Evaluation of computational complexity and shortcomings of non-binary low density decoding algorithms

V V Glotov¹, A V Bashkirov¹, N V Astakhov¹, A A Pirogov¹, S N Panychev²

¹ Voronezh State Technical University, 14, Moscow Ave., Voronezh, 394026, Russian
² State Research and Testing Institute for Technical Information Protection Problems of the Federal Service for Technical and Export Control, 280a, 9 January St., Voronezh, 394020, Russian
E-mail: okipr.vgtu@rambler.ru

Abstract. Operational requirements for processing, receiving and transmitting digital information devices constantly increase, due to the need to attract significant resources, especially intellectual. This is caused by the necessity to perform the tasks that are aimed at improving the efficiency of tools, methods and specific algorithms that implement processing, receiving and transmitting information technologies. One of the most dynamically developing approaches for solving the above problem is the coding theory, in particular noise-resistant coding. As far as the energy costs are concerned, the most effective noise-resistant codes are turbo codes and the codes with a low density of parity checks. The paper reviews the algorithms that allow the decoding of non-binary codes with a low density of parity, as well as the distribution algorithm and its modifications. Their significant drawbacks and major modifications applied to eliminate them are briefly overviewed in the paper; estimates of the computational complexity of the algorithms are given.

1. Introduction

Today, we observe the rapid development of the various digital systems of data transfer, such as space system, satellite system, mobile communication and other. In all the systems similar to each other wireless channels used for data transmission and the channels the transmitted signals are affected by various physical disturbances. As a result, this creates a pretty high probability of errors in the received data. At the same time, for many practical applications a very little percentage of errors within the processed discrete data are permitted. Hence, the problem of provision of reliable digital data transfer along the noisy channels still needs to be resolved.

We provided the following solutions for the anti-noise coding means:
1) The coding for the reliable transmission in the data transfer channels (physical layer of a network).
2) The coding of the feed-back systems (data transmission link layer).
3) The coding of the network transport layer.
4) The coding for the protection from illegal (non-authorized) access (applications’ layer)
5) The coding for compressing the data with losses (‘applications’ layer).
2. Fundamentals and Exploring the importance of the problem

Non-binary Low Density Parity Check codes (LDPC codes) in GF (Galois field) \( d = 2^n \) have evolved from binary LDPC codes, which at present are required by the industrial standards for the channel coding. Efficiency of the codes with a short block length is considerably higher for the non-binary LDPC codes because of higher complexity of decoding. Creating effective hardware for decoder is still a complicated problem. The blocks of multipliers’ computations are used in the majority of the recently suggested ASIC-oriented hardware [1, 3].

LDPC codes belong to a special category of linear block parity-check codes, the matrix \( H \) of which has low density of the units. For the LDPC codes in GF (q) the parity check matrix \( H \) has the elements \( h_{mn} \), determined in GF (q) as \( h_{mn} \in GF(q) \). Let the code word be of \( N \)-length (number of symbols); \( H \) is the matrix of ‘\( M \times N \)’ size, where \( M \) is the number of strings. Every string of \( H \) represents one checking restriction on the input data operation \( x = (x_1, x_2, \ldots, x_N) \), that is \( \sum_{n=1}^{N} h_{mn}x_n = 0 \), for \( m = 1, 2, \ldots, M \).

Let the function \( f_0(x_n) \) be determined as \( f_0(x_n) = -\ln p(x_n/y_n) \), where \( p(x_n/y_n) \) is the conditional distribution of the input symbol of data ‘\( n \)’ at the value \( x_n \), labelled by the output symbol of data ‘\( n \)’ at the value \( y_n \). \( f_0(0) - f_0(x_n) \) is equal to \( \ln p(x_n/y_n)/p(0/y_n) \) – this is the Log Likelihood Ratio (LLR) of the input symbol data ‘\( n \)’ at the value ‘\( x_n \)’ against the value 0.

In these expressions the maximum probability of decoding can be stated as the assignment of optimization with restrictions:

\[
\min_{x_n, x_n \in X} \sum_{n=1}^{N} f_n(x_n) \quad \text{on condition that} \quad Hx^T = 0. \tag{1}
\]

The above-shown function is known as the target function of the decoding of an LDPC code. Identifying the global minimum of a multi-dimensional target function remains the problem of decoding.

Let ‘\( X \)’ be a set of all the variables. Considering ‘\( m \)’ restrictions, \( H_m x^T = 0 \); let \( X_m \) be the subset of all the variables corresponding to nonzero elements in \( H_m \), that is \( X_m \equiv \{ x_n \mid h_{mn} \neq 0 \} \).

Let the function \( f_{X_m}(X_m) \) determined on \( X_m \) as:

\[
f_{X_m}(X_m) = \begin{cases} 0, & \text{if } H_m x^T = 0; \\ \infty, & \text{the rest}. \end{cases}
\]

\( f_{X_m}(X_m) \) be called ‘the restriction function’, representing unspecified ‘\( m \)’ restriction. If the restriction functions are used, the decoding problem (1) can be re-formulated as ‘non-conditional combinatory assignment of optimization by the following target function’:

\[
E(x) = \sum_{m=1}^{M} f_{X_m}(X_m) + \sum_{n=1}^{N} f_n(x_n). \tag{2}
\]

The potential of LDPC codes, developed for finite fields of high order GF (q), is widely applied nowadays. These codes showed better performance than the binary LDPC codes for small and average lengths of the code word. However, the complexity of the decoder is enhanced with the increase of ‘\( q \)’, which limits the possibilities of designing and searching of simplified decoding algorithms. Let’s refer to the following brief review of GF (q) LDPC decoding algorithms, focusing on the matters of complexity.

When directly applied to the GF (q) LDPC codes, the Belief Propagation algorithm (BP algorithm) represents a computational complexity \( O(q^3) \). Hence, in view of \( q \geq 16 \), it results in high complexity of decoding. Nevertheless, as it was suggested in papers [6] and [7], the frequency domain may be considered, if \( q = 2p \). This FFT decoding algorithm, based on the BP, diminishes the complexity \( O \)
This algorithm was also described in the logarithmic domain with the result of the so-called ‘log-BP-FFT’.

Traditionally, an LDPC code is represented by the Tanner-graph. The graphical model serves fine for the understanding of the code structure and decoding algorithm. The Tanner-graph is a two-partite graph with varying junctions (nodes) on one side and restrictions of nodes on the other side. The graph edges are the connections of the check nodes to the varying nodes. The check node is in connection with those varying nodes that are included into the checking programme. In the course of each iteration of the min-sum algorithm, it is informed whether a unit from a varying node reached the check node with subsequent return to the varying nodes from the check nodes [8, 9].

Let N(m) be a set of varying nodes, connected to the check node m. Let M(n) be a set of check nodes, connected to the varying node n. Let the symbol «o» indicate a set of minuses. N(m) \ n means the multitude of varying nodes, excluding the node ‘n’, which are connected to the check node ‘m’. M(n) \ m means the set of control nodes, excluding the check node ‘m’, which are connected to the varying node ‘n’.

Generalization of the min-sum algorithm for the decoding of LDPC codes in GF (q) is elementary. In the iteration ‘k’ let’s label the message, sent from the varying node ‘n’ to the check node ‘m’, as $Z_{nm}^{(k)}(x_n)$. Let’s label the message, sent from the check node ‘m’ to the varying node ‘n’ as $I_{mn}^{(k)}(x_n)$. $Z_{nm}^{(k)}(x_n)$ is the function of the logarithmic likelihood ratio (LLR) from the input symbol ‘n’, having the value $x_n$ in comparison to 0, in reference to the data received by means of the check nodes, excluding the check node ‘m’. Let’s label the message, sent from the check node ‘m’ to the varying node ‘n’ as $I_{mn}^{(k)}(x_n)$. $I_{mn}^{(k)}(x_n)$ is the logarithmic likelihood ratio of the checking performance on the node ‘m’ when the input symbol ‘n’ is fixed on the value 0 in comparison to the value $x_n$ and other symbols are independent from the LLC:

$Z_{nm}^{(k)}(x_n) = Z_{nm}^{(k-1)}(x_n) - I_{mn}^{(k)}(x_n) \ \ n \in M(m) \ \ n$.

The pseudocode of the generalized min-sum decoding algorithm of the LDPC code for GF (q) is set as follows:

**Initialization**

For n = 1, 2, …., N and m = 1, 2,…. M,

$Z_{nm}^{(0)}(x_n) = f_c(x_n)$.

**Iteration (k = 1,2,3, …)**

1) **Horizontal scanning**

Calculation of $L_{mn}^{(k)}(x_n)$ for each $x_n \in GF(q)$,

$L_{mn}^{(k)}(x_n) = \min_{x_m \in \{0,1\}} \sum_{x_m \in \{0,1\}} Z_{nm}^{(k-1)}(x_n)$

$$\sum_{n\in N(m)} h_{mn} x_n = 0,$$

Normalization of $L_{mn}^{(k)}(x_n)$

For each m, and each $n \in N(m)$, $L_{mn}^{(k)}(x_n)$ of $L_{mn}^{(k)}(0)$,

$L_{mn}^{(k)}(x_n) = L_{mn}^{(k)}(x_n) - L_{mn}^{(k)}(0)$.

2) **Vertical scanning**

For n = 1,2,…., N,

$Z_{nm}^{(k)}(x_n) = f_v(x_n) + \sum_{m \in M(n) \ \ m} L_{mn}^{(k)}(x_n)$.

3) **Decoding**
For each symbol, computation of its a posteriori Logarithmic Likelihood ratio (LLR) is performed:

\[ Z_{m}^{(k)}(x_{n}) = f_{m}(x_{n}) + \sum_{n \in R(x_{n})} L_{m}^{(k)}(x_{n}) . \]  

(5)

Subsequently, the original code word \( x^{(k)} \) is evaluated for \( n = 1, 2, \ldots, N \):

\[ x_{n}^{(k)} = \arg \min_{x_{n}} Z_{n}^{(k)}(x_{n}) . \]

If \( H(x^{(i)}) = 0 \) and the number of iterations is beyond a certain value, the iteration is stopped, with the runout \( x^{(k)} \) as the code word being decoded.

The above algorithm \( Z_{mn}^{(k)}(0) - Z_{mn}^{(k)}(x_{n}) \) has a posteriori LLR for the value \( x_{n} \) in the iteration ‘k’.

One of the possible ways of enhancing the efficiency of the generalized min-sum algorithm is to change Equation (4) and Equation (5), as under:

\[ Z_{m}^{(k)}(x_{n}) = f_{m}(x_{n}) + \alpha_{k} \sum_{n \in R(x_{n})} L_{m}^{(k)}(x_{n}) , \]

\[ Z_{n}^{(k)}(x_{n}) = f_{n}(x_{n}) + \alpha_{k} \sum_{m \in R(n)} L_{m}^{(k)}(x_{n}) , \]

where \( \alpha_{k} \) is a scaled constant at the iteration ‘k’, answering to \( 0 < \alpha_{k} < 1 \). In view of these changes, the decoding algorithm is called the normalized min-sum algorithm.

Another possible way of enhancing the efficiency is to change Equations (4) and (5), as under:

\[ Z_{m}^{(k)}(x_{n}) = f_{m}(x_{n}) + \beta_{k} \max_{n \in R(x_{n})} \left( L_{m}^{(k)}(x_{n}) - \beta_{k} \right) , \]

\[ Z_{n}^{(k)}(x_{n}) = f_{n}(x_{n}) + \beta_{k} \max_{n \in R(n)} \left( L_{n}^{(k)}(x_{n}) - \beta_{k} \right) , \]

where \( \beta_{k} \) is the shift (off-set) of the constant in the iteration ‘k’, answering to \( \beta_{k} > 0 \). In view of these changes, the decoding algorithm is called the off-set min-sum algorithm. In order to increase the potential of the decoding power, the scaling coefficient \( \alpha_{k} \) or the permanent off-set \( \beta_{k} \) can be determined experimentally or by the ‘density evolution’ method.

3. Results obtained

The problem of the coding complexity quadratic dependence from the length of the GF(2)-LDPC code and sophistication of hardware implementation is acute enough, however irregular LDPC codes can outdo the turbo codes at approximately equal lengths and rates, in view of sufficiently long blocks. The same noise immunity – at a shorter length of the GF(q)-LDPC code - can be achieved by means of increasing the value ‘q’. [3]. Paper [4] reviews the dependencies of the Bit Error Rate (BER) for irregular LDPC codes and for regular Non-Binary Low Density codes, from the ‘signal-noise’ ratio, as shown in Figure 1.

4. Discussion

Figure 1 shows the dependencies for a binary channel with additive Gaussian white noise for LDPC codes of length 3008, rate 1/2, and indicates the lower margin of spherical package (SP59, [5]). Thus, the perspective of using the Non-Binary LDPC codes (NB-LDPC codes) is related to the serious difficulties in the realization of decoding procedures. Despite this, nowadays a range of algorithms for the decoding of Non-Binary LDPC codes has been developed, some of which may become effective for hardware creation.

Tables 1 and 2. Tabulated values for the number of operations (summations, multiplications, divisions), required for the elementary computation in the bit node (Table 1.) and check node (Table 2.).
Table 1 shows the number of operations required for execution of updating of the varying node for the fixed variable degree of the node, \(d_v = 2\). Special attention is to be paid to the considerable decrease of the complexity of the introduced simplified EMS version in comparison to BP or FFT-BP: only \(n_m(n_m + 2)\). The required maximum number of operations and complements \(n_m\) (at \(n_m << q\)).

Table 2 computes the updates for the check node, which usually represents the basic computational load in LDPC decoders. The number of operations at the initial stage is given for each decoding algorithm.

The lead-tin-base bronze of the BrO10S10 grade (Russian grade acronym) was used as a material for investigation. This bronze contains 10% wt. of lead, 10% wt. of tin and 80% wt. of copper. The multicomponent bronzes under study were melted in the induction high-frequency furnace in crucibles. The crucibles’ material is siliciated graphite. Melting was conducted using the components of technical grade. Cathode copper of the Mk grade (GOST 859-78), sheet lead of the C-2 grade (GOST 3778-77); rod tin of the O1 grade (GOST 860-75) were used as a charge mixture. The phosphorous-copper alloy of the MF1B grade (GOST 4515-93) was used as a deoxidizer. The preliminarily placed in the copper foil powder-modifier was introduced into the melt.

The aluminum oxide powder, being wrapped into the copper foil, was introduced into the bronze melt after its treatment in the copper powder mixture in the ball planetary-type mill. The method of powder treatment is described in [2, 3]. The pouring was realised into the graphite moulds at room temperature. The content of the powder comprised 0.07; 0.15; 0.25; 0.5; 0.75 and 1.5% wt.

**Figure 1.** Dependence of Bit Error Rate from the ‘signal-noise’ ratio for Binary and Non-Binary LDPC codes.
Table 1. Number of Operations for the Elementary Computation in the bit node

| Algorithm | Multiplications | Divisions | Max* | Max | Summations |
|-----------|-----------------|-----------|------|-----|------------|
| BP        | q               | -         | -    | -   | q-1        |
| FFT-BP    | q               | -         | -    | -   | q -1       |
| log-BP    | -               | -         | q-1  | -   | Q          |
| EMS       | -               | -         | -    | nm (2nm) | Nm |

Table 2. Number of Operations for the Elementary Computation in the check node

| Algorithm | Multiplications | Divisions | Max* | Max | Summations |
|-----------|-----------------|-----------|------|-----|------------|
| BP        | $q^2$           | Q         | -    | -   | Q (q-1)    |
| FFT-BP    | $q(dcp + 1)$    | Q         | -    | -   | Dcqp       |
| log-BP    | -               | -         | q(q-1) | -   | $q^2$      |
| EMS       | -               | -         | -    | Nmnop | nm + nop (real) |

5. Conclusion

The comprehensive analysis of decoding algorithms of Non-Binary LDPC codes, presented in this paper, has shown high probability of errors’ correction near the efficiency limit, whereas effective hardware implementations make it possible to perform the correction of LDPC errors with high data throughout in the wire and wireless standards of communication. In fact, as far as the hardware creation is concerned, the most effective and perspective is the Extended Min-Sum algorithm, despite the fact, that it is inferior to the Belief Propagation algorithm in terms of correction ability. However, the gain in computational complexity, as compared to the BP algorithm, is typical for the EMS algorithm only at the restriction length values << q (nop – number of operations required for computation of the max. nm; as a rule, nop = 2nm), and this particular feature also limits the opportunities for its application.

References

[1] Kechiev L N 2007 Proektirovanie pechatnykh plat dlya tsifrovoy bystrodeystvuyushchey apparatury (Moscow: Gruppa IDT)
[2] Surikov V V 2010 Elektromagnitnaya sovmestimost’ priemno-peredayushchikh ustroystv, raspolozhennykh na elementakh konstruktsiy slozhnoy formy (St. Petersburg:Eva)
[3] Knyazev A D 1984 Elementy teorii i praktiki obespecheniya elektromagnitnoy sovmestimosti radioelektronnykh sredstv (Moscow: Radio i syuz)
[4] Hale U K 1980 Frequency assignment. Theory and applications. 68 112
[5] John R B 1990 Electronic System Design: Interference and Noise Control Techniques (Moscow: Mir)
[6] Slivkin V G 2004 Electromagnetic compatibility of electrical equipment of information technologies under the influence of pulsed electromagnetic fields (Samara, SGTU)
[7] Tryapitsyn A V 2004 Development of the methodology for the design of wireless local area networks with EMC (Moscow: Mir)
[8] Williams T E 2004 EMC for Product Designers (Moscow: Publishing house "Technologies")
[9] Habiger E H 1995 Electromagnetic Compatibility. Fundamentals of its provision in technology. (Moscow: Energoatomizdat)