Improved Upper Bounds on Low Density Parity Check Codes Performance for the Input Binary AWGN Channel

Yu Yi and Moon Ho Lee

Institute of Information and Communications,
Chonbuk National University, ChonJu, 561-756, Korea
Email: yuyi1020@hotmail.com and moonho@chonbuk.ac.kr

Abstract

In this paper, we study the improved bounds on the performance of low-density parity-check (LDPC) codes over binary-input additive white Gaussian noise (AWGN) channels with belief propagation (BP) decoding in log domain. We define an extended Gallager ensemble based on a new method of constructing parity check matrix and make use of this way to improve upper bound of LDPC codes. At the same time, many simulation results are presented in this paper. These results indicate the extended Gallager ensembles based on Hamming codes have typical minimum distance ratio, which is very close to the asymptotic Gilbert Varshamov bound and the superior performance which is better than the original Gallager ensembles.

□. Introduction

Gallager first discovered Low Density Parity Check (LDPC) codes in 1963 [1]. However, LDPC codes have been almost forgotten for about thirty years, in spite of their excellent properties. Recently, LDPC codes were rediscovered by Mackay and Neal [2] as good error correcting codes achieving near Shannon limit performance and outperforming turbo codes. Comparing the LDPC codes with turbo codes, we can easily find that LDPC codes possess several distinct advantages over turbo codes: (1) it is easy to create LDPC codes with almost any rate and block length, but turbo code should look for a good interleaver; (2) the simpler decoder based on belief propagation decoding algorithm of LDPC codes is fully parallelizable and accomplishes at a greater decoding speed; (3) the decoding complexity of LDPC codes is lower than that of turbo codes.

In this paper, we study the improved bounds on the performance of low-density parity-check (LDPC) codes over binary-input additive white Gaussian noise (AWGN) channels with belief propagation (BP) decoding in log domain. We define an extended Gallager ensemble based on a new method of constructing parity check matrix and make use of this way to improve upper bound of LDPC codes. At the same time, many simulation results are presented in this paper. These results indicate the extended Gallager ensembles based on Hamming codes have typical minimum distance ratio, which is very close to the asymptotic Gilbert Varshamov bound and the superior performance which is better than the original Gallager ensembles.

This paper is organized as follows. In section II LDPC codes and Gallager ensemble are introduced in details. New Gallager ensemble and improved upper bound are studied in section III. Section IV describes belief propagation (BP) decoding algorithm in log domain. Performance analysis and various simulation results with different parameters are presented in section V. Finally, section VI gives a conclusion.

□. Low Density Parity Check Codes

Low density parity check codes are linear block codes thus the set of all code words, x, span the null space of a parity check matrix H: $H \cdot x = 0$. The parity check matrix H for LDPC codes is a sparse binary matrix where the set row and column elements are chosen to satisfy a desired row and column weight profile. The set elements in the graph are constrained by the requirement that the row and column overlap be minimized. The constraints on the matrix structure enable efficient decoding and produce a powerful code. The example structure of H is illustrated in figure 1. In a block of N bits or symbols, there are M redundant parity symbols and the code rate R is given by: R=(N-M)/N. LDPC codes can also be represented using bipartite graphs where one set of nodes represents the parity check constraints and the other set represents the data symbols or variables which are illustrated in figure 2.

$$H = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Figure 1: an example of parity check matrix

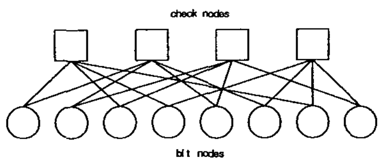


Figure 2: an example of bipartite graph corresponding to the above parity check matrix

A). Gallager ensemble

The binary regular LDPC codes C (N, j, k) have block length N and parity-check matrix with exactly j 1's in each column and k 1's in each row [1]. When constructing the regular LDPC codes, we can use the following way as shown in figure 3 to construct a LDPC code. A parity-check matrix is divided into three sub matrices, each containing a single 1 in each column. The first of these sub matrices contains 1's in descending order; .i.e., the ith row contains 1's in the column (i-1)k+1 to ik, where k is the row weight. The other sub matrices are merely column permutations of the first sub matrix. The permutations of the 2^{nd} sub matrix and the 3^{rd} sub matrix are independently selected.

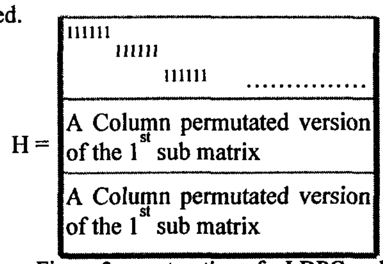


Figure 3: construction of a LDPC code

We call this ensemble based on above construction of a LDPC code as the original Gallager ensemble. Let $N(l)$ be the ensemble average of the number of code words of weight $l(0 \le l \le n)$. Gallager derived an upper bound on $N(l)$:

$$N(l) \le C(\lambda, n)\exp(-B(\lambda)n)$$

Where $B(\lambda) = (j-1)H(\lambda) - \frac{j}{k}\mu(s) - \frac{j}{k}(k-1)\ln 2 + js\lambda$

$$C(\lambda, n) = [2\pi n\lambda(1-\lambda)]^{(j-1)/2} \times \exp[\frac{j-1}{12n\lambda(1-\lambda)}]$$

$$\lambda = l/n, (0 \le \lambda \le 1), \mu(s) = \ln 2^{-k}[(1+e^s)^k + (1-e^s)^k]$$

The function $H(\lambda)$ is the entropy function defined by: $H(\lambda) = -\lambda\ln(\lambda) - (1-\lambda)\ln(1-\lambda)$.

The parameters λ and s must satisfy the following equation: $\lambda = \frac{1}{k} \cdot \frac{\partial \mu(s)}{\partial s}$.

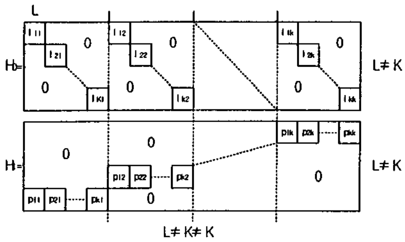
This upper bound can be considered as an upper bound on ensemble average weight distribution of codes belonging to the Gallager ensemble [1]. The average weight distribution is indispensable basis of the performance analysis of regular LDPC codes and used to evaluate the binary input AWGN channel threshold of the Gallager ensemble.

□. Improved Upper Bounds

In this section, we define a new Gallager ensemble and derive the improved upper bound in details.

A). New Gallager Ensemble

First, an H matrix structure is shown in the following:



Structure of submatrices H and H

Figure 4: a new construction of parity check matrix

According to the above structure, we present a new method to construct matrix $\tilde{H} = [H_0^T, H_1^T]^T$ that defines a (2,k)-regular LDPC code [4]. This structure will provide much more freedom on the selection of code length: Given k, any code length that could be factored as $L \cdot k^2$ is permitted, where L cannot be factored as $L = a \cdot b, \forall a, b \in \{0, \ldots, k-1\}$.

In this figure, we can know each block matrix $I_{x,y}$ in H_0 is an $L \times L$ identity matrix and each block matrix $P_{x,y}$ in H_1 is obtained by a cyclic shift of an $L \times L$ identity matrix. Let T denote the right cyclic shift operator where $T^u(Q)$, then $P_{x,y} = T^u(I)$ where $u = ((x-1) \cdot y) \bmod L$ and I represents the $L \times L$ identity matrix. H_2 is the permutation of H_1.

B). Improved Upper Bound

In the description of the new Gallager ensemble, the average number of code words of weights l in the new Gallager ensemble is denoted by $N(l)$. We can get the following formula:

$$N(l) \le C(\lambda, n)\exp(-B(\lambda)n)$$

Where $B(\lambda) = (j'-1)H(\lambda) - \frac{j'}{L}u'(s) - \frac{j'}{L}\ln|C'| + j's\lambda$

$$C(\lambda, n) = [2\pi n\lambda(1-\lambda)]^{(j'-1)/2} \times \exp\left[\frac{j'-1}{12n\lambda(1-\lambda)}\right], \lambda = l/n, (0 \le \lambda \le 1)$$

The parameters λ and s must satisfy the following equation: $\lambda = + \frac{\partial \mu(s)}{L\,\partial s}$.

Comparing the upper bound of based on original H matrix with the improved upper bound based on the new H matrix, we can get the following figure 5:

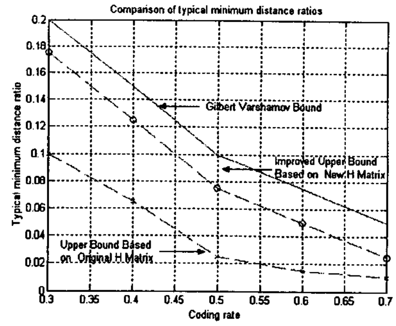


Figure 5: comparison of typical minimum distance ratios

□. The Decoding Algorithm

For LDPC codes, belief propagation (BP) algorithm can be performed more efficiently and more simply for hardware implementation in log domain, where the probabilities are equivalently characterized by the log-likelihood ratios (LLRs) as follows:

$$L(r_{mn}) = \log\frac{r_{mn}^1}{r_{mn}^0},\ L(q_{mn}) = \log\frac{q_{mn}^1}{q_{nm}^0},$$

$$L(p_l) = \log\frac{p_l^1}{p_l^0},\ L(q_l) = \log\frac{q_l^1}{q_l^0}$$

1.Initialization

Each bit node n is assigned an a priori LLR $L(p_n)$. In the case of equiprobable inputs on an AWGN channel with BPSK,

$$L(p_n) = \frac{2}{\sigma^2}y_n$$

Where $\sigma^2 = (1/2R \cdot (E_b/N_0))$ is the variance of the noise. For every position (m, n) such that $H_{mn} = 1$, $L(q_{nm})$ and $L(r_{mn})$ are initialized as:

$$L(q_{nm}) = L(p_n) \text{ and } L(r_{mn}) = 0$$

2.Horizontal step

Each check node m gathers all the incoming information $L(q_{nm})$'s, and updates the belief on the bit n based on the information from all other bits connected to the check node m.

$$L(r_{mn}) = 2\tanh^{-1}\left(\prod_{n' \in N(m)\backslash n} \tanh(L(q_{n'm})/2)\right)$$

3.Vertical step

Each bit node n propagates its probability to all the check nodes that connect to it.

$$L(q_{nm}) = L(p_n) + \sum_{m' \in M(n) \setminus m} L(r_{m'n})$$

The decoder gets the total a posteriori probability (APP) for the bit n by summing the information from all the check nodes that connect to the bit n.

$$L(q_n) = L(p_n) + \sum_{m \in M(n)} L(r_{mn})$$

4. Stop criterion

Hard decision is made on the $L(q_l)$, and the resulting decoded input vector $\hat{x}$ is checked against the parity-check matrix H. If $H\hat{x} = 0$, the decoder stops and outputs $\hat{x}$. Otherwise, it repeats the step 2-4.

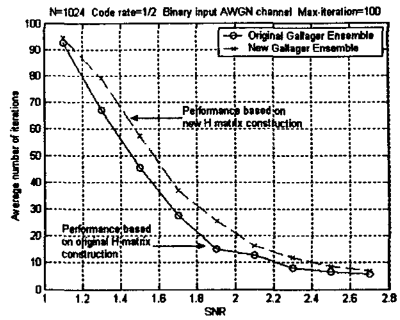


Figure 7: the average number of iterations of the new Gallager ensemble and the original Gallager ensemble

□. Simulation Results

In this section, we analyze the performance of the new Gallager ensemble. Many simulation results are presented, i.e. N=1024, j=3 and k=6. The code rate is 1/2. In this work, LDPC codes are modulated by BPSK modulation and transmitted over binary input AWGN channels. The max decoding iterative number of 100 is simulated.

In figure 6, we can easily know the performance of the extended Gallager ensemble based on the new parity check matrix construction is better than the original case. But in figure 7, the decoding of the new Gallager is more complexity than the original Gallager ensember. So the new Gallager ensemble uses the increase of the decoding complexity as the cost to achieve superior decoding performance.

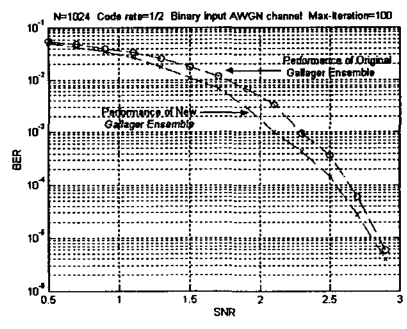


Figure 6: the performance of the new Gallager ensemble and the original Gallager ensemble

□. Conclusion

In this paper, we study the improved bounds on the performance of low-density parity-check (LDPC) codes over binary-input additive white Gaussian noise (AWGN) channels. According to the simulation results, we can draw a conclusion that when we use a new way to construct parity check matrix, the upper bound of LDPC codes is improved, the performance of new Gallager ensemble is better than the original Gallager ensemble. At the same time, we can know the new Gallager ensemble uses the increase of the decoding complexity as the cost to achieve superior decoding performance.

References

[1] R. G. Gallager, "Low-density parity-check codes," IRE Trans. Inform. Theory, vol. IT-8, pp. 21-28,Jan. 1992.

[2] D. J. C. Mackay, "Good error-correcting codes based on very sparse matrices," IEEE Trans. Inform. Theory, vol. 45, pp.399-431, Mar. 1999.

[3] D. J. C. Mackay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," Electron. Lett, vol. 32, no. 18, pp.1645-1646, Aug. 1996.

[4] Tong Zhang, Zhongfeng Wang and Keshab K. Parhi, "On Finite Precision Implementation of Low Density Parity Check Codes Decoder,"