Construction of Regular and Irregular QC-LDPC Codes: a Finite Field Approach and Masking

Xiaopeng Chen[1,a], Lin Zhou[1,2,b], Rui Zhao[1,c] and Yucheng He[1,2,d]

[1]Xiamen Key Laboratory of Mobile Multimedia Communications, National Huaqiao University, Xiamen, China

[2]State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an, China

[a]357929789@qq.com, [b]linzhou@hqu.edu.cn, [c]rzhao@hqu.edu.cn, [d]yucheng.he@hqu.edu.cn

Keywords: LDPC; masking; Quasi-Cyclic

Abstract. Quasi-Cyclic Low-Density Parity-Check (QC-LDPC) codes require less hardware resources due to the quasi-cyclic structure of parity-check matrices. In this paper, two improved methods for constructing QC-LDPC codes are proposed. Firstly, in order to make sure the masked LDPC codes have flexible code rate and code length, an improved construction of masking matrix is presented. The proposed regular masking matrix of QC-LDPC codes have the girth at least 6. Then, the irregular codes are constructed by using improved finite field approach and PEG algorithm, which result in large girth and less short cycles. Simulations demonstrate that the proposed QC-LDPC codes have both lower error floor and good waterfall performance.

Introduction

Low-density parity-check (LDPC) codes were discovered by Gallager in 1962[1], and then rediscovered in the late 1990s. They were proved to be channel-capacity-approaching codes[2]. Since then, various methods for constructing LDPC codes have been proposed.

The construction of LDPC codes can be divided into two categories: random codes[3] and structured codes[4,5]. Random codes have good performance, but it's too complex to application. Structured codes with optimized design can not only performance as well as random codes, but also get lower complexity in practical applications.

Recently, algebraic method have became an effective method to construct structured codes. This method can obtain the codes with good error performance more easily. Based on the algebraic construction of LDPC codes that have quasi-cyclic structure, called QC-LDPC codes[6,7]. In order to improve the bit error rate(BER) performance of QC-LDPC codes, many methods have been proposed to optimize the girth, degree distribution, the trapping set and so on. To improve the error floor performance, masking technique[8] was proposed to construction QC-LDPC codes.

In this paper, we present constructions of both regular and irregular QC-LDPC codes with large girth. First, a general construction based on finite field and masking technology is introduced. Second, an improved construction method of masking matrix of QC-LDPC codes is proposed. This method can obtain codes with a wider range of rate and also have a good performance. Then, we propose an improved method for designing base matrix by using two subsets in the finite field. Based on this base matrix, we can obtain irregular codes via masking by PEG algorithm[9]. At last, the simulation results prove that our methods have good error performance.

QC-LDPC Codes Based on Finite Field and Masking

Construction of base matrix. In general, QC-LDPC codes based on finite field need to construct an $m \times n$ base matrix $\boldsymbol{B}$. It is shown in Eq. 1:

$$\boldsymbol{B}=\begin{bmatrix} \boldsymbol{w}_{1,1} & \boldsymbol{w}_{1,2} & \cdots & \boldsymbol{w}_{1,n} \\ \boldsymbol{w}_{2,1} & \boldsymbol{w}_{2,2} & \cdots & \boldsymbol{w}_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{w}_{m,1} & \boldsymbol{w}_{m,2} & \cdots & \boldsymbol{w}_{m,n} \end{bmatrix} \tag{1}$$

where $w_{i,j}\,(1\le i\le m, 1\le j\le n)$ is an element of Galois field GF(q). Matrix $\boldsymbol{B}$ satisfied the row-column constraint: *any two rows(or two columns) have at most one same non-zero elements at the same place.* This constraint ensures that the constructed codes have girth at least 6.

Let $\boldsymbol{A}_b(w_{i,j})$ be a (q-1)×(q-1) circulant permutation matrix if $w_{i,j}\neq 0$, and it's a (q-1)×(q-1) zero matrix if $w_{i,j}=0$. By replacing each $w_{i,j}$ with $\boldsymbol{A}_b(w_{i,j})$, we obtained a m(q-1)×n(q-1) parity matrix $\boldsymbol{H}$.

Construction via masking. Let $\boldsymbol{Z}=[z_{i,j}]$ be a $m\times n$ masking matrix, where $1\le i\le m, 1\le j\le n$, $z_{i,j}\in\{0,1\}$, the masked matrix $\boldsymbol{M}$ is shown in Eq. 2:

$$\boldsymbol{M}=\boldsymbol{Z}\Theta\boldsymbol{H}=\begin{bmatrix} \boldsymbol{z}_{1,1}\boldsymbol{A}_b(\boldsymbol{w}_{1,1}) & \boldsymbol{z}_{1,2}\boldsymbol{A}_b(\boldsymbol{w}_{1,2}) & \cdots & \boldsymbol{z}_{1,n}\boldsymbol{A}_b(\boldsymbol{w}_{1,n}) \\ \boldsymbol{z}_{2,1}\boldsymbol{A}_b(\boldsymbol{w}_{2,1}) & \boldsymbol{z}_{2,2}\boldsymbol{A}_b(\boldsymbol{w}_{2,2}) & \cdots & \boldsymbol{z}_{2,1}\boldsymbol{A}_b(\boldsymbol{w}_{2,n}) \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{z}_{m,1}\boldsymbol{A}_b(\boldsymbol{w}_{m,1}) & \boldsymbol{z}_{m,2}\boldsymbol{A}_b(\boldsymbol{w}_{m,2}) & \cdots & \boldsymbol{z}_{m,n}\boldsymbol{A}_b(\boldsymbol{w}_{m,n}) \end{bmatrix} \tag{2}$$

where $z_{i,j}\boldsymbol{A}_b(w_{i,j})=\boldsymbol{A}_b(w_{i,j})$ if $z_{i,j}=1$, $z_{i,j}\boldsymbol{A}_b(w_{i,j})=\boldsymbol{0}$ if $z_{i,j}=0$. The masked matrix $\boldsymbol{M}$ gets the same degree distribution as the masking matrix $\boldsymbol{Z}$. So the masking matrix plays a significant part in the performance of the masked LDPC codes.

Construction of Regular and Irregular Codes via the Proposed Method

The improved Construction of regular codes. In [10], a (3,6)-regular masking matrix is shown in Eq. 3:

$$\boldsymbol{Z}(4,8)=\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \tag{3}$$

The girth of the regular QC-LDPC codes increased by his masking matrix from 6 to 8, and result in a masked matrix $\boldsymbol{M}$ with row weight 6 and column weight 3, respectively. It is very effective in decreasing short cycles and increasing the girth, so it has a good BER performance and low error floor. But this masking matrix $\boldsymbol{Z}(4,8)$ only suit condition in fixed size and code rate of base matrix.

To solve the deficiency of this masking matrix, we proposed an improved masking matrix as follows: repeat the first pair of the columns and third pair of columns in $\boldsymbol{Z}(4,8)$ p times, obtain $\boldsymbol{Z}(4,8p)$ with $4\times 8k$ size. Then downward expand $\boldsymbol{Z}(4,8p)$ t times, obtain $\boldsymbol{Z}(4t,8p)$ with $4t\times 8p$ size.

Let $\boldsymbol{R}=\boldsymbol{Z}(4,8)$, improved masking matrix $\boldsymbol{Z}(4t,8p)$ is shown in Eq. 4:

$$\boldsymbol{Z}(4t,8p)=\begin{bmatrix} \boldsymbol{R}_{1,1} & \boldsymbol{R}_{1,2} & \cdots & \boldsymbol{R}_{1,p} \\ \boldsymbol{R}_{2,1} & \boldsymbol{R}_{2,2} & \cdots & \boldsymbol{R}_{2,p} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{R}_{t,1} & \boldsymbol{R}_{t,1} & \cdots & \boldsymbol{R}_{t,p} \end{bmatrix} \tag{4}$$

where $t \geq 1$, $p \geq 1$. Notice that the masking matrix $\boldsymbol{Z}(4t,8p)$ also satisfied the 3×3 SM-constraint in [10], so the masked matrices have the girth-8 at least, which result in good BER performance and low error floor.

The improved Construction of irregular codes. To construct base matrix, let α be the primitive element of GF(q). For $1 \leq m,n \leq q$, let $S_1 = \{\alpha^{k_0}, \alpha^{k_1}, ..., \alpha^{k_{m-1}}\}$, $S_2 = \{\alpha^{l_0}, \alpha^{l_1}, ..., \alpha^{l_{n-1}}\}$ be two subsets of GF(q), we can obtain matrix element $w_{i,j}$ in base matrix $\boldsymbol{B}$, which is shown in Eq. 5:

$$\boldsymbol{w(i,j) = \alpha^{k_i} + \alpha^{l_j}} \tag{5}$$

where $0 \leq k_i \leq m-1$, $0 \leq l_j \leq n-1$. With different choices of two subsets S_1 and S_2, we can obtain different base matrix $\boldsymbol{B}$ with girth 6 or 8. In order to obtain irregular codes, we use PEG algorithm to construct masking matrix. By using degree distribution optimization, a proper masking matrix can be obtained. This method has better BER performance compared with the traditional construction by using PEG algorithm.

Simulation Results

The performance of different codes constructed by our methods are verified for additive white Gaussian noise channel. Codes are modulated by BPSK and decoded by sum-product algorithm. Maximum 50 iterations are considered for iterative decoding.

Example 1: First, we construct base matrix $\boldsymbol{B}(6,121)$ over GF(128). The masking matrix $\boldsymbol{Z}(6,121)$ was constructed according to Eq.4. By masking $\boldsymbol{B}(6,121)$ with $\boldsymbol{Z}(6,121)$, we obtained a masked matrix $\boldsymbol{M}(6,121)$. Every elements in $\boldsymbol{M}(6,121)$ can be replaced by 127×127 permutation matrices. Finally, we obtained a (6,121)-regular (15367,14605) QC-LDPC code C_1 with rate 0.95. The BER performance of this code is shown in Fig. 1. It shows that the performance of the code C_1 is much better than the code C_2 (16120,15345) given in [10]. The code C_1 outperforms the code C_2 by about 0.25dB at BER=1×10^{-5}.

Example 2: In this example, let GF(128) be the field for code construction. Based on this field, we construct a 4×28 base matrix $\boldsymbol{B}(4,28)$. Masking matrix $\boldsymbol{Z}(4,28)$ is given according to Eq. 4. By using masking technology, we can get the masked matrix $\boldsymbol{M}(4,28)$ with row weight 21 and column weight 3. Hence the null space of $\boldsymbol{Z}(4,28)$ gives a (3556,3048) regular QC-LDPC code C_3 with rate 0.86. For comparison, a corresponding regular (3584,3072) code C_4 is given in [11]. The error performance is shown in Fig. 2. We can see that the error performance of C_3 is better than that of the code C_4 at all SNR region. It shows that the code construct with improved masking matrix has good BER performance and low error floor.

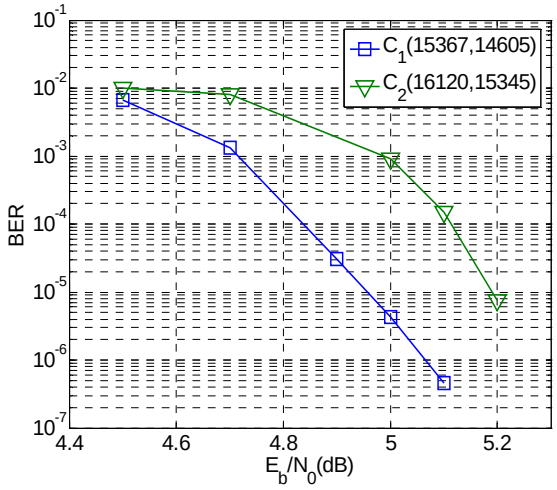

Fig. 1. The error performance of the codes C_1 given in Example 1 and C_2 given in [10].

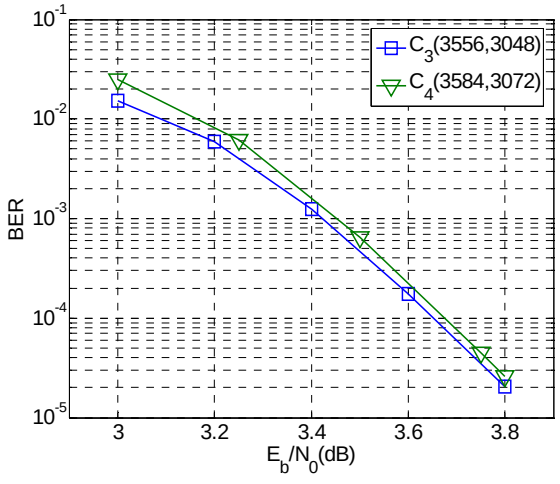

Fig. 2. The error performance of the codes C_3 given in Example 2 and C_4 given in [11].

Example 3: In this example, we construct an irregular QC-LDPC code by using two finite field subsets and PEG masking matrix. Let α be a primitive element of GF(64), we choose $S_1 = \{\alpha^1, \alpha^2, ..., \alpha^{15}\}$ and $S_2 = \{\alpha^{22}, \alpha^{23}, ..., \alpha^{51}\}$ be two subsets of elements, form a 15×30 base matrix $\boldsymbol{B}(15,30)$. Next, the 15×30 masking matrix $\boldsymbol{Z}(15,30)$ was constructed by PEG algorithm with degree distribution $\boldsymbol{\lambda(x) = 0.46x + 0.12x^2 + 0.12x^3 + 0.23x^4 + 0.07x^{14}}$, then we obtained a masked matrix $\boldsymbol{M}(15,30)$. The null space of $\boldsymbol{M}(15,30)$ gives an irregular (1890,945) code C_5 with rate 0.5. For comparison, an irregular (1890,945) code C_6 is given in[12]. The BER performance is shown in Fig. 3. At the BER of 10^{-6}, code C_5 outperforms the code C_6 by about 0.1dB. The code constructed by two subsets performs slightly better than finite field approach in [12].

Example 4: Again, consider the field GF(64) for code construction. Set $S_1 = \{\alpha^1, \alpha^2, \ldots, \alpha^{16}\}$, $S_2 = \{\alpha^{23}, \alpha^{24}, \ldots, \alpha^{54}\}$ be two subsets, form a 16×32 base matrix $\boldsymbol{B}(16,32)$. The masking matrix $\boldsymbol{Z}(16,32)$ was constructed by PEG algorithm with degree distribution $\boldsymbol{\lambda(x) = 0.46x + 0.12x^2 + 0.12x^3 + 0.23x^4 + 0.07x^{14}}$. The null space of masked matrix $\boldsymbol{M}(16,32)$ gives an irregular (2016,1008) code C_7 with rate 0.5. The code performance is shown in Fig. 4. Also included in Fig. 4 is the BER performance of a (2016,1008) code C_8 given in [13]. It shows that the two codes perform the same before SNR of 2.0, but the code C_7 outperforms the C_8 starting from the SNR of 2.0.

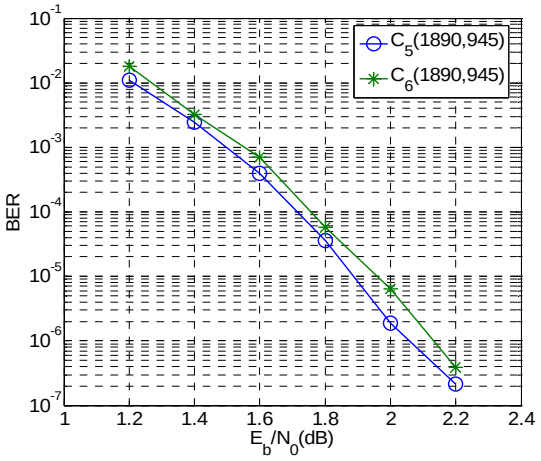

Fig.3. The error performance of the codes C_5 given in Example 3 and C_6 given in [12].

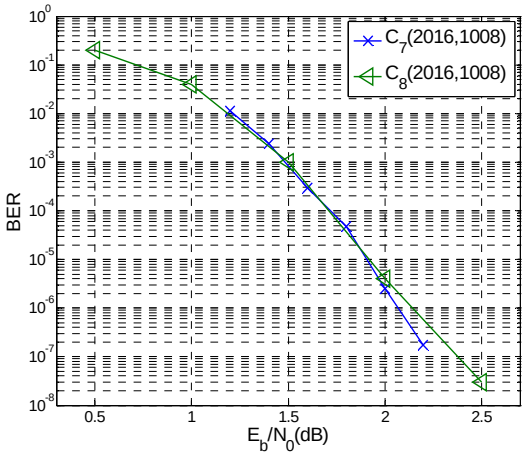

Fig.4. The error performance of the codes C_7 given in Example 4 and C_8 given in [13].

Conclusions

In this paper, we firstly proposed an improved method for construct masking matrix with large girth and low error floor. Based on the improved masking matrix which satisfies the 3×3 SM-constraint, the regular QC-LDPC codes with girth-8 were constructed, it has flexible code rate and good error performance compared to method in [10]. Moreover, we proposed two element subsets in finite field to construct the irregular QC-LDPC codes via PEG algorithm. The construction obeys the row-column constraints, which ensures that the girth is at least 6. Simulation results demonstrate that the proposed construction approaches of QC-LDPC codes have better BER performance and low error floor than some existing methods.

Acknowledgements

This work was supported in part by the grants from the National Natural Science Foundation of China (61302095, 61401165), the Natural Science Foundation of Fujian Province of China (2014J05076, 2014J01243, 2015J01262), the Science Foundation of National Huaqiao University (12BS219,

13Y0384, 13BS101), and the Graduate Student Scientific Research Innovation Ability Cultivation Plan Projects of Huaqiao University under the Grant 1400201028.

References

[1] R. G. Gallager, "Low-density parity-check codes," IRE Transactions on Information Theory, IT-8, pp. 21-28, Jan. 1962.

[2] 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.

[3] S. Y. Chung, G. D. Forney, T. Richardson, and R. Urbanke, "On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit," IEEE Commun. Lett., vol. 5, no. 2, pp. 58–60, Feb. 2001.

[4] Y. Kou, S. Lin, and M. Fossorier, "Low density parity check codes based on finite geometries: A rediscovery and new results," IEEE Trans. Inf. Theory, vol. 47, no. 7, pp. 2711–2736, Nov. 2001.

[5] Y. Kou, S. Lin, and M. Fossorier, "Construction of low density parity check codes: A geometric approach," in Proc. 2nd Int. Symp. Turbo Codes and Related Topics, Brest, France, Sep. 2000, pp. 137–140.

[6] L. Chen, J. Xu, I. Djurdjevic, and S. Lin, "Near-Shannon-limit quasicyclic low-density parity-check codes," IEEE Trans. Commun., vol. 52, no. 7, pp. 1038–1042, Jul. 2004.

[7] M. P. C. Fossorier, "Quasi-cyclic low-density parity-check codes from circulant permutation matrices," IEEE Trans. Inf. Theory, vol. 50, no. 8, pp. 1788–1793, Aug. 2004.

[8] J. Xu, L. Chen, I. Djurdjevic, S. Lin, and K. Abdel-Ghaffar, "Construction of regular and irregular LDPC codes: geometry decomposition and masking," IEEE Trans. Commun., vol. 53, no. 1, pp. 121–134, Jan. 2007.

[9] X.-Y. Hu, E. Eleftheriou, and D.-M. Arnold, "Progressive edge-growth Tanner graphs," in Proc. IEEE GLOBECOM 2001, San Antonio, TX, Nov. 2001, pp. 995–1001.

[10] J. Li, K. Liu, S. Lin, and K. Abdel-Ghaffar, "Algebraic quasi-cyclic LDPC codes: Construction, low error-floor, large girth and a reduced-complexity decoding scheme," IEEE Trans. Commun., vol. 62, no. 8, pp. 2626–2637, Aug. 2014.

[11] Vafi S, Majid N R. , "A New Scheme of High Performance Quasi-Cyclic LDPC Codes With Girth 6," IEEE Commun. Lett., vol. 19, no. 10, pp. 1666–1669, Feb. 2015.

[12] L. Lan et al., "Construction of quasi-cyclic LDPC codes for AWGN and binary erasure channels: A finite field approach," IEEE Trans. Inf. Theory, vol. 53, no. 7, pp. 2429–2458, Jul. 2007.

[13] Zongcheng Li, "Design and implementation of the rate-compatible QC-LDPC codes,"[D]. Xidian University, 2011. (In Chinese)

