UDC 621.391

COMPARATIVE ANALYSIS OF LDPC AND BCH CODES ERROR-CORRECTING CAPABILITIES

Leonid O. Uryvsky, Serhii O. Osypchuk

Telecommunication Networks Department Institute of Telecommunication Systems National Technical University of Ukraine "KPI" Kyiv, Ukraine

The error-correcting capabilities of regular LDPC (Low Density Parity Check) codes and BCH (Bose-Chaudhuri-Hocquenguem) codes are examined. The qualitative analysis and the quantitative assessment of error-correcting abilities are performed for LDPC codes with code word length n=1000 bits and BCH codes with code word length n=1023 bits. The code rates of LDPC and BCH codes are determined for a known signal to noise ratio in the gaussian channel; detected code rates are optimal for predefined modulation type and required information reliability on the receiver side.

Introduction

Significant interest has raised for LDPC (Low Density Parity Check) codes recently. The importance of LDPC codes is shown by different standards and recommendations, where LDPC codes are used: DVB-S2, IEEE802.16 et al. [1]. Theoreticians and practices in error control coding area renewed a level of interest to LDPC codes over the world. Many scientific publications devoted to LDPC: [2-4] (Great Britain), [5] (USA), [1] (Japan) and others.

LDPC codes are block structured linear divisible codes. The LPDC codes are introduced for the first by R. Gallagher in 1962 [6], but interest was not attracted to them so much at that time. These codes have been forgotten for several tens of years. Here is the next explanation [7] of the reason why LDPC codes exploration was held up after Gallagher's publications and resumed in 1998. Turbo codes were discovered in the middle of 1990 and have iterative decoding procedures with attractive error-correcting characteristics; whereas LDPC codes have iterative decoding procedures as well [8], an interest was aroused for these codes too. It was assumed that LDPC codes stand as well closely to Shannon limit as turbo codes, and this was corroborated in relevant researches [2, 7].

BCH codes (Bose-Choudhury-Hocquenguem), in turn, are one of the best block codes. The characteristics of BCH codes are shown in [9].

The goal of this research is LDPC and BCH codes comparison. Criteria for comparison are the next: identical code word length, equal shift keying manipulation, known channel parameter SNR (Signal to Noise Ratio), same required bit error probability on the receiver end.

Problem statement

The entry parameters for task are below:

– Channel parameter: SNR = 0…14 dB;

– Shift keying manipulation: QPSK;

– Code word length for antinoise coding: n=1000 for LDPC codes and n=1023 for BCH codes;

– Requirement to the bit error reliability on the receiver side: 10^{-6}.

Output parameters are LDPC and BCH coding rates: R_{LDPC} and R_{BCH}. To reach the goal of research, the antinoise code rates R_{LDPC} and R_{BCH} are found to achieve required information reliability on the receiver side if the described entry parameters above are known; given code rate values are compared and the best error-correcting method {LDPC, BCH} on the criterion $\{R_{\text{MAX}}, d_{\text{MAX}}\}$ is chosen. This task can be schematically presented as shown on the Fig. 1.

So, the main task is a search of antinoise code with maximal code rate R and code distance d values, and this is a fundamental problem of coding theory [10].

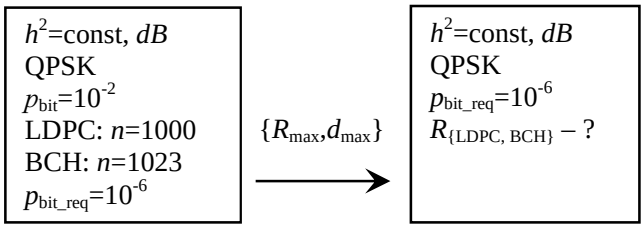

Fig. 1. Statement of the problem

The next subtasks were set up to achieve the goal:

– Development and implementation the search procedure of minimal LDPC code distance when the code length and check matrix parameters are predefined;

– Determination of positions the LDPC and BCH codes points in coordinates $R = f(d/2n)$;

– Definition the maximum antinoise code rate that is able to provide required bit error reliability.

LDPC and BCH codes characteristics

BCH codes are characterized by the possibility to form the antinoise code with predefined error-correcting abilities such as minimal code distance d. The BCH code exists for any values m and $t=(d-1)/2$ with code length $n=2^m-1$ that corrects all combinations of t or less errors number; this code has mt corrective bits in the code word. Thus, the BCH code length can not be chosen randomly and depends from the parameter m; BCH code length always has an odd value. The properties of some BCH codes with parameter $m=10$ and code length $2^{10}-1=1023$ are shown in the Table I.

TABLE I. BCH CODES

n	k	n-k=mt	t	R
1023	1003	20	2	0.98
1023	993	30	3	0.97
1023	983	40	4	0.96
1023	973	50	5	0.95
		. . .		
1023	783	240	24	0.77
1023	773	250	25	0.76
1023	763	260	26	0.75
1023	753	270	27	0.74
		. . .		
1023	243	780	78	0.24
1023	233	790	79	0.23
1023	223	800	80	0.22
1023	213	810	81	0.21
1023	203	820	82	0.20

As follows from example, BCH code with code length $n=1023$ can be formed with code rate step 0.01. Herewith the BCH code rate decreases linearly whereas error-correcting capability increases:

$$R = 1 - 0{,}0097t \text{ , or} \tag{1}$$

$$t = \frac{1-R}{0{,}0098} \tag{2}$$

Inaccuracy of (1) and (2) is lower than 2.2%.

Let's turn to the LDPC codes characteristics. LDPC codes are not analytical and this is one of the differences from BCH codes. LDPC code properties cannot be defined analytically as a result of this.

A lot of LDPC code modifications exist, and most of them are not explored in full. Together with this, all LDPC codes are classified by two groups: regular and non-regular. These two groups are differentiated by the check matrix construction that used for encoding and decoding code words. Non-regular LDPC codes are built based on regular LDPC codes [8].

It is shown in [11] that regular LDPC codes more often demonstrate better characteristics than non-regular LDPC codes. It's shown in [2] that regular LDPC codes have better properties in Gaussian channel than non-regular LDPC codes. Together with this, the conditions are presented in [5] when non-regular LDPC codes have better characteristics actually. Thereby, either regular LDPC codes or non-regular LDPC codes are entitled to existence in the theory and practice of antinoise coding.

Forming of regular LDPC codes is defined in consecutive order. Regular LDPC code with a code length n forms based on the check matrix H. Check matrix H has a fixed value of "ones" in the matrix row W_r and a fixed value of "zeros" in the column W_c [2]. It's considered that check matrix H has a low density of "ones" when density of "ones" in check matrix H is less than 50% of all the check matrix elements.

The LDPC code error-correcting ability is specified based on specific parameters of check matrix H: n, W_r, W_c. At the same time, positions of "ones" in the check matrix H are based on random permutations the basic sub matrix H_1 columns. Each column of basic sub matrix H_1 includes only solus "one". The regular LDPC code rate is defined as a function of check matrix H parameters (3):

$$R = \frac{n - \left(n \cdot \frac{W_c}{W_r} - (W_c - 1) \right)}{n} = 1 - \frac{W_c}{W_r} + \frac{W_c - 1}{n} \tag{3}$$

Withal, LDPC codes check matrices H with the same matrix parameters, but different positions of "ones" in check matrix, can generate antinoise codes with different code distances and respectively different error-correcting abilities. Hence the task raises to search the best check matrix H with known parameters n, W_r, W_c by the criterion of maximal error-correcting ability of LDPC code: $t_{\max} \le (d_{\max} - 2)/2$.

LDPC code check matrix H can be represented as:

$$H = \begin{bmatrix} H_1 \\ \hline \pi_1(H_1) \\ \hline \vdots \\ \hline \pi_{W_C - 1}(H_1) \end{bmatrix}, \tag{4}$$

Where H_1 – basic submatrix, $\pi_i(H_1)$ – submatrices are generated by random rearrangement of basic submatrix columns H_1, $i=1,2,\ldots,W_c-1$.

Check matrix H can be transformed into the matrix form:

$$H = [A \mid I_{n-k}], \tag{5}$$

Where A – some non-sparse fixed matrix with "zeros", "ones" and dimensions $((n-k)\times k)$; I_{n-k} – identity matrix with dimensions $(n-k)\times(n-k)$. The generation matrix G can be represented as:

$$G=\left[I_k \mid -A^T\right] \quad (6)$$

If the check matrix H is presented as (5), then the generation matrix G (6) can be simply given from the matrix H by transformation.

The matrix G is also named as generative matrix so far as code words that can be represented as linear combinations of matrix G rows. The matrices H and G are related as [2]:

$$GH^T=0,\ HG^T=0 \quad (7)$$

Code distance d for regular LDPC code is defined as the least columns number of check matrix H that overall gives 0. The analytical description for LDPC code error-correcting abilities doesn't exist so far; however, the forward and backward theorems exist for LDPC code distance [10].

Theorem 1. If any $l \leqslant d-1$ columns of linear code check matrix H are linearly independent, then a minimal code distance will be at least d. If d linearly independent columns are found, then minimal code distance is equal d.

Theorem 2. If minimal code distance is equal d, then any $l \leqslant d-1$ columns of check matrix H are linearly independent and exactly d linearly independent columns exist.

Thus, it's possible to conclude from theorems 1 and 2 that LDPC code distance d can be identified from matrices H and G as the next: the d value equals the least columns number of matrix H that sum up to 0; the d value equals the least row weight (the number of ones in the row) in matrix G.

The LDPC codes error-correcting ability is researched in current work based on the described properties of check and generating matrices. The same LDPC code word length n=1000 and different check matrix H parameters result in different antinoise code rates R and different numbers of corrected errors per code words respectively. Given results in experiments are compared with error-correcting abilities of BCH codes with code word length n=1023 bits.

LDPC codes error-correcting ability

Known methods for LDPC code distance d search complexity grows exponentially as is shown in [2]. Known search methods give a possibility to define the code distance value for codes with code length less that n<1000 bits in terms of spending sensible time resources for a search. The LDPC code error-correcting value can be found from matrices H and G by search, but the given code distance value can be not the best for used LDPC matrix parameters.

The study of LDPC code error-correcting abilities with code length n=1000 bits is performed in this work based on the theorems 1 and 2. This idea is shown on Fig. 2.

The line #1 (Fig. 2) indicates the code distance d search complexity when use only theorem 1 (by using matrix H); the line #2 designates a code distance d search complexity when use only the theorem 2 (by using matrix G). The "complexity" term means in this context the number of elementary operations to execute in the specific time point and save the same progress of the end results receiving.

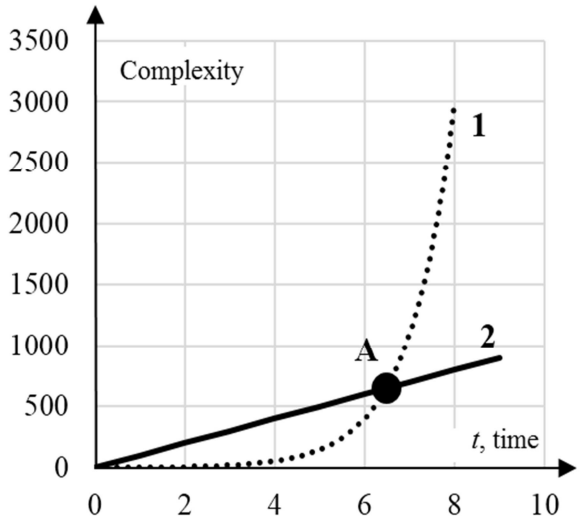

Fig. 2. A graphical representation of application the theorems 1, 2 for code distance search process

The point A (Fig. 2) indicates the moment when it's better to use theorem 1 before that, but it's better to use theorem 2 after point A. The point A corresponds the case when code distance d = 6 (t = 2) is found by theorem 1. As soon as the matrix H has d = 6, then search by theorem 1 stops and further search of code distance d continues by reduction the matrix H to matrix G in canonical form (5). Thus, the minimal time for search LDPC code distance spends if combine theorems 1, 2 for the search process.

The described algorithm above for LDPC code distance search is implemented on Java language. LDPC code distance results for n=1000 are obtained from set of numerical experiments performed on high performance computing cluster in NTUU "KPI". Matrix H and found LDPC code error-correcting parameters are presented in Table II.

TABLE II. GIVEN PARAMETERS OF LDPC CODES

n	Wr	Wc	k	R	d	t
1000	100	10	909	0.91	22	10
1000	100	20	819	0.82	40	19
1000	100	30	729	0.73	64	31
1000	100	40	639	0.64	98	48
1000	100	50	549	0.55	138	68

LDPC and BCH codes comparison

The method for search the best antinoise block code by criterion of maximal approach to the Shannon limit is described in [9]. This method implies the block code selection with using up-to-date theory of antinoise coding. This method is used for calculation and error-correcting abilities comparison of LDPC and BCH codes. Regarding the method [9] and problem statement (Fig. 1), the next factors can be noted: 1) if the manipulation QPSK is used, then an initial bit error probability $p_{bit}=10^{-2}$ is reached when the signal to noise ratio in the channel is $h^2=7.3$ dB; 2) if antinoise block code with code length $n=1000$ bits is used and required reliability is $p_{bit\_req}=10^{-6}$, then it's needed to correct up to $t=28$ errors [9]. Only in this case the required reliability $p_{bit\_req}=10^{-6}$ can be achieved on the receiver side; 3) to satisfy the required reliability $p_{bit\_req}=10^{-6}$, the value $d/2n$ for antinoise code should meet 0.03.

The limit conditions of antinoise codes existence with some error-correcting abilities are described by Plotkin limit [10]. A sufficient condition for antinoise codes with specific error-correcting abilities is defined by the Varshamov-Gilbert limit (VG). Thereby, the Plotkin and VG criteria provides an opportunity to compare different error-correcting block codes in the same relative coordinates $R = f(d/2n)$ for assessment the error-correcting capabilities.

The dependency $R = f(d/2n)$ is shown on the Fig. 3. The Plotkin and VG limits are shown in these coordinates. The positions of some BCH (Table I) and given experimentally LDPC codes (Table II) are plotted on Fig. 3 with code rates 0,55…0.9. If take into account the code length $n \sim 1000$ bits and set the value $d/2n=0.03$, then the triangle between Plotkin and VG limits shows the shaded area (Fig. 3) which outlines the region of antinoise codes parameters that can provide expected reliability $p_{bit\_req}=10^{-6}$ [9]. If compare the characteristics of BCH codes with $n=1023$ bits and LDPC codes with $n=1000$ bits, then it's possible to say that the next code rates fit the ratio $d/2n=0.03$: $R_{BCH}=0.7$ and $R_{LDPC}=0.73$. If $R_{BCH}=R_{LDPC}=0,55$, then $d/2n_{BCH}=0,05$ a nd $d/2n_{LDPC}=0,07$. The above two instances demonstrate a better correcting capabilities of LDPC codes in comparison with BCH codes ($R_{LDPC}>R_{BCH}$ if $d/2n_{LDPC}=d/2n_{BCH}$=const; or $d/2n_{LDPC}>d/2n_{BCH}$ when $R_{LDPC}=R_{BCH}$; or $d_{LDPC}>d_{BCH}$ when n=const).

If continuously change the parameter h^2, then it's possible to get dependency $R=f(h^2)$ (Fig. 4). Both Plotkin and VG limits are stood below the Shannon limit in coordinates $R=f(h^2)$. Consequently, if channel parameter h^2, current bit error probability p_{bit}, required reliability p_{bit_req} are known, then it's not possible to come to Shannon limit nearer, than it's defined by Plotkin limit.

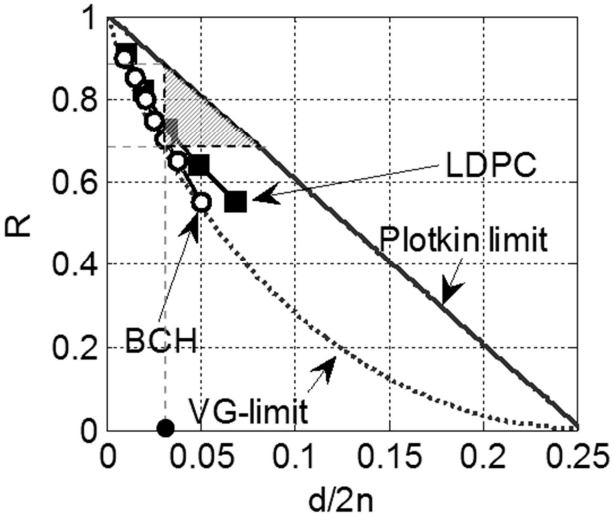

Fig. 3. BCH (n=1023) and LDPC (n=1000)

Specified above conditions give an opportunity to choose the antinoise code that lies to Shannon limit closely as much as possible. The LDPC and BCH codes positions in coordinates $R = f(h^2)$ are shown on Fig. 4.

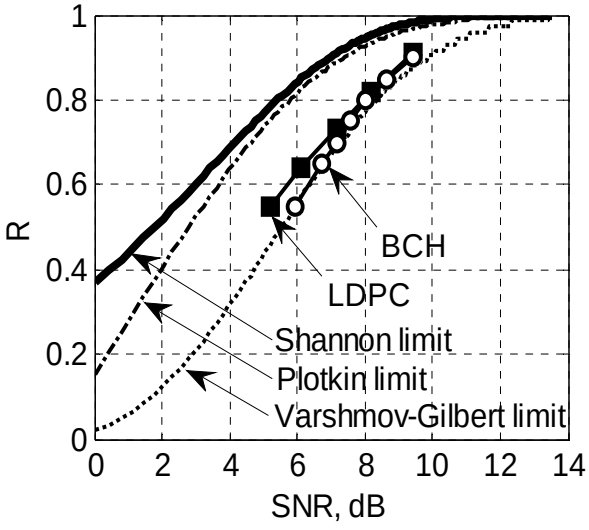

Fig. 4. LDPC (n=1000) and BCH (n=1023) codes

As shown on Fig. 4, LDPC codes stand a little bit closely to Shannon limit than BCH codes. This behavior takes a place more and more if LDPC code rate drops down: $R<0.7$. If $R<0.7$, then LDPC code is preferable when choose between LDPC and BCH.

The indisputable advantage of LDPC code is a possibility to increase the code word length n right up to tens of thousands bits. This explained by relatively simple methods of coding and decoding. Together with that, the advantage of BCH code is the opportunity to define code parameters analytically and choose appropriate code with needed parameters (e.g., it's possible to choose the BCH code rate with a step 0.01 for code length n=1023 bits) to meet the requirements of errors correcting regarding the method described in [9].

Conclusions

The procedure complexity of the LDPC check matrix H searching with good error-correcting ability grows exponentially with increasing a code word length.

There is no need for BCH codes to perform the search matrix procedure because of the nature of encoding/decoding processes. This is an advantage of BCH codes.

Research showed that LDPC codes can be characterized as antinoise codes with good error-correction properties. Relative number of corrected errors per code word is almost the same for LDPC (n=1000) and BCH (n=1023) codes. LDPC codes have a little bit better error-correcting abilities than BCH codes have if code rate $R<0.7$ (it's implied that other parameters like code length, signal to noise ratio, manipulation method, required reliability are the same for LDPC and BCH).

The coded rates are obtained for LDPC (n=1000) and BCH codes (n=1023) for gaussian channel when signal to noise value is known. Given code rates $R_{BCH}=0.7$ и $R_{LDPC}=0.73$ notices that it's possible to use both LDPC and BCH codes with a specific manipulation type to satisfy required information reliability. According to numerical LDPC and BCH code rates values, LDPC code can be recommended as more effective if signal to noise values are bigger than 7 dB. If signal to noise values are smaller than 7 dB, then LDPC and BCH codes can be used pari passu. These recommendations are reasonable for manipulation QPSK, code word length 1000 bits and required information reliability 10^{-6}.

The LDPC code word length can reach tens of thousands. This is possible because of relatively simple code words encoding/decoding procedures, and this is an advantage of LDPC codes. As opposed to LDPC, the BCH codes have more complex encoding/decoding procedures. As a result of this, BCH codes with long code words $n>1000$ are less practical than LDPC codes, or they are technically complicated with realization.

References

1. T. Ohtsuki, "LDPC codes in communications and broadcasting," IEIC Trans. Commun., vol. 90-B, no. 3, pp. 440–453, March 2007.
2. D. MacKay, Information Theory, Inference, and Learning Algorithms. Cambridge University Press, 2003.
3. D. MacKay, "Good error-correcting codes based on very sparse matrices," IEEE Trans. Inf. Theory, vol. 45, no. 2, pp. 339–431, March 1999.
4. D. MacKay, R. Neal, "Near Shannon limit performance of low density parity check codes," Electron. Lett., vol. 32, no. 18, pp. 1645–1646, August 1996.
5. T. Tian, C. Jones, J. Villasenor, R. Wesel, "Construction of irregular LDPC codes with low error floors", Communications, ICC '03, IEEE International Conference, vol. 5, pp. 3125–3129, May 2003.
6. R. Gallager, Low-Density Parity-Check Codes. MIT Press, 1963.
7. V.Vargauzin, "Nearby the Shannon limit," Telemultimedia Journal, pp. 3–10, 2005. [Online]. Available: http://www.telemultimedia.ru/pdf/shennon.pdf
8. M. Luby, M. Mitzenmacher, A. Shokrollahi, D. Spielman, "Improved low-density parity-check codes using irregular graphs and belief propagation," SRC Technical Note, 9 p., 1998.
9. L. Uryvsky, K. Prokopenko, A. Pieshkin, "Noise combating codes with maximal approximation to the Shannon limit," Telecommunication Sciences, vol. 2, no. 1, pp. 41–46, January-June 2011. [Online] Available: http://www.its.kpi.ua/telesc/TS/Telecommunication%20Sciences%20N.1%202011.pdf
10. N. Sloane, F. MacWilliams, The Theory Of Error-Correcting Codes. Bell Laboratories, Amsterdam, North-Holland, 1977.
11. S. Miyamoto, K. Kasai, K. Sakaniva, "Sufficient conditions for a regular LDPC code better than an irregular LDPC code," IEICE Trans. Fundamentals, vol. E90–A, no. 2, pp. 531–534, February 2007.

Received in final form April 19, 2014