Soft Decoding Based on Ordered Subsets of Verification Equations of Turbo-Productive Codes

Alexandr Kuznetsov [1[0000-0003-2331-6326]], Anastasiia Kiian [1[0000-0003-2110-010X]],

Kateryna Kuznetsova [1[0000-0002-5605-9293]], Tetiana Ivko [1[0000-0003-1772-0074]],

Oleksii Smirnov [2[0000-0001-9543-874X]], Dmytro Prokopovych-Tkachenko [3[0000-0002-6590-3898]]

[1]V. N. Karazin Kharkiv National University, Svobody sq., 4, Kharkiv, 61022, Ukraine
kuznetsov@karazin.ua, nastyak931@gmail.com,
kate.kuznetsova.2000@gmail.com, t.ivko@outlook.com
[2]Central Ukrainian National Technical University, avenue University, 8, Kropivnitskiy, 25006, Ukraine, dr.smirnovoa@gmail.com
[3]University of Customs and Finance, st. Volodymyr Vernadsky, 2/4, Dnipro, 49000, Ukraine, omega2@email.dp.ua

Abstract. Methods of soft decoding of cascade code constructions based on the schemes-products of linear block codes (Turbo Product Codes) are considered. An approach is being developed based on the iterative exchange of soft solutions between block codes constituting a cascade design. It is shown that a sequential execution of procedures for the formation of ordered subsets of test equations and the logarithms estimation of a likelihood ratio allows decoding of turbo-productive codes according to the criterion of minimizing the erroneous reception of code symbols.

Keywords. Cascade Structures, Turbo Product Codes, Soft Decoding, Verification Equations, Noise Immunity.

1 Introduction

A promising area in the development of noise-resistant coding theory is cascade code structures [1-7, 32-33], methods and algorithms for their decoding with an iterative exchange of soft solutions that allow to provide a required noise immunity of discrete message transmission [8-14].

It should be noted that the implementation complexity of decoding methods based on the use of decision functions increases with length of the code and the correcting capacity [14-17]. Decoding complexity can be reduced by using decision functions defined on a preformed subset of check equations [18-20]. At the same time, this decrease also leads to a decrease in the energy gain [19, 20].

Thus, an actual direction of research is a development (improvement) of decoding methods with soft solutions based on decisive functions, which, without significantly reducing the energy gain from coding, would significantly reduce the complexity of

practical implementation. A promising direction in this sense is the formation of ordered subsets of test equations and decoding methods based on them.

2 Theoretical substantiation of the proposed decoding method

The theoretical basis for soft decoding methods is a criterion for testing hypotheses, the mathematical justification for which is based on the total probability formula and the Bayes theorem [18-20].

Suppose that one can make mutually M exclusive assumptions (hypotheses) H_1, H_2, …, H_M about the setting of the experience, and an event A can appear only with one of these hypotheses.

Then the probability of an event is calculated by the formula of total probability:

$$P(A) = P(H_1)P(A|H_1) + P(H_2)P(A|H_2) + ... + P(H_M)P(A|H_M) = \\ = \sum_{i=1}^{M} P(H_i)P(A|H_i),$$

where $P(H_i)$ is the probability of the hypothesis H_i; $P(A|H_i)$ - conditional probability of an event A with this hypothesis.

If prior to the experiment, probabilities of the hypotheses were $P(H_i), i = 1,2,...,M$ and as a result of the experiment an event A occurred, then the a posteriori (experimental, subject to the occurrence of the event A) hypotheses probabilities are calculated using the Bayes formula:

$$P(H_i|A) = \frac{P(H_i)P(A|H_i)}{\sum_{i=1}^{M} P(H_i)P(A|H_i)},\ i = 1,2,...,M\ .$$

The Bayes formula makes it possible to calculate the conditional probabilities of occurrences of the following events, taking into account the posterior probabilities of hypotheses, $P(H_i|A)$, $i = 1,2,...,M$. So, if after the first experiment in which an event A occurred, the next experiment B is performed, in which an event may occur, the conditional probability $P(B|A)$ is calculated using the formula of total probability, into which not a priori probabilities $P(H_i)$ are substituted, but a posteriori, calculated after the occurrence of the event A, probabilities $P(H_i|A)$, i.e. we will receive:

$$P(B|A) = \sum_{i=1}^{M} P(H_i|A)P(B|H_iA),\ i = 1,2,...,M\ ,$$

where $H_i A$ is an event A under the hypothesis H_i, $P(B|H_i A)$ is the conditional probability of co-being B under the hypothesis H_i and event A.

Suppose now that the demodulator, based on the observation of the received signal and noise interference, estimates which of the possible signals $S_i \in \{S_1, S_2, ..., S_M\}$ (from an ensemble of signals with power M) was transmitted. You will make mutually exclusive assumptions M (hypotheses) that the corresponding signal S_i $i = 1, 2, ..., M$ has been transmitted,. We calculate the posterior probability of the i hypothesis, subject to admission: $S*$

$$P(S_i|S*) = \frac{P(S_i)P(S*|S_i)}{\sum_{i=1}^{M} P(S_i)P(S*|S_i)},\ i = 1, 2, ..., M, \quad (1)$$

where $P(S_i)$ - a priori probability of formation $S*$ of a signal S_i by the transmitter; $P(S*|S_i)$ - conditional probability of reception under the condition that the signal S_i is formed by the transmitter.

It is usually $S*$ represented as a continuous random variable underlying the hypothesis testing criteria. Consider the probability distribution function $P(S*)$:

$$P(S*) = \sum_{i=1}^{M} P(S_i)P(S*|S_i).$$

$P(S*)$ - is a probability distribution function of the mixture of signal and interference $S*$, which gives test statistics in the full signal space $\{S_1, S_2, ..., S_M\}$.

In equation (1), the value of the function $p(S*)$ is the scaling factor, since the value $P(S*)$ is obtained by averaging over the entire space of the signals.

Consider a case for two signals. Let binary logic elements 1 and 0 be represented by signals $S_1 = 1$ and $S_2 = -1$. A rigid decision rule, called as *a maximum likelihood rule*, determines a choice of one of the hypotheses (corresponding to the transmission of signals S_1 and S_2, accordingly) based on the comparison of probabilities values $P(S* = x|S_1)$ and $P(S* = x|S_2)$ the choice of the larger one. For each data bit transmitted, it is decided that the signal S_1 was transmitted if $S* = x$ falls on the right side of the decision line (indicated γ), or that the signal S_2 was otherwise transmitted.

A similar decision rule, known as the *maximum a posteriori probability* (MAP), can be represented as a minimum error probability rule, taking into account the prior probability of data. In general, the MAP rule is expressed as follows:

$$S = \begin{cases} S_1, if\ P\left(S^* = x \middle| S_1\right) > P\left(S^* = x \middle| S_2\right) \\ S_2, if\ P\left(S^* = x \middle| S_1\right) < P\left(S^* = x \middle| S_2\right) \end{cases}, \quad (2)$$

where S - value of the signal corresponding to the decision.

Thus, expression (2) establishes the rule for choosing one of the hypotheses corresponding to the signals S_1 and S_2. Using expression (1), we obtain the equivalent expression:

$$S = \begin{cases} S_1, if\ P\left(S_1\right)P\left(S^* \middle| S_1\right) > P\left(S_2\right)P\left(S^* \middle| S_2\right) \\ S_2, if\ P\left(S_1\right)P\left(S^* \middle| S_1\right) < P\left(S_2\right)P\left(S^* \middle| S_2\right) \end{cases},$$

where probability

$$P\left(S^*\right) = \sum_{i=1}^{M} P\left(S_i\right)P\left(S^* \middle| S_i\right)$$

in both parts of inequality reduced.

Using (2) we introduce a function as a ratio of likelihood functions $P\left(S^* = x \middle| S_1\right)$ and $P\left(S^* = x \middle| S_2\right)$:

$$F = \frac{P\left(S_1\right)P\left(S^* \middle| S_1\right)}{P\left(S_2\right)P\left(S^* \middle| S_2\right)}, \quad (3)$$

then the rule for choosing one of the hypotheses is written as

$$S = \begin{cases} S_1, если\ F > 1 \\ S_2, если\ F < 1 \end{cases}. \quad (4)$$

Let us translate the expression (3), we get:

$$\ln F = \ln\left(\frac{P\left(S_1\right)}{P\left(S_2\right)}\right) + \ln\left(\frac{P\left(S^* \middle| S_1\right)}{P\left(S^* \middle| S_2\right)}\right).$$

Thus, a logarithm of the ratio of likelihood functions $\ln F$ is a real representation of the soft solution at the decoder input, with first term on right side of the equality being the logarithm of the relations of a priori probabilities $P\left(S_1\right)$ and $P\left(S_2\right)$

$$L_S\left(S_1, S_2\right) = \ln\left(\frac{P\left(S_1\right)}{P\left(S_2\right)}\right),$$

and the second term is the essence of the logarithm of the posterior probability ratio $P\left(S^*\middle|S_1\right)$ and $P\left(S^*\middle|S_2\right)$:

$$L_{DS}\left(S_1,S_2\right)=\ln\left(\frac{P\left(S^*\middle|S_1\right)}{P\left(S^*\middle|S_2\right)}\right)$$

as a result of channel measurements in the receiver.

So, the logarithm of the likelihood function $L_{FS}=\ln F$ is rewritten as

$$L_{FS}\left(S_1,S_2\right)=L_S\left(S_1,S_2\right)+L_{DS}\left(S_1,S_2\right). \tag{5}$$

It should be noted that for AWGN channels, the logarithm of the likelihood function as the result of channel measurements of the received mixture of signal and noise in the receiver will be as follows:

$$L_{DS}\left(S_1,S_2\right)=\ln\left[\frac{P\left(S^*\middle|S_1\right)}{P\left(S^*\middle|S_2\right)}\right]=\ln\left[\frac{\frac{1}{\sigma\sqrt{2\pi}}\exp\left[-\frac{1}{2}\left(\frac{S^*-1}{\sigma}\right)^2\right]}{\frac{1}{\sigma\sqrt{2\pi}}\exp\left[-\frac{1}{2}\left(\frac{S^*+1}{\sigma}\right)^2\right]}\right]=$$

$$=-\frac{1}{2}\left(\frac{S^*-1}{\sigma}\right)^2+\frac{1}{2}\left(\frac{S^*+1}{\sigma}\right)^2=\frac{2}{\sigma^2}S^*.$$

Considering the ratio

$$\frac{1}{\sigma^2}=\frac{2E_b}{N_0},$$

where $\frac{E_b}{N_0}$ - is the ratio of energy of a binary signal E_b to the spectral power density of the noise N_0, we obtain:

$$L_{DS}\left(S_1,S_2\right)=4\cdot\frac{E_b}{N_0}S^*,$$

those value of a logarithm of posterior probability ratio $P\left(S^*\middle|S_1\right)$ and $P\left(S^*\middle|S_2\right)$, as a result of channel measurements at the receiver, depends exclusively on the signal-to-noise ratio and the value of the received signal and noise mixture S^*.

In [20], it was shown that for systematic codes, the soft decision at the decoder output (on a logarithmic scale) about received symbol is written in the form of expression

$$L_{FDK}\left(S_1,S_2,C_1,C_2\right)=L_{FS}\left(S_1,S_2\right)+L_{DK}\left(c_1,c_2\right), \tag{6}$$

where $L_{DK}\left(C_1,C_2\right)$ is the logarithm of the likelihood function relation on the received symbol, obtained as a result of decoding.

Substituting (5) into (6) we get:

$$L_{FDK}\left(S_1,S_2,C_1,C_2\right)=L_S\left(S_1,S_2\right)+L_{DS}\left(S_1,S_2\right)+L_{DK}\left(c_1,c_2\right), \tag{7}$$

those the soft decision at the decoder output depends on three values: $L_S\left(S_1,S_2\right)$ - a logarithm of the ratio of the prior probabilities of the signals S_1 and S_2 ; -a logarithm of the ratio of the posterior probabilities of the signals S_1 and S_2 (the result of channel measurements) and $L_{DK}\left(C_1,C_2\right)$ - a logarithm of ratio of the likelihood functions of binary code symbols C_1 and C_2 as the result of decoding.

To get $L_{FDK}\left(S_1,S_2,C_1,C_2\right)$, you need to sum up the individual contributions, since all three components are statistically independent [20]. Soft decoder output $L_{FDK}\left(S_1,S_2,C_1,C_2\right)$ is a real number, providing both the hard decision itself and its reliability. The sign $L_{FDK}\left(S_1,S_2,C_1,C_2\right)$ sets a hard decision, i.e.:

$$c_i=\begin{cases}C_1=1, if\ L_{FDK}\left(S_1,S_2,c_1,c_2\right)>0\\ C_2=0, if\ L_{FDK}\left(S_1,S_2,c_1,c_2\right)<0\end{cases}, \tag{8}$$

where c_i is the value of the i -th bit corresponding to the taken decision.

An eigenvalue $L_{FDK}\left(S_1,S_2,C_1,C_2\right)$ determines the reliability of the decision.

As a rule, ta value $L_{DK}\left(C_1,C_2\right)$ has the same sign as $L_{FDK}\left(S_1,S_2,C_1,C_2\right)$, thus increasing the reliability of the decision.

For statistically independent values x and y , the sum of two logarithmic likelihood ratios $L(x)$ and $L(y)$ is determined by the following expression:

$$\begin{aligned}&L\left(x\right)\left[+\right]L\left(y\right)=L\left(x\oplus y\right)=\ln\left[\frac{e^{L(x)}+e^{L(y)}}{1+e^{L(x)}e^{L(y)}}\right]\approx\\ &\approx\left(-1\right)\times\operatorname{sgn}\left[L\left(x\right)\right]\times\operatorname{sgn}\left[L\left(y\right)\right]\times\min\left(\left|L\left(x\right)\right|,\left|L\left(y\right)\right|\right),\end{aligned} \tag{9}$$

where function $\operatorname{sgn}\left[z\right]$ returns a sign of its argument z , and the sign "$\oplus$" is used to denote the sum of data modulo 2 represented by binary digits. The sign $\left[+\right]$ is used to denote the sum of the logarithms of the likelihood functions, which is defined as the logarithm of the likelihood function of the sum modulo 2 of the corresponding arguments.

An implementation of the turbo decoding procedure involves the use of decoding methods with a soft solution at the input and a soft solution at the output. During the first iteration on such a decoder, the data is considered equally probable, which gives the initial a priori value $L_S(S_1,S_2)=0$ in equation (7). Channel measurement gives the value $L_{DS}(S_1,S_2)$ that is obtained by taking the logarithm of the ratio of the values $P(S^*=x|S_1)$ and $P(S^*=x|S_2)$ for certain values and is the second member of equation (7). The decoder output $L_{DK}(C_1,C_2)$ is information derived from the decoding process. For iterative decoding, the external likelihood is fed back to the input (of another composite decoder) to update the prior probability of the next iteration information, i.e. updates a priori probability:

$$L_S(S_1,S_2)=L_{DK}(C_1,C_2).$$

Thus, the decision in the final decoding of each character of the code sequence and information about its reliability depends on the value $L_{FDK}(S_1,S_2,C_1,C_2)$. Based on equation (7), we write the algorithm that gives an estimate of the soft output of the decoder $L_{DK}(C_1,C_2)$ and the resulting estimate $L_{FDK}(S_1,S_2,C_1,C_2)$.

1. Install $L_S(S_1,S_2)=0$.

2. We decode with the soft solution the first composite code, i.e. find a soft solution $L_{FDK}(S_1,S_2,C_1,C_2)$.

3. Based on equation (7) we calculate

$L_{DK}(C_1,C_2)=L_{FDK}(S_1,S_2,C_1,C_2)-L_S(S_1,S_2)-L_{DS}(S_1,S_2)$

4. For the following composite code install $L_S(S_1,S_2)=L_{DK}(C_1,C_2)$.

5. With a soft solution, we decode the following composite code, i.e. find a soft solution $L_{FDK}(S_1,S_2,C_1,C_2)$.

6. For all composite codes, repeat steps 3-5.

7. The result of turbo decoding is a hard decision about a code symbol c by expression (8) based on the soft decision obtained in the last step $L_{FDK}(S_1,S_2,C_1,C_2)$.

Thus, as the analysis of above algorithm shows, the main task in implementation of turbo decoding is a development of efficient soft decoding procedures for composite codes, i.e. development of soft decision $L_{DK}(C_1,C_2)$ calculation procedures for an iterative exchange procedure in the process of turbo decoding.

We study the procedures for finding the soft solution $L_{DK}(C_1,C_2)$ at the decoder output, analyze the possible ways to calculate the last term on the right side of equality (7) - the logarithm of the ratio of the likelihood functions of binary code symbols C_1 and C_2 as a result of decoding.

Consider a linear (n,k,d) block code over a finite field $GF(2)$. A linear code as a subspace $GF^k(2)\subseteq GF^n(2)$ is defined by the generator matrix G, the lines of which

form the basis of the linear space $GF^k(2)$. By definition, for each linear code there is an orthogonal completion - a subspace $GF^{n-k}(2) \subseteq GF^n(2)$, all elements of which are orthogonal to the elements of $GF^k(2)$. The basis of the linear space $GF^{n-k}(2)$ is given by the check matrix H, and the mutual orthogonality condition implies equality $GH^T = 0$, where by "0" is meant the $k \times r$ matrix of zero elements $GF(2)$.

We write the last equality in the form $cH^T = 0$, where $c = (c_0, c_1, ..., c_{n-1})$ is the arbitrary code word of the linear block (n, k, d) code under consideration, i.e. $c \in GF^k(2)$ $c_i \in [0,1]$.

Taking into account the fact that all elements $GF^{n-k}(2)$ can be expressed in terms of a linear combination of rows of a check matrix H, we have $ch_i^T = 0$:, where $h_i = (h_{i_0}, h_{i_1}, ..., h_{i_{n-1}})$ is an arbitrary vector obtained by a linear combination of rows of a matrix H, $i = 0,1,..., 2^{n-k} - 1$.

In other words, the last equality holds for all 2^{n-k} vectors from $GF^{n-k}(q)$ and we have a system of test equations:

$$\begin{cases} c_0 h_{0_0} + c_1 h_{0_1} + ... + c_0 h_{0_{n-1}} = 0; \\ c_0 h_{1_0} + c_1 h_{1_1} + ... + c_0 h_{1_{n-1}} = 0; \\ ... \\ c_0 h_{(2^{n-k}-1)_0} + c_1 h_{(2^{n-k}-1)_1} + ... + c_0 h_{(2^{n-k}-1)_{n-1}} = 0. \end{cases} \quad (10)$$

Suppose now that the code word $c = (c_0, c_1, ..., c_{n-1})$ is taken by the criterion of the maximum a posteriori probability, i.e. the values of the log-rhymes of the posterior probabilities $P(S*|S_1)$ and $P(S*|S_2)$:

$$L_{DS}(c_j) = L_{DS}(S_1, S_2) = \ln\left(\frac{P(S*|S_1)}{P(S*|S_2)}\right)$$

about each code symbol c_j, $j = 0,1,..., n-1$ as a result of channel measurements of the corresponding signals in the receiver.

The logarithms of the relations of a priori probabilities $P(S_1)$ and $P(S_2)$, corresponding to each of the code symbols c_j, $j = 0,1,..., n-1$ we denote

$$L_S(c_j) = L_S(S_1, S_2) = \ln\left(\frac{P(S_1)}{P(S_2)}\right).$$

Then, taking into account (7) and rule (9) for the i -th checking equation, we have

$$L_{DK_i}\left(c_j\right)=$$

$$=\begin{cases}\left(L_S\left(c_0\right)+L_{DS}\left(c_0\right)\right)h_{i_0}\left[+\right]\left(L_S\left(c_1\right)+L_{DS}\left(c_1\right)\right)h_{i_1}\left[+\right]...\left[+\right] \\ \left[+\right]\left(L_S\left(c_{j-1}\right)+L_{DS}\left(c_{j-1}\right)\right)h_{i_{j-1}}\left[+\right]\left(L_S\left(c_{j+1}\right)+L_{DS}\left(c_{j+1}\right)\right)h_{i_{j+1}}\left[+\right]...\left[+\right] \\ \left[+\right]\left(L_S\left(c_{n-1}\right)+L_{DS}\left(c_{n-1}\right)\right)h_{i_{n-1}}=\sum\limits_{\substack{l=0,\\ l\neq j}}^{n-1}\left(L_S\left(c_l\right)+L_{DS}\left(c_l\right)\right)h_{i_l} & \text{if } h_{i_j}=1; \\ \\ \left(L_S\left(c_0\right)+L_{DS}\left(c_0\right)\right)h_{i_0}\left[+\right]\left(L_S\left(c_1\right)+L_{DS}\left(c_1\right)\right)h_{i_1}\left[+\right]...\left[+\right] \\ \left[+\right]\left(L_S\left(c_{n-1}\right)+L_{DS}\left(c_{n-1}\right)\right)h_{i_{n-1}}=\sum\limits_{l=0}^{n-1}\left(L_S\left(c_l\right)+L_{DS}\left(c_l\right)\right)h_{i_l} & \text{if } h_{i_j}=0,\end{cases} \tag{11}$$

where the summation of "$\left[+\right]$" and "$\sum$ " is carried out according to the rule of adding likelihood logarithms, i.e. by expression (9).

If we assume that all the estimates $L_{DK_i}\left(c_j\right)$ $j=0,1,...,n-1$ are statistically independent (for example, if the test equations are mutually orthogonal), then the resulting estimate $L_{DK}\left(c_j\right)$ will be written as:

$$L_{DK}\left(c_j\right)=\sum_{i=0}^{2^{n-k}-1}L_{DK_i}\left(c_j\right), \tag{12}$$

where the summation is performed according to the usual arithmetic rule of addition of real numbers.

The soft output of the decoder $L_{FDK}\left(c_j\right)=L_{FDK}\left(S_1,S_2,C_1,C_2\right)$ is a real number, and is determined by the expression (7):

$$\begin{aligned}L_{FDK}\left(c_j\right)&=L_S\left(c_j\right)+L_{DS}\left(c_j\right)+L_{DK}\left(c_j\right)= \\ &=L_S\left(c_j\right)+L_{DS}\left(c_j\right)+\sum_{i=0}^{2^{n-k}-1}L_{DK_i}\left(c_j\right).\end{aligned} \tag{13}$$

The sign $L_{FDK}\left(c_j\right)$ sets a tough decision according to rule (8):

$$c_j=\begin{cases}C_1=1, \text{if } L_{FDK}\left(c_j\right)>0; \\ C_2=0, \text{if } L_{FDK}\left(c_j\right)<0.\end{cases}$$

Expressions (11), (12) and (13) define the decisive function based on using logarithms of the ratio of likelihood functions of received signals (calculated using a priori and a posteriori probabilities), as well as the logarithm of the ratio of likelihood functions of binary code characters as a result of decoding. The corresponding sum (12) defines the decision function based only on the use of the decoding result.

Let us analyze the expression (12). Expanding the summation sign according to rule (11), we obtain that expression (12) contains 2^{n-k} terms, each of which is the result of summation of the n logarithms of the likelihood of code symbols. In turn, the likelihood logarithms of code symbols are the sum of the likelihood logarithms of the received signals (calculated using a priori and a posteriori probabilities). It is obvious that with an increase in the code parameters (n, k, d), the number of terms increases rapidly and already with the application $n-k>32$ of the considered approach it becomes computationally inexpedient. A promising direction in this sense is the development of a rule for the formation of ordered subsets of check equations and a theoretical substantiation on their basis of decisive functions for decoding methods with soft solutions.

3 Conclusions

As a result of the conducted research, the method of soft decoding of cascade code constructions with iterative exchange of soft solutions was improved which differs from the known methods by the accelerated procedure of selecting test equations with the most reliable symbols, which allows realizing decoding of code words by the criterion of minimizing the erroneous reception of code symbols and speeding up the process of turbo decoding of concatenated codes.

The obtained results may be useful in constructing information security code schemes [21-26], for example, as a real alternative to traditional cryptography for post-quantum applications [27]. In addition, research results may be useful for optimizing computing in modern telecommunications networks [28-31, 34-35].

References

1. Gomtsyan, H.A.: Computer simulation of cascade codes for CDMA systems. In: Proceedings of the Second International Symposium of Trans Black Sea Region on Applied Electromagnetism (Cat. No.00TH8519), Xanthi, Greece, 2000, p. 105. (2000) doi:10.1109/AEM.2000.943262
2. Perez, L.C., Costello, D.J.: Cascaded convolutional codes. In: Proceedings of 1995 IEEE International Symposium on Information Theory, Whistler, BC, Canada, 1995, p. 160. (1995) doi:10.1109/ISIT.1995.531509
3. Permuter, H.H., Weissman, T.: Cascade source coding with side information at first two nodes. In: IEEE Information Theory Workshop on Information Theory (ITW 2010, Cairo), Cairo, 2010, pp. 1–5. (2010) doi:10.1109/ITWKSPS.2010.5503190
4. Zhang, S., Song, R., Yang, F.: Joint design of QC-LDPC codes for cascade-based multi-source coded cooperation. In: International Conference on Wireless Communications &

Signal Processing (WCSP), Nanjing, 2015, pp. 1–4. (2015) doi:10.1109/WCSP.2015.7340967
5. Kuznetsov, A., Serhiienko, R., Prokopovych-Tkachenko, D.: Construction of cascade codes in the frequency domain. 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T 2017), Kharkov, 2017, pp. 131–136. (2017) doi:10.1109/INFOCOMMST.2017.8246366
6. Chen, H., Ling, S., Xing, C.: Quantum codes from concatenated algebraic-geometric codes. IEEE Transactions on Information Theory, 2005, vol. 51(8), pp. 2915–2920, (2005) doi:10.1109/TIT.2005.851760
7. Changuel, S., Le Bidan, R., Pyndiah, R.: Iterative Decoding of Block Turbo Codes over the Binary Erasure Channel. In: IEEE International Conference on Signal Processing and Communications, Dubai, 2007, pp. 1539–1542. (2007) doi:10.1109/ICSPC.2007.4728625
8. Landolsi, M.A.: A Comparative Performance and Complexity Study of Short-Length LDPC and Turbo Product Codes. In: 2nd International Conference on Information & Communication Technologies, Damascus, 2006, pp. 2359–2364. (2006) doi:10.1109/ICTTA.2006.1684775
9. Nakajima, S., Sato, E.: Trellis-coded 8-PSK scheme combined with turbo and single-parity-check product codes. In: Proceedings IEEE 56th Vehicular Technology Conference, Vancouver, BC, Canada, 2002, vol. 3, pp. 1782–1786. (2002) doi:10.1109/VETECF.2002.1040523
10. Stasev, Yu.V., Kuznetsov, A.A., Nosik, A.M.: Formation of pseudorandom sequences with improved autocorrelation properties. Cybernetics and Systems Analysis, 2007, vol. 43(1), pp. 1–11. (2007) doi:10.1007/s10559-007-0021-2
11. Berrou, C., Glavieux, A., Thitimajshima, P.: Near Shannon Limit Error- Correcting Coding and Decoding: Turbo Codes. In: Proceedings of ICC '93 - IEEE International Conference on Communications, Geneva, Switzerland, 1993, vol. 2, pp. 1064–1070. (1993) doi:10.1109/ICC.1993.397441
12. Stasev, Yu.V., Kuznetsov, A.A.: Asymmetric code-theoretical schemes constructed with the use of algebraic geometric codes. Kibernetika i Sistemnyi Analiz, 2005, vol. 3, pp. 47–57. (2005)
13. Wang, F.G., Tang, Y., Yang, F.: The iterative decoding algorithm research of Turbo Product Codes. In: The 2010 International Conference on Apperceiving Computing and Intelligence Analysis Proceeding, Chengdu, 2010, pp. 97–100. (2010) doi:10.1109/ICACIA.2010.5709859
14. MacKay, D.J.C., Neal, R.M.: Near Shannon limit performance of low density parity check codes. IEEE Electronics Letters, 1996, vol. 33(6), pp. 457–458. (1996) doi:10.1049/el:19970362
15. Turbo Product Code Encoder / Decoder. www.aha.com
16. IEEE 802.16 Broadband Wireless Access Working Group. Turbo Code Comparison (TCC v TPC). http://ieee802.org/16
17. Turbo Product Code FEC. Comtech EF Data Corp. www.comtechefdata.com
18. MacWilliams, F., Sloane, N.: The Theory of Error-Correcting Codes. Elsevier (1977)
19. Proakis, J.: Digital communications. McGraw Hill (2001)
20. Sklar, B.: Digital Communications: Fundamentals and Applications. Prentice Hall Communications Engineering and Emerging Techno. Pearson Education (2016)
21. QC-MDPC KEM: A Key Encapsulation Mechanism Based on the QC-MDPC McEliece Encryption Scheme", NIST Submission, 2017. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions

22. Wang, Y.: RLCEKey Encapsulation Mechanism (RLCE-KEM) Specifcation. NIST Submission. (2017) http://quantumca.org
23. Melchor, C.A., Aragon, N., Bettaieb, S., Bidoux, L., Blazy, O., Deneuville, J.-C., Gaborit, P., Zemor, G.: Rank Quasi-Cyclic (RQC). NIST Submission. (2017) http://pqc-rqc.org
24. Post-Quantum Cryptography, Round 1 Submissions, 2017. https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions
25. Kuznetsov, A., Kiian, A., Lutsenko, M., Chepurko, I., Kavun, S.: Code-based cryptosystems from NIST PQC. In: 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018, pp. 282–287. (2018) doi:10.1109/DESSERT.2018.8409145
26. Kuznetsov, A., Pushkar'ov, A., Kiyan, A., Kuznetsova, T.: Code-based electronic digital signature. In: 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018, pp. 331–336. (2018) doi:10.1109/DESSERT.2018.8409154
27. Bernstein, D., Buchmann, J., Dahmen, E.: Post-Quantum Cryptography. Springer-Verlag, Berlin-Heidleberg (2009)
28. Rassomakhin, S.G.: Mathematical and physical nature of the channel capacity. Telecommunications and Radio Engineering, 2017, vol. 76(16), pp. 1423–1451. (2017) doi:10.1615/TelecomRadEng.v76.i16.40
29. Krasnobayev, V.A., Koshman, S.A.: A Method for Operational Diagnosis of Data Represented in a Residue Number System. Cybernetics and Systems Analysis, 2018, vol. 54(2), pp. 336–344. (2018) doi:10.1007/s10559-018-0035-y
30. Gorbenko, I.D., Zamula, A.A., Semenko, A.E., Morozov, V.L.: Method for synthesis of performed signals systems based on cryptographic discrete sequences of symbols. Telecommunications and Radio Engineering, 2017, vol. 76(17), pp. 1523–1533. (2017) doi:10.1615/TelecomRadEng.v76.i17.40
31. Tenth UK Teletraffic Symposium. Performance Engineering in Telecommunications Network. In: Tenth UK Teletraffic Symposium, 10th. Performance Engineering in Telecommunications Network, Martlesham Heath, UK
32. Kavun, S.: Conceptual fundamentals of a theory of mathematical interpretation. Int. J. Computing Science and Mathematics, 2015, vol. 6(2), pp. 107–121. (2015) doi:10.1504/IJCSM.2015.069459
33. Kuznetsov, A., Kavun, S., Panchenko, V., Prokopovych-Tkachenko, D., Kurinniy, F., Shoiko, V.: Periodic Properties of Cryptographically Strong Pseudorandom Sequences. In: 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, 2018, pp. 129–134. (2018) doi:10.1109/INFOCOMMST.2018.8632021
34. Zamula, A., Kavun, S.: Complex systems modeling with intelligent control elements. Int. J. Model. Simul. Sci. Comput., 2017, vol. 08(01). (2017) doi:10.1142/S179396231750009X
35. Kavun, S., Zamula, A., Mikheev, I.: Calculation of expense for local computer networks. In: Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), 2017 4th International, Kharkiv, Ukraine, 2017, pp. 146–151. (2017) doi:10.1109/INFOCOMMST.2017.8246369