

# Research on Encoding and Decoding Algorithms of LDPC Codes

Yifeng He, Zhemin Duan

Electronic Information College, Northwestern Polytechnical University, Xi'an, 710000, China

**Keywords:** Encoding algorithms, Decoding algorithms, LDPC codes

**Abstract.** The LDPC code, namely low density parity check code, is essentially a linear block code. Its decoding performance is closer to the Shannon limit than the Turbo code. The definition and description of LDPC codes are introduced in this paper. LDPC coding method includes the Algorithm of LU decomposable encoding and the algorithm of partitioned iterated encoding. the algorithm of message passing, the algorithm of minimum-sum decoding and the algorithm of bit-flipping decoding are the common decoding algorithms of the LDPC codes. The concept and features of the encoding and decoding algorithms are explored in this paper to provide some references for the relative researchers.

## Introduction

Generally, the reliability of the communication system is measured by the bit error rate, and its effectiveness is measured by channel symbol. Early people generally believe that between the effectiveness and reliability of communication system is a pair of irreconcilable contradictions, one is always at the expense of the other party to improve the cost, and pointed out that when the power is limited, the only way is to realize information transmission in arbitrarily small probability of error disturbance on a communication channel is the transmission of information the rate is reduced to zero. It is necessary to understand the characteristics of the channel in the communication system. According to the values of input and output channels of the continuous and whether it can be divided into discrete, continuous and discrete transmission channel. The continuous output channel; channel according to whether the statistical properties change with time can be divided into stationary and non-stationary channel; according to channel output is not has the correlation can be divided into memory channel and memoryless channel; the channel characteristics of the input of symmetry can be divided into symmetric and asymmetric channels. In practical applications, most of the channels are stationary and memoryless symmetric channels. LDPC code is a kind of linear block code, its check matrix is sparse, as the number of non-zero elements in the check matrix is very small. Because of the sparsity of the LDPC matrix, the complexity of the decoding process of LDPC codes and the minimum distance between codes are only linearly increased with the increase of the code length. According to the different characteristics of LDPC codes, we can classify them from different perspectives. For example, in accordance with the parity check matrix of H code in each row or column in the number 1 is the same, is divided into regular and irregular LDPC codes; according to the values of the nonzero elements in the H code check matrix, it can be divided into binary LDPC codes and no binary LDPC codes.

## Concept of LDPC Codes

In 1962, Gallager proposed the linear block code which has a class of sparse parity check matrix, called low density parity check code. LDPC codes have excellent error correction performance, but with the increase of code length, encoding and decoding of LDPC code complexity will rapidly increase pressure plus, limited by the soft and hardware level, the influence of LDPC code once neglected. By the superior performance of Turbo codes, iterative decoding algorithm has been much attention. In the derivation process and product decoding and density evolution theory, we assume that the transmitted message asked qui statistical independence to meet the assumption of independence, and for a given degree distribution, most of the LDPC code in the code length is

limited cannot meet the assumption. This paper analyzes the effect of the non-independence between messages on the performance of LDPC codes and the methods to weaken or eliminate the effects. Each LDPC code has a corresponding Tanner graph representation. It can be proved that when the corresponding Tanner graph is acyclic graph, the messages transmitted in the decoding process must satisfy the independence assumption. But it is through the analysis found that the corresponding acyclic graph Tanner LDPC code because of not having a good distance spectrum distribution, the error correction performance is often not a ring Tanner map of the corresponding LDPC code, when there is a map of length 2, the loop, message passing decoding process only in the front wheel the algorithm meet the independence assumption, the corresponding density evolution theory is only before the news analysis of probability density iteration is accurate. In order to study the influence of the existence of the ring on the decoding performance. The concept of girth length is put forward. The so-called girth refers to a LDPC code corresponding to the minimum length of all the rings in the Tanner diagram, the value and will be even. This chapter systematically expounds the basic principle of LDPC codes encoding and decoding, gives the decoding algorithm of LDPC codes in the common channel, briefly introduced the density evolution theory, and the two main factors affecting the performance of LDPC codes, degree sequence function and girth were analyzed. Note that, based on the design of sequence density evolution theory and girth design are based on the LDPC code decoding performance using belief propagation algorithm can achieve the corresponding theoretical analysis results only when the code length tends to infinity to be fully consistent with the reality. Nowadays, the finite length analysis of LDPC codes has become a research hotspot.

### **Encoding Algorithms of LDPC Codes**

**Algorithm of LU Decomposable Encoding.** Since LDPC code was invented, it has not been widely used for a long time. One disadvantage is that the LDPC coding technology is very complex. If the encoding is done by generating a matrix, a large and sparse matrix is stored. In addition, the LDPC code in the case of long code length can highlight its advantages, once the code length becomes longer, although the LDPC code check matrix is a sparse matrix, but it is difficult to store such a matrix is not a problem. From the point of view of coding, LDPC code is still facing a series of problems. For example, storage space is an important reason for restricting the application of LDPC codes. The code length more storage space is needed. Therefore, the LDPC communication system must have a simpler encoding and decoding process. At the same time, in order to improve the performance of LDPC codes, the LDPC codes can not only improve the speed of communication, but also increase the complexity of the LDPC codes. The research of LDPC coding algorithm is based on this idea. In general, as long as the check matrix has a lower triangular structure, it can always be encoded by an iterative method. The iteration is introduced, which greatly reduces the complexity of coding. The LU decomposition coding algorithm is based on this idea. The check matrix is a row full rank matrix. If the row is not rank, the check matrix  $H$  can be simplified. We can check the matrix  $H$  to approximate diagonal elements are all in the form of  $L$ . The problem of LU decomposition algorithm is that the complexity of preprocessing is very high, and more importantly, after the pretreatment, the new check matrix is likely to be sparse matrix, so the calculation of the coding is very large.

**Algorithm of Partitioned Iterated Encoding.** The computational complexity of partial iterative coding algorithm is linear or approximately linear. Some iterative encoding algorithm is such a clever therapy, its elbow checks matrix  $H$  only permutation of rows and columns replacement, the matrix appears in the upper right corner of the lower triangular form of matrix block, the lower triangular matrix in the upper right corner of independence as a sub matrix, and iterate through special encoding the structure of the sub matrix. This ensures that the newly formed parity check matrix is sparse, and that the coding can be performed in an iterative manner. It should be noted that the conversion from  $H$  to  $H_t$ , in the process of column permutation again, so in the decoder should use the parity check matrix for  $H$ . Since the parity check matrix  $H$  is the parity check matrix  $H$  after column permutation obtained, so that the two matrix code word sets each code word has bit replacement. We can advance

the check matrix  $H$  column to replace the corresponding inverse permutation, because column permutation occurred in the first step here, not the last step, so even if the corresponding reverse column permutation in advance. Although there are a lot of techniques to simplify coding, but because the LDPC code length is very long, and the randomness of the parity check matrix is very strong and so on, the encoding of LDPC codes is a very complicated process in general. If the LDPC code in the design of a number of easy to introduce appropriate coding structure, if such a structure does not affect the performance of the code, then such a coding method is also feasible.

## **Decoding Algorithms of LDPC Codes**

**Algorithm of Message Passing.** In the message passing algorithm, the probability information is transmitted between the variable nodes and the check nodes according to the two points, and the iterative decoding is performed. The information sent by the edge of the node is independent of the information received from the previous one, depending on the information received on the other side of the connection. The purpose is to make any edge, only the transfer of foreign information, thereby ensuring decoding performance. If there is no ring in the two part of the LDPC code, the information received by any node has nothing to do with the information sent from the node, thus ensuring the performance of iterative decoding. If there is a ring in the two graph, after a certain number of iterations, the information received by the node will be related to the information, which will affect the performance of the decoding algorithm. When sending information channel output symbol set and decoding message passing algorithm in the same set of symbols, is the set of real numbers, the continuity of the message, select the information mapping function properly, is the belief propagation algorithm. The core idea of the algorithm is iterative computation between the variable nodes and check nodes with soft information received, so as to maximize the encoding gain, so it has very good performance and is suitable for occasions with higher requirements on the performance of. In the iterative process of the BP algorithm, if the decoding is successful, the decoding process is completed immediately instead of a fixed number of iterations, which effectively reduces the number of iterations and reduces the computational complexity. Moreover, if the algorithm does not find an effective decoding result after the maximum number of iterations is reached, the decoder will be wrong. At the same time, the BP algorithm is a parallel algorithm, which can greatly improve the decoding speed. LDPC code using BP decoding algorithm can get good decoding performance, but due to a large number of multiplication, the use of BP algorithm hardware complexity.

**Algorithm of Minimum-sum Decoding.** The reason for the minimum performance of LDPC codes is the high estimation of the external information of the nodes in the iteration process. The previous minimum and the improved algorithm are correct this high estimate, to compensate for the performance loss, mainly through the statistical information of the information analysis, corrected by the fixed parameters of foreign information, while ignoring the effect of the check node information outside the actual input factors. By analyzing the relationship between the number of nodes and the minimum input information, we propose an improved minimum sum algorithm. In the iterative process, the update information of the check node is modified to approximate the results of the BP algorithm. The simulation results show that the improved decoding algorithm is similar to the BP algorithm, and the performance of the algorithm is better than the BP algorithm in the high SNR region. Minimum sum decoding algorithm is proposed based on BP decoding algorithm in log domain a simplified approximate algorithm, it uses the minimum value for the operation simplifies the function operation, greatly reduces the computational complexity and does not need to estimate the channel noise, but its performance was reduced to a certain extent. The algorithm used to characterize the correction factor between the minimum and the small value of the poor, but because each iteration of each line has a set of minimum value and small value, and each set of minimum value and small value are different, so their difference is a collection of random number obviously, cannot accurately calculate each set minimum value and small value of the poor, and as a correction factor allocation algorithm. So we decided to use all minimum and small values of the sample mean to estimate their difference, and as a result of the correction factor. In the meantime, we I worry for the

first time correction factor iteration, after each iteration of the correction factor is still in use. This is done for two reasons: on the one hand, we try on the back of the iterative re-calculated correction factor and the simulation results show that the performance of the algorithm was not improved; on the other hand, is recalculated for each iteration and the configuration correction factor of the complexity of the algorithm will greatly improve decoding.

**Algorithm of Bit-Flipping Decoding.** Bit flipping decoding algorithm first divides the input data of the hard decision decoder, and then check all the sequences into the equation, find the calibration equation does not hold the largest number of variable nodes, the bit flipping corresponding to the variable nodes, thus completing one iteration. The whole decoding process is iterated until all the calibration equations are established or the maximum number of iterations is reached. Bit flipping decoding algorithm only several bit flip and other simple operation, no complicated operation, so it is very suitable for hardware implementation, but its performance relative to the BP decoding algorithm has been reduced, and is suitable for hardware constrained situations with low performance requirements. We propose an improved BF algorithm with two decoding threshold, the algorithm in each iteration, using two decoding threshold flip the plurality of bits, the probability of error occurrence reduced per bit, to speed up the decoding convergence speed and achieve the decoding performance by comparison; the real amount of computation, the improved BF algorithm real computation quantity is small, the decoding delay is very short and the decoding speed is very fast, very suitable for real-time communication system is high. It is necessary to further study on how to select the appropriate threshold for bit flipping decoding in order to achieve better decoding performance on the basis of low complexity. A large number of real operations will result in a large decoding delay. The real time computation of the improved BF algorithm is very small, so the decoding delay is very short and the decoding speed is very fast.

## Conclusion

LDPC code encoding and decoding methods are various. The computational complexity degrees and the performances of different algorithms are also different. Generally speaking, the encoding and decoding algorithms of relatively better performance have higher complexity degrees. In practical applications, we determine the code length and code rate of LDPC code according to the data of business types, channel environment, hardware conditions and other factors to design the check matrix, select the encoding algorithm to meet the requirements of the encoding or decoding requirements.

## References

- [1] Tang Mingliang, Zhang Hongmei, Design of LDPC Decoder Chip Based on ASIP Architecture [J]. *Microelectronics*, 2015, 45(1): 50-53.
- [2] Du Haoyang, Wang Chenggui, Luan Yating, A HARQ Strategy Based on Decoding Reliability in LDPC Codes [J]. *Radio Communications Technology*, 2016, 42(5): 27-30+52.
- [3] Chen Xucan, Liu Dongpei, Modified Decoding Algorithm of LDPC Codes [J]. *Journal of University of Electronic Science and Technology of China*, 2010, 39(2): 219-222.
- [4] Luo Jian, Li Jiong, A Decoding Algorithm with Iterative Channel Estimation in LDPC Coded SFH System [J]. *Communications Technology*, 2015, 48(3): 306-310.