

Algorithm of multithreshold decoding for self-orthogonal codes over Gaussian channels

V.V. Zolotarev, G.V. Ovechkin, S.V. Averin

Space Research Institute RAS, Moscow; The Ryazan State Radioengineering University, Ryazan;
United Radioelectronic Technologies, Moscow, Russia
zolotasd@yandex.ru, g_ovechkin@mail.ru, ser-averin@yandex.ru

Abstract – Multithreshold decoder (MTD) for self-orthogonal codes and its performance over Gaussian channel are reviewed. It's shown that MTD is in many cases as effective as an optimum decoder. MTD implementation complexity is also discussed.

Keywords: iterative process, optimal decoding, majority and multithreshold decoding, MTD.

Introduction

As it is known, the use of error-correcting coding enables to solve a variety of tasks in digital networks. The main advantage of communications systems using coding amounts to the fact that the efficiency of the channels use appears in many times higher as when codes are not used. The coding gain is usually chosen a measure of the efficiency.

Decoders realizing the well known to specialists Viterbi algorithm (AV) [1], and also much more complex code structures, such as turbo codes [2] and low-density parity-check codes [3], are currently being used in digital communications. Nevertheless, the currently used coding systems, especially those for high-speed channels, are still very complex or inefficient. Below consider the theoretical basis and concrete parameters of a highly efficient, high performance and very simple iterative algorithm for error correction in high noise level channels which is the result of development of the concept of linear convolutional codes majority decoding [4].

The advance in technology of decoding for error-correction codes within many decades surprisingly was not connected in any way to methods of solution of a functional optimization problem for very many discrete variables. Nevertheless decoding, i.e. search of the unique code word among exponentially large number of the possible ones, would be pure naturally to esteem from such stands. However, decoding algorithms developed before have not used in any way for a search of the best decoder solutions of well-known optimization procedures, which ones could be applied to search the code words located at minimally possible distance to the received word. But just threshold decoder (TD) [1], realizing the elementary error correcting method, has the useful properties, which are indispensable for implementation valuable effective and simultaneously extremely simple optimization decoding procedures.

1. Repeated decoding principle

In the past decade the theory and technology of error-correcting coding have progressed greatly. Introduced by many authors in the seventies of the twentieth century methods of repeated decoding turned out to be inefficient due to powerful error grouping at the decoder output. An example of such scheme with the threshold decoder (TD) [4] for a convolutional code is given in fig. 1.

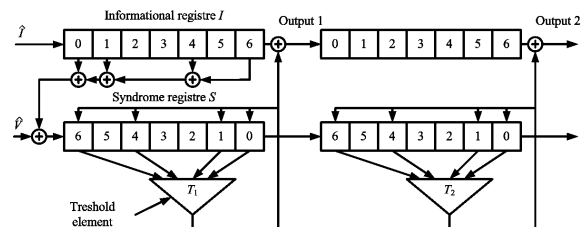


Fig. 1. An example of a scheme of repeated decoding on the basis of the threshold decoder

Such decoder has low efficiency due to intense grouping (propagation) of errors in the threshold decoder. In fact if under a certain noise level in a binary symmetrical channel (BSC) TD make a wrong decision for a decoded information symbol, very dense error packet usually emerges at the output of that TD. For example, assume that a sequence decoded by the first TD decoder has come to the input of the second TD decoder (fig. 1). Then, if there are no errors in the information sequence after the first TD, there is no need for a second decoder. But when an error emerges at the output of the first TD, which is usually a starting point for the typical error packet of this TD, it appears that the second decoder, copying exactly the scheme of the first one and tuned only to random errors correction, will most probably fail to correct the packet. Hence there is no need to use second TD in this case.

It should be noted that codes with low level of error propagation for TD were completely unheard in those days. Nevertheless, the problem was solved in full later with help of methods described in [5–14]. In this connection great importance appears to be the considered further new approach to the realization of simple efficient error correction procedure, which is under development since 1972 and is called multithreshold decoding (MTD) [5].

2. The multithreshold decoding background

Consider an example of the simplest system of coding and threshold decoding for convolutional code of the code rate $R=1/2$ and the minimum code distance $d=3$, as shown in fig. 2.

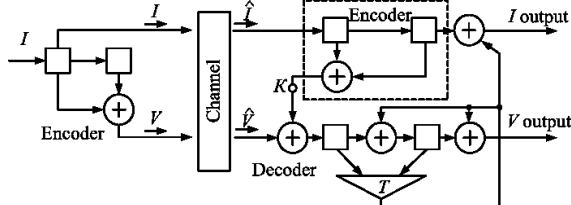


Fig. 2. Special projection of the coding system clarifying the new interpretation of the syndrome

As follows from schemes of the coder and the simplest majority decoder, correcting in this case a single error, the decoder includes exact copy of the coder, which is forming its estimates of the check symbol on basis of the information symbols received from the channel. These estimates appear at the decoder point K and after they adding with the received from the channel checking symbols \hat{V} to form symbols of the syndrome vector S , which depend only on the channel errors. Later these symbols come to the decoder threshold element from the syndrome register, as is shown in fig. 2.

The scheme of TD given in the figure enables to single out an easy way for organization of the proper optimization procedure, i.e. search for the best possible decision during decoding. To that purpose let us stress the fact that has never been mentioned before: in the decoder syndrome register there is a difference by check symbols between the received from the channel vector $Q = [\hat{I}, \hat{V}]$ and such code word A , the information symbols of which equal to the received from the channel information part of vector Q .

It means that the full difference between the current hypothesis-decision of decoder A on the transmitted code word and the received vector Q will be in such modified decoder of the majority type in which only one vector will be appended to TD. This vector shall always contain the difference between the received vector Q and the current hypotheses A of the decoder on the information symbols. In this decoder it will be contained the full value of the difference and, consequently, the full distance between the decoder decision and the received vector. One should strive at decreasing this distance to the minimum possible value, which is correspond to the decision of an optimum decoder (OD).

Such approach to the problem of high efficiency decoding is basis of the developed since 1972 special iterative multithreshold decoders [5–14], almost coinciding with the classic TD and as simple in realization as their prototype.

The changes that should be introduced into ordinary TD to transform it into MTD (as follows from the global optimization principle discussed in the previous section), amount only to the fact that the decisions of all threshold elements on the decoded symbols changes are first committed to memory in an additional differential register D , primarily, filled by zeros. These decisions are later used by the following threshold elements of the decoder as an additional checking procedure in course of further specification of the decoded symbols. Such decoder is already measuring full distances between newer and more likely potential solutions and the received vector Q . It changes the decoded symbols in such way that every new decision of such MTD is always closer to the received vector. In many instances it enables to practically completely realize corrective potential of the used codes. Examples of concrete MTD schemes are given in [9, 10].

After such rather unsophisticated improvement the decoder obtains new very useful properties. The MTD decisions at every change of the information symbols are strictly approaching the optimum decoder decision ensuring in many cases realization of this process even after several dozens of attempts of code block decoding. Certainly, to ensure high MTD efficiency at high noise in the channel it is essential to choose only special codes with low levels of error propagation. This important issue was considered in [6, 8, 9].

Let us further proceed with a more formal consideration of the MTD potential.

3. The MTD main theorem

Consider a binary linear systematic block or convolutional self-orthogonal code [15] with the code rate $R = k/n$, where k is a number of information bits, n is the code length. The parity-check matrix for the code is set in systematic form: $\mathbf{H} = [\mathbf{C}, \mathbf{I}]$.

After transmission over BSC an optimum decoder minimizing the mean error probability chooses from a set of 2^k equiprobable code words $\{A\}$ a vector A_0 for which the Hamming distance $r = |Q \oplus A_0|$ would be minimum for the whole set $\{A\}$. Here Q is the received message, \oplus is addition on module 2.

Let us represent any binary code vector X of length n by a pair of information vector X_I and check vector X_V of length k and $(n-k)$ respectively:

$$X = [X_I, X_V].$$

Then we have the following

Lemma. For each code vector A and the received vector Q the ratio is true

$$A \oplus Q = [D, \mathbf{H}[Q \oplus D, Q_V]], \quad (1)$$

where vector D of the length k is defined by

$$A_I = Q_I \oplus D. \quad (2)$$

Proof. Due to the linearity of the code

$$\begin{aligned} S &= \mathbf{H}[Q_I \oplus D, Q_V] = \mathbf{H}[A_I, A_V \oplus Q_V] = \\ &= \mathbf{H}A \oplus \mathbf{H}[0_I, A_V \oplus Q_V], \end{aligned}$$

where 0_I is a zero vector of length k .

As $\mathbf{H}A = 0$ and $\mathbf{H}[0_I, A_V \oplus Q_V] = A_V \oplus Q_V$, as $A_V \oplus Q_V$ is multiplied only by identity submatrix \mathbf{I} of \mathbf{H} , we get

$$S = A_V \oplus Q_V. \quad (3)$$

After substitutions in the right-hand side (1) with view of (2) and (3), we find that

$$[D, S] = [D, A_V \oplus Q_V] = [D \oplus Q_I \oplus Q_I, A_V \oplus Q_V] = A \oplus Q.$$

Thus the syndrome vector S is actually (as it was given in fig. 2) a difference on check symbols between the received message Q and the code word A .

The lemma is proved.

The essence of the lemma amounts to the fact that the difference $B = Q \oplus A$ for any received vector Q and a code word A is defined by a pair of vectors $[D, S]$. Using exhaustive search over all set vectors $\{A\}$ it is able to find vector A_0 , minimizing $|B|$ and being the optimum decoder solution. By definition with $D = 0$ vector S is a usual syndrome of the received message Q : $S = \mathbf{H}Q$. For simplicity with $D \neq 0$ we shall below call S a syndrome too as the generalization seems natural and is not resulting in any contradictions. It should be also noted that there is no need to calculate again all syndrome components at each change of A . It appears quite sufficient to invert at each change of decoded symbol only components of S with odd amounts of errors in the changed information symbols.

Consider a new decoding algorithm, which use discussed properties of self-orthogonal code.

1. Let the decoder at the first preparatory stage perform calculation and memorizing of vector S . After that the decoding procedure is begun.

2. Choose an information symbol i_j and for the symbol it is calculated the usual sum of the syndrome components s_{j_k} depended on an error e_j in the decoded symbol i_j (i.e. sum of checks $s_{j_k} \in \{S_j\}$, where $\{S_j\}$ is a set of checks corresponded to symbol i_j) and symbol d_j corresponded to the decoded symbol i_j :

$$L_j = \sum_{s_{j_k} \in \{S_j\}} s_{j_k} + d_j. \quad (4)$$

Let us assume that initially $D = 0$ as before decoding there is only one received vector Q in the decoder and the decoder possesses no other more preferable hypotheses of the received message.

Let us assume the threshold T as equal to a half of amount of addends in (4). For self-orthogonal codes $T = d/2 = (J+1)/2$.

3. Let finally all $J = d-1$ checks, i_j and d_j be inverted if $L_j > T$ and stay unchanged if $L_j \leq T$.

4. If decision about stopping decoding is not make go to step 2.

For the first decoding attempt the proposed procedure while all $d_j = 0$ is similar to the usual threshold decoder. Let us below refer to the decoder realizing the proposed algorithm as a multithreshold decoder (MTD).

Theorem (The main theorem of multithreshold decoding). If at a j -th step of decoding MTD changes the currently decoded information symbol i_j , then:

a) at that MTD finds a new code word A_2 , closer to the received message Q , then code word A_1 , to which the i_j meaning corresponded prior to the j -th step of decoding

$$|B_1| = |A_1 \oplus Q| > |A_2 \oplus Q| = |B_2|;$$

b) after completion of the j -th step decoding of any subsequent symbol i_k , $k \neq j$, is possible, so that its change will result in further approaching to the received message.

Proof. Prior to the decoding of symbol i_j it is true pursuant to the lemma

$$[D_1, S_1] = [A_1 \oplus Q, \mathbf{H}[Q_I \oplus D_1, Q_V]] = A_1 \oplus Q,$$

where

$$A_1 = [A_{1I}, A_{1V}], A_{1I} = Q_I \oplus D_1.$$

The weight of vector B_1 , before this step equal to $|B_1| = |D_1| + |S_1|$, can be defined as an ordinary sum of weights $W_1 = L_{1j} + X$, where L_{1j} is defined by (4) and is equal to the sum of checks and symbol d_j at the threshold element, X is the weight of the other components of S_1 and D_1 , not included into L_{1j} .

Consider code vector A_2 differing from A_1 only in one information symbol i_j and the respective difference $B_2 = A_2 \oplus Q$. As B_1 and B_2 differ only in the components coming to the threshold element $|B_2| = L_{2j} + X$, where $L_{1j} + L_{2j} = J + 1$, as due to the code linearity each check and the d_j are surely equal to 1 in only one of vectors B_1 and B_2 .

As MTD change i_j if $L_{1j} > T$, it is essential for that to have $L_2 < L_1$ and, consequently, $|B_1| > |B_2|$, which proves item a) of the theorem.

It is further evident that if symbol i_j was not changed it is possible to decode any other symbol i_k , $k \neq j$, as the conditions of the lemma are hold. In case of change i_j in accordance with the rules of MTD functioning after decoding i_j equations $A_{2I} = Q_I \oplus D_2$ and $S_2 = \mathbf{H}[Q_I \oplus D_2, Q_V]$ hold, where D_2 differs from D_1 in symbol d_j , at changes via feedback from the threshold element of checks referring to i_j , those components of S_1 are inverted, in which S_2 differs from S_1 . Hence, we get that after changing i_j for the

previously defined vectors D_2 , A_2 and S_2 the equation holds

$$[D_2, S_2] = A_2 \oplus Q,$$

similar to the one, occurring prior to the change of i_j . Thereby for subsequent decoding steps and changes of symbols i_k , $k \neq j$, there will be further approaching to the received from the channel message Q .

The main MTD theorem is proved.

It follows from the theorem that with each change of the decoded symbols MTD is getting closer and closer to the received vector Q , thus finding closer and closer to the optimum decision and more likelihood vectors A_i . MTD views and compares not an exponentially great amount of code words but only pairs of ones differing only in a single information symbol with one of the compared words being in the decoder. In case the second code word turns out to be closer to vector Q , than the one in MTD, the decoder will switch over to that word to perform further comparison with the new intermediate vector A_i . It is clear that in principle it is possible to carry out a large number of decoding attempts for all code symbols. In that way convergence to the optimum decoder decision will be realized. It is crucial that MTD complexity remains the same as for customary TD: a linear one.

Let us further assume that MTD has reached the optimum decoder decision, i.e. there are symbols of vector A_0 in the MTD information register. Then it is true that:

Corollary. MTD is not change the decision of an optimum decoder.

Proof. If the MTD changes a single information symbol in vector A_0 , than another code vector A^* was found, which is closer to Q than A_0 . But it is impossible, because by definition the closest to Q is vector A_0 .

The corollary is proved.

Thus, the stability of MTD decision on the optimum decision is shown: having reached that, MTD is going to stay there. It is very important as the algorithm implies an opportunity of multiple changes of the decoded symbols.

It might also be noted that during the proving of the main MTD theorem the uniqueness of the decoded symbol i_j was not used in any meaningful way. It follows that the decoding procedure can be applied to any group of information symbols [6, 8, 9].

To apply MTD algorithm for a channel with additive white Gaussian noise (AWGN) with quantization of the received binary stream into M levels, $M > 2$, it is convenient to present the likelihood function L_j as

$$L_j = \sum_{s_{jk} \in \{S_j\}} w_{j_k} (2s_{j_k} - 1) + w_{d_j} (2d_j - 1). \quad (5)$$

For an ordinary BSC this expression with check weights w_{j_k} equal to 1 is evidently equivalent to (4). With consideration of a Gaussian channel, i.e. in case of $M > 2$ signal quantization levels, weight coefficients for calculation of L_j may be chosen as relatively small real or integer numbers. Thus, the symbols decoded in MTD for a Gaussian channel should be changed with $L_j > 0$. At that, if $M \gg 1$, then, as it is known corrective potential of the used codes and good algorithms of their decoding, MTD included, are usually improved by about 2 dB by the signal/noise ratio at the decoder input.

4. Error propagation in majority decoders

It follows from the results we have proved above that increase of the number of attempts to correct the symbols decoded before with the help of MTD might be actually of use, as with every change of the information bits there is transfer to decisions with higher likelihoods. Nevertheless, it does not mean that MTD is sure to approach the optimum decision. For many codes there exists a rather numerous amount of channel errors combinations, which are corrected with an optimum decoder but not corrected with MTD. To considerable extent it occurs due to the fact that threshold decoders are to great extent subject to influence of the error propagation effect. The second and the rest subsequently connected improved TDs, from which a convolutional MTD comprise, usually have to operate mostly with streams of error packets from prior decoding iterations.

In [6, 8, 9] a method of error propagation estimation for self-orthogonal codes is given, it amounts to the concept that probability estimates for emergence of single and packets of errors at TD output are calculated using multidimensional probability generating functions. This method is helpful both for selection of code in the least degree subject to error propagation influence and for choice of optimum weights and thresholds in MTD ensuring the least probability values for its decoding errors.

Basis for new approach to error propagation estimates is rather convenient way of estimating of the probabilities for emergence of two errors within the constraint length or within each code block. It enables to generalize this method to comprise decoding error packets of any weight. To ensure high efficiency of MTD it usually suffices to consider packet weights not exceeding 3. At that one has to calculate within the parameter space with the number of dimensions 2^{3d} , where d is the minimum code distance of the code. But for codes with $d=7$ and more this task is too complex for computations. Nevertheless,

in course of further investigation, methods of considerable simplification of estimates of packets emergence probability were found, which later enabled to formulate complex criteria for future creation of codes with very low probabilities of the emergence of error packets during majority decoding. The respective algorithms for development of such codes with the length n require realization $O(n^4)$ operations, which enables searching for efficient codes with lengths up to 500000 bits. Recently these algorithms were improved further.

While decoding close to the channel capacity it is essential to use only very long codes. That is why the completed development of constructive methods of the codes creation with required quality solved in full problem of choosing codes with modest error propagation level for high efficiency MTD decoders.

5. Multithreshold algorithms efficiency

The new results obtained in field MTD development are substantiated in fig. 3, which demonstrate potential of MTD algorithm and already known methods for error correction. The curve 1 corresponds to the efficiency of MTD decoder implemented on FPGA Xilinx, curves 5, 6 and 7 are given for MTD application in the simplest concatenated circuits with parity check control. All these results have been discussed in detail in [14]. Fig. 3 also gives efficiency curves for Viterbi algorithm for the standard convolutional code of length $K=7$ (curve 3), for a concatenated circuit of Viterbi decoder and a Reed-Solomon code (curve 4), for a turbo code (curve 9) [2] and for a low-density parity-check code recommended in the DVB-S2 standard (curve 10). It should be noted that at implementation of a high speed decoder for DVB-S2 low-density parity-check codes on FPGA the efficiency loss may

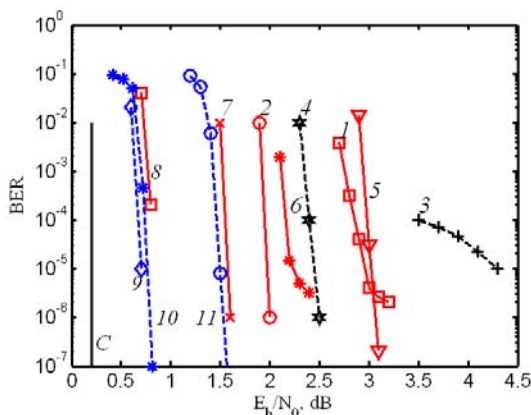


Fig. 3. Performance of error-correcting codes with $R = 1/2$ over a Gaussian channel

be up to 0,5 dB (curve 11). Vertical curve “ $C = 1/2$ ” characterizes the capacity of a Gaussian channel for the code rate $R = 1/2$. Curve 2 present performance of MTD for a long code with $I = 40$ decoding iterations realized in the SRI RAS on FPGA Altera. The new result for MTD and a non-equal energy channel [9] is represented by line 8. It means opportunity of very simple and considerable increase of the decoding efficiency at delay in decision not exceeded 400000 bits, under which the well known and rather high MTD functioning rate is preserved both in the software and (especially) in the hardware format.

Taking into account the achieved closeness of MTD efficient functioning area to the communication channel capacity, the prospects of MTD for further approaching of its characteristics to the Shannon bound can be considered to be good. At that, sufficient advantage of MTD over other algorithms in the number of operations on one-two decimal exponents for different combinations of coding parameters, gives ground to assume that it is possible to use MTD actively in the development of digital data transmission hardware for space and satellite communication channels.

6. The MTD algorithm realization complexity

The main MTD advantage is its extremely low decoding complexity. As in case with traditional TD in MTD at each iteration weighted checks are summed; if the sum is greater than the threshold the checks are changed together with the decoded symbol. The number of decoding iterations I in this case is not exceed 50, and the general MTD decoding complexity is evidently estimated for $d < 25$ as

$$N_1 \sim (d + 2)(I + 4).$$

But it is possible to decrease considerably the amount of iterative sum calculations at the threshold as the symbols at each of the threshold elements change during decoding very seldom. If with the same I and d decrease of MTD performance is possible about by 0,1 dB in energy, which is usually quite acceptable, the amount of operations will be decreased to:

$$N_2 \sim c_1 d + c_2 I,$$

where constants c_1 and c_2 are small integers [8–10].

In case of hardware MTD implementation, for example, on serial FPGA Xilinx or Altera, tests carried out confirmed their good efficiency parameters with simultaneously very high throughput up to 1,6 Gbit/s. Such opportunity emerged after the realization of patented engineering solutions for hardware MTD. Pursuant to these solutions such decoder turns into single-cycle decision circuit, and within each cycle it is able to make up to 40 decisions on

the decoding symbols. As result hardware MTD data rate can formally considerably exceed even 10 Gbit/s. It removes all the restrictions on the processing speed for such devices, which, with the multi-threshold algorithms performance, makes them the sole leaders among all the other methods of digital streams transmission over satellite and other high-speed channels. In particular, the already developed hardware MTD versions for earth remote sensing systems are especially useful, because it is their high-speed flows of digital data with limited transmitter power that should be protected in every possible way using the error-correcting coding methods.

Conclusion

The use of MTD in satellite and other channels enables to realize high processing rate and boost their performance considerably. The extremely simplicity of MTD makes them preferential for hardware realization in high-speed broadband channels. In rather low speed communication channels even software MTD realizations are most efficient; they require execution of only several dozen operations for the threshold element. Absolutely insignificant difference in the efficiency of MTD and other more complex decoders, will be, apparently, overcome in the near future as follows from dynamics of MTD characteristics improvement.

More detailed information and research results on MTD are given at the specialized website of the SRI RAS www.mtdbest.iki.rssi.ru. Realization of research on MTD algorithms was supported by the Council on complex problems of cybernetics of the AS of the USSR, SRI RAS, FSUE NIIRadio and grants of the Russian Foundation of Basic Research №05-07-90024, №08-07-00078.

Bibliography

1. Viterbi A.J. Error Bounds for Convolutional Codes and an Asymptotically Optimum Decoding Algorithm, *IEEE Trans.*, 1967, IT-13, pp.260–269.
2. Berrou C., Glavieux A., Thitimajshima P. Near Shannon Limit Error-Correcting Coding and Decoding: Turbo-Codes, ICC'93, Geneva, 1993, pp.1064–1070.
3. MacKay D.J.C., Neal R.M. Near Shannon limit performance of low density parity check codes, *IEEE Electronics Letters*, 1996, vol.32, no.18, pp.1645–1646.
4. Massey J. Threshold decoding, M.I.T. Press, Cambridge, Massachusetts, 1963.
5. Zolotarev V.V. A device for linear convolutional codes decoding, Inventor's certificate of the USSR no.492878, *Bulletin of inventions*, 1975, no.43.

6. Samoilenko S.I., Davidov A.A., Zolotarev V.V., Tretyakova Ye.I. *Computer Networks*, Moscow: Nauka, 1981.

7. Zolotarev V.V., Ovechkin G.V. Effective algorithms of error-correcting coding for digital communication, *Electrosvyaz*, Moscow, 2003, no.9, pp.34–37.

8. Web site of IKI RAS www.mtdbest.iki.rssi.ru.

9. Zolotarev V.V. *The Theory and Algorithms of Multithreshold Decoding*, Moscow: Radio i svjaz, Gorjachaja linija–Telecom, 2006.

10. Zolotarev V.V., Ovechkin G.V. Error-correcting coding. Methods and algorithms. The quick reference, Moscow: Gorjachaja linija–Telecom, 2004.

11. Zolotarev V.V., Nazirov R.R., Chulkov I.V. The Quick Almost optimal multithreshold decoders for Noisy Gaussian Channels, *RCSGSO International Conference ESA in Moscow*, 2007.

12. Zubarev Yu.B., Zolotarev V.V., Ovechkin G.V., Stokov V.V. Multithreshold Decoders for High-Speed Satellite Communication Channels: New Perspectives, *Electrosvyaz*, 2005, no.2, pp.10–12.

13. Zolotarev V.V., Ovechkin G.V. Multithreshold decoders for channels with extremely high noise level, *Telecommunicatsii*, Moscow, 2005, no.9, pp.29–34.

14. Zubarev Yu.B., Zolotarev V.V., Ovechkin G.V., Dmitrieva T.A. Multithreshold algorithms for Satellite Networks with Optimum Characteristics, *Electrosvyaz*, 2006, no.10, pp.9–11.

15. Townsend R.L., Weldon E.J. Self-Orthogonal Quasi-Cyclic Codes. *IEEE Trans.*, 1967, IT-13, pp.183–195.

16. Zolotarev V.V., Ovechkin G.V. The complexity of high performance methods of error-correcting codes decoding, *Proc. 6th Intern. Conf. Digital signals processing and its application*, Moscow, 2004, vol.1, pp.220–221.

17. Zolotarev V.V., Ovechkin G.V. The use of multithreshold decoder in concatenated coding schemes, *Vestnik RGRTA*, Ryazan, 2003, no.11, pp.112–115.

18. Zolotarev V.V., Averin S.V., Chulkov I.V. Optimum Decoding Characteristics Achievement on the Basis of Multithreshold Algorithms 9-th *ISCTA'07*, Ambleside, 2007.