CHARACTERISTICS OF ERROR-CORRECTING SHORTENED BLOCK TURBO-CODES OF ITERATIVE RECEPTION OF INFORMATION

Lev E. Nazarov
Kotelnikov Institute of Radioengineering and Electronics of RAS, Fryazino Branch, http://fire.relarn.ru
1, Vvedensky sq., Fryazino 141190, Moscow region, Russian Federation

Pavel V. Shishkin
Moscow Office of ISS-Reshetnev Company, http://www.iss-reshetnev.ru
16/37, Mytishchinskaya str., Moscow 129626, Russian Federation
nazarov@sunclass.ire.rssi.ru, shishkin@mail.ru

Abstract. The focus of the paper is directed towards the investigation of the characteristics of error-correcting block turbo-codes which enable communication at relatively low received signal/noise and provide very high power efficiency. Specific feature of investigated turbo-codes is construction with shortened information block for generated error-correcting block-code. According to this the considered shortened turbo-codes have symbol-by-symbol decoding algorithms developed for total class of turbo-codes, namely, decoding algorithms based on modified Chase algorithm. These decoding algorithms with low complexity implementation are iterative and for implementation the channel parameter signal/noise is not required. The resulted characteristics of shortened turbo-codes constructed with usage generated turbo-code (duration of code words, information volume, code rate, error performances) are presented in this paper. The computer simulations for iterative decoding algorithms for the number of turbo-codes with different code rate and information volumes are performed. The results of computer simulations have shown that the investigated shortened turbo-codes are more effective than known convolutional codes with equivalent parameters - the degradation of signal/noise is about 1.85 dB for bit-error 0.00001 for convolutional code with code rate 1/2 concerning the shortened turbo-code based on generated turbo-code with parameters (16384,12769,36).

Keywords: error-correcting codes, block product codes, iterative decoding, error performances

UDC 621.391.01

Bibliography - 12 references
RENSIT, 2018, 10(2):323-328
DOI: 10.17725/rensit.2018.10.323

Content
1. INTRODUCTION (323)

2. FORMULATION OF THE PROBLEM (324)

3. TRUNCATED BLOCK TURBO CODES (325)

4. SIMULATION RESULTS (326)

5. CONCLUSION (327)

References (328)

1. INTRODUCTION

Interference-free codes are used in digital communication systems in order to increase the reliability of information transmission through interference channels [1]. In the literature, the most known are noise-block block codes with a cyclic structure and convolutional codes, for which algorithms for reception using soft solutions from the output of a demodulator of signals have been developed [1, 2].

Codes constructions under the general name block turbo codes constitute an alternative to these codes with respect to probabilistic characteristics and complexity of generation and reception algorithms [3, 4, 5]. These codes are basic for a number of standards, for example, for IESS-15, IESS-315, IESS-316e (Intelsat satellite communication system), for IEEE 802.16 broadband access standard [6].

Block turbo codes are formed on the basis of sequential combination of constituent block codes [3], for these codes algorithms of iterative reception are developed [4]. With the increase in the volume of information blocks of the data of turbo codes and the use of iterative reception algorithms, the
limiting probabilistic characteristics of the Shannon transmission capacity of transmission channels with additive white Gaussian noise (ABGSH) are reached [3].

The class of known constituent codes is limited - block Hamming codes, codes with generalized parity check, low density codes [1, 3, 7, 8] are used. The problem of expanding a number of block turbo codes (BTK) used in the development of digital communication systems for various purposes, for example, with adaptive noise-tolerant transmission modes depending on the efficiency of channel interference, is topical.

The article describes the method of forming an expanded set of BTKs by shortening the information block of the generating turbo code, describes the characteristics of truncated turbo codes, including probabilistic characteristics using the algorithm of iterative reception.

2. PROBLEM STATEMENT
Let \( C_1(n_1, k_1, d_1), C_2(n_1, k_1, d_2) \) be binary block systematic codes whose code words are respectively the rows and columns of the two-dimensional matrix \( B = (b_{ij}; 0 \leq i < n_1; 0 \leq j < n_2) \) of size \( n_1 \times n_2 \) (Fig. 1). This matrix is equivalent to the generating matrix for BTK with the parameters \( n = n_1 \cdot n_2 \), \( k = k_1 \cdot k_2 \), \( R = k / n \), \( d = d_1d_2 \) and specifies the structure of code words [3]. Here \( n \), \( k \), \( R \), \( d \) are the length of code words, the dimension, the code rate and the minimum Hamming distance of the code.

The algorithms for the optimal reception of signals corresponding to codes are based on the calculation of the set of \( 2k \) correlations [9]. For \( k \gg 1 \), the implementation of these algorithms presents an intractable problem.

![Fig. 1. The scheme of the codeword of the block turbo code and the truncated turbo code on the basis of the components of the block codes \( C_1(n_1, k_1, d_1), C_2(n_1, k_1, d_2) \).](image)

Let’s describe the algorithm of the iterative reception of the BTK, the essence of which is the decomposition of the optimal reception rule into a set of processing steps corresponding to the constituent block codes, which leads to a significant simplification of the resulting receiving procedure in relation to the optimal reception with a small energy loss [3, 4, 8].

Let \( A = (a_{ij}; 0 \leq i < k_1; 0 \leq j < k_2) \) be a sequence of information symbols forming a submatrix in the composition of the two-dimensional matrix \( B = (b_{ij}; 0 \leq i < n_1; 0 \leq j < n_2) \) of the turbo code; \( Y = (y_{ij}; 0 \leq i < n_1; 0 \leq j < n_2) \) - realization from the output of the signal demodulator; - likelihood ratio of conditional probability densities \( p(y_{ij} | b_{ij} = 0) \) of samples \( y_{ij} \); Is the ratio of a priori symbolic probabilities.

In the first stage of the \( m \)-th iteration, the increments of the a posteriori probabilities for the code symbols \( b_{ij} \), \( j = 0, 1, ..., n_1 - 1 \) for the \( i \)-th codeword of the constituent code \( C_1 \)

\[
L^{(1,m)}(b_{ij}) = L^{(1,m)}(b_{ij} | y^{(1)}_{i}, L^{(2,m)}(b_{i,j})) - (L(y_{ij} | b_{ij}) + L^{(2,m)}(b_{ij})).
\]

Here ; - an implementation in the composition \( Y \), corresponding to the codeword. For the first iteration \( (m = 1) \), the condition \( L^{(2,1)}(b_{i,j}) = L^{(1,1)}(b_{i,j}) \) is true.

In the second stage of the \( m \)-th iteration, similar calculations are performed for increments of a posteriori character probabilities of words of the code \( C_2 \)

\[
L^{(2,m)}(b_{ij}) = L^{(2,m)}(b_{ij} | y^{(2)}, L^{(1,m)}(b_{ij})) - (L(y_{ij} | b_{ij}) + L^{(1,m)}(b_{ij})).
\]

The quantities \( L^{(2, m)}(b_{ij}) \) are used as a priori information for the first stage of the subsequent \( (m + 1) \) iteration \( L^{(1, m + 1)}(b_{i,j}) = L^{(2, m)}(b_{i,j}) \).

At the last iteration, decisions are made regarding the symbols \( b_{ij} \); \( b_{ij} = 0 \) under the condition \( L^{(2, m)}(b_{i,j}) \) \( y_{ij} \); \( L^{(1, m)}(b_{i,j}) > 0 \), otherwise \( b_{ij} = 1 \).

The estimation algorithm \( L^{(1)}(b_{i,j}) \) is based on the calculation of expression

\[
L(b_{i,j} | Y_{i}, L(b_{i,j})) = \ln \left( \frac{\max_{b_{i,j}} \left\{ p(Y_{i} | B_{i,j}) \Pr(B_{i,j}) \right\}}{\max_{b_{i,j}} \left\{ p(Y_{i} | B_{i,j}) \Pr(B_{i,j}) \right\}} \right). (3)
\]

Assume that the conditions hold for the code words \( B_{i,j}^{(i)} \) and \( B_{i,j}^{(0)} \), respectively. For the AWGN
channel, under the condition that the codewords are equally probable, expression (3) has the form

\[ L(b_i|Y, L(b_j)) = C \cdot \left( y_i + \sum_{t=1}^{n} y_t \cdot (-1)^k \cdot d_t \right). \]  

(4)

Here \( dt = 0 \) if \( bh, t = bl, t \) and \( dt = 1 \) otherwise, \( C \) is a parameter that is constant for all code words. In accordance with the formalism of the iterative method, the second term in (4) is equivalent to the increment of the a posteriori probabilities \( L(1,m) (bij), L(2, m) (bij) \) for the constituent codes C1, C2 [3].

The procedure for searching for the code words \( Bh (i) \) and \( Bl (i) \), \( i = 0, 1, ..., n-1 \), requires the following steps [10].

Step 1. Binary "hard" decisions are made regarding the code symbols of the transmitted word \( B \) based on the samples of the implementation of \( Y \).

Step 2. A set of error vectors \( \{T\} \) is generated, generating with their help the code words \( S_j = BT_j, j = 1, 2, ..., 2p \). The set \( \{T\} \) consists of 2p words containing combinations of errors located in \( p \) the least reliable positions of the word \( B \). Here is the addition operation modulo 2.

Step 3. For each of the non-zero words \( S_j \), the reception for block codes C1 or C2 is performed based on the calculation of algebraic error syndromes and a set of code words \( \{D\} \) with a volume not exceeding 2p is formed.

Step 4. The codeword with the greatest correlation between the signals corresponding to the words from \( \{D\} \) and \( Y \), which is accepted as \( Bh (i) \), is determined. A subset of codewords \( \{D\} \) with maximal correlation coefficients that does not contain \( Bh (i) \) corresponds to \( Bl (i) \) for the symbols \( bi \).

For the symbols \( bi \) for which \( Bl (i) \) exists in the set \( \{D\} \), the increment \( L(\xi, m) (bi), (\xi = 1, 2) \) is calculated. For the symbols \( bi \) for which \( Bl (i) \) does not exist in the set \( \{D\} \), the computation \( L(\xi, m) (bi) \) is carried out using the rule \( L(\xi, m) (bi) = \beta (-1)^{bi}, (\xi = 1, 2) \). Here \( bi \) is the i-th symbol of the code word \( Bh (i) \) computed in step 4; \( \beta = (E1 - E2) / p \). Here, \( E1, E2 \) are the minimum and maximum correlation coefficients between the realization of \( Y \) and code words from the set \( \{D\} \).

The expansion of the set of BTKs with variations of their code rates is possible using the shortening method of generating turbo codes by reducing their information volumes.

The essence of the problem to be solved is to describe the method of forming an expanded set of BTKs based on the generating turbo code with a decrease in its information volume, and also to describe the algorithm of iterative reception of these codes and the results of its simulation for a number of generated codes in order to estimate probabilistic characteristics at reception.

3. REDUCED BLOCK TURBO CODES

The shortening method of block turbo codes is based on the reduction in the volume of the information block of the generating turbo code in the formation of code words: the symbols of the code \( C1, aij; 0 \leq i < B1, 0 \leq j < k2 \) and the code \( C2, aij; 0 \leq i < k1, 0 \leq j < B2 \) are assumed to be equal to zero. The resulting codeword is shown in Fig. 1, the highlighted color shows the location of zero information and verification symbols of the truncated turbo code with parameters \( k = B1\cdot B2, n = n1\cdot n2 - (k1 - B1) n2 - (k2 - B2) n1 + (k1 - B1)(k2 - B2) \).

When forming the code words of truncated turbo codes from the derived series, the procedure for generating a systematic generating turbo code for an input information sequence with a volume of \( k1\cdot k2 \) bits with \( k1\cdot k2 - B1\cdot B2 \) zero components and corresponding code words with zero symbols that are not transmitted in channel.

When applying this method on the basis of a generative turbo code with a code rate \( R \), it is possible to form a series of truncated turbo codes with code rates given by the relation

\[ \frac{B1 \cdot B2}{n1 \cdot n2 - (k1 - B1)n2 - (k2 - B2)n1 + (k1 - B1)(k2 - B2)} \leq R \leq \frac{k1\cdot k2}{n1\cdot n2}. \]

Here \( 2 \leq B1 \leq k1, 2 \leq B2 \leq k2 \).

The minimum Hamming distance of these codes coincides with the minimum Hamming distance of the generating turbo code. Table 1 shows the parameters \( k, n \) and \( R \) for a number of truncated turbo codes generated using this technique for generating turbo codes based on block Hamming codes with generalized parity check \( C1(128,120,4), C2(128,120,4) \) and \( C1(128,113,6), C1(128,113,6), C1(128,113,6), C1(128,113,6) \), in this case \( B1 = B2 = B \).

Code speeds of truncated turbo codes corresponding to the generating turbo code based on the constituent codes \( C1(128,120,4), C2(128,120,4), \)
can take the values $1/81 \leq R_1 \leq 7/8$. Table 1 gives the parameters of a series of truncated turbo codes with code speeds of $7/8$ (generating turbo code), $1/2$, $2/3$, $3/4$ and $4/5$. The code rates of truncated turbo codes corresponding to the generating turbo code based on the constituent codes $C_1(128,113,6)$, $C_2(128,113,6)$, can take the values $1/256 \leq R_1 \leq 4/5$. Table 1 shows the parameters of a number of truncated turbo codes with code rates $4/5$ (generating turbo code), $1/2$, $2/3$ and $3/4$.

When receiving the code words of truncated turbo codes, you can use the iterative algorithm (1) - (4) with the above 4 steps for the generating turbo code. The peculiarity of the reception algorithm is the execution of step 3 - for each of the non-zero words $S_j$, a trick is used for shortened block codes $C_1$ or $C_2$ based on the calculation of algebraic syndromes and a set of code words $\{D\}$ is formed, with a volume not exceeding $2p$. In this case, error detection and correction is performed for code symbols that are not part of the symbols that are assumed to be zero when generating truncated turbo codes.

4. RESULTS OF MODELING

In Fig. 2 and Fig. 3 shows the probabilistic characteristics of the iterative reception algorithms (10 iterations) for truncated turbo codes based on the generative turbo codes considered above. The ordinates represent the error probability values for the information bit $P_b$, the signal/interference values $E_b/N_0$ are plotted along the abscissa axis. Here, $E_b$ is the energy per information bit, $N_0$ is the spectral density of AWGN (one-sided).

When modeling the iterative algorithms of the turbo codes under consideration, an interval estimate of the probability $P_b$ is made by calculating the frequency $w = x/u$. Here, $x$ is the number of erroneous solutions in a sequence of independent computational experiments of size $u$, determined by the size of the confidence interval, the probability $P_b$, the confidence probability $P_d$. Under the condition $u \gg 1$, we have [11]

$$P_{\text{al}}(w-P_1 < \alpha) \equiv 2F\left(\frac{\alpha}{\sqrt{P_1(1-P_1)/u}}\right),$$

$$F(z) = \frac{1}{\sqrt{2\pi}} \int_0^z \exp(-y^2/2) dy.$$

For example, for $P_b = 10^{-5}, \alpha = 0.5P_b$ (confidence interval $[0.5P_b, 0.5P_b]$) and $P_d = 0.95$, the required number of experiments is $u = 1450000$.

In Fig. 2 shows the probabilistic characteristics when receiving the generating turbo code with the parameters $(16384, 14000, 16)$ and the code rate $7/8$ based on the constituent codes $C_1(128,113,6), C_2(128,113,6)$ (curve 1) and the derivative of the truncated series turbo codes with code rates $1/2$ (curve 2), $2/3$ (curve 3), $3/4$ (curve 4) and $4/5$ (curve 5) for the AWGS channel. Curve 6 corresponds to a convolutional code with a code rate of $1/2$ and a code constraint length of 7 [2]. Table 1 lists the corresponding signal/interference $E_b/N_0$ values required to achieve the error probability per bit $P_b = 10^{-5}$ when using these codes.

It is seen that for the generating turbo code (curve 1) with a code rate of $7/8$, the error
probability $P_b = 10^{-5}$ is reached at $E_b/N_0 = 3.95$ dB, which differs by only 1.05 dB from the limiting value for the Shannon capacity of the channel under consideration the bandwidth of the ABGS channel for codes with a code rate of 7/8 is achieved at 2.9 dB [2].

It is also seen that for a shortened turbo code with code speed 1/2 (curve 2), the error probability $P_b = 10^{-5}$ is reached at $E_b/N_0 = 3.1$ dB, which determines the energy gain to 1 dB for a given error probability $P_b$ with respect to to a known convolutional code with an equivalent code rate (curve 6). When the error probability decreases, the energy gain values increase.

In Fig. 3 shows the probabilistic characteristics when receiving the generating turbo code with the parameters (16384,12769,36) and the code rate 4/5 based on the constituent codes $C1(128,113,6)$, $C1(128,113,6)$ (curve 1) and the derivative of the truncated series turbo codes with code rates 1/2, 2/3 (curve 3), 3/4 (curve 4) for the AWGS channel. Table 1 lists the corresponding signal/interference $E_b/N_0$ values required to achieve the error probability per bit $P_b = 10^{-5}$ when using these codes.

It is seen that for the generating turbo code (curve 1) with code speed $\approx 4/5$, the error probability $P_b = 10^{-5}$ is reached at $E_b/N_0 = 3.0$ dB, this value differs only by 0.90 dB from the limiting value for the Shannon capacity of the considered channel (the bandwidth of the AWGN channel for codes with a code rate of 4/5 is achieved at 2.1 dB).

For a shortened turbo code with code speed 1/2 (curve 2), the error probability $P_b = 10^{-5}$ is reached at $E_b/N_0 = 2.25$ dB, which determines the energy gain to 1.85 dB for a given value of the error probability $P_b$ with respect to the convolutional code with an equivalent code rate (curve 6 in Fig. 2).

A comparative analysis of the corresponding probabilistic curves in Fig. 2, Fig. 3 and Table 1 shows the presence of an energy gain of up to 0.25 dB for truncated turbo codes with an equivalent code rate for a generating turbo code with parameters (16384,12769,36) and a generating turbo code with parameters (16384,14400,16).

It should be noted that the probabilistic characteristics of the generating turbo code with the parameters (16384,12769,36) with code speed 4/5 based on the constituent codes $C1(128,113,6)$, $C1(128,113,6)$ and the derivative of a number of truncated turbo codes with the code rates 1/2 and 2/3 for AWGS are sufficiently close to probabilistic characteristics (the difference does not exceed 0.2 ... 0.7 dB) of the most effective low density codes recommended for use in satellite communication systems [12].

5. CONCLUSION

The characteristics of noise-resistant block turbo codes are given, the feature of which is that they are formed by shortening the information volumes of the generating turbo codes. This approach extends the class of block turbo codes with a variation of code rates, information volumes and code word lengths. When receiving truncated turbo codes, a modified iterative technique algorithm is developed, which is developed for generating block turbo codes.

For a number of considered generative and truncated block turbo codes, simulation of iterative reception algorithms has been carried out. In particular, it is shown that the energy gain when using a truncated turbo code with a code rate 1/2 with respect to the known convolutional code with an equivalent code rate for the error probability $P_b = 10^{-5}$ reaches 1.85 dB.

The development of effective algorithms for the iterative reception of the considered generating and shortened turbo codes and a comparative analysis of their probabilistic characteristics represents a promising direction of research.

ACKNOWLEDGMENT

This work was supported by the Russian Foundation for Basic Research, project No. 16-07-00746 “Development of the...
theory and methods of noise-immune digital communications over nonstationary channels with complex interference”.

REFERENCES

1. Peterson W, Weldon E. *Codes that correct errors*. Moscow, Mir Publ., 1976, 594 p.
2. Zyuko AG, Falco AI, Panfilov IP, Banquet VI, Ivaschenko PV. *Immunity and efficiency of information transmission systems*. Moscow, Radio i svyaz Publ., 1985, 272 c.
3. Hagenauer J, Offer E, Papke L. Iterative decoding of binary block and convolutional codes. *IEEE Transactions on IT*, 1996, 42 (2):429-448.
4. Johnson SJ. *Iterative Error Correction: Turbo, Low-density Parity-Check and Repeat-Accumulate Codes*. Cambridge University Press, 2010, 335 p.
5. Nazarov LE, Shishkin PV, Batanov VV. Algorithms for iterative non-coherent signal reception based on serial turbo codes and Walsh signals transmitted over non-stationary channels. *Radiotekhnika i elektronika*, 2016, 61 (4):366-372 (in Russ.).
6. Vishnevsky VM, Lyakhov AI, Portnoy SI, Shakhnovich IV. *Broadband transmission networks*. Moscow, Technosphere, 2005, 592 p.
7. Nazarov LE, Shishkin PV. Investigation of probabilistic characteristics of block turbo codes based on low-density codes of finite geometries. *Journal of Radioelectronics (electronic journal)*, 2018, №5. Access mode: http://jre.cplire.ru/jre/may18/1/text.pdf. DOI: 10.30898/1684-1719.2018.5.1.
8. Nazarov LE, Shishkin PV. Characteristics of jam-resistant block turbo codes based on low-density codes. *Information Technology*, 2018, 24 (6):427-432. DOI: 10.17587/it.24.427-432.
9. Kotelnikov VA. *Theory of potential noise immunity*. Moscow, Gosenergoizda Publ., 1956, 152 p.
10. Pyndiah RM. Near-optimum decoding of product-codes: block turbo-codes. *IEEE Transactions on COM*, 1998, 46(8):1003-1010.
11. Dunin-Barkovsky IV, Smirnov NV. *Theory of Probability and Mathematical Statistics in Engineering*. Moscow, GTTL Publ., 1955, 556 p.
12. Low-Density Parity Check Codes for Use in Near-Earth and Deep Space Applications. Experimental Specification. *CCSDS 131.1-O-2*, 2007, Washington, NASA Headquarters, 44 p.