

Improved Perturbation Method for Decoding of LDPC Aided by CRC

Si Shu, Daiming Qu[#]

Department of Electronics and Information Engineering, Huazhong University of Science and Technology, Wuhan 430074, China

[#]Email: qudaiming@mail.hust.edu.cn

Abstract

In this paper, a fresh belief propagation (BP) decoding algorithm is proposed. The proposed decoding algorithm with improved perturbation method is designed for short length low density parity-check (LDPC) codes aided by cyclic redundancy check (CRC). In the proposed algorithm corresponding to path size L , L decoding paths are considered concurrently. Then, a single codeword is selected according to the checking results of CRC. Simulation results show that the modified CRC-aided decoding scheme can enhance the error-correcting performance of short LDPC codes effectively.

Keywords: Low Density Parity-check Codes; Belief Propagation; Cyclic Redundancy Check; Perturbation

1 INTRODUCTION

One of the leading families of error-correcting codes is known as low-density parity-check (LDPC) codes, which were first introduced by Gallager in [1]. The LDPC code is a kind of linear block codes which is defined by sparse parity-check matrix $\mathbf{H}$ that consists of a large number of zeros and a small number of ones. LDPC codes have attracted a lot of attention because they can asymptotically achieve the Shannon limits with long codeword length [2]. However, as to short LDPC codes, their error-correcting performance deviates from the predicted performance.

LDPC codes corresponding to Tanner graph which has no short cycles show better error-correcting performance than other LDPC codes. For Tanner graph corresponding to no cycles, the performance of log-likelihood ratio belief propagation (LLR-BP) decoding and belief propagation (BP) decoding algorithm [3] [4] can be seen the same as performance of maximum a posterior probability (MAP) decoding. MAP decoding algorithm must satisfy a strict requirement. The detail of the requirement is that every bit uniformly receives information belongs to other bits. Whereas, existence of cycles results to the phenomena that bits included in cycles receive information of bits in the same cycle more than those of the other bits and those contaminated information are propagated to other bits in the next step. The BP and LLR-BP decoding algorithms are the approximate MAP decoding since it is difficult to avoid all cycles when construct parity-check matrix of LDPC codes. For this reason, several works focused on constructing LDPC codes whose Tanner graph has large girth. However, Gallager [1] has proved that there is a relationship between girth and codeword length, which indicates that for long length code, the girth of cycles is usually large, i.e., the probability of constructing short cycles is small while for short length LDPC codes, the negative influence of cycle is more apparent than that of long length LDPC codes. In other words, the fact that short codeword length LDPC codes have smaller girth than that of long codeword LDPC codes is an important reason which results in the degraded error-correcting performance. To overcome the inherent shortcoming of short LDPC codes, some authors concatenated LDPC with other kinds of codes to enhance error-correcting performance, such as LDPC-LDPC [5], LDPC-turbo [6] and LDPC-cyclic redundancy check (CRC) concatenation [7][8].

In this paper, we propose a novel BP decoding algorithm using improved perturbation method aided by CRC. Our decoder has multiple decoding paths corresponding to path size L which is also the total number of decoding paths. It should be noted that when our algorithm finishes, it returns a single codeword. The function of CRC is to tell us what codeword in the path is the transmitted codeword (if the transmitted codeword is indeed present in all paths). With this modification, simulation results show that the proposed BP decoder can improve the error-correcting

performance of conventional BP decoder with moderately higher complexity. LDPC codes with short codeword length decoded by proposed BP decoder corresponding to path size $L=32$ can achieve 0.25 dB gain at frame error rate (FER) $=10^{-2}$. In particular, the performance of BP decoding algorithm with perturbation in [8] is also presented for comparison. From computer simulation, we show that for LDPC codes with same code length and code rate, our proposed BP decoder with improved perturbation method can achieve better FER performance than decoding methods in [8] with same complexity.

The rest of this paper is organized as follows. In Section 2, a general view of LDPC codes and conventional BP decoding algorithm are introduced first. We also give a brief introduction of BP decoding with perturbation method in Section 2. Then in Section 3, the proposed BP algorithm with improved perturbation method is presented. Simulation results are given in Section 4, followed by conclusions in Section 5.

2 BACKGROUNDS

2.1 Low Density Parity Check Codes and Belief Propagation Algorithm

The LDPC code is a class of linear block code defined by sparse matrix $\mathbf{H}$ having dimension $m \times n$ or its equivalent Tanner graph [9]-[13]. Tanner graph has two different types of nodes called as *variable nodes* and *check nodes*. Variable node i and check nodes j are connected via edges if and only if $h_{j,i} \neq 0$, where $h_{j,i}$ denotes the entry of $\mathbf{H}$ at the j th row ($1 \leq j \leq m$) and the i th column ($1 \leq i \leq n$).

We define $\mathbf{H}$ as the parity-check matrix of the LDPC code. The belief message of check node j to variable node i is denoted as $r_{ji}(b)$, $b=0,1$; the belief message of variable node i to check node j is denoted as $q_{ij}(b)$; denote $C(i)$ and $R(j)$ as the set of check nodes related with variable node i and the set of variable nodes in j th parity-check node equation, respectively.

The procedure of LLR- BP algorithm can be described as follows.

1) *Initialization: Assume that codeword transmit through Additive White Gaussian Noise (AWGN) channels $\mathcal{N}(0, N_0)$ where $\sigma^2 = N_0 / 2$ and denotes received bits as $\mathbf{Y} = (y_1, y_2, \dots, y_n)$. Calculate prior probabilities of every variable node:*

$$L^0(q_{ij}) = L(P_i) = \ln \frac{1 + \exp(2y_i / \sigma^2)}{1 + \exp(-2y_i / \sigma^2)} = 2y_i / \sigma^2 \quad (1)$$

2) *Check nodes updating: Calculate the information from variable nodes to check nodes:*

$$L^l(r_{ji}) = 2 \tanh^{-1} \left[\prod_{i \in R_j \setminus i} \tanh\left(\frac{1}{2} L^{(l-1)}(q_{ij})\right) \right] \quad (2)$$

3) *Variable nodes updating: Calculate the information from check nodes to variable nodes:*

$$L^l(q_{ij}) = L(P_i) + \prod_{j \in C_i \setminus j} L^{(l)}(r_{ji}) \quad (3)$$

4) *Decoding decision: Calculate the decoding outputs:*

$$\hat{c}_i = \begin{cases} 0 & L^l(q_i) > 0 \\ 1 & L^l(q_i) \leq 0 \end{cases} \quad (4)$$

where,

$$L^l(q_i) = L(P_i) + \prod_{j \in C_i} L^{(l)}(r_{ji}) \quad (5)$$

Finish decoding when $\mathbf{H}\hat{\mathbf{C}}^T = 0$ or attain maximum iteration times. Otherwise, go back to check nodes updating step, keeping iteration.

2.2 Perturbation Method

In this subsection, a brief introduction about LDPC-CRC codes with perturbation method [8] is given. For each frame, the author conjoins LDPC codes with a r -bit CRC sequence, thus results in a new LDPC-CRC code in

encoder and decoder. At receiver side, perturbation method plays a role when the last decoding result is wrong, i.e., not satisfying the CRC polynomial. More specifically, the details of perturbation method can be described as adding a white Gaussian noise whose variance is smaller than $\sigma^2 = N_0 / 2$ to the selected several bits which has smallest absolute values of initial belief. The decoding procedure with perturbation in [8] is shown in Fig. 1. Obviously, the complexity of this algorithm is T times than the complexity of original BP algorithm, where T is the number of re-decoding times.

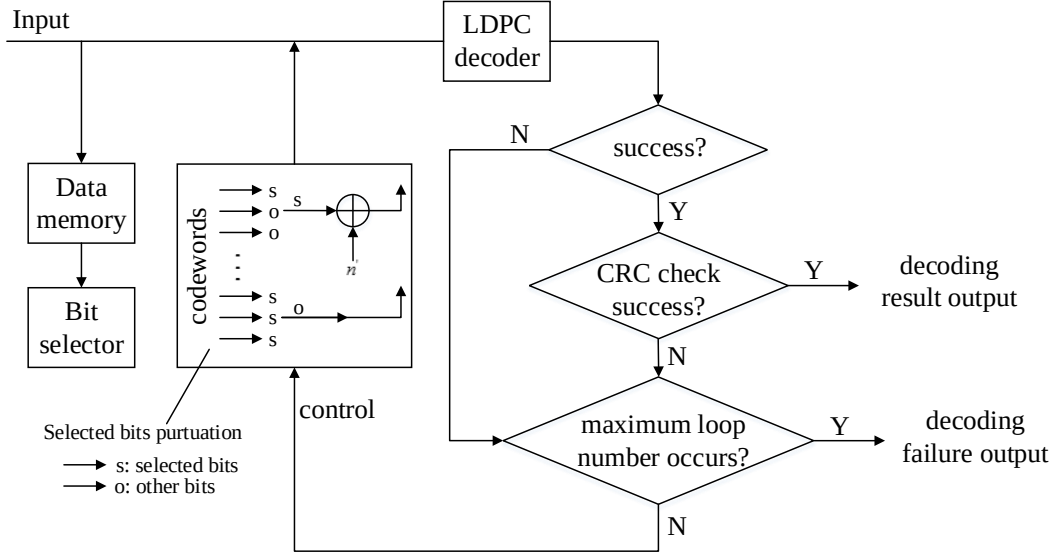


FIG. 1 DECODING WITH PERTURBATION METHOD

3 IMPROVED PERTURBATION METHOD

In this section, we will introduce and define our proposed BP decoding algorithm with improved perturbation method. Our proposed decoder has a parameter L , called as *path size*. It is apparent that larger value of L means better error-correcting performance but higher decoding complexity.

Instead of starting the decoding with the initial LLR values of variable nodes, we choose $\log_2 L$ bits according to a criterion which will be discussed later and set the LLR value of chosen bits to either positive infinity or negative infinity, we inspect both options. Namely, the decoder has L different paths concurrently. Naturally, we would like to choose the “best” path at the end, and thus require another criterion pruning other paths in order to preserve the “best” one. Our pruning criterion is according to the check results of CRC polynomial. The function of CRC is to tell us what codeword in the path is the transmitted codeword (if the transmitted codeword is indeed present in the path).

Thus, we concatenate short LDPC codes with CRC- r codes. It is well known that CRC codes are widespread used to detect error in wireless communication. For example, the 3rd generation partnership project (3GPP) standard [14]. Assume a (n, k) LDPC codes, we have k source bits that we are free to set. Instead of setting all of them to information bits, we set the first $(k-r)$ source bits to information bits we want to transmit. The last r bits are set to be the r -bit CRC value of the first $(k-r)$ information bits. Therefore, a LDPC encoder corresponding to k -bit input block includes two parts. The first is the $(k-r)$ information bits and the second is the r -bit CRC polynomial. Note that this novel encoding scheme suffers a penalty in rate, since the rate of our code is now $(k-r)/n$ instead of the original rate k/n . For this reason, an appropriate number of redundant CRC bits are very significant. With the increasing of the number of CRC bits, the number of undetected errors decreases, which leads to better error-correcting performance. It is worth noting that the number of CRC bits results in the decrease in code rate, which is an indicator of bandwidth efficiency. Therefore, a balance between error-correcting performance and bandwidth efficiency exists.

The proposed BP decoder with improved perturbation is shown in Fig. 2 and the procedure can be described as follows.

Step 1: Based on received bits $\mathbf{Y}$, calculate the initial belief according to (1). Then choose $\log_2 L$ bits corresponding

to smallest absolute values of initial LLR among the subset of all variable nodes which have highest degree. For simplicity, we assume that $\log_2 L$ is an integer number satisfied with $0 \leq \log_2 L \leq n$. When $\log_2 L = 0$, the modified decoding algorithm is equivalent to the original BP decoding algorithm.

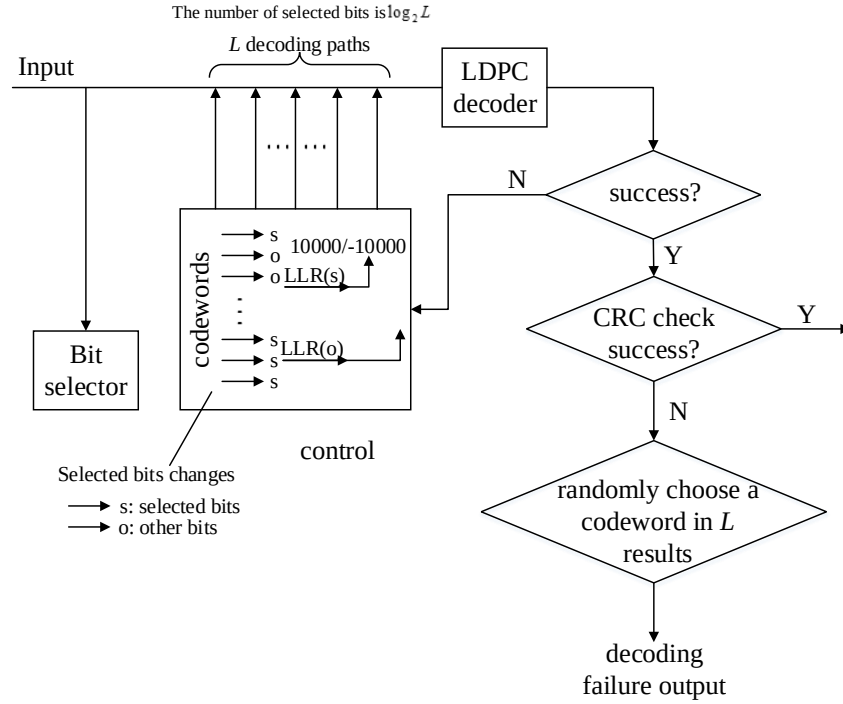


FIG. 2 MODIFIED DECODING WITH IMPROVED PERTURBATION METHOD

Step 2: Decoding received bits $\mathbf{Y}$ by LLR-BP algorithm which has been discussed in last section to get an output codeword $\hat{\mathbf{C}}$.

Step 3: Check output $\hat{\mathbf{C}}$ by the CRC sequence.

- i If $\hat{\mathbf{C}}$ has satisfied with the CRC sequence, stop decoding and take the output $\hat{\mathbf{C}}$ as final decoding results which is also of validity.
- ii Otherwise, go to step 4.

Step 4: Read the initial received signal $\mathbf{Y}$ and do certain changes to those bits which are selected in the step 1. In more details, the change is performed as follows:

$$\text{LLR}(y'_i) = \begin{cases} +\infty / -\infty & i \in S \\ \text{LLR}(y_i) & \text{others} \end{cases} \quad i = 1, 2, \dots, n \quad (6)$$

Here, we define S as the set whose elements are indexes of all chosen $\log_2 L$ bits. From (6), we can see that changes occurred to $\log_2 L$ selected bits resulting in L different cases of initial LLR value as $\text{LLR}_1(\mathbf{Y}'), \text{LLR}_2(\mathbf{Y}'), \dots, \text{LLR}_L(\mathbf{Y}')$, i.e., L different decoding paths.

Step 5: Implement the LDPC decoding on $\text{LLR}_1(\mathbf{Y}'), \text{LLR}_2(\mathbf{Y}'), \dots, \text{LLR}_L(\mathbf{Y}')$ by conventional LLR-BP decoding which has been discussed in last section. Among all LDPC decoding result $\hat{\mathbf{C}}_1, \hat{\mathbf{C}}_2, \dots, \hat{\mathbf{C}}_L$, check the output of the LDPC decoding $\hat{\mathbf{C}}_l (l = 1, 2, \dots, L)$ by CRC sequence. If CRC sequence has been met by $\hat{\mathbf{C}}_l$, choose $\hat{\mathbf{C}}_l$ as the final single output of LDPC decoder; if none of $\hat{\mathbf{C}}_l$ satisfies the CRC polynomial, randomly choose a $\hat{\mathbf{C}}_l$ as the final single output of LDPC decoder.

The reason we choose bits having smallest absolute values of initial LLR among the subset of all variable nodes which have highest degree will be discussed concretely in this paragraph. Firstly, variable nodes with higher degree will tend to their value more quickly. These nodes then provide good information to the check nodes, which subsequently provide information to lower degree message nodes [15]. Thus, BP decoding of irregular LDPC codes

brings about wave influence. Namely, if errors happen to higher degree variable nodes at the start, then variable nodes having little smaller degree will be fault, and so on. Secondly, each bit's initial LLR value is another measurement of reliability. Bits with smaller absolute value of initial LLR are more sensitive to changes, and have comparable reliability contribution compared to those having larger absolute value of belief [8]. Therefore, when we make a criterion about what bits should be selected, we should take both degree of variable nodes and initial LLR value into consideration.

Based on the fact that change initial LLR value of several bits can lead to different decoding results, the number of selected bits should be appropriate. It is obvious that if the number of selected bits is too small to give a different result, performance gain cannot be obtained. On the other hand, it is easily inferred that the complexity of proposed decoding algorithm is L times than the complexity of conventional BP algorithm, if the number of chosen bits is $\log_2 L$. Since the number of selected bits directly decides the decoding complexity of the proposed BP decoder, a balance between error-correcting performance and decoding complexity exists.

4 SIMULATION RESULTS

In this section, we demonstrate the error-correcting performance of short LDPC codes decoded by proposed BP decoder through computer simulation. For LDPC codes with all code rates, we get the degree distribution pairs with maximum variable node degree $d_{v_{\max}} = 4$ by the density evolution technique [16] and design parity-check matrix by progressive-edge growth algorithm [10], which has been widely adopted nowadays. The concatenation CRC-8 code is generated by $X^8 + X^4 + X^3 + X^2 + 1$. For proposed BP decoder with improved perturbation method, conventional BP decoder and BP decoder in [8], the maximum iteration number is 80. In our simulation, the parameters of the BP decoder in [8] are as follows: the number of the perturbed bits is 60 and the perturbation power is 0.3.

Fig. 3 and Fig. 4 display frame error rate (FER) performance of (128, 256) LDPC codes decoded by the proposed BP decoder using improved perturbation method with path size $L=32$ over AWGN channel and uncorrelated Rayleigh channel, respectively. FER performances of the LDPC codes decoded by the conventional BP decoder and modified BP decoder in [8] are also presented for comparison. The number of re-decoding times of the modified BP decoder in [8] is T . To compare our proposed BP decoder with BP decoder in [8] under exactly the same condition about decoding complexity, it is apparent that when the value of re-decoding times T is equal to the value of path size L , the decoding complexity of proposed BP decoder is also equal to the decoding complexity of the modified BP decoder in [8]. As indicated in Fig. 3, LDPC codes decoded by proposed BP decoder with improved perturbation method corresponding to $L=32$ shows nearly 0.25 dB gain of FER improvement over same LDPC codes decoded by conventional BP decoder at $\text{FER}=10^{-2}$ over AWGN channel. As for uncorrelated Rayleigh channel, Fig. 4 illustrates that the FER gain can be achieved as nearly 0.5 dB at $\text{FER}=10^{-2}$. Moreover, Fig. 3 and Fig. 4 both show that our proposed BP decoder with improved perturbation method leads to better FER performance than BP decoder with perturbation method in [8] with same decoding complexity.

FER performance of (192, 256) LDPC codes decoded by the proposed BP decoder with path size $L=32$ over AWGN channel is shown in Fig. 5. Fig. 5 indicates that the proposed BP decoder can be also applied to LDPC codes with higher code rate. For LDPC codes with higher code rate, our proposed BP decoder shows more advantages than BP decoder in [8] in lower SNR. However, they can almost achieve same performance at $\text{FER}=10^{-4}$.

Fig. 6 shows FER performance of (192, 256) LDPC codes decoded by the proposed BP decoder with different path size L over AWGN channel. FER performance of the same LDPC codes decoded by the conventional BP decoder is also presented for comparison. As can be seen in Fig. 6, the achieved FER performance gain increase with larger value of path size L . LDPC codes decoded by proposed BP decoder with improved perturbation method corresponding to $L=8, 32, 128$ show nearly 0.2 dB, 0.25 dB, 0.4 dB FER performance gain over same LDPC codes decoded by conventional BP decoder at $\text{FER}=10^{-2}$, respectively.

All simulation results show that the proposed BP decoder with improved perturbation method leads to better error-correcting performance than that of LDPC codes decoded by conventional BP decoder with moderately higher decoding complexity.

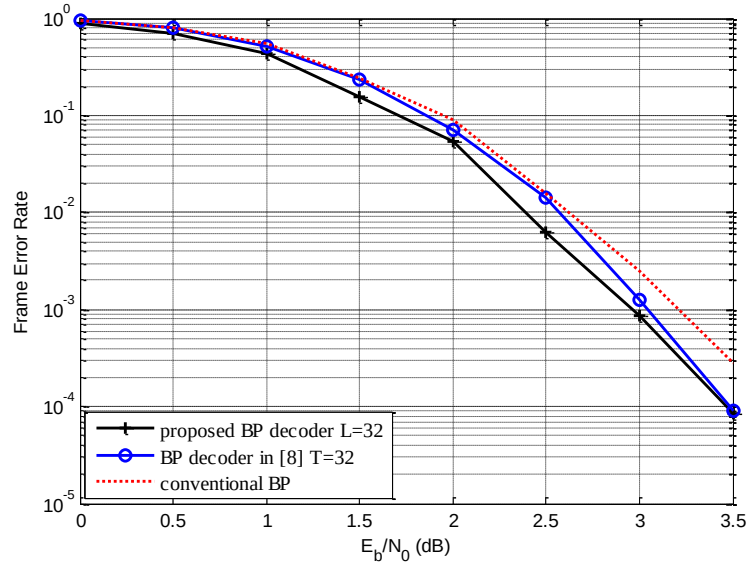


FIG. 3 FER PERFORMANCE OF LDPC CODES OVER AWGN CHANNEL WITH $N=256$ AND $R=1/2$

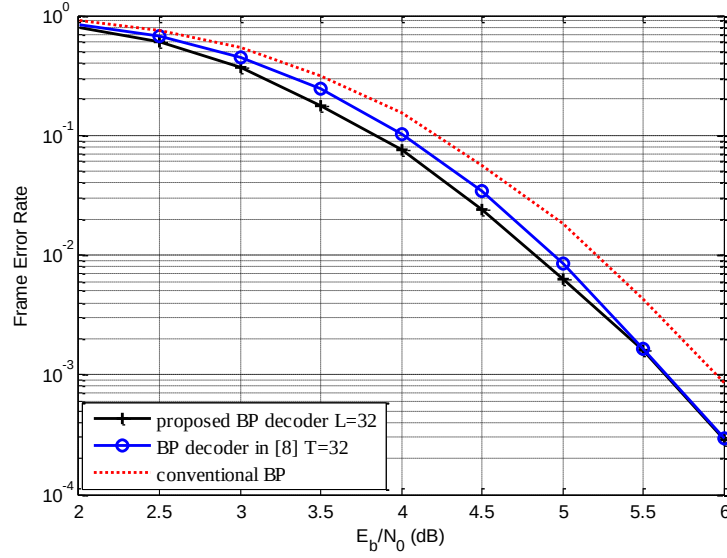


FIG. 4 FER PERFORMANCE OF LDPC CODES OVER RAYLEIGH CHANNEL WITH $N=256$ AND $R=1/2$

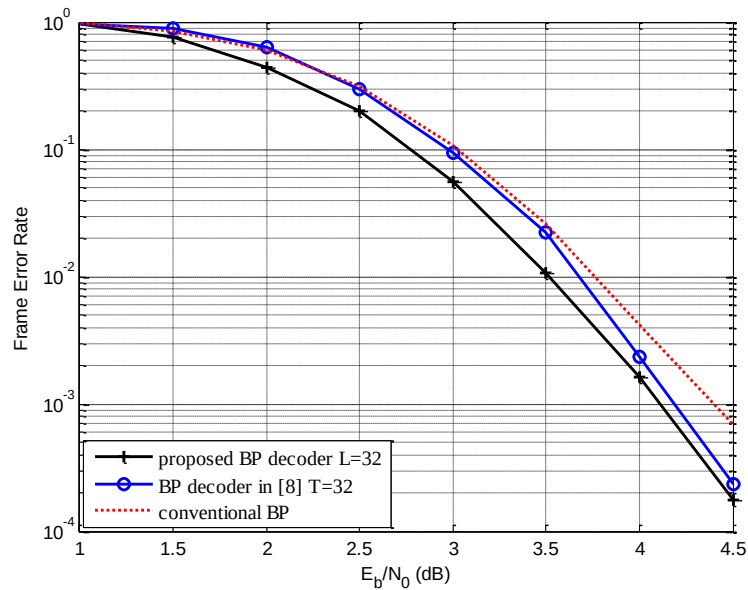


FIG. 5 FER PERFORMANCE OF LDPC CODES OVER AWGN CHANNEL WITH $N=256$ AND $R=3/4$

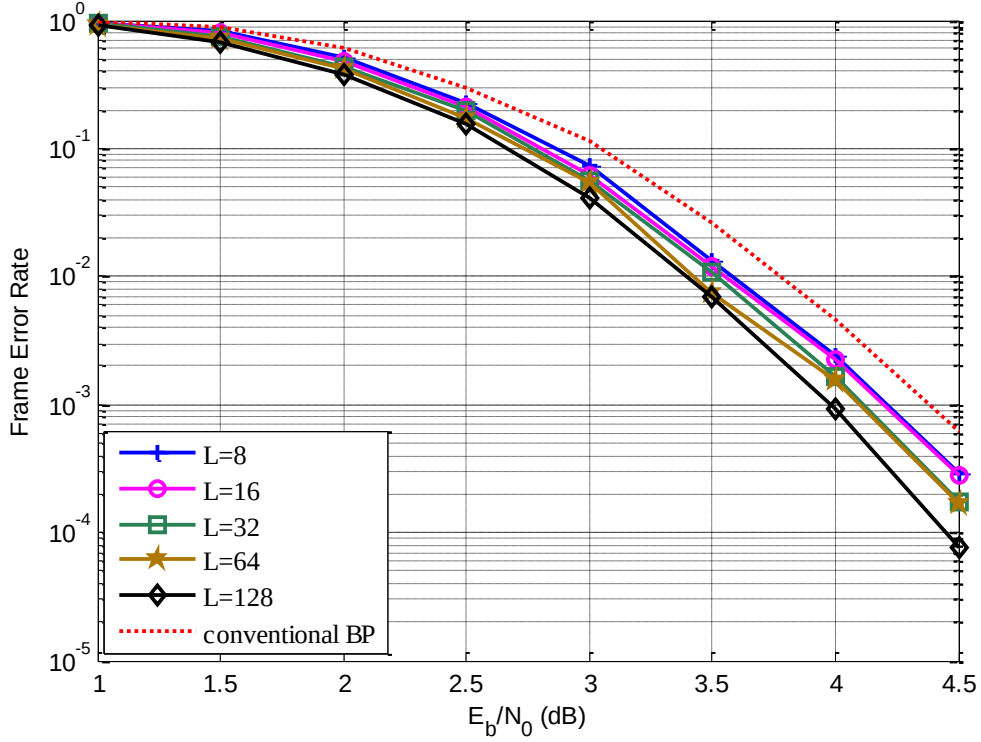


FIG.6 FER PERFORMANCE OF (192,256) LDPC CODES OVER AWGN CHANNEL WITH DIFFERENT L

5 CONCLUSIONS

In this paper, we proposed a novel BP algorithm with improved perturbation method aided by CRC. In the proposed BP decoder, we selected some bits based on a criterion which combine the initial LLR value with variable node degree. After do some changes to selected bits as (7), we obtain L different decoding paths and decode all paths simultaneously. CRC is used to make a choice among all L decoding results. More specifically, the decoding result satisfied with CRC polynomial can be chosen as final output codeword. If there are no decoding results satisfied with CRC polynomial, we randomly choose a decoding result as final output codeword. Therefore, there is always a single output codeword when the proposed BP decoder finishes its decoding. Simulation results showed that BP decoder with improved perturbation method can enhance the error-correcting performance of conventional BP decoder with moderately higher complexity. In particular, for LDPC codes with same code length and code rate, our proposed BP decoder can achieve better FER performance than decoding methods in [8] with same complexity.

ACKNOWLEDGMENT

This work was supported in part by the National Science Foundation of China (No. 61271228).

REFERENCES

- [1] R.G. Gallager. "Low Density Parity-Check Codes." Cambridge, MA: MIT Press, 1963
- [2] S. Chung, G. D. Forney Jr, T. J. Richardson and R. U. D. Urbanke. "On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit." IEEE Communications Letters. 5.2 (2001): 58-60
- [3] MacKay, David JC. "Good error-correcting codes based on very sparse matrices." IEEE Transactions on Information Theory. 45.2 (1999): 399-431
- [4] Pearl, Judea. "Probabilistic reasoning in intelligent systems: networks of plausible inference." Morgan Kaufmann, 1988.
- [5] Fossorier, Marc, and Nenad Miladinovic. "Irregular LDPC codes as concatenation regular LDPC codes." IEEE Communications Letters 9.7 (2005): 628-630
- [6] Lee S. H, Seok J. A, Joo E. K. "Serial concatenation of LDPC and turbo code for the next generation communications." Paper presented at the IEEE Second IFIP International Conference on Wireless and Optical Communications Networks, March 6-8, 2005
- [7] Kwon, Yeong-Hyeon, Mi-Kyung Oh, and Dong-Jo Park. "A new LDPC decoding algorithm aided by segmented cyclic

- redundancy checks for magnetic recording channels.” IEEE Transactions on Magnetics. 41.7 (2005): 2318-2320
- [8] Lin C, Xiao D, Cheng H, Ma M, Jiao B. “A Perturbation Method for Decoding of LDPC Aided by CRC.” IEEE 64th Vehicular Technology Conference, September 25-28, 2006
 - [9] Richardson, Thomas J., Mohammad Amin Shokrollahi, and Rüdiger L. Urbanke. “Design of capacity-approaching irregular low-density parity-check codes.”, IEEE Transactions on Information Theory. 47.2 (2001): 619-637
 - [10] Hu, X-Y., Evangelos Eleftheriou, and Dieter-Michael Arnold. “Regular and irregular progressive edge-growth tanner graphs.” IEEE Transactions on Information Theory. 51.1 (2005): 386-398
 - [11] Fossorier, Marc P C. “Quasicyclic low-density parity-check codes from circulant permutation matrices.” IEEE Transactions on Information Theory. 50.8 (2004): 1788-1793
 - [12] Zhang, L., Huang, Q., Lin, S., Abdel-Ghaffar K, and Blake I. F. “Quasi-cyclic LDPC codes: an algebraic construction, rank analysis, and codes on Latin squares.” IEEE Transactions on Communications, 58.11 (2010): 3126-3139
 - [13] Huang, Q., Diao, Q., Lin, S., and Abdel-Ghaffar, K. “Cyclic and quasi-cyclic LDPC codes on constrained parity-check matrices and their trapping sets.”, IEEE Transactions on Information Theory. 58.5 (2012): 2648-2671
 - [14] 3GPP TS 25.212: “Multiplexing and channel coding (FDD),” Release 9, 2009
 - [15] Luby, M. G., Mitzenmacher, M., Shokrollahi, M. A., and Spielman, D. A.. “Improved low-density parity-check codes using irregular graphs.” IEEE Transactions on Information Theory. 47.2 (2001): 585-598
 - [16] Richardson, Thomas J., Mohammad Amin Shokrollahi, and Rüdiger L. Urbanke. “Design of capacity-approaching irregular low-density parity-check codes.” IEEE Transactions on Information Theory. 47.2 (2001): 619-637

AUTHORS

¹**Si Shu** received the Bachelor’s degree from Huazhong University of Science and Technology, Wuhan, P. R. China, in 2012. She is now working toward the Master’s degree at Huazhong University of Science and Technology, Wuhan, P. R. China. Her current research interest is channel coding for wireless communications.

²**Daiming Qu** received the Ph.D. degree in information and communication engineering from Huazhong University of Science and Technology, Wuhan, P. R. China, in 2003. He is currently a Professor with the Department of Electronics and Information Engineering, Huazhong University of Science and Technology. His current research interests include signal processing, coding, and dynamic spectrum techniques for wireless communications.