Construction method of QC-LDPC codes based on multiplicative group of finite field in optical communication*

HUANG Sheng (黄胜), **AO Xiang** (敖翔)**, **LI Yuan-yuan** (李媛媛), **and ZHANG Rui** (张睿)
Key Laboratory of Optical Communications and Network, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

(Received 20 June 2016; Revised 15 July 2016)

In order to meet the needs of high-speed development of optical communication system, a construction method of quasi-cyclic low-density parity-check (QC-LDPC) codes based on multiplicative group of finite field is proposed. The Tanner graph of parity check matrix of the code constructed by this method has no cycle of length 4, and it can make sure that the obtained code can get a good distance property. Simulation results show that when the bit error rate (*BER*) is 10^{-6}, in the same simulation environment, the net coding gain (*NCG*) of the proposed QC-LDPC(3 780, 3 540) code with the code rate of 93.7% in this paper is improved by 2.18 dB and 1.6 dB respectively compared with those of the RS(255, 239) code in ITU-T G.975 and the LDPC(3 2640, 3 0592) code in ITU-T G.975.1. In addition, the *NCG* of the proposed QC-LDPC(3 780, 3 540) code is respectively 0.2 dB and 0.4 dB higher compared with those of the SG-QC-LDPC(3 780, 3 540) code based on the two different subgroups in finite field and the AS-QC-LDPC(3 780, 3 540) code based on the two arbitrary sets of a finite field. Thus, the proposed QC-LDPC(3 780, 3 540) code in this paper can be well applied in optical communication systems.
Document code: A **Article ID:** 1673-1905(2016)05-0349-4
DOI 10.1007/s11801-016-6143-x

With the upgrading of optical communication system, speeding up the transmission rate, increasing the transmission distance and enhancing the information capacity have become the inevitable development trend. However, the transmission effect produced during the transmission process is also increased, which hinders the improvement of system performance. As a result, the reliability of communication systems cannot be guaranteed[1]. The quasi-cyclic low-density parity-check (QC-LDPC) codes, as a special type of low-density parity-check (LDPC) codes, have the characteristics of LDPC codes[2], such as low decoding complexity and powerful error correction capability. At the same time, they are also characterized by less storage space, flexible code design, convenience for hardware implementation and so forth[3-8]. The application of QC-LDPC codes in optical communication systems can well compensate for various damages in optical channels, to ensure the reliability of high-speed optical transmission system. For this reason, QC-LDPC codes have become a research hotspot in high-speed optical fiber transmission system in recent years[9-14]. For a QC-LDPC code, the distance property is an important factor which affects the performance of the code. A QC-LDPC code with a good distance property can get excellent error correction performance. However, there are relatively few papers that discuss the distance property of a QC-LDPC code[15,16]. Therefore, research on the distance property of a QC-LDPC code is helpful for constructing a good code.

In this paper, a novel QC-LDPC code is designed by using the multiplicative group of finite field for optical communication systems, which can get a good distance property by properly selecting a stray parameter α^{β} set when the basis matrix is constructed. In addition, it is flexible to design the code length and rate by constructing basis matrix with different dimensions. On this basis, an irregular QC-LDPC (3 780, 3 540) code with a code rate of 93.7% is constructed, and the error correction performance of the code is analyzed through simulation.

Finite field, which can be rephrased as Galois field (GF), is expressed as GF(q), in which q is a prime number or an exponent of the prime number. If the set $\{\alpha^{-\infty}, \alpha^0, \alpha^1, \ldots, \alpha^{q-1}\}$ constitutes q elements of GF(q), at the same time, when $\alpha^{-\infty}\equiv 0$ and $\alpha^0=\alpha^{q-1}=1$, the element α is called the primitive element of GF(q). The multiplicative group of GF(q) consists of $q-1$ different nonzero elements except $\alpha^{-\infty}$ and α^{q-1} of the field. In GF(q), every nonzero element α^i ($0\le i\le q-2$) can correspond to a ($q-1$) dimensional array $\boldsymbol{z}(\alpha^i)=(z_0, z_1,\ldots, z_{q-2})$ on GF(2), known as the position vector of element α^i. In $\boldsymbol{z}(\alpha^i)$, the ith

* This work has been supported by the National Natural Science Foundation of China (No.61571072), and the Basic and Advanced Technology Research Project in Chongqing (No.cstc2015jcyjA40015).
** E-mail: 764716452@qq.com

component z_i=1, and all other q−2 components are 0. The position vector $\boldsymbol{z}(\alpha^{-\infty})$ corresponding to the element $\alpha^{-\infty}\equiv 0$ is a q−1 dimensional array of zeros. Setting that η is a nonzero element of GF(q), take the position vector of η, $\alpha\eta$, $\alpha^2\eta$, …, $\alpha^{q-2}\eta$ as the row to form a (q−1)×(q−1) cyclic permutation matrix (CPM) on GF(2), among which the position vector $\boldsymbol{z}(\alpha\eta)$ of $\alpha\eta$ is obtained by circularly shifting the position vector $\boldsymbol{z}(\eta)$ of η by one place to the right, the first row of CPM is gained by circularly shifting the bottom row by one place to the right, and the other rows are got by circularly shifting adjacent previous row by one place to the right.

The construction of QC-LDPC code is also the construction of its parity check matrix. The main steps of general construction method of the parity check matrix of QC-LDPC code based on the finite field are as follows: (1) Design a basis matrix $\boldsymbol{B}$; (2) Replace each element with its corresponding CPM in the basis matrix $\boldsymbol{B}$, to extend $\boldsymbol{B}$ to a parity check matrix.

In GF(q), set $q=2^s$, where s is an arbitrary positive integer, and the power form α^0, α^1, … , α^{q-2} of the primitive element α can be used to express the q−1 elements in the multiplicative group. At the same time, suppose that α^β is an arbitrary element in the multiplicative group, and use all elements in the multiplicative group to construct a basis matrix $\boldsymbol{B}$ which is expressed as

$$\boldsymbol{B}=\begin{bmatrix}\boldsymbol{b}_0\\ \boldsymbol{b}_1\\ \vdots\\ \boldsymbol{b}_{q-2}\end{bmatrix}=\begin{bmatrix}\alpha^{0-0}-\alpha^{0-\beta} & \alpha^{0-1}-\alpha^{1-\beta} & \cdots & \alpha^{0-(q-2)}-\alpha^{(q-2)-\beta}\\ \alpha^{1-0}-\alpha^{0-\beta} & \alpha^{1-1}-\alpha^{1-\beta} & \cdots & \alpha^{1-(q-2)}-\alpha^{(q-2)-\beta}\\ \vdots & \vdots & \ddots & \vdots\\ \alpha^{(q-2)-0}-\alpha^{0-\eta} & \alpha^{(q-2)-1}-\alpha^{1-\beta} & \cdots & \alpha^{(q-2)-(q-2)}-\alpha^{(q-2)-\beta}\end{bmatrix}. \tag{1}$$

In Eq.(1), the structural properties of the basis matrix $\boldsymbol{B}$ are as follow. Firstly, these elements in each row (column) are different. Secondly, for $0\le i\le q-2$, $0\le k, l\le q-2$ and $k\ne l$, in $\alpha^k\boldsymbol{b}_i$ and $\alpha^l\boldsymbol{b}_j$, there is only a position having the same element in GF(q) at most. Thirdly, for $0\le i, j\le q-2$ ($i\ne j$) and $0\le k, l\le q-2$, $\alpha^k\boldsymbol{b}_i$ and $\alpha^l\boldsymbol{b}_j$ can meet the requirement that it is not the same at least on q−2 positions.

Theorem 1[11]: for $0\le i, j\le q-2$ ($i\ne j$) and $0\le k, l\le q-2$, $\alpha^k\boldsymbol{b}_i$ and $\alpha^l\boldsymbol{b}_j$ can be only allowed to be the same on a position at most.

If $\alpha^k\boldsymbol{b}_i$ and $\alpha^l\boldsymbol{b}_j$ have the same element in GF(q) on two arbitrary and different positions (two different columns), use m and n ($0\le m, n\le q-2$) to represent the two positions, then the following expressions are workable:

$$\alpha^k(\alpha^{i-m}-\alpha^{m-\beta})=\alpha^l(\alpha^{j-m}-\alpha^{m-\beta}), \tag{2}$$

$$\alpha^k(\alpha^{i-n}-\alpha^{n-\beta})=\alpha^l(\alpha^{j-n}-\alpha^{n-\beta}). \tag{3}$$

Eqs.(2) and (3) can be simplified as

$$\alpha^{i-j}(\alpha^{m-n}-\alpha^{n-m})=0. \tag{4}$$

So it must be $i=j$ or $m-n=n-m$, and apparently $i=j$ is contradict with the known conditions. Furthermore, when $m-n=n-m$, there is $2(m-n)=c(q-1)$, because $q=2^s$, q−1 cannot be divided evenly by 2. At the same time, because $0\le m, n\le q-2$, we can get c=0, i.e., $m=n$, which is contradict with the assumption. So the assumption is false, which verifies that the constructed parity check matrix $\boldsymbol{H}$ can meet the conditions of Theorem 1. Ensure that $\boldsymbol{H}$ meets the RC-constraint, so that 4 cycles will not exist in the Tanner graph corresponding to $\boldsymbol{H}$.

For the basis matrix $\boldsymbol{B}$ in Eq.(1), by replacing each element in the matrix into a CPM corresponding to its position vector, the element is extended to be a (q−1)×(q−1) matrix $\boldsymbol{A}$ including only 0 and 1 on GF(2). After all the elements in $\boldsymbol{B}$ are replaced, the required parity check matrix $\boldsymbol{H}$ can be obtained as

$$\boldsymbol{H}=\begin{bmatrix}\boldsymbol{H}_0\\ \boldsymbol{H}_1\\ \vdots\\ \boldsymbol{H}_{q-2}\end{bmatrix}=\begin{bmatrix}\boldsymbol{A}_{0,0} & \boldsymbol{A}_{0,1} & \cdots & \boldsymbol{A}_{0,q-2}\\ \boldsymbol{A}_{1,0} & \boldsymbol{A}_{1,1} & \cdots & \boldsymbol{A}_{1,q-2}\\ \vdots & \vdots & \ddots & \vdots\\ \boldsymbol{A}_{q-2,0} & \boldsymbol{A}_{q-2,1} & \cdots & \boldsymbol{A}_{q-2,q-2}\end{bmatrix}, \tag{5}$$

and the dimension of $\boldsymbol{H}$ is (q−1)(q−1)×(q−1)(q−1).

To meet the demand of transmission in optical communication systems, the design of QC-LDPC codes should consider the following several principles: high coding gain, high code rate, fast iterative decoding convergence speed and low error floor or even no error floor phenomenon. Based on the above principles, first of all, determine the simulation parameters as s=6, $q=2^s$=64, and construct a parity check matrix $\boldsymbol{H}$ with 63×63 rows and 63×63 columns according to the designed method in this paper. Secondly, take the check sub-matrix at the front 4×63 rows and the front 60×63 columns, in which the row weight of check sub-matrix is 59, while the column weight is 3 or 4. With this, construct an irregular QC-LDPC(3 780, 3 540) code with an approximate code rate of 93.7%. Carry out performance simulation to the constructed code: first conduct binary phase shift keying (BPSK) modulation, through additive white Gaussian noise (AWGN) channel, and then adopt sum product algorithm (SPA) for iterative decoding after demodulation. 30 times of iteration is taken. The error correction capability is improved with the increase of times of iteration. However, when the times of iteration increase from 30 to 50, the improvement of its error correction capability is low, but the decoding complexity is increased greatly. To achieve the best balance between complexity and performance, in this paper, 30 times of iteration is selected in the simulation of the QC-LDPC code.

Theorem 2[16] : if the ratio of μ_2/μ_1 is smaller, where μ_1 and μ_2 are the maximum and the sub-maximum eigen-

values of the matrix $\boldsymbol{HH}^T$, the corresponding QC-LDPC code will have a good distance property.

In the proposed construction method in this paper, by selecting α^{β} value in basis matrix, the code has a good distance property, which further ensures that the code acquires good error correction performance. Tab.1 gives some specific ratios of μ_2/μ_1 for different β. It is easily seen from Tab.1 that when β is different, μ_2/μ_1 value is also different, and when β=58, the μ_2/μ_1 value is the minimum. Fig.1 shows the corresponding error correction performance of the code. When β=58, the error correction capability is better, which is in accordance with Theorem 2. Therefore, the irregular QC-LDPC(3 780, 3 540) code with an approximate code rate of 93.7% is constructed as the code pattern under the optical communication system by selecting s=6, q=2^s=64 and β=58.

Tab.1 The ratios of μ_2/μ_1 for different β

β	μ_1	μ_2	μ_2/μ_1
9	233.000	63.987	0.275
28	233.000	63.854	0.274
57	236.509	63.012	0.268
58	237.037	63.001	0.266

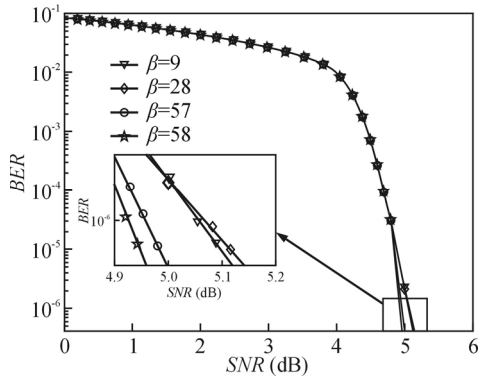

Fig.1 The error correction performances of the constructed QC-LDPC (3 780, 3 540) code for different β

To fully explain the performance of the QC-LDPC code constructed in this paper and prove that it can be better applied in optical communication system, we compare it with the RS(255, 239) code[17] in ITU-T G.975 standard, the LDPC(32 640, 30 592) code[18] in ITU-T G.975.1, the SG-QC-LDPC(3 780, 3 540) code[19] based on the two different subgroups in finite field and the AS-QC-LDPC(3 780, 3 540) code[20] based on the two arbitrary sets of a finite field, which have been widely used in optical communication system. And the simulation results are shown in the Fig.2.

It can be known from Fig.2 that when the bit error rate (*BER*) is 10^{-6}, the net coding gain (*NCG*) of the constructed QC-LDPC(3 780, 3 540) code is improved by 2.18 dB and 1.6 dB than those of the RS(255, 239) code and the LDPC(32 640, 30 592) code, respectively. At the same time, *NCG* is improved by 0.2 dB and 0.4 dB respectively compared with those of the SG-QC-LDPC(3 780, 3 540) code and the AS-QC-LDPC(3 780, 3 540) code.

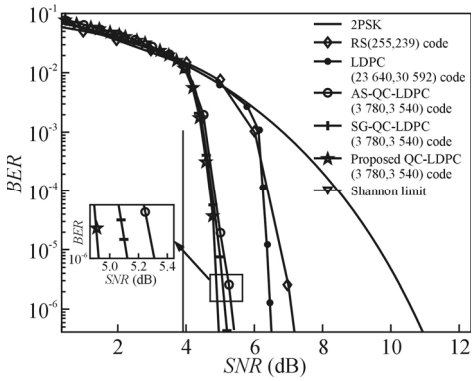

Fig.2 The error correction performances of the constructed QC-LDPC (3780, 3540) code and other codes at the code rate of 93.7%

In this paper, based on the multiplicative group of finite field GF(q), a construction method for QC-LDPC code with simple structure, low decoding complexity and good distance property is proposed, and a novel irregular QC-LDPC(3 780, 3 540) code appropriate for optical communication system is constructed by adjusting the stray parameter α^{β} set in basis matrix. Simulation results show that, compared with the RS(255, 239) code, the LDPC(32 640, 30 592) code, the SG-QC-LDPC(3 780, 3 540) code and the AS-QC-LDPC(3 780, 3 540) code, the code constructed in the paper has higher *NCG*, which indicated that the code constructed in this paper applies to high-speed and long-haul optical communication systems.

References

[1] Lin Zhi-guo, Bai Peng, Fan Wen-tong, Lin Jin-fu and Tan Rui-lian, Chinese Journal of Lasers **42**, 138 (2015).

[2] Gallage R. G., IEEE Transactions on Information Theory **8**, 21 (1962).

[3] Li Juane, Liu Ke-ke, Lin Shu and K. Abdel-Ghaffar, IEEE Transactions on Communications **63**, 1057 (2015).

[4] Huang Sheng, Tian kai, He Li and Liang Tian-yu, Journal of Optoelectronics·Laser **25**, 56 (2014). (in Chinese)

[5] Zheng Jian, Bie Hong-xia, Zhang Xue-kun, Lei Chun-yang, Fang Ming, Li Sha and Kang Zhe, Journal of Optoelectronics·Laser **25**, 1 (2014). (in Chinese)

[6] Zhang Jian-hua and Zhang Guo-hua, IEEE Communications Letters **18**, 656 (2014).

[7] Park Hosung, Hong Seokbeom, No Jong-Seon and Shin Dong-Joon, IEEE Transactions on Communications **61**, 3108 (2013).

[8] Zhao Ming, Zhang Xiao-Lin, Zhao Ling and Lee Chen, IEEE Transactions on Circuits and Systems II: Express Briefs **62**, 56 (2015).

[9] Yuan Jian-guo, Liu Wen-long, Huang Sheng, Wang

Yong, Journal of Beijing University of Posts and Telecommunications **36**, 20 (2013). (in Chinese)
[10] Yuan Jian-guo, Zhou Guang-xiang, Semiconductor Optoelectronics **36**, 615 (2015).
[11] Huang Sheng, Jia Xue-ting, Tian Fang-fang and Yuan Jian-guo, Study on Optical Communications **40**, 24 (2014). (in Chinese)
[12] Yuan Jian-guo, Xie Ya, Wang Lin, Huang Sheng and Wang Yong, Optoelectronics Letters **9**, 42 (2013).
[13] Yuan Jian-guo, Liang Meng-qi, Wang Yong, Lin Jin-zhao and Pang Yu, Optoelectronics Letters **12**, 208 (2016).
[14] Yuan Jian-guo, Liang Meng-qi, Wang Yong, Lin Jin-zhao and Pang Yu, Optoelectronics Letters **12**, 132 (2016).
[15] Roxana Smarandache and Pascal O. Vontobel, IEEE Transactions on Information Theory 58, 585 (2012).
[16] Shin Min-Ho, Kim Joon-Sung and Song Hong-Yeop, IEEE Communications Letters **9**, 240 (2005).
[17] ITU-TG.975, Forward Error Correction for Submarine Systems, 2000.
[18] ITU-TG.975.1. Forward Error Correction for High Bit-Rate DWDM Submarine Systems, 2004.
[19] Yuan Jian-guo, Zhou Guang-xiang, Gao Wen-chun, Wang Yong, Lin Jin-zhao and Pang Yu, Optoelectronics Letters **12**, 61 (2016).
[20] Li Juane, Liu Ke-ke, Lin Shu and Khaled Abdel-Ghaffar, IEEE Transactions on Communications **62**, 2626 (2014).