A novel construction method of QC-LDPC codes based on the subgroup of the finite field multiplicative group for optical transmission systems*

YUAN Jian-guo (袁建国)**, **ZHOU Guang-xiang** (周光香), **GAO Wen-chun** (高文春), **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 20 July 2015)

According to the requirements of the increasing development for optical transmission systems, a novel construction method of quasi-cyclic low-density parity-check (QC-LDPC) codes based on the subgroup of the finite field multiplicative group is proposed. Furthermore, this construction method can effectively avoid the girth-4 phenomena and has the advantages such as simpler construction, easier implementation, lower encoding/decoding complexity, better girth properties and more flexible adjustment for the code length and code rate. The simulation results show that the error correction performance of the QC-LDPC(3 780,3 540) code with the code rate of 93.7% constructed by this proposed method is excellent, its net coding gain is respectively 0.3 dB, 0.55 dB, 1.4 dB and 1.98 dB higher than those of the QC-LDPC(5 334,4 962) code constructed by the method based on the inverse element characteristics in the finite field multiplicative group, the SCG-LDPC(3 969,3 720) code constructed by the systematically constructed Gallager (SCG) random construction method, the LDPC(32 640,30 592) code in ITU-T G.975.1 and the classic RS(255,239) code which is widely used in optical transmission systems in ITU-T G.975 at the bit error rate (*BER*) of 10^{-7}. Therefore, the constructed QC-LDPC(3 780,3 540) code is more suitable for optical transmission systems.

Document code: A **Article ID:** 1673-1905(2016)01-0061-4

DOI 10.1007/s11801-016-5141-3

With the increasing development of optical transmission systems towards longer distance, larger capacity and higher bit rate, the further improvements of the transmission rate and distance are heavily limited due to the accumulated optical effects, such as the dispersion, polarization mode dispersion (PMD) and the accumulated nonlinear optical effects, such as four-wave mixing (FWM), stimulated Raman scattering (SRS) and stimulated Brillouin scattering (SBS) in transmission optical fibers[1,2]. As a result, it has been becoming necessary to develop a more powerful forward error correction (FEC) code type in order to gain higher net coding gain (NCG) and better error correction performance. Because of stronger error correction ability and lower complexity, low density parity check (LDPC) code has become a research focus in the optical fiber transmission systems[3-5].

In recent years, LDPC codes in the quasi-cyclic (QC) form have been deeply investigated. A number of QC-LDPC codes have been constructed and shown to have the good error performance[4,6,7]. QC-LDPC codes are a kind of LDPC codes whose sub-matrix of check matrix $\boldsymbol{H}$ is a circulant permutation matrix (CPM) or zero matrix. Based on the unique structure of QC-LDPC codes, the computational complexity and memory cost of encoding can be efficiently reduced[7,8]. The design method of QC-LDPC code based on the finite field is proposed in Refs.[9] and [10] which show that the QC-LDPC codes have better error correction performance. The key of the method to construct a check matrix $\boldsymbol{H}$ based on the multiplicative group of the finite field is how to construct the basic matrix $\boldsymbol{W}$[11].

According to the characteristics of optical transmission systems, a novel construction method of the basic matrix for constructing QC-LDPC codes based on the subgroup of the finite field multiplicative group is proposed and studied in this paper. The QC-LDPC code with greater code length, higher code rate and the girth at least 6 can be flexibly constructed by this novel method. Furthermore, the QC-LDPC(3 780,3 540) code with code rate of 93.7% constructed by the novel method has better

* This work has been financially supported by the Program for Innovation Team Building at Institutions of Higher Education in Chongqing (No.J2013-46), the National Natural Science Foundation of China (Nos.61472464 and 61471075), 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

error correction performance over the additive white Gaussian noise (AWGN) channel by applying the sum-product decoding algorithm.

Consider the finite field as GF(q)[12], where q is a prime or the power of a prime. Let α be a primitive element of the GF(q), then set $\{\alpha^{-\infty}\equiv 0,\alpha^0=1,\alpha^1,\ldots,\alpha^{q-2}\}$ to give all elements of GF(q), and $\alpha^{q-1}=1$. All non-zero elements of GF(q) constitute the multiplicative group of a finite field. For each non-zero element α^i with $0\le i\le q-2$, form a (q−1) tuple vector over GF(2), $\boldsymbol{Z}(\alpha^i)=(z_0,z_1,\ldots,z_i,\ldots,z_{q-2})$, where the ith component z_i=1, while all other components are equal to 0. The (q−1) tuple vector $\boldsymbol{Z}(\alpha^i)$ is called as the M location vector of α^i, where "M" stands for "multiplicative". The M location vector $\boldsymbol{Z}(0)$ of 0 element is defined as the all zero (q−1) tuple (0,0,…,0).

Let β be an element of GF(q), then the M location vector $\boldsymbol{Z}(\alpha\beta)$ of $\alpha\beta$ is the right cyclic shift (one place to right) of the M location vector $\boldsymbol{Z}(\beta)$ of β. Constituting a (q−1)×(q−1) matrix $\boldsymbol{A}$ with the M location vector of β, $\alpha\beta$,…, $\alpha^{q-2}\beta$ serve as its consecutive rows. Hence if $\beta=0$, $\boldsymbol{A}$ is a (q−1)×(q−1) zero matrix, or if $\beta\ne 0$, $\boldsymbol{A}$ is a circle permutation matrix, each row of which is the right cyclic shift of the row above it and the first row is the right cyclic shift of the last row. The (q−1)×(q−1) matrix $\boldsymbol{A}$ is called as the binary dispersion matrix of β.

The structure of the check matrix can seriously affect the performance of QC-LDPC codes, and the basic characteristic of the constructed QC-LDPC code is determined by the construction of its parity check matrix $\boldsymbol{H}$. The method to construct a QC-LDPC code based on finite field is mainly divided into two steps: Firstly, construct a basic matrix $\boldsymbol{W}$; Secondly, expand the basic matrix by (q−1)-fold vertical expansion and (q−1)-fold horizontal expansion. In fact, those two expansions can be regarded as replacing each element of the basic matrix $\boldsymbol{W}$ by its own binary dispersion matrix $\boldsymbol{A}_{\boldsymbol{w}(i,j)}$ and then get the check matrix $\boldsymbol{H}$.

Let α be a primitive element of GF(q), q=2^s, where s is a positive integer, then set $\{\alpha^{-\infty}\equiv 0,\alpha^0=1,\alpha^1,\ldots,\alpha^{q-2}\}$ to give all elements of GF(q). Assuming that c and m are two distinct multiplication factors of (q−1), let $\beta=\alpha^{(q-1)/c}$, $\gamma=\alpha^{(q-1)/m}$. Obviously, β and γ are also two disparate elements of GF(q). Let $G1=\{\beta^0,\beta^1,\ldots,\beta^{c-1}\}$ and $G2=\{\gamma^0,\gamma^1,\ldots,\gamma^{m-1}\}$ be two different subgroups of the multiplicative group over GF(q), furthermore, it is clear that $G1\cap G2=\{1\}$. And then form a $r\times l$ basic matrix $\boldsymbol{W}$ over GF(q), where $r\le m, l\le c$. For any $0\le i\le r-1$, $0\le j\le l-1$, the element of the basic matrix is $w_{i,j}$, and define $w_{i,j}$ as $\gamma^i+\beta^j$. The construction of the basic check matrix $\boldsymbol{W}$ is shown as follows.

$$\boldsymbol{W}=\begin{bmatrix} w_0\\ w_1\\ \vdots\\ w_{r-1}\end{bmatrix}=\begin{bmatrix} \gamma^0+\beta^0 & \gamma^0+\beta^1 & \cdots & \gamma^0+\beta^{l-1}\\ \gamma^1+\beta^0 & \gamma^1+\beta^1 & \cdots & \gamma^1+\beta^{l-1}\\ \vdots & \vdots & \ddots & \vdots\\ \gamma^{r-1}+\beta^0 & \gamma^{r-1}+\beta^1 & \cdots & \gamma^{r-1}+\beta^{l-1}\end{bmatrix}. \quad (1)$$

Here, the above check matrix $\boldsymbol{W}$ has the structural properties as follows:

1) All the entries of a row (column) are distinct elements in GF(q);

2) Each row or each column contains at most one zero element;

3) For $0\le i\le r-1, 0\le k,t\le q-2$ and $k\ne t$, $\alpha^k\boldsymbol{W}_i$ and $\alpha^t\boldsymbol{W}_i$ lie in at least l−1 diverse places;

4) For $0\le i,j\le r-1, i\ne j, 0\le k,t\le q-2$, $\alpha^k\boldsymbol{W}_i$ and $\alpha^t\boldsymbol{W}_j$ lie in at least l−1 diverse places.

The above structural properties 3) and 4) are the constraint conditions on the rows of $\boldsymbol{W}$ and are respectively taken as the α-multiplied row-constraint conditions 1 and 2. The proof that the basic check matrix $\boldsymbol{W}$ meets the α-multiplied row-constraint conditions 1 and 2 is given as follows.

Proof: s is a certain column, where $0\le s\le l-1$. If the α-multiplied row constraint condition 1 can't be met, the equation $\alpha^k w_{is}=\alpha^t w_{is}$ can be got, where $0\le i\le r-1$, $0\le k,t\le q-2, k\ne t$. If and only if w_{is}=0, the former equation is legal. Nevertheless, each row of $\boldsymbol{W}$ has at most one 0 element, so $\alpha^k\boldsymbol{W}_i$ and $\alpha^t\boldsymbol{W}_i$ lie in at least l−1 diverse places. Thus, the α-multiplied row constraint condition 1 is proved out. If the α-multiplied row constraint condition 2 can't be met, assuming s and g are two certain columns, then $\alpha^k w_{is}=\alpha^t w_{js}$ and $\alpha^k w_{ig}=\alpha^t w_{jg}$, where $0\le i,j\le r-1, i\ne j, 0\le k,t\le q-2$, $0\le s,g\le l-1$ and $s\ne g$. Hence $\alpha^k w_{is}\alpha^t w_{jg}=\alpha^t w_{js}\alpha^k w_{ig}$, which means that $w_{is}\cdot w_{jg}=w_{js}\cdot w_{ig}$. While $\beta=\alpha^{(q-1)/c}$, $\gamma=\alpha^{(q-1)/m}$ and $w_{i,j}=\gamma^i+\beta^j$, where $c\ne m$, the equation $(\gamma^j+\beta^s)\cdot(\gamma^j+\beta^g)=(\gamma^j+\beta^s)\cdot(\gamma^j+\beta^g)$ can be obtained as a result, and then the following Eq.(2) can be further deduced.

$$(\alpha^{\frac{q-1}{m}i}+\alpha^{\frac{q-1}{c}s})\cdot(\alpha^{\frac{q-1}{m}j}+\alpha^{\frac{q-1}{c}g})=(\alpha^{\frac{q-1}{m}j}+\alpha^{\frac{q-1}{c}s})\times(\alpha^{\frac{q-1}{m}i}+\alpha^{\frac{q-1}{c}g}). \quad (2)$$

Successively, Eqs.(3) and (4) can be obtained.

$$\alpha^{\frac{q-1}{c}s+\frac{q-1}{m}j}+\alpha^{\frac{q-1}{c}g+\frac{q-1}{m}i}=\alpha^{\frac{q-1}{c}s+\frac{q-1}{m}i}+\alpha^{\frac{q-1}{c}g+\frac{q-1}{m}j}, \quad (3)$$

$$\begin{cases}\alpha^{\frac{q-1}{c}s+\frac{q-1}{m}j}=\alpha^{\frac{q-1}{c}s+\frac{q-1}{m}i}, \alpha^{\frac{q-1}{c}g+\frac{q-1}{m}i}=\alpha^{\frac{q-1}{c}g+\frac{q-1}{m}j}\\ \text{or}\\ \alpha^{\frac{q-1}{c}s+\frac{q-1}{m}j}=\alpha^{\frac{q-1}{c}g+\frac{q-1}{m}j}, \alpha^{\frac{q-1}{c}g+\frac{q-1}{m}i}=\alpha^{\frac{q-1}{c}s+\frac{q-1}{m}i}\end{cases}. \quad (4)$$

In Eq.(4), i=j or s=g. In fact, $i\ne j$ and $s\ne g$, so the two equations of $\alpha^k w_{is}=\alpha^t w_{js}$ and $\alpha^k w_{ig}=\alpha^t w_{jg}$ can't be got at the same time. Therefore, the α-multiplied row constraint condition 2 is proved out. From the above, the basic matrix $\boldsymbol{W}$ can meet the α-multiplied row constraint conditions 1 and 2 at the same time.

Considering the basic matrix $\boldsymbol{W}$ in Eq.(1), replace each element w_{ij} of the basic matrix $\boldsymbol{W}$ by its own binary dispersion matrix $\boldsymbol{A}_{w(i,j)}$. Thus, an $r\cdot(q-1)\times l\cdot(q-1)$ parity check matrix $\boldsymbol{H}$ is obtained, and a version of this extension method is introduced in Ref.[9]. Because the basic matrix $\boldsymbol{W}$ can meet both the α-multiplied row constraint conditions 1 and 2, the check matrix $\boldsymbol{H}$ obtained by the extension can also meet the row-column (RC) constraint condition, that is to say, there are no more than two "1"s in the same position in the check matrix $\boldsymbol{H}$. Therefore, the tanner graph of the constructed QC-LDPC code has no girth-4 phenomenon, in other words, its girth is at least 6. The check matrix $\boldsymbol{H}$ of the constructed QC-LDPC code is shown as follows.

$$\boldsymbol{H}=\begin{bmatrix} \boldsymbol{A}_{0,0} & \boldsymbol{A}_{0,1} & \cdots & \boldsymbol{A}_{0,l-1} \\ \boldsymbol{A}_{1,0} & \boldsymbol{A}_{1,1} & \cdots & \boldsymbol{A}_{1,l-1} \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{A}_{r-1,0} & \boldsymbol{A}_{r-1,1} & \cdots & \boldsymbol{A}_{r-1,l-1} \end{bmatrix}, \tag{5}$$

where $\boldsymbol{A}_{ij}$ is a $(q-1)\times(q-1)$ matrix over GF(2), which is either zero if $w_{ij}=0$ or a circulant permutation matrix if $w_{ij}\neq 0$. As c and m are two distinct multiplication factors of $q-1$, for arbitrary two integers r and l with $r\le m, l\le c$, there exist l different elements over GF(q) in each row of the basic matrix $\boldsymbol{W}$, and the zero element of row 1 is evidently in the first place. However, for $2\le i\le r$, whether row i has zero element or not is determined by m/c. If m/c is a positive integer, each row of the basic matrix $\boldsymbol{W}$ has one zero element. Assuming the zero element is located in the jth ($j\le l$) column in row i ($2\le i\le r$), only if $i-1/j-1=m/c$, we can get $w_{i,j}=0$. As a consequence, $\boldsymbol{H}$ is an $r\cdot(q-1)\times l\cdot(q-1)$ matrix over GF(2), whose null space gives an approximate regular QC-LDPC code with row weight $l-1$, column weights r and $r-1$. If m/c is not a positive integer, there exists no zero element in the other rows except row 1. Consequently, $\boldsymbol{H}$ is an $r\cdot(q-1)\times l\cdot(q-1)$ matrix over GF(2), and also its null space gives an approximate regular QC-LDPC code with row weights $l-1$ and l, as well as column weights r and $r-1$.

A novel QC-LDPC code is constructed by the proposed method based on the finite field. The parameters are chosen as follows: $q=2^6$, $m=21$, $c=63$, $r=4$, $l=60$, where α is a primitive element of GF(2^6), thus, $\beta=\alpha^{63/21}=\alpha^3$, $\gamma=\alpha^{63/63}=\alpha$. Owing to 63/21=3, each row of the basic matrix $\boldsymbol{W}$ contains one zero element. Consequently, the check matrix $\boldsymbol{H}$ is a 252×3 780 matrix with the row weight of 59 and the two column weights of 3 and 4, whose null space gives a approximate regular QC-LDPC(3 780,3 540) code with the code rate of 93.7%. The basic simulation environment is under the condition of GF(2), with the binary phase shift keying (BPSK) modulation mode and the additive white Gaussian noise (AWGN) channel with sum-product decoding algorithm of the soft iteration decoding algorithm at the 16 iterations by applying the MATLAB programmer.

No girth-4 phenomenon is found in the check matrix $\boldsymbol{H}$ of QC-LDPC(3 780,3 540) code through the girth-4 testing in the simulation platform. In order to fully demonstrate the error correction performance of the QC-LDPC(3 780,3 540) code for optical transmission systems, the simulation analysis of its error correction performance compared with those of other four codes with the same code rate of 93.7% is performed and studied, and the four codes are respectively the classic RS(255,239) code which is widely used in optical transmission systems in ITU-T G.975[13], the LDPC(32 640,30 592) code in ITU-T G.975.1[14], the SCG-LDPC(3 969,3 720) code constructed by the systematically constructed Gallager random method in Ref.[15] and the QC-LDPC(5 334,4 962) code proposed in Ref.[11] based on the inverse element characteristics in the finite field multiplicative group. The simulation results are shown in Fig.1. It can be seen from Fig.1 that the net coding gain (NCG) of the novel QC-LDPC(3 780,3 540) code is respectively 0.3 dB, 0.55 dB, 1.4 dB and 1.98 dB higher than those of the QC-LDPC(5 334,4 962) code, the SCG-LDPC(3 969,3 720) code, the LDPC(32 640,30 592) code in ITU-T G.975.1 and the classic RS(255,239) code at the bit error rate (*BER*) of 10^{-7}.

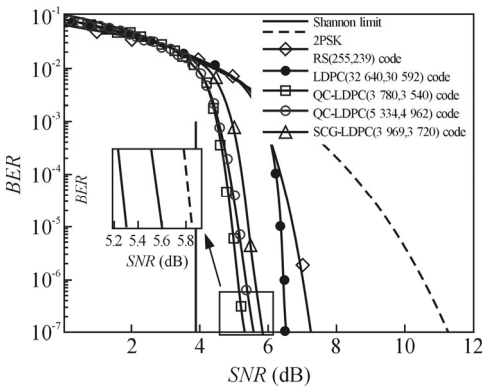

Fig.1 Performance of the constructed QC-LDPC(3 780, 3 540) code compared with other four codes with the same code rate of 93.7%

A novel construction method of the QC-LDPC code, based on the subgroup of the finite field multiplicative group, is proposed in this paper. This construction method can effectively avoid the girth-4 phenomenon and has the advantages, such as simpler construction, easier implementation, lower encoding/decoding complexity and better girth properties, as well as more flexible adjustment for the code length and code rate. According to the characteristics of optical transmission systems, the novel QC-LDPC(3 780,3 540) code with the code rate of 93.7% is constructed by this novel method. The simulation results show that the constructed QC-LDPC(3 780,3 540) code has excellent error correction performance. As a result, the proposed construction method of the QC-LDPC code can be more suitable for optical transmission systems.

References

[1] Binh. L. N, Huynh. T. L, Pang. K K and Sivahumaran. T, Journal of Lightwave Technology **26**, 1586 (2008).

[2] Yuan Jianguo, Ye Wenwei, Jiang Ze, Mao Youju and Wang Wei, Optics Communications **273**, 421 (2007).

[3] Zhang Peng, Yu Shou, Liu Changyin and Jiang Lanxiang, Electronics Letters **50**, 320 (2014).

[4] Yuan Jianguo, Liu Feilong, Ye Wenwei, Huang Sheng and Wang Yong, OPTIK **125**, 1016 (2014).

[5] Djordjevic. I .B, Cvijetic. M, Xu Lei and Wang Ting, Journal of Lightwave Technology **25**, 3619 (2007).

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

[7] Sung. Lk. Park, Heung. Mook. Kim, Wu Yi-yan and Jeongchang. K, IEEE Transactions on Broadcasting **59**, 155 (2013).

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

[9] Song Shu-mei, Zhou Bo, Lin Shu and Abdel-Ghaffar. K, IEEE Transactions on Communications **57**, 84 (2009).

[10] Juane. Li, Liu Ke-ke, Lin Shu and Abdel-Ghaffar. K, IEEE Transactions on Communications **62**, 2626 (2014).

[11] Yuan Jian-guo, Xu Liang and Tong Qing-zhen, Optoelectronics Letters **9**, 378 (2013).

[12] Kang Jin-yu, Huang Qin, Zhang Li, Zhou Bo and Li Shu, IEEE Transactions on Communications **58**, 1383 (2010).

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

[14] ITU-T G.975.1, Forward Error Correction for High Bit-rate DWDM Submarine Systems, 2004.

[15] Yuan Jian-guo, Xie Ya, Wang Lin, Huang Sheng and Wang Yong, Optoelectronics Letters **9**, 0042 (2013).