Application Analysis of Low Density Parity Check Code for Wireless Network

Peixiao Fang

1 Dispatching Center for Quality Inspection and Customer Service, Shanghai Branch North District, China Mobile Tietong, Shanghai 200082, China
zhangjinghe@bjbari.com

Abstract. The Low Density Parity Check (LDPC) codes use an iterative decoding algorithm. The advantages of this algorithm are: the algorithm is completely parallel, so the decoding speed is extremely high; the complexity of the decoding algorithm is low, and the amount of calculation will not increase sharply due to the increase of the code length. It is incomparable with convolutional code and other group codes. A good compromise can be obtained in complexity and performance. Even for the same decoding algorithm, different iteration times can be selected according to channel conditions and system requirements, which is very flexible. In this paper, we review the construction and decoding of LDPC, analyze their advantages and provide their direction of future works.

1. Introduction

In generally, the Wireless Network (WN) is a distributed network [1-5]. Compared with traditional wired network, the information is transmitted via the wireless channel in WNs. The diverse scenarios as well as mobile/fixed obstacles, the channel state will be influenced. Therefore, the wireless network is susceptible to interference. The channel coding is taken as a valuable anti-interference technology [6-11].

The channel coding is mainly used to achieve the error correction by adding some error corrected symbols in the transmission information of from the supervision of the [12-15]. In 1962, Gallager proposed a linear block code based on a sparse check matrix, that is, a low-density block check code, and gave the construction method of the LDPC code, the iterative decoding algorithm and the theoretical proof of its performance. Due to the limited development of computers and the difficulty in hardware implementation at that time, LDPC codes were not correctly understood, but were forgotten for a long time. It was not until the Turbo code was proposed by Berrou et al. in 1993. It was discovered that Turbo codes are actually a kind of LDPC codes. , LDPC codes have re-aroused people's research interest. Later, Mackay and Neal rediscovered that LDPC codes and Turbo codes have similar excellent performance, and in some respects have surpassed Turbo codes. After that, LDPC codes have attracted everyone's attention and become a new research hotspot.

At present, the research on LDPC codes mainly focuses on the following directions.
(1) Consider the construction of LDPC codes on non-GF(2).
(2) Construct irregular LDPC codes by relaxing the restriction on the weight of rows and columns.

2. LDPC code’s structure

LDPC code is a linear block code, and its code length is \( n \) can be uniquely determined by its generator matrix \( G \) or parity check matrix \( H \). \( H \) is a sparse matrix, and each column contains only a few ‘1’, and
all other elements are '0'. According to the number of 1 in the parity check matrix, LDPC codes are divided into two types: regular code and irregular code. The number of '1' in each rule or each row is equal in regular code, and just the opposite in irregular code.

For LDPC code, let the information sequence \( u = (u_0, u_1, u_2, u_3, \ldots, u_{k-1}) \), the length of \( k \), the encoded codeword \( C = uG = (c_0, c_1, c_2, c_3, \ldots, c_{n-1}) \), which

\[
G = \begin{bmatrix}
g_0 \\
g_1 \\
g_2 \\
\vdots \\
g_{k-1}
\end{bmatrix}
= \begin{bmatrix}
g_{00} & g_{01} & \cdots & g_{0,k-1} \\
g_{10} & g_{11} & \cdots & g_{1,k-1} \\
g_{20} & g_{21} & \cdots & g_{2,k-1} \\
\vdots & \vdots & \cdots & \vdots \\
g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,k-1}
\end{bmatrix}
\] (1)

then, can be calculated as follows:

\[
C = uG = (u_0, u_1, u_2, \ldots, u_{k-1})
= \begin{bmatrix}
g_0 \\
g_1 \\
g_2 \\
\vdots \\
g_{k-1}
\end{bmatrix}
= u_0g_0 + u_1g_1 + u_2g_2 + \ldots + u_{k-1}g_{k-1}
\] (2)

Because \( g_i, (0 \leq i \leq k-1) \) is \( 1 \times n \) matrix, the code length of the resulting codeword \( C \) is \( n \), the parity bit length is \( m = n-k \), and the code rate is \( r = k / n \), the check matrix \( H \) is a matrix. If the codeword \( C \) and check matrix \( H \) satisfy the equation

\[
s = CH^T = 0
\] (3)

Then the codeword \( C \) is a valid code word. And the generator matrix \( G \) and the parity check matrix \( H \) have the following relational expression

\[
GH^T = 0
\] (4)

When the parity check matrix of LDPC codes is represented by Tanner graph, its structure is shown in Figure 1. Tanner graph consists of two parts of the node: a part of the \( N \) variable nodes, with \( C \) to represent, each node corresponds to a check matrix or a codeword in the bit; the other part of the \( j \) check nodes is represented by \( S \), where each node represents a check equation or a row in the check matrix. When a bit in a codeword is included in a check equation, that is, when the check equation corresponding to the bit position is 1, the Tanner graph exists between the variable node and its corresponding check node Connection.

\[
H = \begin{bmatrix}
1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 1
\end{bmatrix}
\] (5)

The parity check matrix corresponding to equation (5) should satisfy the formula (3), which is

\[
s_0 = c_0 + c_1 + c_2 = 0 \\
s_1 = c_1 + c_4 + c_5 = 0 \\
s_2 = c_0 + c_4 + c_6 = 0 \\
s_3 = c_1 + c_4 + c_7 = 0
\] (6)
Figure 1 shows the form of the check matrix. The corresponding matrix is shown in equation (5).

In the above equation $S_m (M = 0, 1, 2, 3)$ corresponds to the check node in Figure 1, the error of any codeword $c_n$ in this formula will result in the result of the corresponding check equation $S_m$ is not 0. For example, when an error $c_0$ occurs, $S_1$ and $S_2$ the value is not 0, you can judge the error $c_0$, and correct.

For the above LDPC code check matrix, it satisfies the following four basic conditions:

1. Check matrix $H$ each row has $\rho'1'$, that is to say its line weight $\rho$;
2. Check matrix $H$ each column has $\gamma'1'$, that is, its column weight $\gamma$;
3. Check matrix $H$ any two rows (or two columns) between the same bit are '1' number does not exceed 1, if such a number is 2, we say it constitutes 4 ring, if there are four rings, try to eliminate the existence;
4. The value of $\rho$ and $\gamma$ is small compared with the code length and the number of rows of $H$ matrix, that is, most of the elements in the check matrix are '0', only a small number of elements are non-zero elements'1', That is to say that the parity check matrix of the LDPC code is a sparse matrix.

For matrices satisfying the above conditions, we refer to these codewords as rule codes, and we call these codewords as irregular codes for check matrices whose number of '1' in each row or column is not the same. In general, it is also referred to as regular and non-regular codes. In general, irregular codes have better decoding performance, but the number of '1' in each row and each column in the check matrix of irregular codes is different, which leads to higher coding and decoding complexity, The hardware implementation is also more complex, so the rule code encoding is considered.

3. LDPC codes’ construction and decoding algorithms

As early as 1962, Gallager had proposed LDPC codes in his doctoral dissertation and proved its excellent performance. However, due to application limitations and the VLSI technology at that time was not yet mature. So LDPC codes have not been developed. Attract enough attention. The invention of Turbo codes that can achieve performance close to the Shannon limit in 1993 caused an upsurge in the study of channel codes close to the Shannon limit. In 1996, Mackay et al. re-studied LDPC codes and found that LDPC codes can also achieve close to Shannon limits. Performance, LDPC codes have gained a new life.

3.1. LDPC codes’ construction

For channel coding, an important factor affecting coding performance is the minimum code distance. For LDPC codes, due to the limitation of the decoding algorithm, the distribution of degrees in the Tanner graph, the distribution of circles and the size of the girth will also affect the decoding performance. Usually we hope that the LDPC code has the smallest code weight, that is, the smallest code distance, and also hope to avoid the short circle in the Tanner graph. But these factors are contradictory. Increasing the minimum code weight of the LDPC code will inevitably increase the row weight and column weight of the check matrix $H$, and consequently the occurrence of short circles in the Tanner graph may increase. Therefore, for the LDPC code whose degree distribution polynomial has been determined, how to construct the check matrix $H$, which can increase the minimum code
weight while avoiding the existence of short loops, and has low hardware implementation complexity, has always become a hotspot in the research on LDPC codes.

Generally speaking, there are two ways to construct the parity check matrix of LDPC codes: one is random or pseudo-random structure, that is, under certain restrictions on factors such as degree distribution and minimum cycle length, computer search methods are used to perform Random or similar random generation of parity check matrix; the other is to use algebra or combination theory to construct the parity check matrix of LDPC code, so that it has a regular structure and is easy for theoretical analysis. Quasi-Cyclic LDPC is a very important type of LDPC code constructed according to the second method mentioned above. In addition, there are some construction methods related to hardware implementation.

3.2. LDPC codes’ decoding algorithm

The decoding algorithms of LDPC codes are mainly divided into two categories, hard decision decoding algorithms and soft decision decoding algorithms, which are shown in Figure 2. An important type of hard decision decoding algorithm is the Bit Flipping (BF) algorithm. The advantage of the BF algorithm is its low decoding complexity and simple implementation; its disadvantage is that the decoding performance is far from soft-decision decoding algorithm. An improvement of the BF algorithm is based on the Weighted Bit Flipping (WBF). The WBF algorithm uses the obtained bit reliability to weight the criteria during flipping. The WBF algorithm has a certain gain in performance due to the use of the reliability of the bits, but it is still hard decision decoding in essence, so it has the same decoding performance defects compared with the soft decoding method. The soft decoding method of LDPC mainly includes the Belief Propagation (BP) algorithm and its simplified algorithm, the minimum sum decoding algorithm (Min-Sum, MS). The BP algorithm is an iterative decoding algorithm that exchanges variables of the soft information between the node and the check node is used to achieve the purpose of decoding. The complexity of the BP algorithm mainly comes from the soft information calculation of the single check node. The MS algorithm reduces the complexity of the algorithm by simplifying the soft information calculation of the check node, and is more suitable for hardware implementation. However, there is a certain gap between MS algorithm and BP decoding algorithm in performance, so various improved versions have been proposed.

In addition, there are some 3.2. LDPC codes’ decoding algorithms, which involve the Descent Bit Flipping Algorithms (GDBF), Adaption Weight Multi-bit Flipping Algorithms (AWMBF), as well as Multi-Threshold Bit-Flipping Algorithm (MTBF).

4. Application Analysis of LDPC code for WN

Because LDPC codes have better performance than Turbo codes in many occasions, and have greater parameter flexibility and lower bit error rate, the decoding complexity is lower. In theory, complete
parallel operation can be achieved to implement into hardware conveniently. With the advantages of high-speed coding and decoding potential, LDPC codes have become a research hotspot in the field of channel coding. LDPC code is widely regarded as the channel coding scheme of the next generation mobile communication system. Now it has been adopted by many communication standards. The main advantages of LDPC are shown as follows:

1. Improving energy efficiency
   The adoption of LDPC codes will increase the computational complexity for wireless communication. Consequently, the energy consumption of information transmission for terminals will become larger. Fortunately, the LDPC provides the strong anti-interference ability, which allows the terminals to use lower transmit power, in order to decrease the PLR (packet loss rate). On the whole, the energy efficiency with LDPC codes can be enhanced.

2. Increasing transmission distance
   Considering LDPC codes can provide the reliable transmission in WNs, it means that longer transmission distance becomes longer at the same power consumption with LDPC codes. The advantage of this is that could reduce the number of deployed terminals, so that the deployment cost of the network is also reduced correspondingly. However, the resource limit of terminals also makes the application of LDPC codes in WNs have some limitations, which can be summarized as follows:
   1. Encoding length
      Since the computational power of the terminals is limited, and the decoding complexity of the LDPC code decoding algorithm increases linearly with the code length, the code length of the LDPC code applied to the Wireless Network should not be too long to be applied to calculate limits for terminals.
   2. Storage
      In recent years, with the development of electronic technology, the terminals of the internal storage, while also increasing, but its storage space is still limited. The parity check matrix of the LDPC code can be considered as a cyclist or quasi-cyclic construction in order to store only the position of '1' in one row or a certain column of the parity check matrix, and then cyclically shift to generate the entire matrix to reduce the storage of nodes.
   3. Decoding Complexity
      The higher the complexity of the decoding operation, the higher the energy consumption is required, and energy conservation has been an important issue in WN, so from the energy conservation point of view, the decoding complexity of the WN algorithm should not be too high. In view of the soft decision algorithm, there are a large number of floating-point and multiplication, the decoding complexity is higher, so we can consider some hard-decision algorithms, such as MTBF [18], code 1023, Which is 1 ~ 2dB compared with the performance of soft decision decoding, but the decoding complexity is greatly reduced compared with 4.4dB iteration 20 times.

5. Conclusion
   At present, the main work in the field of LDPC code research focuses on performance analysis of decoding algorithms, coding methods, code optimization algorithms, etc. The main research directions in the future include: LDPC code check matrix construction, and joint optimization design of LDPC coding systems, wireless fading channel and LDPC code performance analysis methods and optimization design criteria under MIMO technology.

   The optimization design of the existing LDPC codewords is mainly obtained under the additive white Gaussian noise channel, and under the wireless fading channel, especially the performance analysis method of the codeword under the nonlinear environment of the time-varying channel, the optimization design criteria and the influence of the channel estimation It is also a very critical topic and requires further research and exploration.
References

[1] Fang W, Zhang W, Liu Y, et al. (2020) BTDS: Bayesian-based trust decision scheme for intelligent connected vehicles in VANETs. Wiley Transactions on Emerging Telecommunications Technologies. 2020; e3879. doi: 10.1002/ett.3879

[2] Fang W, Chen W, Zhang W, et al. (2020) Digital signature scheme for information non-repudiation in blockchain: a state of the art review. EURASIP Journal on Wireless Communications and Networking. 2020, 56. doi: 10.1186/s13638-020-01665-w

[3] Fang W, Zhang W, Chen W, Liu Y, Tang C. (2020) TMSRS: trust management-based secure routing scheme in industrial wireless sensor network with fog computing. Wireless Networks, 26(5): 3169-3182. doi: 10.1007/s11276-019-02129-w.

[4] Fang W, Zhang W, Chen W, Pan T, Ni Y and Yang Y. (2020) Trust-based Attack and Defense in Wireless Sensor Networks: A Survey. Wireless Communications and Mobile Computing. doi: 10.1155/2019/2643546 (Early Access Paper)

[5] Fang W, Cui N, Chen W, Zhang W, Chen Y. (2020) A Trust-based Security System for Data Collecting in Smart City. IEEE Transactions on Industrial Informatics, doi: 10.1109/TII.2020.3006137 (Early Access Paper)

[6] Fang W, Zhang W, Shan L, Assefa B, and Chen W, (2020) Hierarchical Routing Protocol in Wireless Sensor Network: a State-of-the-art Review, International Journal of Computational Science and Engineering, 22(1): 107-113.

[7] Fang W, Xu M, Zhu C, Han W, Zhang W, Rodrigues Joel J. P. C. (2019) FETMS: Fast and Efficient Trust Management Scheme for Information-Centric Networking in Internet of Things. IEEE Access. 7(1): 13476-13485

[8] Fang W, Zhang W, Shan L, et al. (2020) DDTMS: Dirichlet-Distribution-Based Trust Management Scheme in Internet of Things. Electronics, 2019, 8(7), 744; doi: 10.3390/electronics8070744.

[9] Fang W, Zhang W, Zhao Q, et al. (2019) Comprehensive analysis of secure data aggregation scheme for industrial wireless sensor network. Computers, Materials and Continua, 61(2): 583-599.

[10] Fang W, Zhang C, Chen W, et al. (2018) An Energy-efficient Secure AODV Protocol in Industrial Sensor Network. Journal of Internet Technology. 19(1): 237-246.

[11] Fang W, Zhang W, Xiao J, et al. (2017) A Source Anonymity-based Lightweight Secure AODV Protocol for Fog-based MANET. SENSORS, 17(6): 1421; doi: 10.3390/s17061421

[12] Fang W, Zhang W, Yang Y, Liu Y, Chen W. (2017) A resilient trust management scheme for defending against reputation time-varying attacks based on BETA distribution. SCIENCE CHINA Information Sciences, 2017, 60(4): 040305, doi: 10.1007/s11432-016-9028-0

[13] Fang W, Zhang C, Shi Z, Zhao Q, Shan L. (2016) BTRES: Beta-based Trust and Reputation Evaluation System for Wireless Sensor Networks. Journal of Network and Computer Applications. 59(1): 88-94.

[14] Fang W, Li F, Sun Y, Shan L, Chen S, Chen C, and Li M. (2016) Information Security of PHY Layer in Wireless Networks. Journal of Sensors. Volume 2016, Article ID 1230387, 10 pages. doi: 10.1155/2016/1230387.

[15] Fang W, Shan L, Jia G, Ji X, Chen S. (2016) A Low Complexity Secure Network Coding in Wireless Sensor Network. Journal of Internet Technology. 17(5): 905-913.

[16] Chen T C. (2013) Adaptive-Weighted Multibit-Flipping Decoding of Lowdensity Parity-check Codes based on Ordered Statistics. IET Communication, 14(3): 1517-1521.