Simulation Analysis of Multiple BP Decoding Algorithm and FFT-BP Decoding Algorithm

Xin Wei, Zhigang Li, Zheng Dou

College of Information and Communication Engineering, Harbin Engineering University, Harbin, China
Email: weixin@hrbeu.edu.cn

Abstract

In order to solve the problem that the original decoding algorithm of multi-band LDPC codes is high and is not conducive to hardware implementation, two simplified decoding algorithms for multi-band LDPC codes are studied: the reliability propagation based on fast Fourier transform Code algorithm (FFT-BP) and log-BP decoding algorithm based on logarithmic operations. The simulation results show that the FFT-BP decoding algorithm is more convenient and efficient.

Keywords

LDPC, FFT-BP, BP

1. Introduction

Multicomponent coding is the key technology of multivariate wireless transmission, and its core lies in multivariate codec. Most of the current multi-code modulation using multiple LDPC code, multi-LDPC code was first proposed by Gallager, 1998 Davey and MacKay studied the finite field of multiple LDPC code. Compared with the binary LDPC code, the main advantages of multiple LDPC codes are reflected in the following aspects: 1) better error correction performance: multiple LDPC code will be a number of bits into a multi-symbol, which has the potential of eliminating LDPC code small ring of binary map and getting better error correction performance; 2) Strong anti-burst error capability: Because of Multiple LDPC codes making multiple burst bit errors can be combined into fewer multi-symbol errors, the error correction performance is better than binary LDPC codes; 3) Suitable for high-speed transmission: Based on high-order finite-domain multivariate LDPC codes are designed and are well suited for combining high-order modulation schemes with multi-antenna systems to pro-

vide higher data rates and spectral efficiency. It can be seen that multi-LDPC coding and modulation technology is more suitable for wireless channel transmission [1].

2. Multivariate LDPC Coding Algorithm

2.1. Definition and Operation of Finite Field GF (*q*) Domain

Field F is a set of elements that define two operations, plus "+" and multiplication " "and both of which satisfy the law of union, distribution law, and exchange law, both of these operations are closed [2], that is, for any, there are: $\alpha + \beta \in F, \alpha \bullet \beta \in F$.

If there is a domain F which has only a finite number of *q* elements, then the domain is called a finite field, or Galois Filed, denoted as GF (*q*). There is a finite field GF (*q*) only if *q* is a power of prime number, the extended domain GF (p^m) can be constructed according to the base domain GF (*p*) domain. The extension field GF (2^m) of the binary domain GF (2), where any of the nonzero elements can be expressed by the power of α. In the infinite set of elements, the elements are generated according to element set $\{0, 1, \cdots, \alpha\}$

$$F = \{0, 1, \alpha, \cdots, \alpha^i, \cdots\} = \{0, \alpha^0, \alpha^1, \cdots, \alpha^i, \cdots\} \tag{2-1}$$

The last element in the field is obtained by multiplying the previous element α. The domain *F* must be conditional so that the domain can contain only 2^m element to get the GF (2^m) field. The multiplicative closure of domain *F* can be represented by an irreducible polynomial (2-2), that is:

$$\alpha^{2^{m-1}} + 1 = 0 \tag{2-2}$$

Then $\alpha^{2^{m-1}} = 1 = \alpha^0$. According to the polynomial constraint, any element whose power is greater than or equal to 2^{m-1} is reduced to an element whose power is less than 2^{m-1}, that is:

$$\alpha^{2^m+n} = \alpha^{2^m-1}\alpha^{n+1} = \alpha^{n+1} \tag{2-3}$$

So the elements of the finite field GF (2^m) are:

$$GF(2^m) = \{0, \alpha^0, \alpha^1, \cdots, \alpha^{2^m-2}\} \tag{2-4}$$

2.2. Construction of Multiple LDPC Codes

The multi-band LDPC code defined on the finite field GF (*q*), which evaluates the value of the nonzero element $\{0, 1, \cdots, q-1\}$ in the matrix *H* on the GF (*q*), Where *q* is a prime or prime power, which is constructed in a manner similar to that of a binary construct, requiring the following characteristics when constructing a rule sparse check matrix *H*:

1) Row weight *p*, column weight *q*, *p* and *q* are very small with respect to *m* and *n*.

2) In H, any two rows and two columns of the corresponding position on the same non-zero elements no more than one.

The irregular polygon LDPC codes *p* and *q* are not fixed. The second row

constraint ensures that the constructed parity check matrix has no four rings on its Tanner graph [3], thereby further improving its coding performance. And for the multi-band LDPC codes, there is a fixed relationship between the symbol symbols and the bits relative to the binary code of the same length, so that it has not only good ability to correct random errors, but also has a good Correct the performance of sudden errors. In the literature [4], it is shown that the LDPC codes with better short and medium length have better potential performance. Similar to the construction of binary LDPC parity check matrix, the construction of LDPC parity check matrix is divided into two categories: One is the random construction method; the second is the algebraic construction method. The first class of construction methods, mainly divided into Gallger structure method, PEG construction method, Bit-filling, Mackey structure method [5] four kinds of algorithms. The Gallger construction method and the Mackey construction method are mainly applied to the construction of regular LDPC codes, while the other two can be used to construct irregular LDPC codes. In the design of the LDPC code, it is the premise of the random construction method to know the distribution of the check node and the variable node. The distribution is generally obtained by EXIT, density evolution or Gaussian approximation. Although the LDPC codes constructed by the random method have strong randomness and good progress, the parity check matrix has no regularity, and the coding and hardware implementation are high in complexity. Generally, this kind of construction is not adopted.

Compared with the random construction method, LDPC codes constructed by combinatorial and algebraic methods have little difference in performance loss and low hardware implementation. The algebraic construction method with the theoretical research value is composed of the LDPC code and the quasi-cyclic LDPC codes with quasi-cyclic algebra structure proposed by Tanner and Fossorier *et al.*, however, the parameters of the algebraic structure of the regular LDPC code length, bit rate and other parameters of the selectivity is not strong, cannot be pre-set code length and bit rate, which can be based on these parity check matrix itself to determine the code length and bit rate and other parameters. On the basis of Tanne and Fossorier *et al.*, Lin S. propose a method for constructing quasi-cyclic LDPC codes based on finite field GF (q) and affine mapping [6].

For multivariate QC-LDPC coding, since the generation matrix of multiple LDPC codes and binary LDPC is similar in construction, therefore, according to the construction of binary QC-LDPC, and each sub-matrix is independent, it is only necessary to obtain the generator in its generation matrix *G*, which can be encoded in serial or parallel way.

The information sequence is denoted as $s = [s_1, s_2, \cdots, s_{L-J}]$, where $s = [s_1, s_2, \cdots, s_{L-J}]$ represents the symbols contained in the segment. After encoding it, we can get the encoded codeword sequence $c = sG = [s, p_1, p_2, \cdots, p_J]$, then the code after the paragraph of the parity bit code is:

$$p_j = s_1 G_{1,j} + s_2 G_{2,j} + \cdots + s_{(L-J)} G_{(L-J),j}.$$

3. Multivariate LDPC Decoding Algorithm

At present, the practical implementation of multi-band LDPC code coding structure is no longer difficult, but the multi-band LDPC decoding of the highly complex problem has not been a very good solution. Davey and MacKay put forward the classic belief transmission (Belief Propagation, BP), the core idea is to pass the Tanner map to probability information [7], will be divided into check node and variable node update two processes. However, compared with the binary, multi-LDPC code encoding process is based on GF (q) domain, thus, the elements that are passed between every two nodes in the Tanner graph are no longer only "0" or "1", but are , they cannot be expressed directly in a connected way, instead of adding to the replacement node. As shown in **Figure 1**.

3.1. Multiple BP Decoding Algorithm

Binary and multivariate LDPC codes can adopt BP decoding algorithm, but the two are slightly different in the process, in which the multiple BP decoding algorithm has message replacement and inverse permutation process. In the decoding process, we must first calculate the initial probability information, in practice, usually among the multi-band values are independent of each other, therefore, an element on the GF (q) ($q = 2^b$) field can be represented by a b-bit binary sequence, there is a relationship between the initial probability information of the binary and multivariate ($q = 2^b$) LDPC codes [9]:

$$f_n^a = \prod_{i=0}^{b-1} g_{n_i}^{a_i} \qquad (3\text{-}1)$$

Among them, $a \in (0, 1 \cdots, q-1)$, f_n^a is the probability of the q corresponding, $a = (a_0, a_1 \cdots, a_{b-1})$, $g_{n_i}^{a_i}$ is the binary probability of taking a_i. For f_n^a, $g_{n_i}^{a_i}$ according to the channel conditions and modulation methods, the value is different.

The decoding process of multiple LDPC codes can be summarized as follows:

1) Initialization: The variable node q_{mn}^a initial channel probability probability f_n^a:
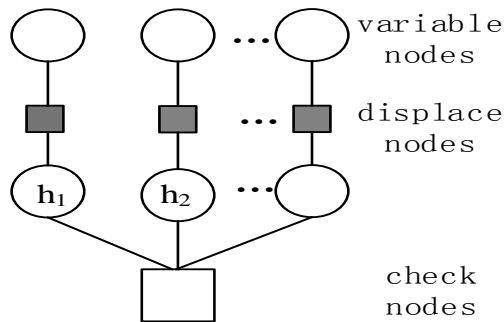

Figure 1. Multivariate LDPC code Tanner connection diagram.

$$q_{mn}^a = f_n^a \tag{3-2}$$

2) Information replacement: Unlike binary LDPC code BP decoding, it is necessary to transpose the variable node information sequence. The rule is that the value of each variable in the information sequence is multiplied by h_{mn} (Non-zero elements in row m and column n of the parity check matrix), the multiplication of ah_{mn} is in the GF (q) field, which is equivalent to a permutation of the transmitted information. Similarly, the way reversal is similar.

$$q_{mn}^{\prime a} = q_{mn}^{ah_{mn}} \tag{3-3}$$

3) Check node update: Check the node information r_{mn}^a according to the full probability formula can be expanded to the following formula:

$$
\begin{aligned}
r_{mn}^a &= P\left(c_m = 0 \middle| x_n = a\right) \\
&= \sum_{V:x_n=a} P\left(c_m = \sum_{n' \in N(m)} h_{mn'} = 0 \middle| V\right) P\left(V \middle| x_n = a\right) \\
&= \sum_{V:x_n=a} P\left(c_m = \sum_{n' \in N(m)} h_{mn'} = 0 \middle| V\right) \prod_{n' \in N(m)\backslash n} P\left(x_{n'}\right) \\
&= \sum_{V:x_n=a} P\left(c_m = \sum_{n' \in N(m)} H_{mn'} x_{n'}\right) \prod_{n' \in N(m)\backslash n} q_{mn'}^{\prime a}
\end{aligned} \tag{3-4}
$$

where V represents the set of vectors satisfying the math parity equation c_m.

4) Replacement: This process is the inverse of the check node transfer message and the parameter h_{mn} (the m row and the n column in the parity check matrix), and the reverse of the process (2):

$$r_{mn}^{\prime a} = r_{mn}^{ah_{mn}^{-1}} \tag{3-5}$$

5) Variable Node Update: After the transcoding of the check node information by the process (4), the new check sequence $r_{mn}^{\prime a}$ $\left\{a \in (0,1,\cdots,q-1)\right\}$ is obtained. According to the Bayesian formula,

$$
\begin{aligned}
q_{mn}^a &= P\left(x_n = a \middle| \{c_k\}_{k \in M(n)\backslash m}, y_n\right) \\
&= \frac{P\left(x_n = a \middle| y_n\right)}{P\left(\{c_k\}_{k \in M(n)\backslash m} \middle| y_n\right)} P\left(\{c_k\}_{k \in M(n)\backslash m} \middle| x_n = a, y_n\right) \\
&= \frac{P\left(x_n = a \middle| y_n\right)}{P\left(\{c_k\}_{k \in M(n)\backslash m} \middle| y_n\right)} \prod_{k \in M(n)\backslash m} P\left(c_k \middle| x_n = a, y_n\right) \\
&= \alpha_{mn} f_n^a \prod_{k \in M(n)\backslash m} r_{kn}^{\prime a}
\end{aligned} \tag{3-6}
$$

In order for equation $\sum_{a=0}^{q-1} q_{mn}^a = 1$ to be established, the introduction coefficient α_{mn} completes the normalization of the equation.

6) Posterior probability of the calculation, the decision:

$$P\left(x_n = a \middle| y_n, \{c_k\}_{k \in M(n)}\right) = z'_n r^a_{mn} q^a_{mn} = z'_n f^a_n \prod_{k \in M(n)} r^a_{kn} \quad (3\text{-}7)$$

The decision to use the information from the information and outside the information, rather than the variable node update, just update the external information.

Perform a hard decision expression:

$$\hat{x}_n = \arg\max_a P\left(x_n = a \middle| y_n, \{c_k\}_{k \in M(n)}\right) = \arg\max_a r^a_{mn} q^a_{mn} \quad (3\text{-}8)$$

Selecting the highest codeword as the decision codeword, and finally obtaining $\hat{\boldsymbol{x}} = [x_1, x_2 \cdots x_N]^T$, If the equation $\mathbf{H}\hat{\boldsymbol{x}} = \mathbf{0}$ is satisfied, the decoding can be ended, otherwise the operation (2) is continued until the equation is established or the iteration is reached.

3.2. FFT-BP Decoding Algorithm

In the traditional BP decode algorithm, the check node update process uses many addition and multiplication operations. In the hardware implementation, it will seriously consume the logic resources, which will affect the practical application to a large extent. (3)-(4) can be regarded as convolution in the BP decoding algorithm, and the algorithm is optimized for this performance. A FFT-BP decoding algorithm is proposed, in the process of decoding iterations, fast Fourier transform (Fast Fourier Transform) is introduced to transform the convolution of the time domain into the product of the frequency domain [10], thus simplifying the process (3), while the other process does not change, the complexity. Since the operation in the multivariate BP decoding algorithm process (3) is based on the GF (q) domain ($q = 2^b$), when the FFT operation is used, it becomes a b-dimensional 2-point FFT operation. In the GF (4) domain, that is, (b = 2) has a 2-dimensional 2-point FFT operation, the expression is:

$$
\begin{aligned}
F^0 &= [f^0 + f^1] + [f^2 + f^3] \\
F^1 &= [f^0 - f^1] + [f^2 - f^3] \\
F^2 &= [f^0 + f^1] - [f^2 + f^3] \\
F^3 &= [f^0 - f^1] - [f^2 - f^3]
\end{aligned}
\quad (3\text{-}9)
$$

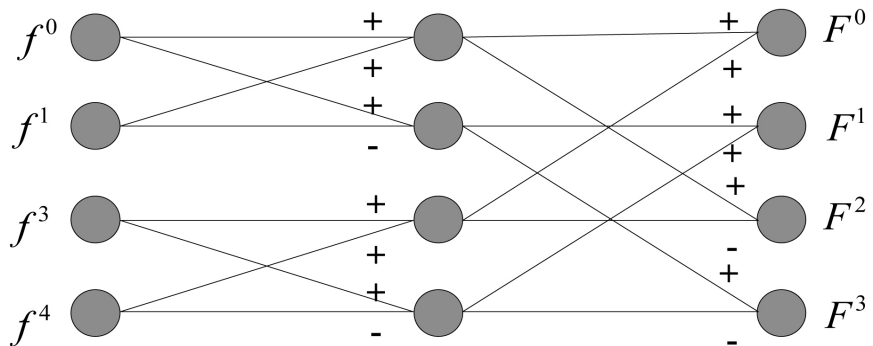When GF (4), the corresponding butterfly chart as shown in **Figure 2**.

Figure 2. FFT-BP algorithm based on GF (4) butterfly chart.

The initialization process in the FFT-BP decoding algorithm is the same as the BP decoding algorithm. The iterative decoding steps are as follows:

1) FFT transforms the information variables to obtain intermediate values $\left(\hat{q}_{mj}^0, \hat{q}_{mj}^1, \cdots, \hat{q}_{mj}^{q-1}\right)$

$$\left(\hat{q}_{mj}^0, \hat{q}_{mj}^1, \cdots, \hat{q}_{mj}^{q-1}\right) = \text{FFT}\left(q_{mj}^0, q_{mj}^1, \cdots, q_{mj}^{q-1}\right), j \in N(m) \tag{3-10}$$

2) Make $\left(\hat{q}_{mj}^0, \hat{q}_{mj}^1, \cdots, \hat{q}_{mj}^{q-1}\right)$ accumulate operations according to the following formula:

$$\left(\prod_{j \in N(m)\backslash n} \hat{q}_{mj}^0, \prod_{j \in N(m)\backslash n} \hat{q}_{mj}^1, \cdots, \prod_{j \in N(m)\backslash n} \hat{q}_{mj}^{q-1}\right) \tag{3-11}$$

3) Transform the results obtained by the above formula:

$$\left(r_{mn}^0, r_{mn}^1, \cdots, r_{mn}^{q-1}\right) = \text{IFFT}\left(\prod_{j \in N(m)\backslash n} \hat{q}_{mj}^0, \prod_{j \in N(m)\backslash n} \hat{q}_{mj}^1, \cdots, \prod_{j \in N(m)\backslash n} \hat{q}_{mj}^{q-1}\right) \tag{3-12}$$

Due to the fast Fourier transform introduced in the FFT-BP decoding algorithm, the convolution of the time domain becomes the product of the frequency domain, which simplifies the updating process of the check node to a certain extent, Compared with the BP decoding algorithm, the complexity of the FFT-BP decoding algorithm is reduced, but it can be seen from Equation (3)-(12) whether a lot of multiplication is required, so it need to use a large number of multipliers, and high precision for data accuracy, in the hardware implementation, still need to take up more hardware resources.

4. Simulation Analysis

The FFT-BP decoding algorithm is based on the traditional BP decoding algorithm, and the fast Fourier transform algorithm is used to replace the convolution operation in the variable node updating process of the BP decoding algorithm, reducing the amount of computation and speeding up the decoding rate. At the same time, compared with the traditional BP decoding algorithm, because of the use of fewer multipliers, so the hardware is also more convenient to achieve, improve the hardware resource utilization. The simulation results are shown in **Figure 3**:

It can be seen from the simulation results that the multivariate BP decoding algorithm and the FFT-BP decoding algorithm are simplified by the fast Fourier transform performance and simplification of the operation due to the same information probabilistic initialization method. The performance of the decoding algorithm is the same, but the FFT-BP decoding algorithm is more convenient and efficient.

Acknowledgements
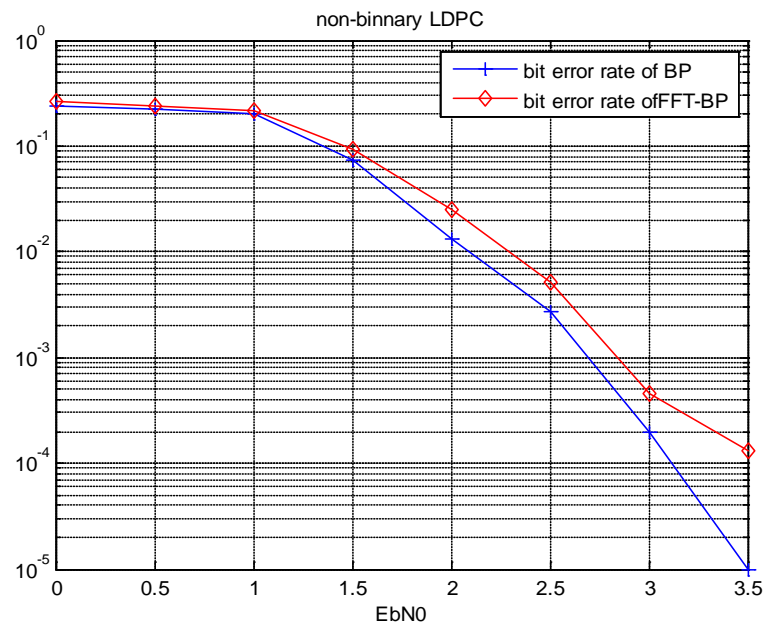
Figure 3. Simulation results.

References

[1] Rui, X., Qiang, W. and Xi, C.X. (2015) Dynamic Iterative Stop Algorithm in Multivariate LDPC-CPM System. *Applied Science and Technology*, No. 1, 169-174.

[2] Guang, H.H. and Bao, M.B. (2011) Implementation of Multivariate LDPC Decoder Using EMS Algorithm. *Journal of Xidian University*, No. 5, 27-33.

[3] Yu, Y., Hui, C.L., Xue, S.L. and Xing, C.L. (2012) Design and FPGA Implementation of Multipath LDPC Code Decoder Based on FFT-BP Algorithm. *Journal of Circuits and Systems*, **4**, 7-12.

[4] Ten, S. (2013) Convergence of Iterative Decoding. *Electron. Lett*, **37**, 806-808.

[5] Ping, N. (2014) Implementation and Simulation of LDPC Coding in IEEE 802.16e Standard. *Application of Electronic Technology*, **15**, 101-104.

[6] Ming, Z.W. (2016) Design and FPGA Implementation of High Speed LDPC Codec. University of Electronic Science and Technology.

[7] Rui, L. (2014) Research and Implementation of QC-LDPC Coding Algorithm in WIFI System. University of Electronic Science and Technology.

[8] Liu, B., Gao, J., *et al.* (2011) Weighted Symbol-Flipping Decoding Algorithm for Non-Binary LDPC Codes with Flipping Patterns. *Journal of Systems Engineering and Electronics*, **22**, 848-855. https://doi.org/10.3969/j.issn.1004-4132.2011.05.018

[9] Cong, Y.H. (2016) Research on Encoding Implementation of LDPC Codes. Harbin Institute of Technology.

[10] Richardson, T.J., Shokrollahi, M.A. and Urbanke, R.L. (2015) Design of Capacity-Approaching Irregular Low-Density Parity-Check Codes. *IEEE Transactions on Information Theory*, **47**, 619-637. https://doi.org/10.1109/18.910578

Submit or recommend next manuscript to SCIRP and we will provide best service for you:

Accepting pre-submission inquiries through Email, Facebook, LinkedIn, Twitter, etc.

A wide selection of journals (inclusive of 9 subjects, more than 200 journals)

Providing 24-hour high-quality service

User-friendly online submission system

Fair and swift peer-review system

Efficient typesetting and proofreading procedure

Display of the result of downloads and visits, as well as the number of cited articles

Maximum dissemination of your research work

Submit your manuscript at: http://papersubmission.scirp.org/

Or contact ijcns@scirp.org