A novel QC-LDPC code based on the finite field multiplicative group for optical communications*

YUAN Jian-guo (袁建国)**, **XU Liang** (许亮), **and TONG Qing-zhen** (仝青振)

Key Lab. of Optical Fiber Communication Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

(Received 5 June 2013)

A novel construction method of quasi-cyclic low-density parity-check (QC-LDPC) code is proposed based on the finite field multiplicative group, which has easier construction, more flexible code-length code-rate adjustment and lower encoding/decoding complexity. Moreover, a regular QC-LDPC(5334,4962) code is constructed. The simulation results show that the constructed QC-LDPC(5334,4962) code can gain better error correction performance under the condition of the additive white Gaussian noise (AWGN) channel with iterative decoding sum-product algorithm (SPA). At the bit error rate (BER) of 10^{-6}, the net coding gain (NCG) of the constructed QC-LDPC(5334,4962) code is 1.8 dB, 0.9 dB and 0.2 dB more than that of the classic RS(255,239) code in ITU-T G.975, the LDPC(32640,30592) code in ITU-T G.975.1 and the SCG-LDPC(3969,3720) code constructed by the random method, respectively. So it is more suitable for optical communication systems.

Document code: A **Article ID:** 1673-1905(2013)05-0378-3

DOI 10.1007/s11801-013-3102-7

The low-density parity-check (LDPC) code is discovered by Gallager[1] in 1962, and is also a kind of the linear block codes which can approach the Shannon limit[2,3]. Because of its low encoding/decoding complexity and flexible code-length/code-rate adjustment, the LDPC code is widely used in optical communication system, mobile communication system, satellite communication system and storage system[2].

Quasi-cyclic low-density parity-check (QC-LDPC) code is a kind of LDPC code whose sub-matrix of check matrix $\boldsymbol{H}$ is the circulant permutation matrix (CPM) or zero matrix[2,3]. The CPM is a kind of square matrix with the fixed row weight and column weight. Every row of CPM is formed by the cyclic shift of upper row, and the first row is formed by the last one. Similarly, every column is also formed by the cyclic shift of former column, and the first column is formed by the last one. The special structure of CPM makes it easy to achieve the encoding process through the simple cyclic shift registers with the linear complexity[2,4]. So the research of the construction for QC-LDPC codes has become a hot spot in optical communication systems.

The construction methods of LDPC codes can be classified into two general categories[5,6] of pseudo random construction method and structured construction method. The construction method of QC-LDPC codes based on the CPM of finite field is an effective construction method in structured QC-LDPC codes.

According to the transmission characteristics of optical communication systems, a novel construction method of QC-LDPC codes based on finite field multiplicative group is proposed and studied in this paper. Furthermore, a regular QC-LDPC(5334,4962) code is constructed, and the error correction performance of it and other three codes is comparatively simulated and analyzed.

Consider the finite field as $GF(q)$[7,8], where q is the power of a prime. Let α be a primitive element of $GF(q)$, $\{\alpha^{-\infty}\equiv0,\ \alpha^{0}=1,\ \alpha,\cdots,\ \alpha^{q-2}\ \}$ can form all the elements of $GF(q)$, and $\alpha^{q-1}=1$. The q–1 non-zero elements in $GF(q)$ field form the multiplicative group of $GF(q)$ under the multiplicative operation. For each non-zero element α^{i} with $0\le i\le q-2$, form a (q–1)-tuple over $GF(2)$ as $z(\alpha^{i})=(z_0, z_1,\cdots, z_{q-2})$, whose components correspond to the q–1 non-zero elements of $GF(q)$, where the ith component z_i=1 and all the other q–2 components are equal to 0. The (q–1)-tuple $z(\alpha^{i})$ with a single 1-component is referred as the location vector of α^{i} with respect to the multiplicative group of $GF(q)$. $z(\alpha^{i})$ is called as the M-location vector of α^{i}, where M stands for "multiplicative". The location vector $z(0)$ of the 0 element of $GF(q)$ is defined as the all-zero (q–1)-tuple of (0,0,···,0).

Let γ be a non-zero element in $GF(q)$, then the M-location vector $z(\alpha\gamma)$ of $\alpha\gamma$ is the right cyclic shift of the M-location vector $z(\gamma)$ of γ. Form a (q–1)×(q–1) ma-

* This work has been supported by the National Natural Science Foundation of China (Nos.61071117, 61275077 and 61003256), and the Natural Science Foundation of CQ CSTC (No.2010BB2409).

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

trix $\boldsymbol{A}$ over $GF(2)$ with the M-location vectors of γ, $\alpha\gamma,\cdots,\alpha^{q-2}\gamma$ as rows. $\boldsymbol{A}$ is a circulant permutation matrix, but each row of $\boldsymbol{A}$ is a right cyclic shift of the row above it, and the first row is the right cyclic shift of the last row.

The innate characteristic of constructing a QC-LDPC code is the construction of its parity check matrix $\boldsymbol{H}$. Using general finite field method to construct QC-LDPC codes is mainly divided into three steps: construct basic matrix, $(q-1)$-fold vertical expansion, and $(q-1)$-fold horizontal expansion. The performance of the code is determined by the structure of the basic matrix. So the core target is to construct a basic matrix. If there is no zero matrix in the basic matrix, the constructed code is called as the regular QC-LDPC code, otherwise, the code is called as the irregular QC-LDPC code. A novel construction method for QC-LDPC codes based on the finite field multiplicative groups is introduced as follows in detail.

Let α be a primitive element in $GF(q)$, where $q=2^p$, p is a positive integer. For $0\le i\le q-1$, $\alpha^i\in GF(q)$, the set $\{\alpha^0, \alpha^1,\cdots, \alpha^{q-2}\}$ forms a multiplicative group of the finite field. $(\alpha^i)^{-1}$ is the inverse element of α^i, and the inverse element of α^i is unique. It is clear that $(\alpha^i)^{-1}\in GF(q)$ froms the property of finite field. That is to say, the set $\{(\alpha^0)^{-1}, (\alpha^1)^{-1},\cdots, (\alpha^{q-2})^{-1}\}$ also forms the elements of finite field. Then form a $(q-1)\times(q-1)$ basic matrix $\boldsymbol{W}$. For any $0\le i$, $j\le q-2$, the elements of the basic matrix are determined by $w_{i,j}=\alpha^i+(\alpha^i)^{-1}$, so we can obtain

$$\boldsymbol{W}=\begin{bmatrix} \alpha^0+(\alpha^0)^{-1} & \alpha^0+(\alpha^1)^{-1} & \cdots & \alpha^0+(\alpha^{q-2})^{-1} \\ \alpha^1+(\alpha^0)^{-1} & \alpha^1+(\alpha^1)^{-1} & \cdots & \alpha^1+(\alpha^{q-2})^{-1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{q-2}+(\alpha^0)^{-1} & \alpha^{q-2}+(\alpha^1)^{-1} & \cdots & \alpha^{q-2}+(\alpha^{q-2})^{-1} \end{bmatrix} .(1)$$

The matrix has the following structural properties. First, each row (column) has and only has one 0 element, while $i+j= q-1$, $w_{i,j}=0$. Second, the elements in each row (column) are different in $GF(q)$. Third, the elements at the same position but in different row (column) are also different.

For each row of $\boldsymbol{W}$ with $0\le i\le q-2$, we expand it vertically into a $(q-1)\times(q-1)$ matrix $\boldsymbol{V}_i$ over $GF(q)$ by multiplying it with α^0, $\alpha,\cdots$, α^{q-2} as:

$$\boldsymbol{V}_i=\begin{bmatrix} \alpha^0 W_{i,0} & \alpha^0 W_{i,1} & \cdots & \alpha^0 W_{i,q-2} \\ \alpha^1 W_{i,0} & \alpha^1 W_{i,1} & \cdots & \alpha^1 W_{i,q-2} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{q-2} W_{i,0} & \alpha^{q-2} W_{i,1} & \cdots & \alpha^{q-2} W_{i,q-2} \end{bmatrix}. \qquad (2)$$

The same procedure is taken to each row of $\boldsymbol{W}$, then a $(q-1)^2\times(q-1)$-tuple vertical expansion matrix $\boldsymbol{V}$ is obtained.

For $0\le i\le q-2$, replacing each entry of $\boldsymbol{V}_i$ by its M-location vector, a $(q-1)\times(q-1)^2$ matrix over $GF(2)$ is obtained, and each entry of $\boldsymbol{V}_i$ consists of $q-1$ M-location vectors $\boldsymbol{A}_{i,j}$. Then the complete $(q-1)^2\times(q-1)^2$ -tuple parity check matrix $\boldsymbol{H}$ over $GF(2)$ is obtained as

$$\boldsymbol{H}=\begin{bmatrix} H_0 \\ H_1 \\ \vdots \\ H_{q-2} \end{bmatrix}=\begin{bmatrix} A_{0,0} & A_{0,1} & \cdots & A_{0,q-2} \\ A_{1,0} & A_{1,1} & \cdots & A_{1,q-2} \\ \vdots & \vdots & \ddots & \vdots \\ A_{q-2,0} & A_{q-2,1} & \cdots & A_{q-2,q-2} \end{bmatrix}. \qquad (3)$$

If there are short cycles in check matrix, the updated message will be related during the iterative process. It makes the convergence rate slow or even not convergent, and then impacts the decoding performance. So we should avoid the girth-4 phenomenon when check matrix is constructed. That is to say, we should follow the row-column (RC) constraint. The RC constraint points out that in different rows (columns) of check matrix, there shouldn't be more than one "1" in the same position. Simulation result shows that the check matrix constructed by the proposed method meets the RC constraint.

For any pair (γ, ρ) of integers with $1\le\gamma\le q-2$ and $1\le\rho\le q-2$, let $\boldsymbol{H}(\gamma, \rho)$ be a $\gamma\times\rho$ submatrix of $\boldsymbol{H}$. $\boldsymbol{H}(\gamma, \rho)$ is a $\gamma(q-1)\times\rho(q-1)$ matrix over $GF(2)$. Since it is a submatrix of $\boldsymbol{H}$, it also meets the RC constraint. The null space of $\boldsymbol{H}(\gamma, \rho)$ gives a QC-LDPC code C_{qc}. The length of the code is $\rho(q-1)$, and the rate is at least $(\rho-\gamma)/\rho$. Also, its girth is at least 6. If the column weight and row weight are constant, and there is no zero matrix in $\boldsymbol{H}(\gamma, \rho)$, the constructed code is a regular QC-LDPC code. Otherwise, the code is an irregular QC-LDPC code.

The following construction principles should be taken into consideration when constructing regular LDPC codes for optical communication systems[9-12]. ①There ought to be low error floor or no error floor at best. ② The net coding gain (NCG) should be high, and the redundancy of the code type should be low. ③The codeword length cannot be too long, the time delay arisen from encoding/decoding should not be too much, and the software/hardware implementation should be favorable. ④The constructed LDPC codes should have no girth-4 to suffice the requirements of the Steiner limit, making the decoding of the LPDC code with better decoding constringency. ⑤The constructed LDPC codes should have lower density, that is, in the parity-check matrix $\boldsymbol{H}$ of LDPC codes, the number of ones should be absolutely less than that of zeros. In this way, there is less calculation each time when iteratively decoding and the decoding complexity is reduced.

Based on the above principles, the basic simulation environment under the condition of $GF(2)$, binary phase shift keying (BPSK) modulation and additive white Gaussian noise (AWGN) channel with decoding sum-product algorithm (SPA) at the sixteen iteration is used in this paper. Considering the characteristics of optical communication systems and the requirements of the higher code-rate for QC-LDPC codes, choose the parameter $q=2^7=128$, column weight $\gamma=3$ and row weight $\rho=42$. Construct a 127×127 matrix of $\boldsymbol{H}$. Then take a 3×42 submatrix from the left top corner of $\boldsymbol{H}$. The null space of the taken check matrix gives a regular QC-LDPC(5334,4962) code with the code rate of 0.937.

The relevant performance curve between the bit error rate (BER) and signal-to-noise ratio (SNR) for the regular QC-LDPC(5334,4962) code can be achieved by the Matlab programming. Then compare the error correction performance of QC-LDPC(5334,4962) code and other codes. Fig.1 shows the error correction performance of QC-LDPC (5334,4962) code and the classic RS(255,239) code in ITU-T G.975[13] as well as the LDPC(32640,30592) code in ITU-T G.975.1[14] and SCG-LDPC(3969,3720) code[15] constructed by the random construction method.

From Fig.1, it can be seen that NCG of the constructed QC-LDPC(5334,4962) code is respectively 1.8 dB, 0.9 dB and 0.2 dB more than that of the classic RS(255,239) code in ITU-T G.975, the LDPC(32640, 30592) code in ITU-T G.975.1 and the SCG-LDPC(3969, 3720) code constructed by the random method at the BER of 10^{-6}.

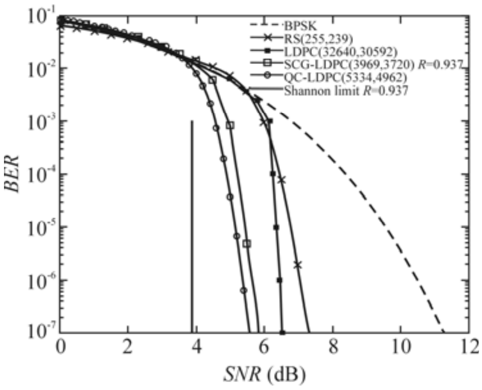

Fig.1 The error correction performance comparison of QC-LDPC (5334,4962) code and other codes

A novel construction method of QC-LDPC codes is proposed based on the finite field multiplicative group in this paper. This construction method has advantages of easier construction, more flexible code-length code-rate adjustment and lower encoding/decoding complexity. Moreover, a regular QC-LDPC (5334,4962) code is constructed by this construction method. The simulation results show that the error correction performance of the regular QC-LDPC(5334,4962) code is better than that of the classic RS(255,239) code and LDPC (32640,30592) code, which are widely used in optical communication systems, as well as the SCG-LDPC(3969, 3720) code constructed by the random construction method. Therefore, the constructed regular QC-LDPC (5334,4962) code can be more suitable for optical communication systems.

References

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

[2] Xu Chen and F. C. M. Lau, Construction of High-Rate QC-LDPC Codes, 2011 IEEE International Conference on Advanced Technologies for Communications, 24 (2011).

[3] M. P. C. Fossorier, IEEE Transaction on Information Theory **50**, 1788 (2004).

[4] I. B. Djordjevic, M. Arabaci and L. L. Minkov, Journal of Lightwave Technology **27**, 3518 (2009).

[5] William E. Ryan and Shu Lin, Channel Codes Classical and Modern, England: Cambridge University Press, 523 (2009).

[6] Lan Lan, Zeng Liqing and Ying Y. Tai, IEEE Trans. Inform. Theory **53**, 2429 (2007).

[7] S Song, B. Zhou and S. Lin, IEEE Trans. Commun. **57**, 71 (2009).

[8] J. Kang, Q. Huang and S. Lin, IEEE Trans. Commun. **58**, 1383 (2010).

[9] YUAN Jian-guo and YE Wen-wei, Journal of ChongQing University of Posts and Telecommunications (Natural Science Edition) **20**, 78 (2008). (in Chinese)

[10] YUAN Jian-guo, WANG Wang and LIANG Tian-yu, Journal of Optoelectronics·Laser **23**, 906 (2012). (in Chinese)

[11] YUAN Jian-guo, WANG Wang, TANG Bin, LIANG Tian-yu and WANG Yong, Journal of Optoelectronics·Laser **23**, 1304 (2012). (in Chinese)

[12] YUAN Jian-guo, XIE Ya, WANG Lin, HUANG Sheng and WANG Yong, Optoelectronics Letters **9**, 42 (2013).

[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, TONG Qing-zhen, XU Liang and HUANG Sheng, Optoelectronics Letters **9**, 204 (2013).