Journal of Mechatronics, Automation and Identification Technology
Vol. 4, No.1. pp. 28 -33

Permutational Cognitive Decoding of Nonbinary Redundant Codes and Their Statistical Characteristics

Anatoly GLADKIKH, Dmitry GANIN, Artyom MENOVSHCHIKOV, Sergey SHAKHTANOV, Maria SHIBAEVA

Knyagininsky University
Institute of Information Technologies and Communication Systems, Knyaginino, Russia
a_gladkikh@mail.ru, ngiei135@mail.ru, m.art.vl@mail.ru, r155p@bk.ru, shibaevamarya@yandex.ru

***Abstract* — The principle of matching high-speed optical communication systems at the data link layer using permutation decoding of redundant codes is considered. The expediency of such an approach is proved when applying the cognitive data processing procedure. Indicates the parameters of such systems. Considering the widespread use in data exchange systems and in automatic control systems, in computing systems and similar computing devices of non-binary noise-resistant Reed-Solomon (RS) codes, a subtle analysis of the complexity of decoding such codes using the permutation method is carried out. The estimation is made according to the number of code vectors of elementary arithmetic operations performed in the decoding procedure. Two approaches are compared: firstly, the classical principle of decoding RS codes, secondly, the permutation decoding method using a cognitive map. It is shown that the results obtained for rearrange decoding can be generalized for other code structures, including those implemented on the basis of binary codes. Various approaches to the formation of soft solutions for non-binary symbols of RS codes are presented, and a likelihood ratio method is proposed, which is based on comparing the obtained sequence of estimates of a non-binary code symbol with some predetermined reference set of estimates. The expediency of using the analyzed method in a number of important applied areas is proved.**

***Keywords* — Coherent network; non-binary redundant code; cognitive map; fast matrix transformations, soft decoding.**

I. INTRODUCTION

In modern data exchange systems, robust coding is a powerful means of increasing their spectral and energy efficiency [1]. There are several main areas of information protection from errors. These include systems with serial or parallel turbo coding, systems with multi-threshold decoding and low-density codes [2–6]. Despite the relatively high noise immunity of fiber optic communication lines, they require data protection systems based on sequential turbo codes. This approach of proactive error correction (FEC - from the English Forward Error Correction) is used in coherent networks at the present stage of their development. It is believed that at the output of the optical communication channel, the probability of a bit-level error is provided $10^{-3}...10^{-5}$. The use of the system of verification coding as an internal code provides an increase of this indicator when using the Viterbi algorithm by at least three orders of magnitude. An external decoder based on the RS code completes the confidence increase procedure by another three or four orders of magnitude, which is quite acceptable for the needs of not only the digital economy, but also for many application areas and technological processes that require high reliability and speed of data processing. However, in the described data processing scheme, a conflict situation is brewing. The essence of it can be described as follows. On the one hand, in optical communication lines, there is a constant increase in data transfer rates due to an increase in the spectral efficiency of such channels. In coherent networks, speeds equal to and lower than 100 Gbit / s are already considered to be fully developed and the issue of speeds of around 400 Gbit / s is becoming increasingly apparent. On the other hand, the data coding and decoding technique as a material basis continues to use computing devices on programmable logic integrated circuits (FPGAs), which for objective reasons are not high-speed. It is precisely on this contradiction that the problem of matching high-speed optical communication lines and insufficiently high-speed processors of receiving devices and computing elements arises.

II. A. ASSESSMENT OF THE COMPLEXITY OF THE IMPLEMENTATION OF THE TRADITIONAL DECODING SCHEME

In [7, 8], an assessment was made of the complexity of the implementation of a RS code decoder when using the classical approach to recovering the code vectors of such a code based on solving a system of linear equations. This method involves the implementation of a three-step decoding procedure, when using half of the equations of their allowable number in the system of equations is spent on identifying error locators, and the other half of the equations are used to correct errors identified in the first step. The admissible number of linear equations is determined by the Hamming metric [6, 9]. It should be noted that the identification of error locators is carried out using the trial and error method (Berlekampa-Messi algorithm (ABM)), which allows us to find the generator

polynomial of error locators. The irregularity of the ABM method requires ambiguous time intervals for its implementation [10].

Let *(n, k, d)* be a linear block code *V* with a generator matrix *G* and a check matrix *H*, where *n* is the length of the code combination, *k* is the number of information bits, *d* is the Hamming metric. If the dimension of the vector space *V* is equal to *k* with *q* possible values for each *k*, then the space *V* contains all q^k vectors $v \in V$, and the fundamental basis for decoding such codes is the ratio of the form $v \times H^T = 0$. If $v = (x_1, x_2, ..., x_n)$, and the element of the matrix *H* is denoted by h_{ij}, then for each row of the matrix the condition $\sum_j x_j h_{ij} = 0$. When transmitting the code word *v* through the channel with errors, the received word $v_e \neq v$, because $v_e = (x_1 \oplus e_1, \ x_2 \oplus e_2, ..., x_n \oplus e_n)$, where $e_i \neq 0$ the element of the field *GF (q)* represents the influence of the interfering factor. In the latter case $\sum_j x_j h_{ij} \neq 0$, and the result obtained *Sj* is a syndrome. Knowing the value of *Sj*, you can always specify the numbers j, on which $e_j \neq 0$. In matrix form, this condition is represented as:

$$\|S\|_{n-k} = \|h_{ij}\|_{n,n-k} \times \|e_i\|_n^T \quad (1)$$

and the error polynomial has the form:

$$e(X) = \sum_{n=0}^{n-1} e_n x^n \quad (2)$$

As shown in [11], the implementation of calculations using the specified scheme in the signal-code processor will require

$$O_{SA} = O_+ + O_\times = (n-k) + (n-k)k = \\ = (n-k)(2k+1) \quad (3)$$

operations of addition and multiplication. To search for the error locator polynomial, as a rule, use the autoregressive model of the form:

$$\sigma(x) = (1+\Lambda_1 x)(1+\Lambda_2 x)...(1+\Lambda_\gamma x) = \\ = 1 + \sigma_1 x + \sigma_2 x^2 + ... + \sigma_\gamma x^\gamma \quad (4)$$

where the roots for $\sigma(x)$ are values $1/\Lambda_1$, $1/\Lambda_2$, ..., $1/\Lambda_\gamma$.

The organization of the computational process in accordance with (4) is complicated by matrix transformations in the GF (q) field in accordance with the classic of solving linear equations [11]. It should be emphasized that in this case the most time-consuming steps are considered to be transformations for searching for the inverse matrix adopted for processing a system of linear equations. The complexity of any algorithm with matrix transformations is estimated at the level $O_2 = (t^3)$. The complexity of the implementation of ABM by a rough estimate [9] requires order $O_{ABM_1} = (t^2)$, insofar as:

$$O_{ABM_1} = 2t(3t+1) + 2t(6t+2) = \\ = 4{,}5(n-k)^2 + 3(n-k) \quad (5)$$

The hardware costs for implementing the Chen and Forni procedures are

$$O_{Ch\&F} = (n-k-1)^2 + (n-k)^2 \quad (6)$$

The presented algorithms are focused on error correction. Obviously, if the condition $\gamma \leq t$ is not met, there may be failures in decoding v_e. In soft decoders, erasing helps to shorten the search cycle of the generating polynomial, but the decoder always lays the possibility of correcting erasures and at least one error. The condition for the implementation of such an algorithm is of the form $d = 2t + s + 1$, where *s* is the number of erased positions in n. To reduce the complexity of the implementation of the decoder in [11] it is proposed to use soft data processing methods.

III. B. SOFT DECODING EFFICIENCY

In the soft decoder, each i-th bit of the received code vector is represented as a hard decision, accompanied by a soft decision of the symbol (MPC) in the form of some real value λ_i. Denoting hard decisions through a «minus» for an information zero and a «plus» for a unit, a tuple of data $...+\lambda_i - \lambda_{i+1} - \lambda_{i+2} + \lambda_{i+3} + \lambda_{i+4}...$ is obtained at the output of the receiver, which is subsequently processed in the decoder, based on the decoding principle as a whole [5].

In the course of channel processing of data protected by a redundant code in real time, soft methods of their processing are used, which are quite well developed for binary codes. However, the processing of non-binary symbols and the calculation of reliable values of MPC for them remain relevant tasks. A feature of many decoding methods is the need to transform the generating matrix G of the main redundant code into a permuted matrix of the equivalent G code. This is most clearly manifested in terms of permutation decoding (PD). From a mathematical point of view, this transformation is performed in accordance with the structure of the permutation matrix P. The matrix P is formed on the basis of sorting the MPC in descending order of their absolute values. A convenient form for the representation of MDCs is their integer expression, which is slightly less (only 0.2 dB) in terms of the code energy gain (EEC) but less than the actual EEC estimates, but contributes to the speed of the computation process. The analytical expression for calculating integer MDCs using binary modulation types is:

$$\lambda_i(z) = \left\lfloor \left| \frac{\lambda_{\max}}{\rho M_z} \times z \right| \right\rfloor \quad (7)$$

where $\lambda_{\max}$ is the maximum MPC value adopted for this system;

$M_z = \pm\sqrt{E_b}$ – the mathematical expectation of the values of the received signals, where E_b is the signal energy per bit;

ρ - erase interval (usually $0 \le \rho < 1$);

z – the value of the received signal, taking into account the influence of interfering factors [5]. It is convenient to evaluate the reliability of a nonbinary symbol in the $GF(2^n)$ field by the aggregate λ_i, where $i = \overline{1,n}$, in the form of a likelihood coefficient

$$K_{np} = \sum_{i=1}^{n} \lambda_i \Big/ \sum_{i=1}^{n} \lambda_{\max} = \sum_{i=1}^{n} \lambda_i \Big/ n\lambda_{\max} \qquad (8)$$

at the same time $0 \le K_{np} \le 1$.

The frequency F of the appearance of different estimates for the parameter K_{np} when using different degrees of expansion of the binary field n is presented in Figures 1 and 2. Expression (8) is convenient to use in systems with binary modulation types, which is unlikely in the conditions of using optical communication channels, in which the struggle to increase spectral efficiency is based on complex QPSK and KAM-m modulation types. In such channels, it is practically impossible to organize an erase communication channel, otherwise it is almost impossible to obtain the value of ρ. In this case, the MPC parameter $\lambda_i(z)$ is formed on the basis of concentric circles [10] or on the basis of the principle of equality of rectangular zones for the purpose of λ_i [1, 10]. In this case, expression (8) turns out to be fair with some correction coefficient equal to 2, for systems with QPSK and a coefficient equal to m for systems with KAM-m. The specified expression takes the form:

$$K^m{}_{np} = m\sum_{i=1}^{n} \lambda_i \Big/ n'\lambda_{\max}$$

Where $n' = n/2$ is for $m = 2$ for a system with QPSK and a m value for signals with m -modulated KAM. The frequencies of the likelihood coefficient for different signal-to-noise drops for binary modulation types are presented in Figures 1 and 2.

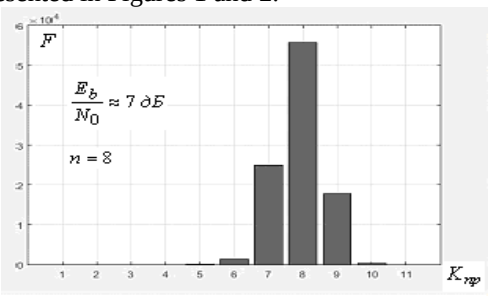

Fig. 1. Frequency of Likelihood Ratio high signal-to-noise ratio

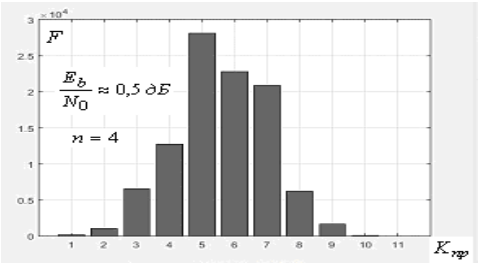

Fig. 2. Frequency of Likelihood Ratio low signal-to-noise ratio

Analysis of the simulation results of a channel with an independent error stream for various signal-to-noise ratios in E_b/N_0 format showed that the F frequency of the K_{np} parameter values for different estimates depends largely on the E_b/N_0 index and is not monotonous, which causes difficulties in determining the best estimates. This leads to the expediency of applying the cognitive procedure for determining the likelihood coefficient using the histogram parameters known to the decoder, which are characteristic of different values of the signal-to-noise ratio [12–14].

Most often, coherent communication systems use complex multi-level modulation formats (DP-QPSK, DP-mQAM), which are considered to be quite demanding on the amount of noise in an optical line. For this reason, the reception followed by the detection of the optical signal in the transponder contains several blocks that gradually restore the signal code states. Basic coherent receiver contains both optical and electrical parts. To restore the phase states of a signal, a digital processing unit is used, inside which the phase of carrier oscillation is restored, adaptive adjustment, compensation of chromatic and mode polarization dispersion are performed.

IV. C. The use of cognitive metaphors in the data decoding system

Particularly stringent requirements for the reliability and reliability of the data being processed are imposed on real-time control systems, which additionally require an increased readiness to perform control tasks. The PD method [12, 13] largely meets these requirements. A remarkable feature of the method is the possibility of preliminary calculation of all possible permutations of the symbols of code vectors and the organization of some similarity of the code book, in which specific permutations are associated with the corresponding equivalent codes. This opens up the possibility of organizing a cognitive procedure for teaching a decoder to identify such links and fill in the code book as these or other permutations appear. Actually, a book or a cognitive map contains samples of generating matrices of equivalent codes, which depend on the ranking order of the tuple $\ldots + \lambda_i - \lambda_{i+1} - \lambda_{i+2} + \lambda_{i+3} + \lambda_{i+4} \ldots$ for the implementation of PD. Consider the RS code with parameters (7,3,5) and number the columns of the generator matrix of this code from 1 to 7 and call them numerators. As a result of the ranking, two matrices must be formed.

The permutation matrix P, from which a transposed permutation matrix P^T is formed to perform the inverse actions. The formation of the matrix P must take exactly n operations. As a result, the vector of numerators of characters of the rearranged combination of the source code, which contains two parts of numerators, should be obtained. In the left part of the vector (at the positions of k information bits) are the numerators of the most reliable characters from the tuple $\lambda_1, \lambda_2, ..., \lambda_n$, the remaining $(n-k)$ positions are the least reliable characters that are more likely to contain erroneous solutions. Therefore, direct and inverse permutations require exactly $2n$ arithmetic operations, and taking into account the comparison operation of the vector obtained from the channel and the rearranged vector, we obtain $3n$ operations.

During subsequent data processing, the combination of reliable characters of a non-binary code combination, for example, of the form (2 4 5), can be repeated with a high probability. To save the decoder's computational resource in the future, it is advisable to keep in its memory the calculated expression of the generating matrix of the equivalent code and use it for possible permutations of the elements (2 4 5).

The system of reliable symbols makes it possible to lexicographically order the search for the desired matrix in the memory of the decoder. A matrix with a strictly increasing sequence of column numbers is called canonical, and the matrix itself is a reference one. This is convenient from the point of view of quickly finding the desired reference matrix in the list of such matrices [14–17]. Each reference sample is stored in a table, as shown in Figure 3, and there is no need to store a systematic part of the matrix [18, 19].

$$\begin{array}{ccccc} \alpha^6 & \alpha^2 & \alpha^6 & \alpha^2 & 2 \\ \alpha^3 & \alpha^3 & \alpha^1 & \alpha^1 & 4 \\ \alpha^5 & \alpha^4 & \alpha^4 & \alpha^5 & 5 \\ 1 & 3 & 6 & 7 & \end{array}$$

Fig. 3. The structure of the reference matrix in canonical form on a sequence of reliable characters

Following the principles of cognitive data processing, the decoder, having received, for example, a tuple of K_{np} values in the form (5 2 4) for the first k reliable symbols of the adopted combination and the remaining $(n-k)$ less reliable symbols in the form (3 7 1 6), forms the matrix G_{nep}, based on structures of the reference matrix, as shown below.

$$\begin{array}{ccccc} \alpha^6 & \alpha^2 & \alpha^6 & \alpha^2 & 2 \\ \alpha^3 & \alpha^3 & \alpha^1 & \alpha^1 & 4 \\ \alpha^5 & \alpha^4 & \alpha^4 & \alpha^5 & 5 \\ 1 & 3 & 6 & 7 & \end{array} \Rightarrow \begin{array}{ccccc} \alpha^5 & \alpha^4 & \alpha^4 & \alpha^5 & 5 \\ \alpha^6 & \alpha^2 & \alpha^6 & \alpha^2 & 2 \\ \alpha^3 & \alpha^3 & \alpha^1 & \alpha^1 & 4 \\ 1 & 3 & 6 & 7 & \end{array}$$

$$\Rightarrow \begin{array}{ccccc} \alpha^4 & \alpha^5 & \alpha^5 & \alpha^4 & 2 \\ \alpha^2 & \alpha^2 & \alpha^6 & \alpha^6 & 4 \\ \alpha^3 & \alpha^1 & \alpha^3 & \alpha^1 & 5 \\ 3 & 7 & 1 & 6 & \end{array}$$

It is easy to see that the decoder extracts the reference matrix in the canonical form from the cognitive map and transforms it into the required form in n steps. To implement the full decoding cycle, you need to multiply the transposed vector by the resulting generating matrix of the equivalent code. In fact, it is necessary to consider operations only for the check matrix, as shown in Figure 3. For this, the decoder needs only n operation cycles, which is incommensurably less than with algebraic decoding of such codes. Comparing the decoding process of the RS code with the classical method of using ABM and the classical method of PD, one can see the advantage of the proposed method of using a cognitive card in the structure of a non-binary code decoder. Indeed, to implement the proposed method when decoding a RS code with parameters (7,3,5), only 64 arithmetic operations will be required. For the implementation of the ABM method, 109 operations are required, which is 1.7 times worse, and when implementing a classical PD, 336 arithmetic operations are required, which is 5.25 times worse than the proposed method.

V. D. Evaluation of speed ratios in the control system

To assess the possibilities of implementing certain algorithms, it is necessary to take into account the rate at which combinations of the RS code enter the receiver input and the processing time of such a combination by the processor. In this case, of fundamental importance is the type of processor, its capabilities for parallel data processing in a system of several cores. For further research, RS codes were chosen in a nibble data exchange system (a binary Galois field of the fourth expansion degree) and in a binary field system of the eighth expansion degree. FPGAs of the Altera type (Virtex-5) and the Elbrus-8CB processor were chosen as processors. The evaluation results are shown in Tables 1 and 2, respectively.

Table 1. Altera FPGA features (Virtex-5) in the PD system

Channel speed (Gbit / s)	Working clock frequency (MHz)	RS code (15, 13, 3), arrival time of one combination	The processing time of one combination (ns)	RS code (255, 253, 3), arrival time of one combination	Time of processing (ns)

1	550	$6 \cdot 10^{-8}$	30 (has time)	$\approx 2 \cdot 10^{-6}$	255 (has time)
10	550	$6 \cdot 10^{-9}$	can not get in time	$\approx 2 \cdot 10^{-7}$	255 can not get in time
100	550	$6 \cdot 10^{-10}$	can not get in time	$\approx 2 \cdot 10^{-8}$	255 can not get in time
400	550	$1{,}5 \cdot 10^{-10}$	can not get in time	$\approx 5 \cdot 10^{-9}$	can not get in time

Table 2. Opportunities Elbrus-8 CB in the system permutation decoding

Channel speed (Gbit / s)	Performance (GFlops / s)	RS code (15, 13, 3), arrival time of one combination	The processing time of one combination (ns)	RS code (255, 253, 3), arrival time of one combination	Time of processing (ns)
1	576	$6 \cdot 10^{-8}$	30 (has time)	$\approx 2 \cdot 10^{-6}$	255 (has time)
10	576	$6 \cdot 10^{-9}$	30 (has time)	$\approx 2 \cdot 10^{-7}$	255 on the limit
100	576	$6 \cdot 10^{-10}$	30 (has time)	$\approx 2 \cdot 10^{-8}$	255 can not get in time
400	576	$1{,}5 \cdot 10^{-10}$	30 (has time)	$\approx 5 \cdot 10^{-9}$	can not get in time

The analysis of the tables shows that an increase in the channel speed in the system of coherent networks must be accompanied by an adequate selection of processors performing data decoding in the system of direct error correction. It is advisable to consider parallel data processing in multi-core processors in conjunction with a control system of a similar process.

VI. Conclusion

The data obtained are valid for the conditions when the MPC indices quite well accompany erroneous decisions. This suggests that research in this area should be continued with an emphasis on complex types of modulation. Reliable circuit solutions are needed to detect erroneous characters and accompany them with low MPC values.

Using the methods of PD codes RS can serve as an alternative to traditional methods of decoding such codes based on solving a system of linear equations. The exchange of the process of reducing the complexity of decoding code vectors for expanding the memory volume of a cognitive decoder card is practically proposed.

Additional research is needed in the field of organizing the memory of a cognitive decoder card on the principles of searching for the required information using the principle of its lexicographic placement in the decoder's memory. Experimental tests are required using simulation models of time delays when searching for reference matrices for long codes.

In general, the proposed PD method is a significant alternative to the classical methods for processing combinations of non-binary codes.

References

[1] Ganin D.V., Gladkikh A.A., Shamin A.A., Shagarova A.A. A comprehensive method for improving the energy and spectral efficiency of digital radio communications. Vestnik NGIEI. 2016. № 6 (61). Pp. 16-23.

[2] Tamrazyan G.M., Gladkikh A.A., Ganin D.V. hardware implementation of an optimal low-density code decoder // Automation of control processes. 2015. № 3 (41). Pp. 106-112.

[3] Smooth A.A. Application of the method of hypercoding in data transmission systems // Automation of management processes. - 2011. - № 2 (24). - pp. 77–81.

[4] Morelos-Zaragoza R. The art of noise-tolerant coding. Methods, algorithms, application. - M.: Technosphere, 2005. - 320s.

[5] Sklar Bernard. Digital communication. Theoretical foundations and practical application. - Ed. 2nd, rev. Per. from English - M.: Williams Publishing House, 2003. - 1104 p.

[6] Forney D. Cascade Codes. - M.: Mir, 1970. – 207

[7] Berlekamp P. R. Coding technique with error correction // TIIER. - 1980. - V. 68, №5, - P. 24–58.

[8] Dilip V.S., Naresh R.S. High-speed Architects for Reed-Solomon decoders // IEEE Trans. VLSI systems - 2001, - vol. 34. - pp. 388–396.

[9] Konopelko V. K., Lipnitsky V.A. The theory of norms of syndromes and permutation decoding of error-correcting codes. - M.: Editorial URSS, 2004. - 176 p.

[10] Smooth A.A. Fundamentals of the theory of soft decoding of redundant codes in the erasing

communication channel. - Ulyanovsk: UlSTU, 2010. - 253 p.
[11] Gladkikh A.A., Baskakova ES, Maslov AA, Tamrazyan G.M. Effective decoding of non-binary codes with provocation of the erased element // Automation of control processes. № 2 (32) 2013.– C. 87–93.
[12] Mac-Williams F. J. Permutation decoding of systematic codes // Cybernetic collection. New series, 1965, Vol. 1. - pp. 35–57.
[13] McWilliams, F. J., N.J. Sloan. The theory of error correction codes. - M.: Communication, 1979. - 354 p.
[14] Gladkikh, A.A., Al Tamimi, T.F. Kh. The concept of cognitive data processing in a permutation decoding system of a non-binary redundant code // Telecommunication. - 2018. - № 9. - p. 69–74.
[15] Smooth, A.A., Al Tamimi T.F.H. The system of fast matrix transformations in the procedure of forming equivalent redundant codes. Radio engineering. - 2017. - №6. - pp. 41–44.
[16] Smooth, A.A. Permutation decoding as a tool for increasing the energy efficiency of data exchange systems / A.A. Smooth // Telecommunications. - № 8. - 2017, P. 52–56.
[17] Shakhtanov, S.V. Permutation decoding of non-binary redundant codes / S.V. Shakhtanov // Vestnik NGIEI - 2017. - №8, p. 7-14.
[18] Gladkikh A.A., Pchelin N.A., Shakhtanov S.V. Minimizing the memory capacity of a cognitive decoder card in the equivalent code search system // Radio Engineering. - № 6. - 2018, pp. 38-41.
[19] Ganin D.V., Gladkikh A.A., Pchelin N.A., Sorokin I.A. Adaptive data processing in the system of soft decoding // Vestnik NGIEI. 2016. № 10 (65). Pp. 15–23.