Method of Forming the Ring Codes

Serhii Otrokh[1], Valeriy Kuzminykh[2] and Olena Hryshchenko[1]

[1] State University of Telecommunication, Kyiv, Ukraine
[2] National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
2411197@ukr.net, vakuz0202@gmail.com, elena.grischenko1@gmail.com

Abstract. The article considers a method of forming a ring code, which was created to compress information and protect it unauthorized access. The structure of the forming matrix and the mathematical model of the ring code formation are presented. To identify the ring codes the shift indexes vector is proposed. An algorithm for constructing a shift indexes vector is given by the example of a specific ring code.

The properties of shift indexes vector, created by summing the number of the units obtained from binary transformations of the XOR, OR, AND elements of the initial sequence (first line) of the ring code and successively on each subsequent line, are investigated. The formulas for the summing decimal values of the elements of the shift indexes vector are given.

This method can be used to build an effective channel for the transmission of the future network. There is determined that compressing the information with ring code is 2.7 times higher compared with the amount of information transmitted.

Keywords: Ring Codes, Shift Indexes Vector, Forming Matrix, Binary Transformations

1 Introduction

Ring codes are built on the principle of block cyclic codes, the rows of forming matrices which are interconnected as a condition of cyclicality. Cyclic codes are a subclass of linear codes and have applications in data storage systems and communication systems as they have efficient encoding and decoding algorithms. In accordance with [1-9] the ring code is based on the principle of modular cyclic codes, and represents a binary square matrix of size N × N where each row contains m unit symbols and N - m zero symbols.

The elements shift of the code sequence of the ring code is done from right to left, and, the leftmost symbol is always transferred to the right at the end of the code sequence. Each line of the forming matrix of the ring code has the same number of elements and the same structure of combinations of units and zeros, the number of rows and columns in the forming matrix are always equal.

2 The Algorithm of the Ring Codes Formation

The algorithm for the formation of a ring code is shown in Fig. 1.

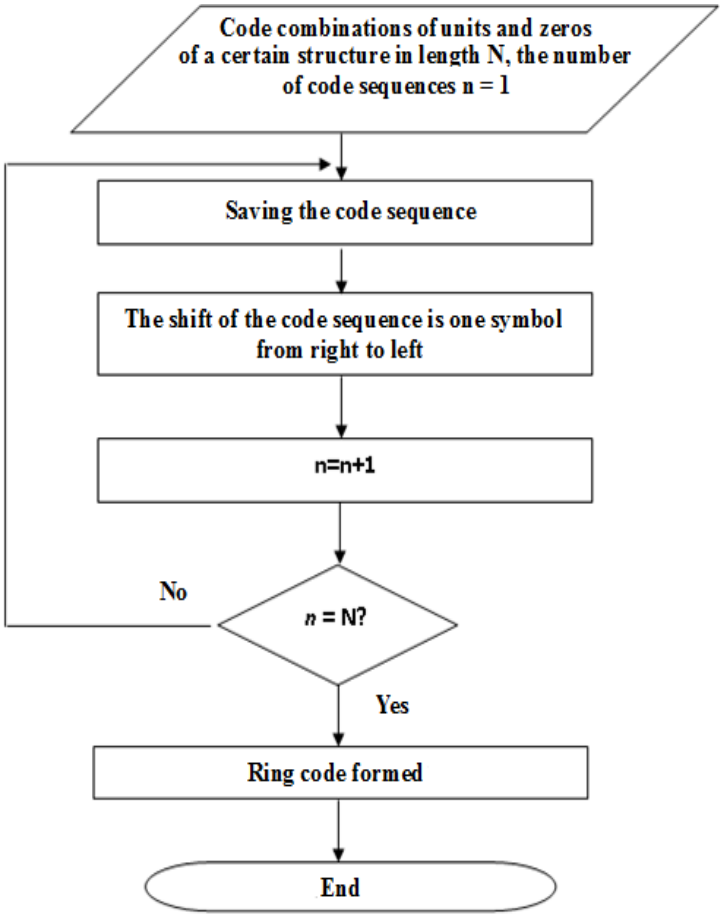

Fig. 1. The algorithmof the ring code formation

In general, the code sequence of the ring code can be determined as:

$$C(x) = k \cdot x^{N-1} \ldots + \cdots k \cdot x^2 + k \cdot x^1 + k \cdot x^0, \quad (1)$$

where k– coefficient that acquires the value of 1 or 0, and x –2 (the basis of the binary number system), and 0,1, ... N-1–is the bit number of the binary system of the number.

Then the forming matrix of a circular code of size N × Nin the general form is formed so that the number of rows equals the number of columns, that is, the matrix has a square shape. In this case, the matrix can be recorded that (2):

$$C(N,N) = \begin{bmatrix} k \cdot x_1^{N-1} \dots + \cdots k \cdot x_1^2 + k \cdot x_1^1 + k \cdot x_1^0 \\ k \cdot x_2^{N-1} \dots + \cdots k \cdot x_2^2 + k \cdot x_2^1 + k \cdot x_2^0 \\ \cdot \\ \cdot \\ \cdot \\ k \cdot x_N^{N-1} \dots + \cdots k \cdot x_N^2 + k \cdot x_N^1 + k \cdot x_N^0 \end{bmatrix} \quad (2)$$

3 The Mathematical Model of the Ring Code Formation

The process of forming a ring code possible to describe mathematically. The binary code sequences of the ring code can be represented in the decimal system in the form of their decimal values, the mathematical model for the formation of which takes on this form:

$$C_i(N,m) = S_1 \cup S_2, \quad (3)$$

where $C_i(N,m)$ – total set of decimal values of code sequences, S_1 is a set of a first decimal values of the code sequences of the ring code, S_2– a set of a second code decimal values of the ring code sequences, N– the number of code sequences of the ring code equal to the number of elements of the code sequence, m–the number of units in code sequence.

At that

$$S_1 = \{s_{11}, s_{12}, \dots, s_{1n)}\}, S_2 = \{s_{21}, s_{22}, \dots, s_{2l}\} \quad (4)$$

where s_{11}– the decimal value of the first code sequence of the set 1, s_{1n}– the decimal value of the last code sequence of the set 1, s_{21}– the decimal value of the first code sequence of the set 2, s_{2l}– the decimal value of the last code sequence of the set 2.

Common expressions for computing the decimal values of the elements setS_1 are as follows:

$$s_{11} = \sum_{i=0}^{N-1} k * 2^i \tag{5}$$

where k – coefficient that acquires the value of 1 or 0, N is the number of elements of the code sequence, and s_{11} - the least decimal value of the code sequence.

It should be noted that the decimal value of each subsequent code sequence is twice the decimal value of the previous code sequence of the set S_1. Therefore:

$$s_{12} = 2 \cdot s_{11}; s_{1n} = 2 \cdot s_{1(n-1)}, \tag{6}$$

where n – the number of code sequences in a setS_1.

The general expressions for computing the decimal values of the set S_2 are as follows:

$$s_{21} = s_{1n} - S_p; s_{22} = 2 \cdot s_{21}; s_{2l} = 2 \cdot s_{1(l-1)}. \tag{7}$$

Where S_p– the difference, the calculation formula of which depends on the structure of the combinations of one and zero symbols of the code sequences of the ring code; l- the quantity of code sequences in a set 2.

4 The Mathematical Model of a Shift Indexes Vector Formation

The ring code is characterized by a shift indexes vector (SIV), which is formed by summing the number of units obtained as a result of one of the binary transformations *XOR*, *OR*, *AND* (with N_{ot} or without it) of the elements of the initial sequence (first line) of the ring code and successively each of the next line.

Moreover, the quantity of symbols in the shift indexes vector per unit is less than the number of lines of the ring code. It should also be noted that the shift indexes vector is a group integral index of the whole ring code, rather than a single line of it.

For example, the shift indexes vectors of the ring code of 7 × 7, each line contains 4 units and 3 zeros, and the initial vector consists of a code sequence [0101011], which are formed by summing the number of units obtained as a result of one of the binary transformations *XOR*,*AND*,*OR* are shown in tables1-3.

Table 1. The process of creating the shift indexes vector as a result of one of the binary transformations *XOR*

Formation matrix	The matrix of shift indexes vector in the binary system as a result of the logical operation XOR	Shift indexes vector in decimal (number of units)	The matrix of shift indexes vector in in a binary system	Shift indexes vector in a binary system
0101011	1111101	6	110	
1010110	0000110	2	010	
0101101	1110001	4	100	
1011010	1110001	4	100	1100101001000010110
0110101	1000001	2	010	
1101010	1111110	6	110	
1010101				

Table 2. The process of creating the shift indexes vector as a result of one of the binary transformations *AND*

Formation matrix	The matrix of shift indexes vector in the binary system as a result of the logical operation *AND*	Shift indexes vector in decimal (number of units)	The matrix of shift indexes vector in in a binary system	Shift indexes vector in a binary system
0101011	0000010	1	001	
1010110	0101001	3	011	
0101101	0001010	2	010	
1011010	0100001	2	010	0010110100100110001
0110101	0101010	3	011	
1101010	0000001	1	001	
1010101				

Table3. The process of creating the shift indexes vector as a result of one of the binary transformations *OR*

Formation matrix	The matrix of shift indexes vector in the binary system as a result of the logical operation *OR*	Shift indexes vector in decimal (number of units)	The matrix of shift indexes vector in in a binary system	Shift indexes vector in a binary system
0101011	1111111	7	111	
1010110	0101111	5	101	
0101101	1111011	6	110	
1011010	0111111	6	110	111101110110101111
0110101	1101011	5	101	
1101010	1111111	7	111	
1010101				

Thus, in the communication channel, we can transfer 49 binary information symbols, unless we use the ring code. If we use ring code in the communication channel, we transmit instead of 49 symbols only 18. Due to the use of the ring code, avoid redundancy and the gain is 49/18 ≈ 2.7 times.

The shift indexes vectors of the ring code of 9×9, each line contains 5 units and 4 zeros, and the initial vector consists of a code sequence [001001111], which are formed by summing the number of units obtained as a result of one of the binary transformations *XOR*,*AND*,*OR* are shown in tables 4-6.

Table 4. The process of creating the shift indexes vector as a result of one of the binary transformations *XOR*

Formation matrix	The matrix of shift indexes vector in the binary system as a result of the logical operation *XOR*	Shift indexes vector in decimal (number of units)	The matrix of shift indexes vector in in a binary system
001001111	011010001	4	100
010011110	101110011	6	110
100111100	000110110	4	100
001111001	010111101	6	110
011110010	110101011	6	110
111100100	110000110	4	100
111001001	111011100	6	110
110010011	101101000	4	100
100100111			

Table 5. The process of creating the shift indexes vector as a result of one of the binary transformations *AND*

Formation matrix	The matrix of shift indexes vector in the binary system as a result of the logical operation *AND*	Shift indexes vector in decimal (number of units)	The matrix of shift indexes vector in in a binary system
001001111	000001110	3	011
010011110	000001100	2	010
100111100	001001001	3	011
001111001	001000010	2	010
011110010	001000100	2	010
111100100	001001001	3	011
111001001	000000011	2	010
110010011	000000111	3	011
100100111			

Thus, in the communication channel, we can transfer 81 binary information symbols, unless we use the ring code. If we use ring code in the communication channel, we transmit instead of 81 symbols only 24. Due to the use of the ring code, avoid redundancy and the gain is $81/24 \approx 3.4$ times.

Table 6. The process of creating the shift indexes vector as a result of one of the binary transformations *OR*

Formation matrix	The matrix of shift indexes vector in the binary system as a result of the logical operation *OR*	Shift indexes vector in decimal (number of units)	The matrix of shift indexes vector in in a binary system
001001111	011011111	7	0111
010011110	101111111	8	1000
100111100	001111111	7	0111
001111001	011111111	8	1000
011110010	111101111	8	1000
111100100	111001111	7	0111
111001001	111011111	8	1000
110010011	101101111	7	0111
100100111			

The mathematical expressions of the formation of shift indexes vector (SIV) by summing up the number of units obtained as a result of the implementation of the binary transformations *XOR*, *OR* and *AND*, respectively, become as follows:

$$SIV_{XOR}=\sum_{i=1}^{N}(x_{1i}\,XOR\,x_{2i})\cup\sum_{i=1}^{N}(x_{1i}\,XOR\,x_{3i})\ldots\cup\ldots\sum_{i=1}^{N}(x_{1i}\,XOR\,x_{Ni}), \quad (8)$$

$$SIV_{OR}=\sum_{i=1}^{N}(x_{1i}\,OR\,x_{2i})\cup\sum_{i=1}^{N}(x_{1i}\,OR\,x_{3i})\ldots\cup\ldots\sum_{i=1}^{N}(x_{1i}\,OR\,x_{Ni}), \quad (9)$$

$$SIV_{AND}=\sum_{i=1}^{N}(x_{1i}\,AND\,x_{2i})\cup\sum_{i=1}^{N}(x_{1i}\,AND\,x_{3i})\ldots\cup\ldots\sum_{i=1}^{N}(x_{1i}\,AND\,x_{Ni}), \quad (10)$$

where $x_{1i}, x_{2i}, x_{3i}, \ldots, x_{Ni}$ i-th element 1-st, 2-nd, 3-th, *N*-th lines of the ring code.

As a result of research of the structure of SIV formed through the binary transformations XOR, OR, AND, the following patterns were found:

— the elements of any SIV are placed symmetrically with respect to its center;

— the sum of the decimal value of the element formed by the binary XOR transformation, and the decimal value of the element formed by the binary transformation AND, is equal to the decimal value of the element, formed by binary OR;

— vectors of the indices of the shift of the ring code can be obtained both in rows and in the columns of the matrix of the ring code;

— the structure of the XOR vector of shift indices remains unchanged if the value of the symbols of the code sequence of the ring code changes to the opposite. The AND and OR vectors of the displacement indices do not have this property.

The sum of the decimal values of the SIV elements formed by the OR-transformation consists of the sum of the decimal values of the SIV elements formed by the XOR transformation and from the sum of the decimal values of the SIV elements generated by the AND transformation. At the same time, the analysis of the structure of the vector of shift indices and their total values allows to note that, regardless of the number of elements of *N* and the number of single symbols m in the code sequence, there is a functional dependence between the sum of the decimal values of the elements of the shift indexes vector and the number of zero and single symbols. It represented by the following formulas:

1) for SIV, created by the XOR-transformation:

$$S_{SIV(XOR)} = (N - m)\cdot 2m, \quad (11)$$

where $S_{VSI(XOR)}$ – the sum of decimal values elements of the SIV generated by the binary XOR-transformation.

In order to determine the number of one and zero symbols in the code sequence, you can apply the formula for calculating the discriminant and the roots of the quadratic equation:

$$x_{1,2} = \frac{N \pm \sqrt{N^2 - 4\frac{S_{SIV(XOR)}}{2}}}{2} \quad (12)$$

where $x_{1,2}$- the quantity of one and zero symbols m and (N- m), N - the length of the code, $S_{SIV(XOR)}$- the sum of the decimal values of the elements SIV generated by the binary XOR-transformation.

2) for SIV, created by binary AND-transformation:

$$S_{SIV(AND)} = (m-1) \cdot m, \tag{13}$$

where $S_{SIV(AND)}$ – the sum of the decimal values of the SIV elements generated by the binary AND-transformation.

In order to determine the number of one and zero symbols in the code sequence, you can apply the following simple formulas

3) for SIV, created by the binary OR-transformation:

$$S_{SIV(OR)} = (N-m) \cdot 2m + (m-1) \cdot m = N \cdot 2m - 2m^2 + m^2 - -m = N \cdot 2m - m^2 - m = m \cdot (2N - m - 1), \tag{14}$$

where $S_{SIV(OR)}$ – the sum of the decimal value SIV elements generated by the binary OR-transformation.

InTable 2 and on the Fig. 2 shows the dynamics of change in the sum of the decimal value SIV elements generated by the binary transformations *XOR, OR, AND*, depending on the number of single elements *m* of the code sequence of ring code.

Table 2. The dynamics of change in the sum of the decimal values of the shift indexes vector elements, depending on the number of elements of *N* and the number of single symbols of *m* code sequences

Number of units *m*	The sum of the decimal values of the elements SIV		
	XOR-SIV	AND-SIV	OR-SIV
The number of items *N*=7			
1	12	0	12
2	20	2	22
3	24	6	30
4	24	12	36
5	20	20	40
6	12	30	42

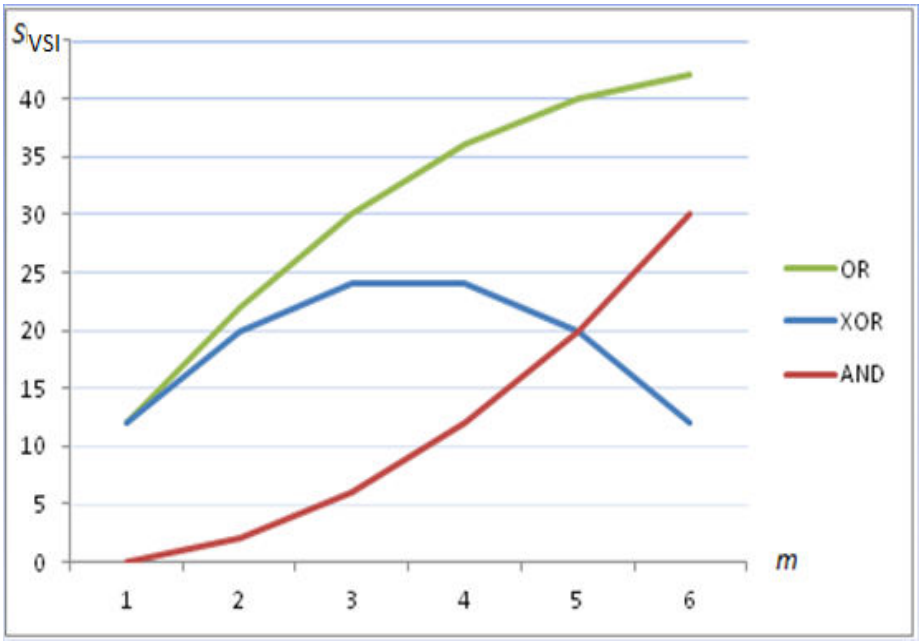

Fig. 2. Dynamics of the change of the sum of the decimal values of the elements of the SIV, created by the binary transformations XOR, OR, AND, from the number of single elements m for a 7x7 ring code

5 Conclusion

The method of the ring code generation was developed and the mathematical models of forming the ring code families for the construction of an effective channel for the transmission. The mathematical models of forming the ring code families were developed with using the values of code sequences in the decimal system.

Vector of shift indices, created by summing the number of units obtained as a result of one of the binary transformations of the XOR, OR, AND elements, was developed. The shift indexes vector is analog of the ring code, which can be transmitted via a communication channel instead of code.

Formulas for determining the sum of the decimal values of the e shift indexes vector elements, obtained by the AND, OR and XOR transformation, were derived. It was determined that there is a functional dependence between the sum of the decimal values of the elements of the shift indexes vector and the number of zero and single symbols in the code sequence of ring code.

The dynamics of change in the sum of the decimal value SIV elements generated by the binary transformations XOR, OR, AND, depending on the number of single elements m of the code sequence of ring code showed in article.

The gain from the use of the ring code using the vector of shift indices is 2.7 times compared with the amount of information transmitted.

References

1. V.B. Tolubko, S.I. Otrokh, L.N. Berkman, O.G. Pliushch, V.I. KravchenkoNoise Immunity Calculation Methodology for Multi-Positional Signal Constellations// 14th IEEE International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET'2018): Conference Proceedings. – Lviv, 20-24 of February, 2018. – Paper #436.
2. S.I. Otrokh, L.M. Hryshchenko, V.V. Dubrovsky, U.V. Melnik Peculiarities of the Formation of Commemoration of Kilts Kodiv Type 001011: Mathematical Model – Kyiv: Communication –2018 – № 1 – p.33-40 (in Russian).
3. V.B. Tolubko, S.I. Otrokh, L.N. Berkman, V.I. Kravchenko Manipulation coding of signal n-dimensional multi-position constellations based on the optimal noise immunity of regular structures– Kyiv: Telecomunication and information texnology –2017 – № 3(56) – p.5-11 (in Russian).
4. S.I. Otrokh, V.A. Kuzminykh, I.O. Sosnovsky Future network in action, online life– Kyiv: Communication –2018 – № 6 – p.42-45 (in Russian).
5. L.M. Hryshchenko Patterns of formation of ring codes. Mathematical model – Kyiv: Communication – 2016 – № 5(123). – p.27-31 (in Ukrainian).
6. L.M. Hryshchenko Mathematical model for creating the 010101 type family ring code– Kyiv: Communication – 2017– № 1(125). – p.58-61 (in Ukrainian).
7. E.V. Havrylko, S.I. Otrokh, V.I. Yarosh, L.M. Hryshchenko Improving the quality
8. of the future network by using the ring– Minsk: Communication Herald –2018 –№2 –p.60-64(in Russian).
9. Security of information systems (in Russian) [Electronic Resource]. Mode of access: http://intuit.valrkl.ru/course-1312/index.html.