ATLANTIS PRESS

*Advances in Engineering Research, volume 164*

8th International Conference on Manufacturing Science and Engineering (ICMSE 2018)

# Quasi-Cyclic LDPC Codes with Large Girth and Few Short Cycles

LIU Yuan Hua

Xi'an University of Posts and Telecommunications, Xi'an, China

E-mail: yuanhliu@163.com

**Keywords:** Low-density parity-check codes; quasi-cyclic; cycles; girth

**Abstract.** In this paper, we present an improved method for obtaining quasi-cyclic low-density parity-check (QC-LDPC) codes of larger length by combining some component QC-LDPC codes of smaller length. Large girth can be obtained by carefully designing one large girth component code of smaller length. The other component codes are properly designed to obtain a lot of QC-LDPC codes with much few short cycles. Simulations show that compared with CRT based QC-LDPC codes and PEG based QC-LDPC codes, the proposed QC-LDPC codes have much less short cycles and better performance.

## Introduction

Low-density parity-check (LDPC) codes are considered as a class of error-correcting codes with near-optimum performance under belief-propagation (BP) decoding. Based on methods of construction, LDPC codes can be divided into two categories: random LDPC codes [1] and structured LDPC codes [2]. Although random LDPC codes of large length provide excellent performance, structured LDPC codes can lead to much simpler implementations, particularly for encoding. Quasi-cyclic (QC) LDPC codes are the most promising class of structured LDPC codes due to their ease of implementation and excellent performance.

Since the short cycles may degrade the performance of BP decoding, good LDPC codes tend to have large girth and a small number of short cycles. A combining method to design QC-LDPC codes based on Chinese Remainder Theorem (CRT) was first proposed in [3]. Then, a large girth CRT (LG-CRT) method [4] was presented to improve the performance by enlarging the girth of the code. In addition, Z. Li et al. [5] added a constraint into original progressive edge-growth (PEG) algorithm to construct structured LDPC codes, named PEG-QC LDPC codes. To improve the PEG-QC algorithm, [6] proposed a modified PEG-QC method to construct girth-maximized QC-LDPC codes (GM-PEG-QC). However, large girth is not enough to judge the quality of a LDPC code. The number of short cycles is another important metric for quality. In this letter, we propose an improved combining method to construct better QC-LDPC codes, which can ensure as few short cycles as possible, while maintaining the large girth.

The rest of this paper is organized as follows. Section II presents some definitions related to QC-LDPC codes. The improved combining method is proposed in Section III. The performance of several QC-LDPC codes is verified by simulations in Section IV. Finally, Section V concludes the paper.

## QC-LDPC Codes

A binary QC-LDPC code can be defined by its parity-check matrix $\boldsymbol{H}$, which consists of $q \times q$ CPMs or zero matrices as sub-matrices as follows:

$$\boldsymbol{H} = \begin{bmatrix} \boldsymbol{I}_{a_{11}} & \boldsymbol{I}_{a_{12}} & \mathbf{L} & \boldsymbol{I}_{a_{1r}} \\ \boldsymbol{I}_{a_{21}} & \boldsymbol{I}_{a_{22}} & \mathbf{L} & \boldsymbol{I}_{a_{2r}} \\ \mathrm{M} & \mathrm{M} & \mathbf{O} & \mathrm{M} \\ \boldsymbol{I}_{a_{g1}} & \boldsymbol{I}_{a_{g2}} & \mathbf{L} & \boldsymbol{I}_{a_{gr}} \end{bmatrix} \tag{1}$$

where $a_{ij} \in$ {-1, 0, 1, ..., $q$-1} and $\boldsymbol{I}_{a_{ij}}$ $(1 \le i \le g\ ,\ 1 \le j \le r\ )$ is a $q \times q$ CPM if $a_{ij} \neq$-1. $I_0$ is an identity matrix of size $q \times q$ and $\boldsymbol{I}_{a_{ij}}$ can be obtained by cyclically shifting the rows of $I_0$ to the right by $a_{ij}$ times, and the zero matrix is denoted by $I_{-1}$. If there is no zero sub-matrix, the row and column weights of such a code are $n$ and $m$, respectively. The null space of $\boldsymbol{H}$ gives a $(g\ ,\ r\ )$-regular QC-LDPC code. In the following, we consider these $(g\ ,\ r\ )$-regular QC-LDPC codes.

The shifting matrix $\boldsymbol{S}\left(\boldsymbol{H}\right)$ of $\boldsymbol{H}$ is denoted as

$$\boldsymbol{S}\left(\boldsymbol{H}\right)=\begin{bmatrix} a_{11} & a_{12} & \mathbf{L} & a_{1r} \\ a_{21} & a_{22} & \mathbf{L} & a_{2r} \\ \mathbb{M} & \mathbb{M} & \mathbf{O} & \mathbb{M} \\ a_{g1} & a_{g2} & \mathbf{L} & a_{gr} \end{bmatrix} \tag{2}$$

It can be seen that $\boldsymbol{H}$ can be easily obtained by replacing each element $a_{ij}$ of $\boldsymbol{S}\left(\boldsymbol{H}\right)$ by $\boldsymbol{I}_{a_{ij}}$, which is called matrix extension. Since the sub-matrix $\boldsymbol{I}_{a_{ij}}$ has exactly one "1" in each row and column and "0"s elsewhere, a cycle of length $2l$ in the Tanner graph of $\boldsymbol{H}$ can be represented as a chain $(a_{m_1n_1}, a_{m_1n_2}, a_{m_2n_2}, ..., a_{m_ln_1}, a_{m_1n_1})$ in the shifting matrix $\boldsymbol{S}\left(\boldsymbol{H}\right)$. The number of cycles in the QC-LDPC codes can be easily calculated through the smaller shifting matrix $\boldsymbol{S}\left(\boldsymbol{H}\right)$, which satisfies the following theorem.

Theorem 1 ([7]) Denote a $2l$-cycle in $\boldsymbol{S}\left(\boldsymbol{H}\right)$ as $(a_{m_1n_1}, a_{m_1n_2}, a_{m_2n_2}, ..., a_{m_ln_1}, a_{m_1n_1})$. A necessary and sufficient condition for the existence of a $2l$-cycle in $\boldsymbol{H}$ is

$$\sum_{k=1}^{l}\left(a_{m_kn_k}-a_{m_{k+1}n_k}\right)\equiv 0 \bmod q \tag{3}$$

where $m_k \neq m_{k+1}, n_k \neq n_{k+1}$, and $m_{l+1}=m_1$.

**Improved combining method**

A CRT combining method was proposed in [3] to design QC-LDPC codes of larger length by combining QC-LDPC codes of smaller length. Let $L_1, L_2, \mathbf{L}, L_s$ be $s$ relatively prime integers, i.e., $\gcd(L_k, L_l)=1$ , $(1 \le k, l \le s,\ k \neq l)$ , and $L = L_1L_2\ \mathbf{L}\ L_s$. Let $\boldsymbol{C}_k$ $(k=1,2,\mathbf{L},s)$ be a QC-LDPC code whose parity-check matrix $\boldsymbol{H}_k$ is a $g \times r$ array of $L_k \times L_k$ circulant permutation matrices and $\boldsymbol{S}\left(\boldsymbol{H}_k\right)=(a_{ij}^{(k)})$ be the corresponding shifting matrix. A QC-LDPC code $\boldsymbol{C}$ can be designed based on the CRT combining method. The procedure is given as follows.

(1) Calculate the shifting matrix $\boldsymbol{S}\left(\boldsymbol{H}\right)=(a_{ij}),(1 \le i \le g\ ,1 \le j \le r\ )$ according to (4) below.

$$a_{ij}=\begin{cases}\sum_{k=1}^{s} a_{ij}^{(k)}A_kL_k' \bmod L,\ \ if\ \ a_{ij}^{(k)} \neq \infty\ ,(1 \le k \le s) \\ \infty, \qquad\qquad\qquad others\end{cases} \tag{4}$$

where $L_k'=L/L_k$ and $A_kL_k'=1 \bmod L_k$.

(2) The parity check matrix $\boldsymbol{H}$ of $\boldsymbol{C}$ can be obtained by matrix extension.

It can be seen from the CRT combining method that if there exists 6-cycle in $\boldsymbol{H}_k$ for all $1 \le k \le s$ in the same position, $\boldsymbol{H}$ will have 6-cycle in that position [8]. It is known that the iterative decoding of LDPC codes converges to the optimal solution provided that the Tanner graph of the code is free of cycles. Girth and the number of the short cycles are both important metrics for quality of a LDPC code. To improve the performance of iterative decoding, we propose an improved CRT (ICRT) combining method to construct QC-LDPC codes with large girth and few short cycles.

It can be seen from [3] that the girth of the constructed code based on CRT is larger than or equal to that of the component code. Consequently, we can translate a difficult problem of designing QC-LDPC codes with girth g into a task of designing one component QC-LDPC code with girth $g$ [4]. And the other component codes can be carefully designed based on a progressive cycle growth (PCG) algorithm to ensure as few short cycles as possible. To construct a regular QC-LDPC code, whose parity check matrix H consists of $g \times r$ array of $L \times L$ circulant permutation matrices, the proposed ICRT combining method is given as follows.

For simplicity, assume there are two component codes. Choose two relatively prime integers $L_1$ and $L_2$, i.e., $\gcd(L_1, L_2) = 1$ such that $L = L_1 L_2$, and $L_1 > L_2$. Construct an $L_1 \times L_1$ shifting matrix $\boldsymbol{S}'(\boldsymbol{H}_1)$, then carefully delete rows and columns of $\boldsymbol{S}'(\boldsymbol{H}_1)$ to eliminate cycles of length $2l < g$ based on the equations (3) and obtain a $g \times r$ shifting matrix $\boldsymbol{S}(\boldsymbol{H}_1)$. And the first component code $\boldsymbol{C}_1$ with girth g is designed, and the shifting matrix $\boldsymbol{S}(\boldsymbol{H}_2)$ of the second component code $\boldsymbol{C}_2$ is designed as follows.

Firstly, all the entries of $\boldsymbol{S}(\boldsymbol{H}_2)$ are initialized to be $\infty$.

Secondly, the entries in the first row and the first column of $\boldsymbol{S}(\boldsymbol{H}_2)$ are set to random values from {0,1,2,…, $L_2$-1} and the other entries of $\boldsymbol{S}(\boldsymbol{H}_2)$ are carefully designed one by one from left to right and top to bottom. Each time a new entry is added to $\boldsymbol{S}(\boldsymbol{H}_2)$, the following procedure is performed: let this entry be taken over all elements from {0,1,2,…, $L_2$-1} and count the number of cycles with length equals to girth $g$ ($g$-cycles) in the current shifting matrix S(H) constructed based on the equations (4), then select the element corresponding to the minimum g-cycles as this new entry. If there are several elements corresponding to no g-cycle, count the number of ($g$+2)-cycles in the current shifting matrix $\boldsymbol{S}(\boldsymbol{H})$ constructed based on the equations (4), then select the element corresponding to the minimum ($g$+2)-cycles as this new entry. If there exists more than one element corresponding to the minimum $g$-cycles or ($g$+2)-cycles, then select one randomly as this new entry.

Finally, construct the shifting matrix $\boldsymbol{S}(\boldsymbol{H})$ and the parity check matrix H by combining $\boldsymbol{S}(\boldsymbol{H}_1)$ and $\boldsymbol{S}(\boldsymbol{H}_2)$ via CRT method. The null space of the obtained parity-check matrix $\boldsymbol{H}$ gives a QC-LDPC code $\boldsymbol{C}$ with girth equals to or larger than g. It can be seen that $\boldsymbol{S}(\boldsymbol{H}_2)$ is carefully designed by adding the entries one after another provided the current parity check matrix H has minimal short cycles. And short cycles can be effectively avoided, and the parity-check matrix $\boldsymbol{H}$ with as few short cycles as possible is obtained. In addition, if the first component code $\boldsymbol{C}_1$ is designed to be an irregular QC-LDPC code, then the irregular QC-LDPC code C with the same degree distribution can be designed. By modifying parameters $L_1, L_2, g, r$ both regular and irregular QC-LDPC codes with flexible lengths and rates can be constructed. For irregular QC-LDPC codes, we assume all nodes corresponding to the same sub-matrices column or row block have the same degree. So this method can be extended to construct irregular QC-LDPC codes easily.

## Simulations

All the following results are obtained by simulation for the Additive White Gaussian Noise (AWGN) channel, the Binary Phase Shift Keying (BPSK) modulation and BP decoding with a maximum of 50 iterations.

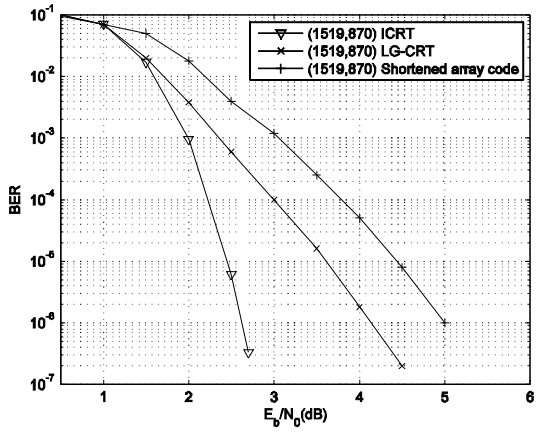


Fig1. Performance of QC-LDPC codes (1519, 870)

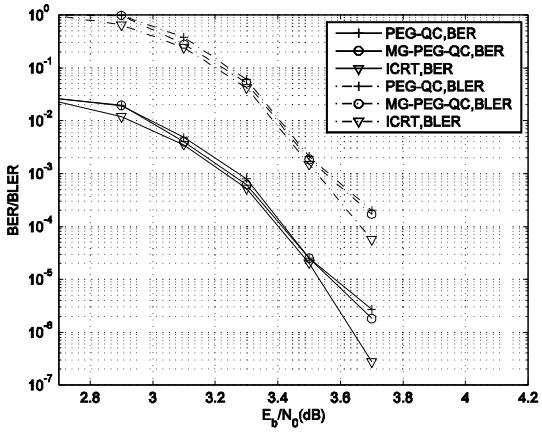


Fig2. Performance of QC-LDPC codes (4959, 4176) and (4864, 4096)

Choose the same parameters as the example in [4]: $L_1$=31, $L_2$=7, $g$ =3, $r$ =7 and $\boldsymbol{C}_1$ is a shortened array code with girth 8. A QC-LDPC code (1519, 870) with girth 8 is constructed by the ICRT method. Fig.1 shows the BER performance of the constructed code. For comparison purpose, the BER performances of the code designed by the LG-CRT method and the shortened array code are also

shown. The code (1519, 870) designed by the LG-CRT method has 18879 8-cycles and only 1736 8-cycles exist in the ICRT code. As shown in Fig.1, the QC-LDPC code designed using the ICRT method performs much better. At a BER of $10^{-6}$, the QC-LDPC code designed by the ICRT method outperforms that designed by the LG-CRT method by 1.6 dB.

Choose the parameters as follows: $L_1$=29, $L_2$=9, $g$ =3, $r$ =19 and $\boldsymbol{C}_1$ is a shortened array code with girth 6. A QC-LDPC code (4959, 4176) with girth 8 is constructed by the ICRT method. In Fig. 2, the performance of the proposed QC-LDPC code (4959, 4176) is presented and the simulation result is compared with PEG-QC code [5] and MG-PEG-QC code [6] (4864, 4096). The girth of PEG-QC code is 6, and the girths of the other two codes are both 8, in addition, the code designed by the ICRT method has much fewer 8-cycles than the MG-PEG-QC code, which can improve the decoding performance. At a BER of $10^{-6}$, the QC-LDPC code designed by the ICRT method outperforms that designed by the MG-PEG method by 0.15 dB.

## Conclusions

An improved combining method based on the CRT algorithm and the PCG algorithm for designing of QC-LDPC codes with large girth and few short cycles has been proposed. Based on the CRT combining method, the difficult problem of designing QC-LDPC codes with girth $g$ is translated into a task of designing one component code with girth $g$. By properly designing the shifting matrices of other component codes based on the PCG algorithm, a lot of QC-LDPC codes with much less short cycles and better performance can be designed. Simulation results show that compared with LG-CRT method, PEG-QC method and MG-PEG-QC method, the proposed method can design QC-LDPC codes with much less short cycles and better performance.

## Acknowledgements

This work was financially supported by the Natural Science Basic Research Plan in Shaanxi Province of China (2016JQ6033) and National Natural Science Foundation of China (61471294).

## References

[1] X.-Y. Hu, E. Eleftheriou, and D.-M. Arnold: Regular and irregular progressive edge-growth tanner graphs, IEEE Trans. Inform. Theory, (2005), 51, p. 386-98.
[2] J. Kang, Q. Huang, L. Zhang, B. Zhou, and S. Lin: Quasi-cyclic codes: an algebraic construction, IEEE Trans. Commun., (2010), 58, p. 1383-1396.
[3] S. Myung and K. Yang: A combining method of quasi-cyclic LDPC codes by the Chinese remainder theorem, IEEE Commun. Lett., (2005), 9, p. 823-825.
[4] M. Jiang and M. H. Lee: Large girth quasi-cyclic LDPC codes based on the Chinese remainder theorem, IEEE Commun. Lett., (2009), 13, p. 342-344.
[5] Z. Li and B V K V. Kumar: A class of good quasi-cyclic low-density parity check codes based on progressive edge growth graph, Conference Record of the Thirty-Eighth Asilomar Conference on Signals, Systems and Computers, Brest, (2004), p. 1990-1994.
[6] P. Prompakdee, W. Phakphisut and P. Supnithi: Quasi cyclic-LDPC codes based on PEG algorithm with maximized girth property, International Symposium on Intelligent Signal Processing and Communication Systems, Chiang Mai, (2011), p.1-4.
[7] M P C. Fossorier: Quasi-cyclic low-density parity-check codes from circulant permutation matrices, IEEE Trans. on Inform. Theory, (2004), 50(8), p. 1788-1793.
[8] Y. Liu, X. Wang, R. Chen: Generalized Combining Method for Design of Quasi-Cyclic LDPC Codes, IEEE Commun. Lett., (2008), 12(5), p. 392-394.