A novel construction method of QC-LDPC codes based on CRT for optical communications*

YUAN Jian-guo (袁建国)**, **LIANG Meng-qi** (梁梦琪), **WANG Yong** (王永), **LIN Jin-zhao** (林金朝), **and PANG Yu** (庞宇)

Key Laboratory of Optical Communication and Networks, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

(Received 27 November 2015; Revised 11 December 2015)

A novel construction method of quasi-cyclic low-density parity-check (QC-LDPC) codes is proposed based on Chinese remainder theory (CRT). The method can not only increase the code length without reducing the girth, but also greatly enhance the code rate, so it is easy to construct a high-rate code. The simulation results show that at the bit error rate (*BER*) of 10^{-7}, the net coding gain (*NCG*) of the regular QC-LDPC(4 851, 4 546) code is respectively 2.06 dB, 1.36 dB, 0.53 dB and 0.31 dB more than those of the classic RS(255, 239) code in ITU-T G.975, the LDPC(32 640, 30 592) code in ITU-T G.975.1, the QC-LDPC(3 664, 3 436) code constructed by the improved combining construction method based on CRT and the irregular QC-LDPC(3 843, 3 603) code constructed by the construction method based on the Galois field (*GF*(*q*)) multiplicative group. Furthermore, all these five codes have the same code rate of 0.937. Therefore, the regular QC-LDPC(4 851, 4 546) code constructed by the proposed construction method has excellent error-correction performance, and can be more suitable for optical transmission systems.

Document code: A **Article ID:** 1673-1905(2016)03-0208-4

DOI 10.1007/s11801-016-5238-8

With the increasing development of optical transmission systems beyond 100 Gbit/s, the digital signal processing (DSP), coherent detection and forward error correction (FEC) are becoming important for optical communication systems. Regardless of the data destination, optical transmission systems must provide the predefined bit error rate (*BER*) performance. To achieve a target *BER*, it needs stronger FEC techniques[1-3]. Low density parity check (LDPC) codes have become one hot research of channel codes because they have the approximate Shannon limit error-correcting characteristics[4,5]. Due to quasi-cycle characteristics, quasi-cyclic LDPC (QC-LDPC) codes[6-8] have lower complexity of the encoding/decoding algorithm and easier hardware implementation.

In 2005, Seho Myung and Kyeongcheol Yang[9] used the Chinese remainder theory (CRT) to construct the LDPC codes, and then some related construction methods of QC-LDPC codes based on CRT were reported[10-12], in which the code length can be extended without reducing the girth, but the code rate can be changed.

A novel construction method of QC-LDPC code, which can enhance the code rate and extend the code length without reducing the girth, is proposed in this paper. This proposed method can construct the high bit-rate codes more easily. Furthermore, a regular QC-LDPC (4 851, 4 546) code with the code rate of 0.937 is constructed, and its error-correction performance is compared and analyzed.

A QC-LDPC code is characterized by the parity-check matrix consisting of the zero matrix and the circulant permutation matrix (CPM) as follows:

$$\boldsymbol{H}=\begin{bmatrix} \boldsymbol{P}^{a_{11}} & \boldsymbol{P}^{a_{12}} & \cdots & \boldsymbol{P}^{a_{1n}} \\ \boldsymbol{P}^{a_{21}} & \boldsymbol{P}^{a_{22}} & \cdots & \boldsymbol{P}^{a_{2n}} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{P}^{a_{m1}} & \boldsymbol{P}^{a_{m2}} & \cdots & \boldsymbol{P}^{a_{mn}} \end{bmatrix}_{m\times n}, \tag{1}$$

where $a_{ij}\in\{\infty, 0, 1, \dots, L-1\}$, and L is a prime. $\boldsymbol{P}=(p_{ij})$ is the $L\times L$ CPM defined by

$$p_{ij}=\begin{cases}1\ , & i+1\equiv j \bmod L \\ 0\ , & \text{otherwise}\end{cases}. \tag{2}$$

If $a_{ij}=\infty$, $\boldsymbol{P}^{a_{ij}}$ represents an $L\times L$ zero matrix or an $L\times L$ CPM. The exponent matrix $\boldsymbol{E}(\boldsymbol{H})$ of $\boldsymbol{H}$ is defined as

* This work has been supported by the National Natural Science Foundation of China (Nos.61472464 and 61471075), the Program for Innovation Team Building at Institutions of Higher Education in Chongqing (No.J2013-46), the Natural Science Foundation of Chongqing Science and Technology Commission (Nos.cstc2015jcyjA0554 and cstc2013jcyjA40017), and the Program for Postgraduate Science Research and Innovation of Chongqing University of Posts and Telecommunications (Chongqing Municipal Education Commission) (No.CYS14144).

** E-mail: yuanjg@cqupt.edu.cn

$$\boldsymbol{E}(\boldsymbol{H})=\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}, \tag{3}$$

and $\boldsymbol{H}$ can be obtained by replacing each element a_{ij} of $\boldsymbol{E}(\boldsymbol{H})$ with $\boldsymbol{P}^{a_{ij}}$.

Theorem 1[13]: Let $(a_1, a_2, \ldots, a_{2l-1}, a_{2l})$ be represented as a $2l$-block-cycle in template matrix $\boldsymbol{E}(\boldsymbol{H})$. Both a_i and a_{i+1} are located in either the same column block or the same row block, and both a_i and a_{i+2} are located in the different column and row blocks. If there is the smallest positive integer r to meet the following formula:

$$r\cdot\sum_{i=1}^{2l}(-1)^{i-1}a_i\equiv 0 \bmod L, \tag{4}$$

the $2l$-block-cycle in $\boldsymbol{E}(\boldsymbol{H})$ leads to a $2lr$-cycle in $\boldsymbol{H}$. Through detecting the exponent matrix $\boldsymbol{E}(\boldsymbol{H})$, the results can show whether there is the girth-4 occurrence in the check matrix or not. Then the detection workload can be greatly reduced.

The specific construction by CRT is as follows. For k=1, 2, …, s, let gcd(L_l, L_k)=1 and C_k be a QC-LDPC code whose parity-check matrix $\boldsymbol{H}_k$ is an $mL_k\times nL_k$ matrix. The exponent matrix, which is an $m\times n$ matrix, is given by $\boldsymbol{E}(\boldsymbol{H}_k)=(a_{ij}^k)$. With $L=L_1L_2\ldots L_k$, the new parity-check matrix $\boldsymbol{H}$ which is an $mL\times nL$ matrix and the exponent matrix $\boldsymbol{E}(\boldsymbol{H})$ given by $\boldsymbol{E}(\boldsymbol{H})=(a_{ij})$ have the same size as $\boldsymbol{E}(\boldsymbol{H}_k)$. According to CRT, a_{ij} can be got as

$$a_{ij}=\begin{cases}\infty, & a_{ij}^k=\infty \\ (\sum_{k=1}^{s}a_{ij}^kA_kL_k')\bmod L, & a_{ij}^k\neq\infty\end{cases}, \tag{5}$$

where $L_k'=L/L_k$, and $A_kL_k'=1\bmod L_k$. And then the parity-check matrix $\boldsymbol{H}$ of the new code C can be obtained by replacing each element a_{ij} of $\boldsymbol{E}(\boldsymbol{H})$ by the $L\times L$ CPM.

Theorem 2[11]: If r_k (k=1, 2, …, k) and r are the least positive integers, which means that

$$r_k\cdot\sum_{i=1}^{2l}(-1)^{i-1}a_i^{(k)}\equiv 0\bmod L_k, \tag{6}$$

then $r=\prod_{k=1}^{s}r_k$.

Theorem 1 shows that a $2lr_k$-cycle in $\boldsymbol{H}_k$ leads to a $2lr$-cycle in $\boldsymbol{H}$. Theorem 2 implies that the $2lr$-cycle in $\boldsymbol{H}$ is larger than or equal to the corresponding $2lr_k$-cycle in $\boldsymbol{H}_k$. It means that the girth of C is larger than or equal to that of C_k. By CRT, a large class of QC-LDPC codes can be designed. But this method just can increase the code length without reducing the original girth and changing the code rate.

For the lack of the original construction method by CRT, a novel construction method is proposed, which can greatly enhance the code rate through choosing the exponent matrices with distinct sizes. So the QC-LDPC codes constructed by the novel method can meet the requirements of the high bit-rate codes in the optical communication system. Here, the construction process is given by two short QC-LDPC codes with exponent matrices with distinct sizes.

Under the condition of $n_1\neq n_2$ and gcd (L_1, L_2)=1, let C_1 be a short QC-LDPC code whose parity-check matrix $\boldsymbol{H}_1$ is an $mL_1\times n_1L_1$ matrix and whose exponent matrix $\boldsymbol{E}(\boldsymbol{H}_1)=(a_{ij})$ is an $m\times n_1$ matrix. And let C_2 be another short QC-LDPC code whose parity-check matrix $\boldsymbol{H}_2$ is an $mL_2\times n_2L_2$ matrix and whose exponent matrix $\boldsymbol{E}(\boldsymbol{H}_2)=(b_{ij})$ is an $m\times n_2$ matrix. And the exponent matrix $\boldsymbol{E}(\boldsymbol{H})=(c_{ij})$ of C is an $m\times n_1n_2$ matrix. According to Eq.(5), it can be obtained that

$$c_{ij}=\begin{cases}\infty, & a_{ij}'=\infty \text{ or } b_{ij}'=\infty \\ (a_{ij}'A_1L_1'+b_{ij}'A_2L_2')\bmod(L), & \text{otherwise}\end{cases}, \tag{7}$$

where $L=L_1L_2$, $L_1'=\frac{L}{L_1}=L_2$, $L_2'=\frac{L}{L_2}=L_1$, $A_1L_1'\equiv 1\bmod L_1$, $A_2L_2'\equiv 1\bmod L_2$, and a_{ij}' and b_{ij}' are the elements of $\boldsymbol{E}(\boldsymbol{H}_1')$ and $\boldsymbol{E}(\boldsymbol{H}_2')$, respectively. $\boldsymbol{E}(\boldsymbol{H}_1')=(a_{ij}')$ and $\boldsymbol{E}(\boldsymbol{H}_2')=(b_{ij}')$ are shown as

$$\begin{aligned}\boldsymbol{E}(\boldsymbol{H}_1')&=\overbrace{\left[\boldsymbol{E}(\boldsymbol{H}_1)\ \boldsymbol{E}(\boldsymbol{H}_1)\ \cdots\ \boldsymbol{E}(\boldsymbol{H}_1)\right]}^{\text{repeat } n_2 \text{ times}} \\ \boldsymbol{E}(\boldsymbol{H}_2')&=\overbrace{\left[\boldsymbol{E}(\boldsymbol{H}_2)\ \boldsymbol{E}(\boldsymbol{H}_2)\ \cdots\ \boldsymbol{E}(\boldsymbol{H}_2)\right]}^{\text{repeat } n_1 \text{ times}}\end{aligned}. \tag{8}$$

Thus the code rate of the new code C is $(n_1n_2-m)/n_1n_2$, and it is larger than those of C_1 and C_2 which are $(n_1-m)/n_1$ and $(n_2-m)/n_2$, respectively. If there is no condition of the existence of girth-4 in $\boldsymbol{E}(\boldsymbol{H}_1)$ and $\boldsymbol{E}(\boldsymbol{H}_2)$, there is also no girth-4 in the new code C.

The demonstration is shown as follows:

Take any sequence $(c_{i_1j_1},c_{i_1j_2},c_{i_2j_1},c_{i_2j_2})$ in exponent matrix $\boldsymbol{E}(\boldsymbol{H})$, and the sequences in the corresponding exponent matrixes $\boldsymbol{E}(\boldsymbol{H}_1')$ and $\boldsymbol{E}(\boldsymbol{H}_2')$ are $(a_{i_1j_1},a_{i_1j_2},a_{i_2j_1},a_{i_2j_2})$ and $(b_{i_1j_1},b_{i_1j_2},b_{i_2j_1},b_{i_2j_2})$, respectively. Let r_1, r_2 and r all be the least positive integers, which can make $(a_{i_1j_1},a_{i_1j_2},a_{i_2j_1},a_{i_2j_2})$ in exponent matrix $\boldsymbol{E}(\boldsymbol{H}_1')$, $(b_{i_1j_1},b_{i_1j_2},b_{i_2j_1},b_{i_2j_2})$ in exponent matrix $\boldsymbol{E}(\boldsymbol{H}_2')$ and $(c_{i_1j_1},c_{i_1j_2},c_{i_2j_1},c_{i_2j_2})$ in exponent matrix $\boldsymbol{E}(\boldsymbol{H})$ satisfy Eq.(4). According to theorem 2, $r=r_1r_2$ can be known. To prove r>1, namely, there is no condition under which the check matrix consists girth-4 in exponent matrix $\boldsymbol{E}(\boldsymbol{H})$, three kinds of conditions are classified.

The first condition: When $|j_1-j_2|=xp_1$ (x is the positive integer), namely, when $a_{i_1j_1}=a_{i_1j_2}$ and $a_{i_2j_1}=a_{i_2j_2}$ in $\boldsymbol{E}(\boldsymbol{H}_1')$, r_1=1; but when $b_{i_1j_1}\neq b_{i_1j_2}$ and $b_{i_2j_1}\neq b_{i_2j_2}$ in $\boldsymbol{E}(\boldsymbol{H}_2')$ under the same condition, r_2>1. As a result, $r=r_1r_2$>1.

The second condition: When $|j_1-j_2|=xp_2$ (x is the positive integer), namely, when $a_{i_1j_1}\neq a_{i_1j_2}$ and $a_{i_2j_1}\neq a_{i_2j_2}$ in $\boldsymbol{E}(\boldsymbol{H}_1')$, r_1=1; but when $b_{i_1j_1}=b_{i_1j_2}$ and $b_{i_2j_1}=b_{i_2j_2}$ in $\boldsymbol{E}(\boldsymbol{H}_2')$ under the same condition, r_2>1. As a result,

$r=r_1r_2>1$.

The third condition: When $|j_1-j_2|\neq xp_1$ and $|j_1-j_2|\neq yp_2$ (x and y are the positive integers), namely, when both $a_{i_1j_1}$ and $a_{i_1j_2}$ in $\boldsymbol{E}\left(\boldsymbol{H}_1'\right)$ or both $a_{i_2j_1}$ and $a_{i_2j_2}$ in $\boldsymbol{E}\left(\boldsymbol{H}_1'\right)$ are located in the distinct column in $\boldsymbol{E}(\boldsymbol{H}_1)$, $r_1>1$, because there is no girth-4 in $\boldsymbol{E}(\boldsymbol{H}_1)$. Similarly, when both $b_{i_1j_1}$ and $b_{i_1j_2}$ in $\boldsymbol{E}\left(\boldsymbol{H}_1'\right)$ or both $b_{i_2j_1}$ and $b_{i_2j_2}$ in $\boldsymbol{E}\left(\boldsymbol{H}_1'\right)$ are located in the distinct column in $\boldsymbol{E}(\boldsymbol{H}_2)$, $r_2>1$, because there is no girth-4 in $\boldsymbol{E}(\boldsymbol{H}_2)$. As a result, $r=r_1r_2>1$.

Therefore, if there is no girth-4 in codes C_1 and C_2, there is also no girth-4 in the new code C. So this novel construction method can increase the code rate when the code length is increased without reducing the original girth.

According to the requirement of QC-LDPC codes with the high bit-rate for optical communication systems, the regular QC-LDPC(4 851, 4 546) code with column weight, row weight and code rate of 4, 63 and 0.937 is constructed by using the proposed construction method. The selected specific parameters are shown as follows. C_1 and C_2 are selected as the exponent matrix $\boldsymbol{E}(\boldsymbol{H}_1)$ with the size of 4×7 based on $GF(7)$ and the exponent matrix $\boldsymbol{E}(\boldsymbol{H}_2)$ with the size of 4×9 based on $GF(11)$, respectively, and the exponent matrixes are constructed by the additive group construction method. Moreover, there is no girth-4 in the parity-check matrixes of the two short codes. The exponent matrix $\boldsymbol{E}(\boldsymbol{H})$ of the new code C is a 4×63 matrix, and the order of CPM is $L=77$.

The simulation analyses of the constructed QC-LDPC(4 851, 4 546) code, the classic RS(255, 239) code[14] in ITU-T G.975, the LDPC(32 640, 30 592) code[15] in ITU-T G.975.1, the QC-LDPC(3 664, 3 436) code constructed by the improved combining construction method based on CRT[12] and the QC-LDPC(3 843, 3 603) code constructed by the construction method based on the Galois field ($GF(q)$) multiplicative group[16] are performed by Matlab program software. And all these five codes have the same code rate of 0.937. The simulation environment is under additive white Gaussian noise (AWGN) channel, binary phase shift keying (BPSK) modulation method and the decoding algorithm of the sum product algorithm (SPA). When the iteration time is 16, the simulation result is shown in Fig.1. The net coding gain (NCG) of the regular QC-LDPC(4 851, 4 546) code is respectively improved by 2.06 dB, 1.36 dB, 0.53 dB and 0.31 dB compared with those of the RS(255, 239) code, the LDPC(32 640, 30 592) code, the QC-LDPC(3 664, 3 436) code and the QC-LDPC(3 843, 3 603) code at the bit error rate of 10^{-7}.

In the process of constructing QC-LDPC codes by using the proposed construction method, the moderate QC-LDPC code with different code bit-rates can be obtained by selecting the exponent matrices with different sizes of short codes. The QC-LDPC codes with the same code bit-rate and different code lengths can be obtained by selecting the different orders of CPM. Thus, the choices of the code length and the code bit-rate for the proposed construction method of QC-LDPC codes are more flexible.

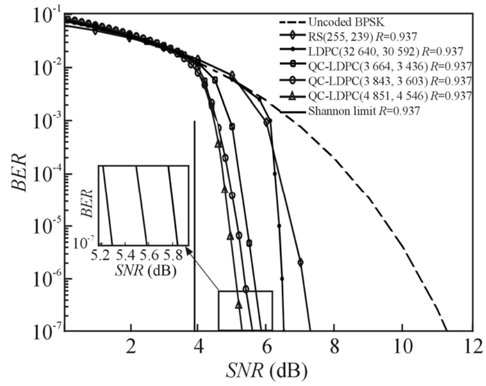

Fig.1 The error correction performances of the QC-LDPC(4 851, 4 546) code and other four codes

A novel construction method is proposed in this paper, which can increase the code length without reducing the girth, and also enhance the code rate. Moreover, the code length and the code rate can be adjusted flexibly by selecting different parameters. The simulation result shows that the regular QC-LDPC(4 851, 4 546) code constructed by the proposed construction method has better error-correction performance than the classic RS(255, 239) code in ITU-T G.975, the LDPC(32 640, 30 592) code in ITU-T G.975.1, the QC-LDPC(3 664, 3 436) code constructed by the improved combining construction method based on CRT and the QC-LDPC(3 843, 3 603) code constructed by the construction method based on the $GF(q)$ multiplicative group. Therefore, the constructed QC-LDPC(4 851, 4 546) code can be better used for high-speed long-haul optical communication system.

References

[1] CHENG Zhi-Hui, BAI Cheng-lin, LUO Qing-Long and SUN Wen-Tao, Journal of Optoelectronics·Laser **26**, 1094 (2015). (in Chinese)

[2] I. B. Djordjevic, Journal of Lightwave Technology **31**, 2669 (2013).

[3] HUANG Sheng, TIAN Kai, HE Li and LIANG Tian-yu, Journal of Optoelectronics·Laser **25**, 56 (2014). (in Chinese)

[4] Qin Huang, Qiuju Diao, Shu Lin and K. Abdel-Ghaffar, IEEE Transactions on Information Theory **58**, 2648 (2012).

[5] ZHU Lian-xiang and YANG Hai-yan, Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition) **23**, 570 (2011).

[6] YUAN Jian-guo, XU Liang and TONG Qing-zhen, Optoelectronics Letters **9**, 378 (2013).

[7] I. B. Djordjevic, W. Ryan and B. Vasic, Coding for Optical Channels, New York: Springer, (2010).

[8] Yuan Jianguo, Xu Liang, Jia Yuexing, Tong Qingzhen and Wang Yong, Optik - International Journal for Light and Electron Optics **124**, 3181 (2013).

[9] Seho Myung and Kyeongcheol Yang, IEEE Communications Letters **9**, 823 (2005).

[10] Xueqin Jiang, Xiang-Gen Xia and Moon Ho Lee, IEEE Transactions on Communications **62**, 442 (2014).

[11] Panteleev P., Fast Systematic Encoding of Quasi-Cyclic Codes using the Chinese Remainder Theorem, IEEE International Symposium on Information Theory, 1916 (2015).

[12] Yuan-hua Liu, Mei-ling Zhang and Xin-liang Niu, Electronics Letters **50**, 518 (2014).

[13] Fossorier M. P. Marc, IEEE Transactions on Information Theory **50**, 1788 (2004).

[14] ITU-T G.975, Forward Error Correction for Submarine Systems, (2000).

[15] ITU-T Recommendation G.975.1, Forward Error Correction for High Bit Rate DWDM Submarine Systems, (2003).

[16] Yuan Jianguo, Liu Feilong, Ye Wenwei, Huang Sheng and Wang Yong, Optik - International Journal for Light and Electron Optics **125**, 1016 (2014).