Optimized Puncturing of the Check Matrix for Rate-Compatible LDPC Codes

Liang Zhang, Jiahui Meng, Danfeng Zhao

College of Information and Communication Engineering, Harbin Engineering University, Harbin 150001, China

Abstract. In the wireless communication system, it is necessary to change the transmitted code word or code rate in real time according to the channel environment, designing and implementing rate compatible codes is of great practical significance. In allusion to the defects of algebraically constructed QC-LDPC codes algorithm and the time-varying characteristics of wireless channel, we propose an algorithm based on check matrix optimization puncturing technique to construct QC-LDPC codes in this paper. The algorithm selects a high rate matrix with excellent performance as the parent matrix, and then uses the backward node puncturing method to puncture the information bits in the code word from the last column of the check matrix by a multiple of the number of rows to obtain a low rate matrix. The simulation results show that the rate-compatible non-binary LDPC codes constructed by this algorithm not only reduces the complexity of hardware implementation, but also improves the error correction performance of the non-binary LDPC codes, realizes the rate-compatible coding at the same time, and improves the average effectiveness and reliability of the communication system.

1 Introduction

Low density parity check code (LDPC) [1-3], which is a good code for error correction performance close to Shannon limit, has become one of the research hot spots in recent years. The Quasi-Cyclic LDPC (QC-LDPC) code [4,5] is a very important type of LDPC code. Compared with a general LDPC code, it has a simpler coding and decoding complexity and it is very suitable for practical applications and realizations. Furthermore, the excellent performance can be achieved through the design of the structuring and degree distribution. At present, it has become a standard code word for many systems, such as deep space communication [6], DVB-S2 [7], WIMAX [8]. In wireless communication applications, the channel state changes continuously with time. In order to maximize the wireless communication throughput, it is necessary to change the code rate according to the channel state. Therefore, it is practically meaningful to implement a rate-compatible puncture code design. Puncture techniques are widely used in different types of forward error correction codes [9,10]. The rate-compatible code is a code containing a series of code rates, where the low code rate is included in the code of the high code rate [11]. In 2002, Li and Narayanan proposed a rate-compatible code based on LDPC, also known as rate-compatible LDPC (RC-LDPC). The puncturing technique was introduced to generate RC-LDPC codes by which a series of low rate codes can be obtained directly from a high code rate codes.

In this paper, according to the defects of QC-LDPC codes constructed by traditional algebra and the time-varying characteristics of wireless channels, an algorithm based on check matrix optimized puncturing technique to construct QC-LDPC codes (OPPMRC-LDPC) is proposed. The algorithm firstly selects a high code rate parent matrix with excellent performance, then uses the method of backward node puncturing method to delete the column from the end of the check matrix. The information bits in the codeword are punctured to obtain a low code rate codeword to achieve rate compatibility. By designing a set of check matrix that can be compatible with a variety of code rate QC-LDPC codes, the same codec and decoder can be used to complete different code rate switching, and each code rate has excellent error correction performance. The QC-LDPC codes constructed by this algorithm not only reduces the complexity compared with the traditional random structure method, but also does not generate the loop with a length of four. Then, through the design of the degree distribution, a lower error leveling layer code can be obtained, which not only reduces the hardware implementation complexity, but also improves the error correction algorithm, and at the same time impros the average effectiveness and reliability of the communication system. OPPMRC-LDPC has the same performance in each code rate as a single constructed LDPC code of the same code length with an optimal degree distribution.

2 Principle of algorithm

Designing an error correction coding system involves selecting a fixed code which has a certain code rate and error correction capabilities to adapt to the expected average or worst channel conditions. However, in many cases, it is more desirable to be flexible because the transmitted data has different protection requirements, and the channel is time-varying or its parameters are uncertain. Therefore, flexible channel coding and adaptive decoders are needed. This flexible system can be achieved by using a set of decoders, but in this case the hardware implementation complexity will increase significantly. Therefore, rate-compatible codes are introduced in systems with stringent hardware complexity requirements. In order to improve the transmission efficiency, it is desirable to transmit the check information as little as possible. On this foundation, we propose the OPPMRC-LDPC algorithm.

The design steps of specific error correction coding system are as follows:

1. Using PEG algorithm to generate basic matrix

Given the number of symbol nodes, check nodes, and symbol node degrees in the Tanner graph to be constructed, the edges between the symbol nodes and the check nodes are placed one by one so that each newly added edge affects the current graph as little as possible. That is, each non-zero element on the GF(q) field newly added to the check matrix H affects the girth of the current graph as little as possible.

2. Using QC-LDPC algorithm to generate a check matrix

(1) According to a specific degree distribution, a PEG algorithm is used to obtain a $J \times L$ dimensional binary basic matrix $\boldsymbol{H}_m = [m_{j,l}]$;

(2) Following the sequential trial method to determine the cyclic shift coefficient matrix $S_{J\times L}$;

A. If the number of row j and column l in H_m is "0", then the corresponding position shift coefficient $s_{j,l}$=Inf ;

B. If the number of row j and column l in H_m is "1", then any number of $s_{j,l}$ in $\{0,1,\cdots,p-1\}$ will be selected. According to the determined loop length, using equation (1) to determined whether $s_{j,l}$ meets the requirements of the constraint type, if it meets the requirement, the number of $s_{j,l}$ is determined; if it does not meet the requirement, the new number is determined from B again;

$$\sum_{k=1}^{m}\left(s_{j_k,l_k}-s_{j_{k+1},l_k}\right)\neq 0 \bmod p \qquad (1)$$

Among them, $2 \le m \le i$, $1 \le j_k \le J$, $1 \le j_{k+1} \le J$, $1 \le l_k \le L$, $j_0 = j_m$.

C. The "1" in the basic matrix of the selected coefficient is replaced with a randomly selected number in $1,2,\cdots,q-1$ to generate a non-binary matrix.

(3) The corresponding basic matrix $\boldsymbol{H}_m = [m_{j,l}]$ and its cyclic shift coefficient matrix $S_{J\times L}$ are obtained, and the zero matrix is used to replace the "0" element at the position of (m,n) in H_m. The "1" element at the position of (m,n) in H_m is replaced by a non-binary matrix right shifted by $s_{j,l}$, finally, we can obtain the required check matrix $H_{(p\times J)\times(p\times L)}$.

The selection of non-binary numbers in each matrix block and the determination of the shift factor of each matrix block must be based on the principle of reducing or eliminating short loops. If the constructed matrix does not meet the requirements, it is necessary to reselect the shift factor or non-binary domain number. Due to the randomness in choosing the shift factor and the non-binary field number, the short loop of the matrix needs to be finally counted. The matrix which has too many short loops are directly discarded, the high-performance check matrix is searched again. That is a search and comparison process, the process stops until a good matrix is found to meet the requirements.

3. A puncturing algorithm based on check matrix optimization is compatible with multiple code rates

The implementation process of the puncturing algorithm based on check matrix optimization is to first select a high-rate parent code with excellent performance generated by the QC-LDPC codes check matrix construction algorithm described above, and then use the backward node puncturing algorithm to puncture the information bits in the codeword. That is, starting from the last column of the check matrix, several columns in the check matrix (m is the number of check matrix rows) are deleted in multiples of m, so as to obtain the required codeword with a low code rate. In case of good channel conditions, a high code rate QC-LDPC codes may be used. Conversely, when the channel environment is poor, a low code rate QC-LDPC codes may be used, thereby the efficiency of the communication system is improved. Since the non-zero elements in the puncturing matrix are sparse and have a certain regularity, the hardware implementation complexity of a code rate-compatible non-binary LDPC code communication system can be greatly reduced.

Given the puncturing code rate r_m, Gaussian approximation-based density evolution algorithm can be used to obtain the degree distribution under this rate condition. According to the optimized degree distribution, a puncturing algorithm optimized by the check matrix is used to obtain the non-binary LDPC code word under the punctured code rate r_m. From the perspective of hardware realizability and real-time performance, this scheme has practical significance.

4. Coding using partial parallel QC-LDPC codes encoding algorithm

The sub-matrix of the QC-LDPC generator matrix has a cyclic shift form, so that only the first row in the sub-matrix is stored, and the remaining elements are cyclically shifted by the first row, thereby the amount of encoding operations and storage is reduced. So we can use partial parallel encoding method to increase coding efficiency and reduce complexity. The check matrix of the non-binary QC-LDPC codes consists of $a \times b$ cyclic matrices of size $q \times q$, whose structure is shown in equation (2). $\boldsymbol{H}_{i,j}$ is a cyclic matrix or zero matrix of size $q \times q$, the code length is $n = b \times q$, and the check bit length is $m = a \times q$.

$$\boldsymbol{H} = \begin{bmatrix} \boldsymbol{H}_{1,1} & \boldsymbol{H}_{1,2} \cdots \boldsymbol{H}_{1,(b-a)} & \boldsymbol{H}_{1,(b-a+1)} \cdots & \boldsymbol{H}_{1,(b-1)} & \boldsymbol{H}_{1,b} \\ \boldsymbol{H}_{2,1} & \boldsymbol{H}_{2,2} \cdots \boldsymbol{H}_{2,(b-a)} & \boldsymbol{H}_{2,(b-a+1)} \cdots & \boldsymbol{H}_{2,(b-1)} & \boldsymbol{H}_{2,b} \\ \vdots & & & \vdots & \\ \boldsymbol{H}_{a,1} & \boldsymbol{H}_{a,2} \cdots \boldsymbol{H}_{a,(b-a)} & \boldsymbol{H}_{a,(b-a+1)} \cdots & \boldsymbol{H}_{a,(b-1)} & \boldsymbol{H}_{a,b} \end{bmatrix} \quad (2)$$

The check matrix must be a full rank matrix. The check matrix can be represented as $\boldsymbol{H} = \begin{bmatrix} \boldsymbol{M} & \boldsymbol{D} \end{bmatrix}$, among that, $\boldsymbol{D}$ is composed of $a \times a$ cyclic matrix or zero matrix. The structure of the generator matrix obtained by the non-binary QC-LDPC check matrix conversion is shown in equation (3). The generator matrix consists of $(b-a) \times b$ circular matrices of size $q \times q$, and $\boldsymbol{I}$ is of size $q \times q$. In the matrix, $\boldsymbol{O}$ is a zero matrix of size $q \times q$, and $\boldsymbol{G}_{i,j}$ is a cyclic matrix of size $q \times q$.

$$\boldsymbol{G} = \begin{bmatrix} \boldsymbol{G}_1 \\ \boldsymbol{G}_2 \\ \vdots \\ \boldsymbol{G}_{b-a} \end{bmatrix} = \begin{bmatrix} \boldsymbol{I} & \boldsymbol{O} & \cdots \boldsymbol{O} & \boldsymbol{G}_{1,1} & \boldsymbol{G}_{1,2} & \cdots \boldsymbol{G}_{1,a} \\ \boldsymbol{O} & \boldsymbol{I} & \cdots \boldsymbol{O} & \boldsymbol{G}_{2,1} & \boldsymbol{G}_{2,2} & \cdots \boldsymbol{G}_{2,a} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \boldsymbol{O} & \boldsymbol{O} & \cdots \boldsymbol{I} & \boldsymbol{G}_{(b-a),1} & \boldsymbol{G}_{(b-a),2} & \cdots \boldsymbol{G}_{(b-a),a} \end{bmatrix} \quad (3)$$

The generator matrix can be represented as $\boldsymbol{G} = \begin{bmatrix} \boldsymbol{U} & \boldsymbol{Z} \end{bmatrix}$, $\boldsymbol{U}$ is made up of $(b-a) \times (b-a)$ cyclic matrices of size $q \times q$, and $\boldsymbol{Z}$ is composed of $(b-a) \times a$ cyclic matrices of size $q \times q$. Because the generator matrix and check matrix are satisfied $\boldsymbol{H} \times \boldsymbol{G}^{\mathrm{T}} = \boldsymbol{0}$, you can get:

$$\boldsymbol{M} \times \boldsymbol{U}^{\mathrm{T}} + \boldsymbol{D} \times \boldsymbol{Z}^{\mathrm{T}} = \boldsymbol{0} \quad (4)$$

Since $\boldsymbol{H}$ is a full rank matrix, we have:

$$\boldsymbol{Z}^{\mathrm{T}} = -\boldsymbol{D} \times \boldsymbol{M} \times \boldsymbol{U}^{\mathrm{T}} \quad (5)$$

Let $\mathbf{z}_i = [\mathbf{g}_{i,1}, \mathbf{g}_{i,2}, \cdots, \mathbf{g}_{i,a}]$ be the first row of $[\mathbf{G}_{i,1}, \mathbf{G}_{i,2}, \cdots, \mathbf{G}_{i,a}]$ in the $\boldsymbol{Z}$ matrix, and $\mathbf{g}_{i,j}$ be the generator of $\mathbf{G}_{i,j}$. Since the generator matrix $\boldsymbol{G}$ is also composed of a cyclic matrix, partial parallel encoding is used for encoding. The SSRAA unit with the number a is simultaneously calculated to obtain all the check bits $\mathbf{p} = [\mathbf{p}_1, \mathbf{p}_2, \cdots, \mathbf{p}_a]$. Figure 1 shows the partial parallel coding structure of SSRAA-based non-binary QC-LDPC codes. It makes only $q(b-a)$ clock cycles to calculate all a segment check bits, which is a times faster than the classic encoding method.

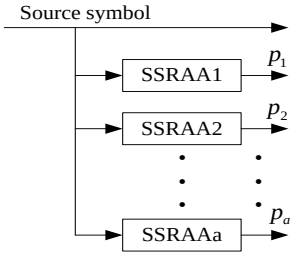

Figure 1. Partial parallel coding structure of non-binary QC-LDPC codes.

5. The software simulation part uses the Mixed Log-FFT-BP decoding algorithm to decode

In order to reduce the computational complexity, the Mixed Log-FFT-BP algorithm is used for decoding. The algorithm transforms the multiplication in the frequency domain into addition and lookup table operations in logarithmic domain, and then directly calculates the logarithm of the probability information to decode it in the logarithmic domain, which saves the process of solving the log-likelihood ratio, thereby computational complexity is reduced.

3 Simulation analysis

On the basis of QC-LDPC coding and Mixed Log-FFT-BP decoding, we analyzed the performance of the constructed check matrix. The parameters are set as follows: the number of multiple domains is 8, the code rate is 1/2, 2/3, 3/4, the maximum iteration number is 20 times, the fixed check bits number is 576bit, the channel is Gauss white noise channel, and BPSK modulation is used. The BER performance analysis with different rate is shown in Figure 2. We can see that when signal to noise ratio is 3dB, the bit error rate at 1/2 bit rate can reach 10^{-8} level, the bit error rate under 2/3 code rate can reach 10^{-7} level, and bit error rate under the 3/4 code rate is 10^{-6} level. Therefore, compared with reference [12,13], the check matrix constructed by the puncturing algorithm optimized by the check matrix improves the error correction performance of the non-binary LDPC code, and at the same time realizes the code rate-compatible coding.

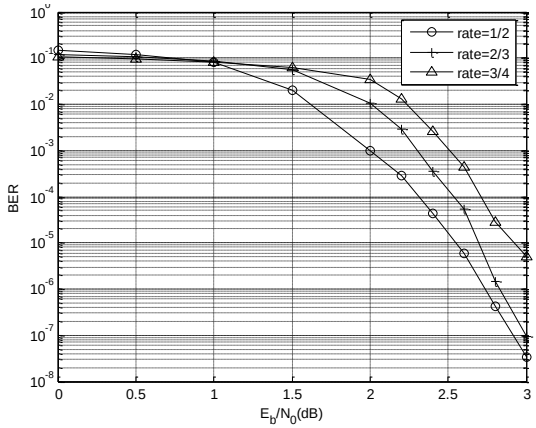

Figure 2. BER analysis of different code rates.

4 Hardware implementation

The hardware implementation of the encoder is based on FPGA, making full use of the parallel computing features of the FPGA to increase the encoding efficiency and reduce the encoding delay. The code rate-compatible non-binary LDPC coding design adopts partial parallel QC-LDPC codes coding algorithm and is divided into two main parts: the code rate control module and the core coding module. The structure of the design is shown in Figure 3.

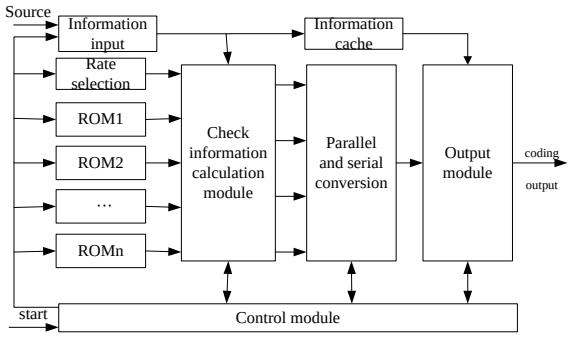

Figure 3. Structure diagram of code rate-compatible non-binary LDPC encoder.

Since the QC-LDPC matrix has a quasi-cyclic characteristic and made up of cyclic matrix blocks of $q \times q$, the control of rate can be achieved by controlling the number of sub matrices involved in operation. Each column block corresponds to q-bit check bits, so that all column blocks can be calculated synchronously, all check bits are obtained within the same clock, and coding efficiency is improved.

1. Rate control module

According to the characteristics of the sub-matrix as the unit of the generator matrix and the check matrix, the rate control can be achieved by controlling the number of sub-matrices participating in the operation. When we construct the check matrix, the low code rate is included in the high code rate, and the generator matrix obtained through the check matrix also has this feature. The code rate-compatible of the check matrix is represented by the fact that the matrix at low rate behaves as part of the high rate matrix row, while the generator matrix shows that the matrix at low rate is part of the high rate matrix column. Therefore, the length of the column affects the coding rate, and different matrix blocks with different lengths can be used to achieve code rate compatibility at different code rates.

2. Core coding module

The core coding module is the core part of the encode which completes the calculation of the check bit and outputs the code word. First, the control module controls the selection and displacement of generators. Each check information calculation module uses the generated generator and information bits to perform Galois field operations to obtain q-bit check bits, and all check information calculation modules simultaneously perform check bit calculation. Then all check bits blocks are converted to check bits in the codeword, and finally combined with the cache information sequence into a complete codeword.

5 Conclusion

In order to improve the adaptation performance of non-binary LDPC codes, we propose an RC-LDPC code design method based on check matrix puncturing optimization, which combines the rate-compatible conditions to optimize the progressive performance of parent codes. According to the desired code rate, the information bits that need to be deleted are determined, and the backward node puncturing algorithm performs puncturing from the back to the forward. The matrix constructed by this algorithm has no loop and has good performance. The simulation results show that the algorithm reduces the hardware implementation complexity and improves the error correction performance of the LDPC code.

References

1. S. Zhao, X. Ma, X. Zhang. A Class of Nonbinary LDPC Codes with Fast Encoding and Decoding Algorithms. *IEEE Transactions on Communications*, **61**, 1 (2013)
2. M. Gholami, M. Samadieh. Design of Binary and Nonbinary Codes from Lifting of Girth-8 Cycle Codes with Minimum Lengths. *IEEE Communications Letters*, **17**, 4 (2013)
3. D.J.C. MacKay. Good error-correcting codes based on very sparse matrices. *IEEE Transactions on Information Theory*, **45**, 2 (1999)
4. V. Dragoi, H.T. Kalachi. Cryptanalysis of a public key encryption scheme based on QC-LDPC and QC-MDPC codes. *IEEE Communications letters*, **2**, 22 (2018)
5. C.M. Stuart, P. Deepthi. Nonlinear cryptosystem based on QC-LDPC codes for enhanced security and reliability with low hardware complexity and reduced key size. *Wireless personal communications*, **3**, 96 (2017)
6. A.A.S. Afshar, T. Eghlidos, M.R. Aref. Efficient secure channel coding based on quasi-cyclic low-density parity-check codes. *IET communications*,

2, 3 (2009)
7. J.J. Zhang, M.K. Dong, D. Wang. Construction of Quasi-cyclic low-density parity-check codes for simplifying shuffle networks in layer decoder. *China Communications*, **12**, 10 (2013)
8. X.M. Wang, T.T. Ge, J. Li. Efficient multi-rate encoder of QC-LDPC codes based on FPGA for WIMAX standard. *Chinese journal of electronics*, **2**, 26 (2017)
9. X.L. Liu, Q.H. Liu, Z.Q. Chen. Study on construction methods of RC-LDPC code. *Journal of Guilin university of electronic technology*, **6**, 30 (2010)
10. Y. Xu, B. Liu, L. Gong. Improved shortening algorithm for irregular QC-LDPC codes using known bits. *IEEE transactions on consumer electronics*, **3**, 57 (2011)
11. K. Zhang, X.M. Huang, Z.F. Wang. A High-throughput LDPC decoder architecture with rate compatibility. *IEEE transactions on circuits and systems i-regular papers*, **4**, 58 (2011)
12. N.N. Tong, Y.P. Wu. A new nonbinary quasi-cyclic LDPC codes construction algorithm. *International journal of advancements in computing technology*, **5**, 8 (2013)
13. D.F. Zhao, N.N. Tong, Y.P. Wu. The research of construction algorithm of irregular QC-LDPC codes based on masking technique. *Journal of Jiamusi university*, **6**, 25 (2007)