**Performances of the Decoding Algorithms near Shannon Limit**

Valery ZOLOTAREV\(^1\), Gennady OVECHKIN\(^2\), Dina SATYBALDINA\(^3,\)*, Nurlan TASHATOV\(^4\) and Erlanbek OMIRBAYEV\(^4\)

\(^1\)Space Research Institute of the Russian Academy of Sciences, 84/32 Profsoyuznaya str, 117997 Moscow, Russian Federation
\(^2\)Ryazan State Radio Engineering University, 59/1 Gagarin str., 390005 Ryazan, Russian Federation
\(^3\)National Research Nuclear University "MIFI", 31 Kashirskoe road, 115409 Moscow, Russian Federation
\(^4\)L.N. Gumilyov Eurasian National University, 2 Satpayev str., 010008 Nur-Sultan, Kazakhstan
*Corresponding author

**Keywords:** Coding Theory, Multithreshold Decoder, Shannon Limit.

**Abstract.** Forward error correction technique based on the optimization procedures for multithreshold decoding algorithms is considered. Recent advances as well as new opportunities of the multithreshold decoders for use in the systems working at the Shannon’s limit are analysed. Performances of the multithreshold decoders for self-orthogonal binary and non-binary codes over Gaussian channels are presented. Simulation results of BER performance of proposed decoder is shown to be close to the results provided by optimum total search methods.

**Introduction**

Shannon’s theorem for capacity of the channels with Additive White Gaussian Noise (AWGN), and is basic both in information theory and in and communication systems design as defining the “ideal”, most efficient trade-off between the power, bandwidth and information transfer reliability [1]. A forward error correction (FEC) techniques such as Reed–Solomon (RS) codes, low-density parity-check (LDPC) codes and turbo codes, come much closer to reaching the theoretical Shannon limit, but at a cost of high computational complexity. In [2] it was shown that LDPC codes can reach within 0.0045 dB of the Shannon limit for binary AWGN channels, with block length of $10^7$. The number of decoding iterations was about 800-1100.

However, for realization enough effective decoding algorithms for LDPC codes are required the considerable calculated expenses i.e. a large number of operations that leads to very significant increase in time of coding and decoding. For practice using these highly efficient codes the computing power of the digital signal processors is required, but it leads to increased costs.

Therefore the objective of contemporary communication systems design is develop of the decoding algorithms for codes that have low computational complexity and high error correction performance at the near to the Shannon’s limit.

In present paper the basic principles of the simple majority iterative decoding method for linear codes as a global extremum search for functional on discrete variables are described. Performances of proposed error correction technique over binary Gaussian and non-binary channels are considered. A comparison is made of the characteristics of multithreshold decoders (MTD) and a Viterbi decoder, the decoders for turbo and low-density codes, as well as some error correction methods for RS codes that turn out to be much more complicated than majority algorithms. Simulation results show the MTD decoders were most simple and fast, and their performance was among the best ones for the communication systems working at the Shannon’s limit.

**Majority Decoding Algorithms for Error-correction Codes**

For some codes, an iterative decoding procedure, which converging to the optimal solution, is possible. Such an algorithm is the majority voting algorithm or, as it is also called, the majority algo-
The idea is quite simple. Let to suppose that each information bit can be represented by several equations that include codeword symbols (in general, both information and check bits). The decision that a bit is equal to one (zero) is made in the case of a preference for one (zero) in most equations for this bit. For example, classic Hamming block codes, extended with a single parity check, can be decoded by a majority algorithm. For such a code, each information bit can be represented by four check equations, therefore the decision on the equality of one (zero) value of a bit is made with at least three votes in favor of one (zero). In the terminology of majority decoding, three voices are the threshold. Therefore, such decoding is also called threshold decoding [3]. The simplest example of coding/threshold decoding system with the code rate $R = 1/2$ and the minimum code distance $d = 3$, shown in Fig. 1.

![Figure 1. The coding/threshold decoding system with the code rate $R = 1/2$ and the minimum code distance $d = 3$.](image)

A simple majority decoder that corrects one error in this simple example contains an exact copy of the coder. This copy forms its own estimates of the code check symbols by informational code symbols taken from the channel, perhaps, with errors. These symbols appear at the point $K$ of the decoder and then, after summation in the half-adder with check symbols received from the channel $\hat{V}$, form a syndrome vector symbols $\hat{V}$, which depends only on the channel error vector. Then these symbols are going to the threshold element $T$ from the syndrome register.

The form of threshold element $T$ in the shown coding/decoding scheme allows specifying a simple way to organize proper optimization procedure, i.e. to find the best possible decoding decision. Let us turn to the fact, which has never been discussed relating to any linear code before: the decoder syndrome register contains the check symbol difference between the vector $\hat{V}$ received from the channel with noise and the code word $\hat{V}$, which informational symbols coincide with the informational part of the vector $\hat{V}$ received from the channel.

Hence, the total difference between the current decoder’s decision $\bar{A}_i$ and received noisy vector $\bar{Q}$ will be in such a modified decoder of majority type. This decoder will contain the current value of a total difference, and therefore, will allow measuring the full distance between the current decoder decisions contained in its information register and received vector. This distance should be reduced to minimum that will correspond to decision of the optimum decoder, which is usually achieved by the exponentially complicated total search methods.

The low efficiency of this decoding scheme was due to strong grouping, i.e. error propagation in the threshold decoder. Thus, changes that need to be done in the usual threshold decoder (TD) to convert it to multithreshold decoder (MTD), are the next: decisions of all threshold elements about decoding symbols changes must be stored in the new additional difference register, originally, of course, containing zeros. These decisions are then used by subsequent threshold decoder elements as an additional check for further correction of decoding symbols. At the first iteration of error correction, MTD works just like a conventional TD. Only at subsequent decoding attempts, MTD starts to really take into account the contents of the corresponding cells in register $D$, as a result of which it keeps the properties to improve TD decisions at all changes of the message informational symbols. MTD parameters are optimized according to many hundreds criteria (thresholds values, weight of checks, differences in polynomials, etc) in constructing self-orthogonal codes (SOC) with a low error propagation level. This enables us to assume that the optimization theory constitutes the basis of MTD methods and all algorithms based on them.
Due to the use of optimization procedures with the increase in the number of error-correcting iterations and the appearance codes with less degree of susceptibility to error propagation, MTD capabilities grow substantially under maintaining the very small complexity of the algorithm itself. By now, the characteristics of multithreshold decoders have become much better than all other algorithms in comparison with other methods for all the parameters of systems that are practically interesting for communication technology [4-6].

Below we first consider the possibilities of MTD corresponding to the main code clusters (typical sets of code parameters and channel models), and then a discussion of the presented results will take place.

Simulations Results and Discussion

Gaussian Channels

Let us consider the performances of basic decoding algorithms operating in a Gaussian channel at the code rate \( R = 1/2 \) (Fig. 2). The dependences of the bit error rate \( P_b(e) \) of different decoding algorithms are traditionally shown in terms of function \( Eb/No \), i.e., the level of the bit energy of a channel, as dB. The vertical line \( C = R = 1/2 \) designates the noise level at which channel capacity \( C \) is equal to the code rate: \( C = R = 1/2 \). Dashed line \( P_0 \) shows error probabilities in this channel. The curve Turbo points to the limiting capabilities of turbo codes, which, however, still can’t be embodied in the characteristics of the equipment due to the complexity of the algorithms of this class. Curve VA:K7 illustrates the possibilities of the widespread Viterbi algorithm (VA) for short convolutional codes with the code length \( K = 7 \). Graph CC: VA*RS corresponds to the concatenated scheme based on this VA and Reed–Solomon code [6]. The min-sum decoder of the DVB-S2 low-density parity-check (LDPC) code, the length of which is 64 800 bits, is characterized by curve LDPC, implemented in the Scientific Research Institute Radio [7]. Graph TR defines the real potential of the decoder of CDMA2000 turbo codes with a length \( n=3060 \) bits.

MTD algorithm in the convolutional implementation in the binary Gaussian channel with 4-bit signal quantization in the demodulator is shown in Fig. 2 on the MTD1 graph. At the present time, it is really as optimal as the exhaustive search algorithms and it decodes long codes at a very low power of the Gaussian channel \( Eb/N0 = 1.2 \) dB, that is more than its throughput \( C \) only at 1 dB [4]. Thus, MTD1 operates at such a noise level, when the transmitter power is only at ~ 26%, that is, only a quarter higher than its level at \( C = 1/2 \). The decoder requires no more than \( I = 192 \) iterations. The decoding delay for the constructed code with a small EP and with a code distance \( d = 21 \) is less than 8 Mbits code symbols. The amount of collected statistics for all points of this graph exceeds \( 2.3 * 10^9 \) bits.

![Figure 2. Performances of error-correcting codes with \( R = 1/2 \) over AWGN channel and FM2.](image-url)

Further, with an insignificant noise level reduction to \( Eb / N0 = 1.5 \) dB, only \( I = 90 \) iterations are needed for the MTD and the delay of the convolutional decoder solution is about 1 Mbits, as shown by the MTD2 graph. And at \( Eb/N0 = 1.8 \) dB an ordinary MTD decoder with 40 iterations and at a
delay of only three times more than the incomparably more complex sequential concatenated scheme of the Viterbi algorithm (VA) with the Reed-Solomon (RS) code decoder. We should remember that this concatenated scheme also has a lower code rate R by ~ 0.6 dB (by 12.5%) than the considered MTD algorithms that further demonstrates the great advantages of algorithms created in accordance with optimization theory.

A detailed comparison of MTD decoders and other basic algorithms for Gaussian channels, which are relatively successfully developed by coding researchers in our country and abroad, shows that no algorithms such as LDPC have even approached the MTD characteristics at Eb / N0 ~ 1.2 dB for the last decade, no turbo or any other ones with reasonable complexity. Their actual characteristics over the past decade have not overcome yet the conventional energy boundary Eb / N0 ~ 1.5 dB, even with concatenated schemes, that at such proximity to the Shannon boundary is a great difference compared to the first MTD curve. It is specified that for these codes "the procedure of forming of code words determined by absence of the ordered structures of generating and checking matrices is difficult" [4]. From our viewpoint, as we have repeatedly pointed out, algorithms for LDPC codes, being iterative, nevertheless do not measure the distance of their decisions to the received message and therefore do not belong to the global search extremum procedures. Therefore, their relatively acceptable efficiency is the result of high computational costs of these algorithms, which however does not provide their good characteristics at R~1/2 in the energy domain of the Gaussian channel less than 1.5 dB. At present, there is no indication that this boundary will be overcome at a reasonable level of LDPC codes decoding complexity.

Symbolic Codes

The symbolic multithreshold decoding (QMTD) implementation is also extremely simple, as in the case of their binary analogs. Strictly speaking, J. Massey dealt with these codes belonging to the class of majority decoded non-binary codes and proved theorems 1–4 concerning them in [3]. However, he very negatively estimated the potential of these codes in Sections 1.2, 6.2, 6.5, 6.6 and 8.2 of his book and has never returned to this subject. Nowadays, there are no any informative studies into the majority decoding of non-binary codes and, especially, publications devoted to the iterative algorithms for these codes.

Let us consider the capabilities of non-binary codes. The Reed-Solomon code (RS) decoder and QMTD characteristics obtained at the code rate R = 1/2 are presented in Fig. 3. The horizontal axis incorporates the symbol error rate calculated for different alphabet sizes q (q = 2^8 = 256 and 2^16 = 65536). The decoder symbol error rate Pd(e) are plotted on the vertical axis for all values of q.

The graph P0 shows the error probability in the q-ary non-binary symmetric channel (qSC). Curve RS2^8 characterizes the possibilities of the algebraic decoders for RS code with (n, k, d) parameters (255, 128, 128), where the size of the symbol corresponds to one byte. Next dashed curve RS-Su2^8 corresponds to the lower estimate of the complex decoder capabilities for the same code, proposed by Sudan. The graph RS2^16 refers to the RS code of length 65536, which else for a long time will be considered as a very difficult one to implement.

As the most important currently applied result, which has a serious ideological support from the OT, the recent achievement of symbolic MTD can be called with a code rate R = 1/2 for q=2^16 of particularly high noise immunity even in the qSC with an error probability p0 = 0.3, as it is shown in Fig.2 for a graph QMTDconv2^16 [5]. This noise level is unattainable at R = 1/2 even for RS codes in the GF(2^16), it is extremely difficult to realize this decoder, and because of the low decoding characteristics it is useless.

As the most important applied result at a special current moment, one can point to the recent achievement of convolutional QMTDs for codes with code rate R=1/2 at q=2^16 the possibility of suboptimal decoding in QSC at error probability P0=0,325, which is illustrated in Fig. 3 by curve "new". The total number of iterations of this convolutional decoder MTD did not exceed I=185. This result is unattainable for decoders of other practically realizable codes with R=1/2.
Conclusion

Our results presents the achievement with simple methods the required reliability of digital streams at the noise levels of the of the main classical channel types close to the capacity of communication channels. The complexity of the procedures of search for global extremum rises with the increasing length of the codes with the theoretically minimum rate, i.e., only linearly. It is the distance (never an achievement!) workspace of the MTD algorithms to the channel capacity discussed above, which follows from the graphs in Fig. 2-3, is especially clear the evidence of absolute success and perceptiveness of created optimization theory.

Thus, the data set out in the article testify to the successful solution of the main scientific and technological problem of all our information digital civilization—the creation extensive classes of simple methods to achieve high reliability of digital information transmission in the closely of the Shannon limit.

References


