http://doi.org/10.35784/iapgos.2413

POLYPARAMETRIC BLOCK CODING

Julia Milova, Yuri Melnyk
State University of Telecommunications, Educational-Scientific Institute of Telecommunications, Kiev, Ukraine

Abstract. *The principles of poly-parametric information coding have been considered. The methods for developing poly-parametric codes have been presented. It is shown that the protection of block codes from channel interference using check patterns can be developed by a mono- or poly-parametric method. A special type of block codes has been presented, the check patterns of which are formed on the basis of their neighbours, which are functionally related to the given code combination. Such codes have been called poly-parametric. Binary poly-parametric ring codes, the check patterns of which are designed to detect and correct channel errors, are developed using the properties of Galois fields and on the basis of the vector shift indicators of the codewords. To obtain digital poly-parametric block codes, the properties and features of the normalized natural sequence are used. It is shown that each codeword of a binary block code can be represented as a certain positive integer in the decimal number system, which is an element of the natural sequence. Its elements on an interval that equals the norm acquire a functional dependency.*

Keywords: codeword, vector shift indicators, natural sequence, poly-parametric codes

POLIPARAMETRYCZNE KODOWANIE BLOKOWE

Streszczenie. *Rozważono zasady poliparametrycznego kodowania informacji. Przedstawiono metody tworzenia kodów poliparametrycznych. Wykazano, że ochrona kodów blokowych przed zakłóceniami kanałowymi za pomocą wzorców kontrolnych może być realizowana metodą mono- lub poliparametryczną. Przedstawiono specjalny typ kodów blokowych, których wzorce kontrolne są tworzone na podstawie ich sąsiadów funkcjonalnie związanych z daną kombinacją kodową. Takie kody zostały nazwane poliparametrycznymi. Z wykorzystaniem własności pól Galois oraz na podstawie wskaźników przesunięcia wektorowego słów kodowych, zostały opracowane binarne poliparametryczne kody pierścieniowe, których schematy kontrolne przeznaczone są do wykrywania i korekcji błędów kanałowych. Do otrzymania cyfrowych poliparametrycznych kodów blokowych wykorzystuje się właściwości i cechy znormalizowanego ciągu naturalnego. Pokazano, że każde słowo kodowe binarnego kodu blokowego może być reprezentowane jako pewną dodatnią dziesiątkową liczbę całkowitą, która jest elementem ciągu naturalnego. Jego elementy w przedziale równym normie uzyskują zależność funkcyjną.*

Słowa kluczowe: słowo kodowe, wskaźniki przesunięcia wektorów, ciąg naturalny, kody poliparametryczne

Introduction

Block codes play a vital role among a large number of different methods for coding digital information. Although block codes have the most ancient history in terms of time creation, they have not lost their significance even now [7, 9]. They are mainly used for coding and exchange of book documentary information that requires special accuracy. This defines the usual structure of block codes, consisting of two parts – useful information and check symbols for error detection and correction. The symbol error correction is built on the informational part of the codeword and is often built into the general structure of the block. Over the years of its existence, truly unique, sophisticated methods of creating check patterns have been developed, which were often named after their developers – Hamming, Halley, BCH codes, etc. All of these codes use the information of only the useful part of the transmitted block [5, 10, 14]. This imposes certain limitations on the creation of the check part of a codeword separate block.

1. Fundamentals for constructing polyparametric binary block codes

Let us consider the following example. Let the useful information, presented in a block of length N binary symbols be bitwise shifted left or right N-1 times. Moreover, after each shift, the number of bitwise coinciding units in the original and offset numerical vectors is determined (V). It is clear that after such actions, we will receive the vector shift indicators (VSI) consisting of N-1 numeric elements. Note that the original vector and its N-1 close equivalents have a linear relationship with each other, which can be used to create check patterns. Individual elements of the vector shift indicators can be subjected to linear and non-linear operations, the results of which can also be used to obtain a check pattern. The considered example is shown in Fig. 1.

Fig. 1 shows that in this case, to obtain a check pattern, the structure of not only the original vector is used, but also the other N-1 shift vectors that functionally depend on it. This provides an advantage when creating a check pattern and expands the possibilities for obtaining it [4, 8, 12].

$$
\mathrm{V} = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1
\end{bmatrix}
\qquad
\mathrm{VSI} = \begin{bmatrix}
2 & 4 & 6 & 8 & 8 & 6 & 4 & 2 \\
 & 2 & 4 & 6 & 8 & 8 & 6 & 4 \\
 & & 2 & 4 & 6 & 8 & 8 & 6 \\
 & & & 2 & 4 & 6 & 8 & 8 \\
 & & & & 2 & 4 & 6 & 8 \\
 & & & & & 2 & 4 & 6 \\
 & & & & & & 2 & 4 \\
 & & & & & & & 2
\end{bmatrix}
$$

Fig. 1. Receiving the elements of the vector shift indicators

In other words, there are mono- and poly-parametric code combinations:

- mono-parametric block codes are the codes in which the check pattern of each block is formed only on the basis of its internal structure;
- polyparametric block codes are the codes, the check pattern of which are formed by a given block and a set of neighbouring codewords functionally depending on a given codeword.

When block codes are used, information is transmitted by codewords of constant selected length L. The check patterns of these codes are based on an internal structure, namely, the distribution of 0s and 1s within one codeword.

Let us consider the structure of 0s and 1s located between the first and last single symbols of the codeword called the delta factor. A delta factor structure of some type allows ring codes with special properties to be created. Namely, when expanding the size of the codeword by several zero symbols, the vector shift indicators are completely determined by the type of the delta factor, which enables codes with special properties to be obtained. These codes can be used as entropy codes.

The information resource for block codes is a relative value indicating the number of units of its information part, for which a check pattern is created for channel error detection and correction. For mono-parametric codes, the information resource has a limit equal to one. For polyparametric codes, it equals |L/2|+1, where L is the length of the codeword.

The information reserve is the amount of information for obtaining a check pattern in block codes, which exceeds the capabilities of the useful information part of the transmitted codeword. For mono-parametric codes, the information reserve is equal to zero, and for poly-parametric codes interconnected by functional dependency, it is equal to |L/2|-1.

Earlier, it was shown that the construction of poly-parametric codes requires a functional dependency between the received code combination and its nearest neighbours. In Fig. 1, there are N-1 of such nearest neighbours equal to the length of the code combination. Thus, binary codes that are segments of Galois fields have functional dependency [1–3].

2. Polyparametric digital decimal block codes

But it turned out that decimal codes, which are elements of the normalized natural sequence, have a similar functional dependency [9].

Deviations of the characteristics of the normalized natural series from the non-normalized ones can be used as parameters of the set of codewords built on their basis.

Such features of the normalized natural series create conditions for varying its elements in order to create new codes with new characteristics. These characteristics can be used as parameters.

Polyparametric codes are closely related to the usual natural series, which is an infinite sequence of integers differing by one on a unit interval.

Under the concept of a normalized natural sequence, a natural sequence should be taken after each of its elements by the same integer. It is convenient to choose this integer equal to the length of the information part of the transmitted block. After normalization, the natural sequence begins to possess the following features:

- elements of the natural sequence are converted into real numbers, consisting of an integer part (modulus) and a fractional part (remainder);
- with respect to the remainders, the normalized sequence or its segments are divided into sections of the same length equal to the size of the norm, which we have proposed calling cycles;
- in all cycles of the normalized natural sequence and in its segments, the remainders are repeated and depend only on the size of the norm;
- cycles are separated from each other by a normalized element with a zero remainder.

When an element of the natural series becomes equal to or a multiple of the value of the norm, its remainder becomes zero, and the value of the integer part is increased by one and becomes equal to the ordinal number of the next cycle. Up to this point, the integer part of all normalized elements is equal to the cycle ordinal number reduced by one. The fractional part of each normalized element in the cycle is determined only by the value of the norm.

Below are examples of two cycles of normalized natural series for two different norms and two different lengths of clippings.

These features are shown in Fig. 2.

Here, Gx(n) and Gx(k) are the cycles obtained by normalizing the natural sequence, L = 7 and 11 are the size of the norm, and *n* and *k* are the lengths of the line segment of the normalized natural series, from which cycles are selected. The parameters of the given cycles are as follows:

G(n), L = 7, n = 70…84
G1(n), L = 11, n = 70…84
G(k), L = 7, k = 56…70
G1(k), L = 11, k = 56…7

If you select elements of the normalized natural sequence as decimal codes, they will have the abovementioned properties. It can be considered that any deviation of the properties of the normalized natural sequence and various combinations of its elements are the basis for getting new parameters of codewords obtained due to this sequence or its normalized equivalent. Such parameters, with the help of adjacent codewords, enable check patterns to be obtained for channel error detection or correction.

In particular, the elements of the normalized natural sequence, used as code combinations, receive two parameters: the ordinal number of the cycle from the beginning of the natural sequence in which the code combination is located and which can be considered as the index of this combination, as well as its number from the beginning of the cycle, used as an offset. Using these parameters, it is easy to check the correctness of the code combination and to correct existing errors.

It is worth noting the fundamental feature of the given parameters: their one-to-one correspondence with the parental code combination. In fact, these two parameters can be transmitted with equal success instead of the parent code combination, and vice versa.

$n = 70..84$ $\qquad$ $k = 56..70$

$G(n) = \frac{n}{7}$	$G1(n) = \frac{n}{11}$	$G(k) = \frac{k}{7}$	$G1(k) = \frac{k}{11}$
10	6.364	8	5.091
10.143	6.455	8.143	5.182
10.286	6.545	8.286	5.273
10.429	6.636	8.429	5.364
10.571	6.727	8.571	5.455
10.714	6.818	8.714	5.545
10.857	6.909	8.857	5.636
11	7	9	5.727
11.143	7.091	9.143	5.818
11.286	7.182	9.286	5.909
11.429	7.273	9.429	6
11.571	7.364	9.571	6.091
11.714	7.455	9.714	6.182
11.857	7.545	9.857	6.273
12	7.636	10	6.364
…	…	…	…

Fig. 2. Cycles of a normalized natural sequence

3. Coefficients before normed codes

Problems of coefficients in front of normalized codes arise due to the fact that the coefficient "k" located in front of the value of an element of the natural series is divided by the norm L. As a result of this, at least three varieties of the quotient from the division are formed: the quotient is equal to, less than or greater than one. Moreover, the value of the quotient can be very different in magnitude.

The first kind of quotient occurs when the norm is the largest multiple of the coefficient or is equal to it. For example:

*84*k:7=12*k*
*48*k:8=6*k*
*17*k:17=k*

The second type of quotient occurs when a quotient is a fractional number greater than or less than one. For example:

*67*k:13=5.154*k*
*13*k:24=0.542*k*

The third kind of quotient appears when the numerator and denominator have a common factor. Then the quotient becomes basically a real number. Its peculiarities, in this case, are preserved. For example:

*66*k:26=33*K:13*
*9*K:39=3*K:13*

Four examples of the resulting cycles of a normalized natural series with coefficients in front of the elements are given below:

The sampling interval of the natural range is from 65 to 85 elements.

Figure 3 shows the cycles in more detail.

$$n := 67..85$$

$$G5(n) = \frac{3n}{8} \quad G6(n) = \frac{3n}{10} \quad G2(n) = \frac{3n}{11} \quad G8(k) = \frac{3n}{13}$$

$G5(n) =$	$G5(n) =$	$G5(n) =$	$G5(n) =$
25.125	20.1	18.273	15.462
25.5	20.4	18.545	15.692
25.875	20.7	18.818	15.923
26.25	21	19.091	16.154
26.625	21.3	19.364	16.385
27	21.6	19.636	16.615
27.375	21.9	19.909	16.846
27.75	22.2	20.182	17.077
28.125	22.5	20.455	17.308
28.5	22.8	20.727	17.538
28.875	23.1	21	17.769
29.25	23.4	21.273	18
29.625	23.7	21.545	18.231
30	24	21.818	18.462
30.375	24.3	22.091	18.692
...	...	...	...

Fig. 3. Coefficients of elements of normalized natural series

From the examples above, you can see that:

- the cyclicity of the normalized natural series remains, which is equal to the size of the norm;
- each time, the product "coefficient multiplied by the current value of the row element" is subjected to normalization;
- a normalized natural series with coefficients relative to the fractional part (remainders) is divided into segments of the same length – cycles separated from each other by elements with zero remainder;
- the residuals during normalization of the natural series with coefficients are formed not for each successive element of the natural series, but for those elements that are created after multiplying each element by the corresponding coefficient;
- cycles are equal to the value of the norm;
- if the coefficients are real numbers, then the normalized natural series loses its cyclicity;
- a normalized natural series with coefficients at a rate of 10 forms normalized elements with residuals of one digit (multiple of 10).

4. Constructing polyparametric codes

Considering the line segments of the normalized natural series with coefficients in front of each element, we come to the conclusion that, by combining the elements of the natural series and then normalizing them, it is possible to construct new polyparametric digital codes with two or more parameters. An example of the result of such a construction is the so-called summary code and its varieties. Each code combination of the total code is obtained by arithmetic addition of all elements of the natural series up to this number, including it. It is clear that if the n-th code combination is created (constructed), it will be equal to the sum 1 + 2 + 3 + … + n. The sequence of code combinations obtained in this way is then normalized using the selected rate.

For the summary codes, the following patterns are observed:

- the normalized natural series, as well as its individual segments with respect to the fractional part (remainders) of neighbouring elements, splits into cycles-segments of the same length, equal to the size of the norm L;
- within each cycle with respect to its middle part, for all remainders, the even symmetry is established: at the same distance from the centre of the cycle, the residuals of normalized elements are equal to each other;
- in each cycle, there is a pair of normed elements with zero residuals, which can be used to frame the cycles;
- if the norm is an even number, then, relative to the remainders, each element of the cycle has its own pair, with an odd norm, the middle element of the pair does not have.

These patterns can be seen in more detail in Fig. 4.

The sequences designated S3, S4 and S7 represent cycles of normed codewords at rates equal to 6, 8, and 9, respectively.

Here, the cyclic essence of the normed natural series is immediately revealed, and the cycle size is equal to the norm, as well as zero residuals of codes at the ends of the cycles (however, the beginning of the cycles can be selected from any element in the cycle and this will be correct). It is more convenient to start and end cycles with zero remainders. One asymmetric element is well traced with remainders 0.857 for the L = 7 norm and 0.222 for the L = 9 norm. For an even norm, such as L = 8, the remainders of all normed elements in the cycle are repeated twice.

S3(n) L=70 0; 0.143; 0.429; 0.857; 0.429; 0.143; 0
S4(n) L=8 0.25; 0.75; 0.5; 0.5; 0.75; 0.25; 0
S7(n) L=9 0; 0.222; 0.667; 0.333; 0.222; 0.333; 0.667; 0.222; 0.

$$n := 35..54$$

$$S3(n) = \sum_{k=1}^{n} \frac{k}{7} \qquad S3(n) = \sum_{k=1}^{n} \frac{(2k)}{8} \qquad S3(n) = \sum_{k=1}^{n} \frac{(2k)}{9}$$

$G3(n) =$	$G4(n) =$	$G7(n) =$
90	157.5	140
95.143	166.5	148
100.429	175.75	156.222
105.857	185.25	164.667
111.429	195	173.333
117.143	205	182.222
123	215.25	191.333
129	225.75	200.667
135.143	236.5	210.222
141.429	247.5	220
147.857	258.75	230
154.429	270.25	240.222
161.143	282	250.667
168	294	261.333
175	306.25	272.222
...	...	

Fig. 4. Total code combination loops

5. Digital total codes and their features

It is known that any binary code combination can be represented by a positive integer. Since the total codes are numerical, and in their structure, each total codeword is derived from a natural number series, we agree to number the counting set of total codes in order with the elements of the natural series 1, 2, 3, …, n and form them by simply adding the elements of this series. Also, the total codeword can be easily represented as a binary number [13]. For example, a code with sequence number n = 5 is obtained as a binary representation of the total of decimal numbers S(n) = 1 + 2 + 3 + 4 + 5 = 15, i.e. as Z = 1111, and a code with sequence number n = 10 is encoded as a binary representation of the total of decimal numbers S(n) = 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10 = 55, namely Z=110111.

A feature of total codes is that they are polyparametric. Each codeword typically has several parameters by which it can be extracted from a plurality of similar codewords and, against the background of external interference distorting the codeword structure, reconstructed. Let us indicate two main parameters of total codes, which make it possible to check the correctness of the code word of the total code and in many cases restore it to its original form:

- belonging of the codeword to the group of total codes. If the received codeword, in accordance with its value, does not belong to the group of total codes constructed in accordance with

the above algorithm, it is erroneous. The sum structure of the codeword is its main parameter;
- the remainder of dividing the total codeword by a given number. If the remainder of dividing the codeword by some selected pre-known integer has a remainder other than the expected remainder, it is erroneous. The type and value of the remainder of dividing the total codeword by a given number is its second parameter.

There are two properties of total codes that can be easily verified experimentally.
1) A set of codewords on a certain interval of their lengths n, being correlated to any small integer K, necessarily gives one or several dual multiplicities. Dual multiplicities D are the pairwise results of dividing the total codeword with the number of elements n by K without the remainder. Dual multiplicities are quite common. Therefore, such code words are convenient to use in practice.
2) If one integer is divided by the second, the result is the whole part and the remainder, which is always less than the divisor. For total codes, there is such a pattern that, starting from any dual multiplicity, the remainders of dividing integers of the total codes S (n) by the divisor K up and down the set of ordinal numbers n are symmetric and pairwise equal to each other, starting from any dual multiplicity [11].

The remainder values are stored over the entire set of codeword numbers.

Thus, for each total codeword, there are three of its identification parameters:
- serial number n;
- value of the total codeword S(n);
- remainder of dividing the total codeword by the selected number k.

Note that two adjacent dual-fold total codewords have zero residuals.

There are three types of total codes: natural numbers, even and odd total codes. The last two codes can be considered as derivatives of the total natural number code.

Even total codes are formed on the basis of even numbers of natural numbers 1, 2, 3, … n according to the formula 2*n, and odd total codes according to the formula 2*n + 1. Here, the next codeword is recursively obtained from the previous codeword by adding the next even or odd number, respectively. The result is a sequence of codewords. In particular, the first ten codewords of an even total code have the form 2 6 12 20 30 42 56 72 90 110. Similarly, the first twelve odd codewords form a sequence of 3 7 13 21 43 57 73 91 111. As follows from the logic of things, code combinations with the same sequence numbers differ by one, and the odd summary codes prevail over the even ones. Therefore, the basic properties in both codes must be the same.

The properties of even and odd sum codes demonstrate the following patterns.
- at any interval, the normalized sequence of the sum code breaks down into cycles of equal length, the size of which is determined by the size of the norm; each cycle is bordered by an integer multiple of the norm value;
- normalized code words in cycles are real numbers, the fractional part of which is a set of values symmetric with respect to the average code and equal to each other.

These fractional parts for each norm-different and are stored as constants for all received cycles on an infinite sequence of codewords.

6. Conclusions

The protection of block codes from channel interference using check correcting patterns can be performed in a mono-parametric or poly-parametric way, i.e. either one code combination at a time or using the code combinations of its neighbours functionally related to it.

For this purpose, a methodology for creating binary and digital decimal poly-parametric codes have been proposed.

Binary poly-parametric codes are developed using the properties of Galois fields, whereas digital block codes are based on the natural sequence. In this case, the basis of poly-parametric codes (Galois fields and the original natural sequence) is subjected to linear transformations to obtain a functional dependency of the neighbouring codes.

Based on the thinned natural sequence, poly-parametric codes can be developed to detect, correct errors, and protect from unauthorized access.

For detecting and correcting combinations of poly-parametric codes, new possibilities open up due to additional information embedded in adjacent codewords.

Poly-parametric codes, in comparison to mono-parametric codes, using only one code combination, simplify, improve and diversify the choice of code protection from errors and interference.

References

[1] Arora S., Barak B.: Computational Complexity: A Modern Approach. Cambridge University Press, Cambridge 2009.
[2] Berlekamp E.: Algebraic coding theory. Mir, Moscow 1971.
[3] Blahut R. E.: Algebraic Codes for Data Transmission. Cambridge University Press, 2012.
[4] Bronshtein I. N., Semendyaev K. A.: Mathematics reference book for engineers and students of technical colleges. GITTL, Moscow 1957.
[5] Brouwer E., Shearer J. B., Sloane N. J. A., Smith W. D.: A new table of constant weight codes. IEEE Trans. Inform. Theory 36/1990, 1334–1380.
[6] Carrasco R. A., Johnston M.: Non-binary error control coding for wireless communication and data storage. J. Wiley & Sons, 2008.
[7] Conway J. H., Sloane N. J. A.: Lexicographic codes: error-correcting codes from game theory. IEEE Trans. Inform. Theory 32/1986, 337–348.
[8] Dikarev A. V.: Codes based on binary rings. Control systems, navigation and communication 1(29)/2014. 50–53.
[9] Etzion T.: Optimal constant weight codes over Zk. and generalized designs. Discrete Math. 169/1997, 55–82.
[10] MacKay D., Neal R.: Near Shannon limit performance of low density parity check codes. IEEE Electronics Letters 32(18)/1996, 1645–1646.
[11] Milova J. A.: Parameters of total codes. Zvyazok 4/2018, 3–32.
[12] Milova Y.: Rationed natural row. Polyparametric coding. The European Journal of Technical and Natural Sciences 3/2020, 19–23 [http://doi.org/10.5604/20830157.1121333].
[13] Milova J. A. et al.: Total codes. Zvyazok 3/2018, 47–50.
[14] Robinson J. P., Bernstein A. J.: A class of binary recurrent codes with limited error propagation. EEE Transactions on Information Theory 13(1)/1967, 106–113 [http://doi.org/10.1109/TIT.1967.1053951].

M.Sc. Julia Milova
e-mail: milovajul25@gmail.com

Ph.D. student of the Educational-Scientific Institute of Telecommunications of the State University of Telecommunications. Teaches at the Kiev College of Communications. Works on the development of information coding methods.

http://orcid.org/0000-0002-9977-2195

Ph.D. Yuri Melnyk
e-mail: milovajul25@gmail.com

Doctor of Technical Sciences. Director of the Educational-Scientific Institute of Telecommunications of the State University of Telecommunications. Scientific direction – telecommunications network management. Deals with issues of hierarchical management of telecommunications networks and issues of fuzzy logic in management problems. Development of the human-operator information model in ergatic systems.

http://orcid.org/0000-0002-5028-8749

otrzymano/received: 30.11.2020 *przyjęto do druku/accepted: 15.03.2021*