Brief Article

A New Decoding Algorithm based on Equivalent Parity Check Matrix for LDPC Codes

Nguyen Tung Hung

Telecommunication University, Nhatrang - Khanh Hoa, Vietnam

Correspondence: Nguyen Tung Hung, tunghungus@yahoo.com

Manuscript communication: received 21 April 2013, accepted 25 June 2013

Abstract– **The article introduces a new LDPC decoding algorithm based on Equivalent Parity Check Matrix. Simulation results show that the new LDPC decoding algorithm can improve LDPC decoding performance. Compared to some other improvements, the new LDPC decoding algorithm, which is simpler, can detect errors and be applied to LDPC codes for great-length LDPC codes.**

Keywords– **Equivalent Parity Check Matrix, soft syndrome, iterative decoding algorithm.**

1 Introduction

Belief Propagation Algorithm (BPA) decoding algorithm for short or medium length low-density parity-check (LDPC) codes [1] is affected by short cycles in the parity check matrix H, so it does not achieve the performance of Maximum Likelihood (ML) decoding. Several study results publicized at [2, 3] with BPA-OSD (Ordered Statistic Decoding) algorithm can considerably improve the quality of LDPC codes. However, this algorithm is quite complex and difficult to apply to great-length LDPC codes. In this article, we introduce the concept of equivalent parity check matrix and soft syndrome to build a new decoding algorithm called Belief Propagation Algorithm based on Equivalent parity check matrix H (BPA-EH) with performance to reach Union Bound (UB) – UB is used to estimate of ML decoding performance in high signal noise ratio region. New decoding algorithm BPA-EH is much simpler than a decoding algorithm BPA-OSD and it can be applied to great-length LDPC codes.

2 Low-Density Parity-Check Codes

Assume a binary (n, k) LDPC code with length n and dimension k, then parity check matrix is $H_{m\times n}$, where $m = n - k$ is number of check sums. Information bits $u = u_1, u_2, \ldots, u_k$ are encoded into a codeword $Y = y_1, y_2, \ldots, y_n$, then modulated and transmitted through channel. The input of the BPA decoder is Log Likelihood Ratio (LLR):

$$L(\bar{y}_i) = \log \frac{\Pr(\bar{y}_i = 0\,|r)}{\Pr(\bar{y}_i = 1\,|r)} \tag{1}$$

where r is the set of symbols acquired from channel and $\Pr(\bar{y}_i = 0\,|r)$ is the conditional probability. Normally, the matrix H is a sparse matrix with a small number of values "1" in each row and each column. The matrix of LDPC codes can also be described by Tanner graph [4] with bit nodes $v_1, v_2, \ldots, v_n$ and check nodes $s_1, s_2, \ldots, s_m$. If value "1" is available at each position of the matrix, then there is a connection between bit nodes and check nodes. A BPA algorithm [1, 5, 6] is an iterative decoding algorithm with two main steps: 1) make calculation in rows to update information for all check nodes and send information from check nodes to bit nodes, 2) make calculation in columns to update information for bit nodes and send information from bit nodes to check nodes. The output of the BPA decoder is LLR of bits $L(\bar{y}_{i=1,2\ldots,n})$, which is used for hard decision to become a codeword $\bar{Y} = (\bar{y}_1, \bar{y}_2, \ldots, \bar{y}_n)$. If syndrome s of I^{th} iteration:

$$s = \bar{Y}.H^T = [0, 0, \ldots, 0] \tag{2}$$

then stop iterative decoding. The process is repeated until the number of times of iteration I reaches $I_{\max}$. Next, we will study LDPC codes with the code rate $R = 1/2$: C_1: 96.48.3.964 with size (48,96), C_2: 252.252.3.252(252,504), C_3: 504.504.3.504(504,1008), and C_4:4000.2000.3.243(2000,4000), which are introduced at [7]. The maximum number of iteration is $I_{\max} = 100$. Suppose that modulation is ideal BPSK and Additive White Gaussian Noise (AWGN) memoryless channel has spectral density $N_0/2$

3 Definition of Equivalent Parity Check Matrix and Soft Syndrome

Definition 1: An Equivalent Parity Check Matrix (H_e) of the matrix H is a matrix that satisfies the equation:

$$Y.{H_e}^T = [0, 0, \ldots, 0],\ (\forall Y, H_e \neq H) \tag{3}$$

From the theory of linear codes,

$$Y.H^T = [0, 0, \ldots, 0] \tag{4}$$

is a set of linear equations. As a result, if one of its rows is replaced with a sum of two other rows, then a new set of equations are still satisfied. Accordingly, the matrix H_e can be created from the matrix H. To ensure the sparse property of the matrix H_e, we only consider the case in which the row $r(a)$ of the matrix $H(a = 1, 2 \ldots, m)$ is replaced with the sum of modulo 2 of rows $r(b)$ and $r(c)$:

$$H_e = H \Big|_{r(a)=r(b)\oplus r(c), a\neq b\neq c} \tag{5}$$

Definition 2: Soft Syndrome (SS) $L(s_{i=1,2\ldots,m})$ is defined as LLR of check nodes $s_{i=1,2\ldots,m}$ with:

$$L(s_{i=1,2\ldots,m}) = \log \frac{\Pr\left(s_i = 1 \,|L\left(\bar{y}_{j=1,2\ldots n}\right)\right)}{\Pr\left(s_i = 0 \,|L\left(\bar{y}_{j=1,2\ldots n}\right)\right)} \tag{6}$$

We have an equation:

$$s_i = \sum_{\oplus} \left(\bar{y}_j \oplus H\left(i, j\right)\right),\ j \in V_i,\ i = 1, \ldots, m \tag{7}$$

where V_i is a set of edges from bit nodes to check nodes in the Tanner graph (the positions at which the value of the row i of the matrix H is "1") and the operation $\oplus$ is operator of modulo 2. From algebraic studies of LLR at [8, 9], we have:

$$\begin{aligned} L(s_i) &= \log \frac{\prod\limits_{j\in V_i}\left(e^{L(\bar{y}_j)}+1\right)+\prod\limits_{j\in V_i}\left(e^{L(\bar{y}_j)}-1\right)}{\prod\limits_{j\in V_i}\left(e^{L(\bar{y}_j)}+1\right)-\prod\limits_{j\in V_i}\left(e^{L(\bar{y}_j)}-1\right)} \\ &\approx \prod_{j\in V_i} sign\left(L(\bar{y}_j)\right) \min_{j\in V_i} \left|L(\bar{y}_j)\right| \end{aligned} \tag{8}$$

4 Proposed Decoding Algorithm

The matrix H_e satisfies a condition that it is a check matrix for LDPC codes and a sparse matrix with the number of the values "1" only increasing at the row a is not considerable, so it can be used to decode LDPC. A new LDPC decoding algorithm includes two following stages:

Stage 1: Decoding LDPC with the input (1) by BPA algorithm with a regular check matrix H. Similar to BPA decoding, check the condition at each time of iteration is

$$\bar{Y}_1.H^T = [0, 0, \ldots, 0] \tag{9}$$

If (9) satisfied, stop iterative decoding and give a codeword $\bar{Y}_1$. If (9) not satisfied, perform the stage 2.

Stage 2: Re-decoding BPA with the input 1 by equivalent parity check matrix H_e At each re-decoding γ, the check condition is

$$\bar{Y}_2.{H_e}^T = [0, 0, \ldots, 0] \tag{10}$$

where $\bar{Y}_2$ is a hard decision codeword according to the matrix H_e. Combine both decoding stage, we have LLR:

$$\bar{L}(\bar{y}_{i=1,2\ldots,n}) = L_1(\bar{y}_{i=1,2\ldots,n}) + L_2^{\gamma}(\bar{y}_{i=1,2,\ldots,n}) \tag{11}$$

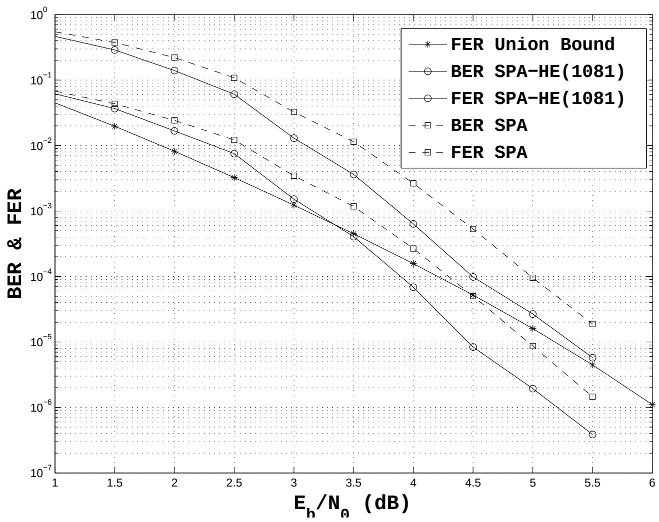

Figure 1. BER and FER of codes C_1

where $L_1(\bar{y}_{i=1,2,\ldots,n})$ is LLR of the stage 1, $L_2^{\gamma}(\bar{y}_{i=1,2,\ldots,n})$ is LLR of the stage 2 at re-decoding γ, if (10) is not satisfied, then check:

$$\bar{Y}_3.{H_e}^T = [0, 0, \ldots, 0] \tag{12}$$

where $\bar{Y}_3$ is hard decision according to $\bar{L}(y_{i=1,2,\ldots,n})$.

If the decoded codeword is valid, then get out the stage 2 and give a codeword $\bar{Y}_2$ or $\bar{Y}_3$. If (9), (10) and (12) are not satisfied, then keep re-decoding other matrices H_e until $\gamma = \gamma_{\max}$. This algorithm is called BPA-EH (BPA based on Equivalent H). For a matrix H with the size $m \times n$, there will be $m \times \binom{m-1}{2}$ matrices H_e, so it requires method to select a matrix H_e, which provides re-decoding first to reduce the average number of times of re-decoding.

Experimental results shows that the average number of times of re-decoding can be reduced if select $r(a)$, $r(b)$ and $r(c)$ based on the ascending order of absolute values of $L_1(s_{i=1,2,\ldots,m})$.

We propose a method to select $r(a)$, $r(b)$ and $r(c)$ as follows: After the stage 1 is conducted, the value of $L_1(s_{i=1,2,\ldots,m})$ will be calculated and $r(a)$, $r(c)$ are selected based on the ascending order of $|L_1(s_i)|$, $r(b)$ is selected based on the descending order of $|L_1(s_i)|$, and $a \neq b \neq c$.

5 The Performance of BPA-EH

Figure 1 and 2 show Monte-Carlo simulation results of Bit Error Ratio (BER) and Frame Error Rate (FER) of BPA and BPA-EH for codes C_1 and C_2. In this case, the maximum number of times of re-decoding $\gamma_{\max} = \binom{m-1}{2} = (m-1) \times (m-2)/2$ Figure 1 shows the performance of BPA-EH is 0.5 dB better than that of BPA at error ratio region of BER=10^{-5} for the code C_1. Figure 2 shows the performance of BPA-EH can be improved up to 0.8 dB at error ratio region of BER=10^{-7}

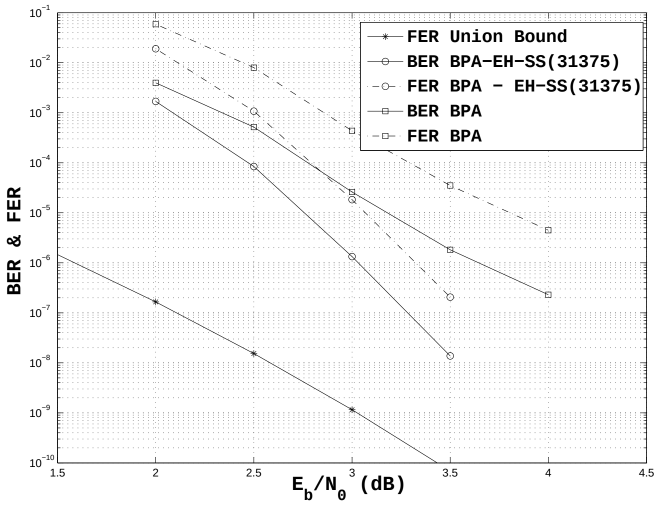

Figure 2. BER and FER of code C_2.

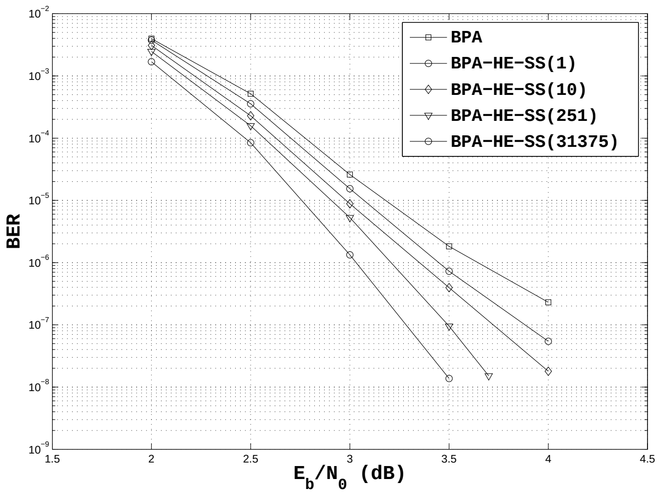

Figure 3. BER of code C_2 with different $\gamma_{\max}$

for the code C_2.

$$\mathrm{P_e} < \sum_{\mathrm{d=d_{min}}} aQ\left(\sqrt{2dRE_b/N_0}\right), \quad Q(x) = \frac{1}{2}erfc\left(\frac{x}{\sqrt{2}}\right) \tag{13}$$

where a is the number of codewords with distance d and $d_{\min}$ which is a minimum distance. Distance spectrum of LDPC codes is calculated as (10) for C_1 is $a = [2,0,9,0,42,0,470]$, $d_{\min} = 6$. It means code C_1 has 2 codewords with the minimum distance $d_{\min} = 6$, 9 codewords with the distance $d_{\min} = 8$, 42 codewords with the distance $d_{\min} = 10$,... Distance spectrum of code C_2 is $a = [2,0,22,0,117,0,481]$ with $d_{\min} = 20$.

Simulation results in the Figures 1 and 2 show that the performance of decoding BPA-EH can reach the performance of decoding ML when the codeword length is short. Figure 3 shows the performance of BPA-EH of code C_2 with the maximum number of times of re-decoding in the stage 2 is $\gamma_{\max} = 1, 10, 251, 31375$. It is found out that BER and FER will reduce if increase $\gamma_{\max}$. Specifically, in Figure 3, the BPA-EH with $\gamma_{\max} = 1$ (one time of re-decoding) achieves 0.2dB at BER=10^{-7}. While the BPA-EH with $\gamma_{\max} = 10$, $\gamma_{\max} = 251$ and $\gamma_{\max} = 31375$ outperform the BPA by 0.4dB, 0.6dB and 0.8dB, respectively.

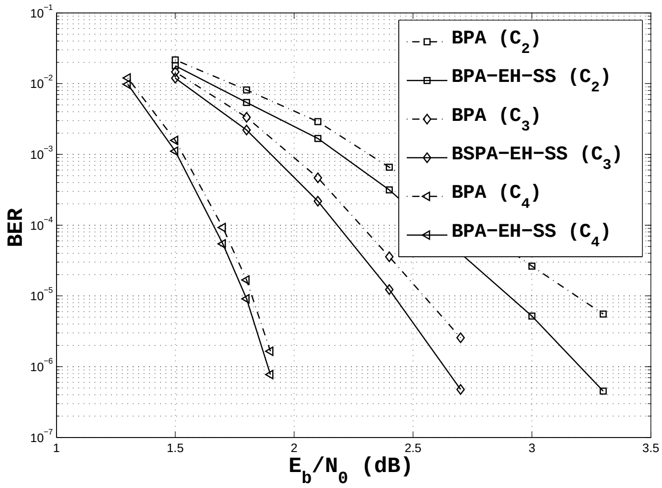

Figure 4. BER of codes C_2, C_3, C_4 with $\gamma_{\max} = 50$

Figure 4 shows the performance of C_2, C_3, C_4 with $\gamma_{\max} = 50$. The BER of BPA-EH can increase considerably for codes with medium and great length. For a set of codes with great length C_3, C_4, it requires to increase $\gamma_{\max}$ to reach an effective gain.

6 Compare the Complexity and Performance of BPA-EH and BPA-OSD

To bridge the gap between BPA and ML decodings for short or medium length LDPC codes, a reliability-based order statistic decoding (OSD) was proposed to combine with the BPA decoding [2, 3]. For such a BPA-OSD reprocessing strategy, if no valid codeword is found at some iteration of the BPA decoding (stage 1), the delivered reliability information is used as the input to the OSD (stage 2). In the stage 2, the OSD performs a Gaussian estimation on the generator matrix. Next, re-encode all the codewords with the total number of error bits from 1 to p based on systematic form of G, and compute the decoding metric associated with each constructed codeword. Select the most likely codeword among the $\sum_{\ell=0}^{p}\binom{k}{\ell}$ constructed candidate codewords.

The BPA-OSD decoder is quite complex. According to [2, 3], the binary operations for Gaussian elimination is of the order $O\left(n^3\right)$ the integer and binary operations for each phase ℓ $(1 \leq \ell \leq p)$ of order-p OSD is $O\left(n^{\ell+1}\right)$.

As a result, the length of n is large and the complexity increases by the exponential function of n, so it is too complex to be implemented.

The difference between an algorithm BPA-EH and an algorithm BPA-OSD is that we use the re-decoding technique. The matrix H_e is created from the matrix H, which is also a sparse matrix. Therefore, similar to the algorithm BPA, the complexity of an algorithm BPA-EH increases by the function $\gamma_{\max}O\left(n\right)$

Besides, the BPA-EH algorithm can check and detect errors, then early stop re-decoding in the stage 2, so the

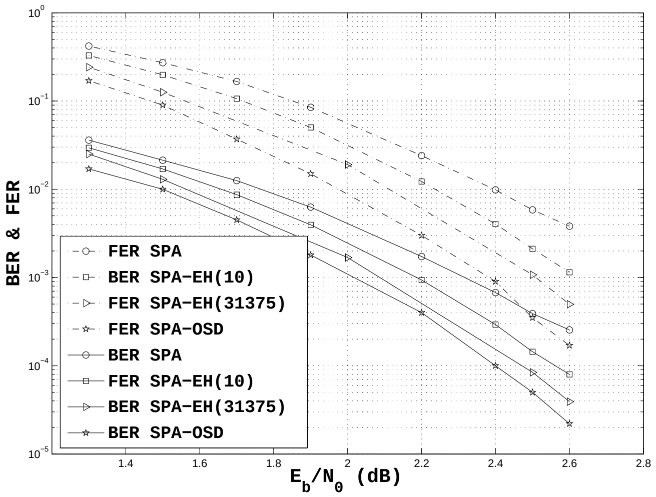

Figure 5. Compare BPA-EH with BPA and BPA-OSD of C_2

real complexity is only the function $\gamma_a O(n)$ of which γ_a is the average number of times of re-decoding.

On the other hand, the BPA-EH algorithm is flexible, which enables to freely adjust γ_a to improve the quality at given E_b/N_0. Besides, the BPA-EH algorithm can early stop re-decoding in the stage 2; meanwhile the algorithm BPA-OSD always has to perform to the end of Gaussian estimation and re-encoding. As a result, the decoder BPA-EH is simpler and more flexible than a BPA-OSD algorithm.

In addition, the BPA-OSD algorithm has no property to detect errors because its output is always a valid codeword; meanwhile the algorithm BPA-EH can still detect errors and be convenient to be applied to the Automatic Repeat Request (ARQ) system. The comparison of performance of the BPA-EH and the BPA-OSD for C_2 is shown in Figure 5. As seen in the Figure 5, the decoding performance of BPA-EH(251) and that of BPA-EH(31375) is only about 0.2dB and 0.1dB respectively lower than that of BPA-OSD.

7 Conclusion

The article proposes a new LDPC decoding algorithm, which enables to improve the performance of LPDC decoding. This new decoding BPA-EH algorithm is based on definitions of equivalent check matrix and Soft Syndrome.

From mathematical analyses of Soft Syndrome related to error events, we propose a method to create equivalent check matrix based on the order of Soft Syndrome, which enables to reduce the number of times of re-decoding.

The simulation results show the performance of an algorithm BPA-EH can be close to the optimal decoding quality ML for LDPC codes with short-length codeword. Compared to regular BPA algorithms, an BPA-EH algorithm can considerably improve the performance at low error ratio region with acceptable complexity.

A BPA-EH decoding algorithm with complexity is a 1st-grade linear function with the length of codewords, so it can be used for LDPC codes with great lengths. Compared to other improvements of LDPC decoding such as a BPA-OSD algorithm, a BPA-EH algorithm is simpler and more flexible, but still can ensure an important function of LDPC codes, which is to detect errors after decoding.

In this article, we only propose a method to replace a row of matrix H with the sum of its two other rows while there are many other ways to create matrix H_e Our suggested way to select a, b, c is not optimal yet. There must be a better method so as to reduce the number of times of re-decoding and that is our direction of further study.

References

[1] R. Gallager, "Low-density parity-check codes," *IRE Transactions on Information Theory*, vol. 8, no. 1, pp. 21–28, 1962.
[2] M. Fossorier, "Iterative reliability based decoding of ldpc codes," in *IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2001, p. 233.
[3] G. Li and G. Feng, "Generalised reliability-based syndrome decoding of ldpc codes," *European Transactions on Telecommunications*, vol. 19, no. 8, pp. 873–877, 2008.
[4] R. Tanner, "A recursive approach to low complexity codes," *IEEE Transactions on Information Theory*, vol. 27, no. 5, pp. 533–547, 1981.
[5] M. P. Fossorier, M. Mihaljevic, and H. Imai, "Reduced complexity iterative decoding of low-density parity check codes based on belief propagation," *IEEE Transactions on Communications*, vol. 47, no. 5, pp. 673–680, 1999.
[6] D. J. MacKay and R. M. Neal, "Near shannon limit performance of low density parity check codes," *Electronics letters*, vol. 32, no. 18, p. 1645, 1996.
[7] D. J. MacKay, "Encyclopedia of sparse graph codes," 2005.
[8] D. Declercq and M. Fossorier, "Improved impulse method to evaluate the low weight profile of sparse binary linear codes," in *IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2008, pp. 1963–1967.
[9] G. Battail, "Building long codes by combination of simple ones, thanks to weighted-output decoding," *Proc, URSI-ISSSE*, pp. 634–637, 1989.