclusions. Codes based on IRB are based on well-studied properties of bundle, which have a complex structure for reproduction by attackers. In addition, we use different IRBs, we sort the construction results according to different parameters. BCH-based codes based on Galois fields are theoretically more complex, as the number of operations for their construction increases, and the number of polynomial options is limited and they are all already known.

References:

1. Aljalai A.M.N., Feng C., Leung V.C.M., Ward R. Improving the energy efficiency of dft-s-ofdm in uplink massive mimo with barker codes», in 2020 International Conference on Computing, Networking and Communications (ICNC), 2020, pp.731-735. doi:10.1109/ICNC47757.2020.9049829.

2. Fu J., Ning G. Barker coded excitation using pseudo chirp carrier with pulse compression filter for ultrasound imaging, *BIBE 2018: International Conference on Biological Information and Biomedical Engineering*, Shanghai, China, 2018, pp.1-5.

3. Kellman M., Rivest F., Pechacek A., Sohn L., Lustig M. Barker-coded nodepore resistive pulse sensing with built-in coincidence correction: in 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2017, pp.1053-1057. doi: 10.1109/ICASSP.2017.7952317.

4. Lakshmi R., Trivikramarao D., Subhani S., Ghali V.S. Barker coded thermal wave imaging for anomaly detection: in 2018 Conference on Signal Processing And Communication Engineering Systems (SPACES), 2018, pp.198-201. doi:10.1109/SPACES.2018.8316345.

5. Matsuyuki S., Tsuneda A. A Study on Aperiodic Auto-Correlation Properties of Concatenated Codes by Barker Sequences and NFSR Sequences: in 2018 International Conference on Information and Communication Technology Convergence (ICTC), Jeju, 2018, pp.664-666. doi:10.1109/ICTC.2018. 8539367.

6. Riznyk O., Povshuk O., Kynash Y., Yurchak I. Composing method of anti-interference codes based on non-equidistant structures», in 2017 XIIIth International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH), Lviv, 2017, pp.15-17. doi:10.1109/MEMSTECH.2017. 7937522.

7. Riznyk V., Riznyk O., Balych B., Parubchak V., Information Encoding Method of Combinatorial Optimization. 2006 International Conference – Modern Problems of Radio Engineering, Telecommunications, and Computer Science, Lviv-Slavsko, 2006, pp.357-357. doi: 10.1109/TCSET. 2006.4404550.

8. Tsmots I., Rabyk, Riznyk O., Kynash Y. Method of synthesis and practical realization of quasi-barker codes: in 2019 V.IEEE 14th International Conference on Computer Sciences and Information Technologies (CSIT), 2019, Vol.2, pp.76-79. doi:10.1109/STC-CSIT.2019.8929882.

9. Tsmots I., Riznyk O., Rabyk V., Kynash Y., Kustra N., Logoida M. Implementation of fpga-based barker's-like codes», in Lytvynenko, V., Babichev, S., Wo´jcik , W., Vynokurova, O., Vyshemyrskaya, S., Radetskaya, S. (eds.) Lecture Notes in Computational Intelligence and Decision Making, 2020, pp.203-214. Springer International Publishing, Cham. doi:10.1007/978-3-030-26474-115.