Construction of type-II QC-LDPC codes with fast encoding based on perfect cyclic difference sets*

LI Ling-xiang (李玲香)[1], LI Hai-bing (李海兵)[2], LI Ji-bi (李季碧)[3], and JIANG Hua (江华)[4]**

1. *School of Electronics and Information Engineering, Hunan University of Science and Engineering, Yongzhou 425199, China*
2. *BNP Paribas, 787 Seventh Avenue, New York 10019, U.S.A.*
3. *College of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*
4. *Key Laboratory of Granular Computing, Minnan Normal University, Zhangzhou 363000, China*

(Received 13 April 2017; Revised 12 June 2017)

In view of the problems that the encoding complexity of quasi-cyclic low-density parity-check (QC-LDPC) codes is high and the minimum distance is not large enough which leads to the degradation of the error-correction performance, the new irregular type-II QC-LDPC codes based on perfect cyclic difference sets (CDSs) are constructed. The parity check matrices of these type-II QC-LDPC codes consist of the zero matrices with weight of 0, the circulant permutation matrices (CPMs) with weight of 1 and the circulant matrices with weight of 2 (W2CMs). The introduction of W2CMs in parity check matrices makes it possible to achieve the larger minimum distance which can improve the error-correction performance of the codes. The Tanner graphs of these codes have no girth-4, thus they have the excellent decoding convergence characteristics. In addition, because the parity check matrices have the quasi-dual diagonal structure, the fast encoding algorithm can reduce the encoding complexity effectively. Simulation results show that the new type-II QC-LDPC codes can achieve a more excellent error-correction performance and have no error floor phenomenon over the additive white Gaussian noise (AWGN) channel with sum-product algorithm (SPA) iterative decoding.

Document code: A **Article ID:** 1673-1905(2017)05-0358-5
DOI https://doi.org/10.1007/s11801-017-7082-x

Quasi-cyclic low-density parity-check (QC-LDPC) codes, as a class of structured low-density parity-check (LDPC) codes[1], have already become the research hotspot in the coding field because of its less storage space and the lower complexity of the hardware implementation. In general, each entry of the parity check matrix $\boldsymbol{H}$ of a QC-LDPC code is a circulant. If each entry of $\boldsymbol{H}$ is either zero matrix or circulant permutation matrix (CPM), the corresponding code is termed as the type-I QC-LDPC code[2], and the constructed QC-LDPC codes in most references belong to type-I QC-LDPC codes[3-5]. The parity check matrix of a type-II QC-LDPC code is the combination of zero matrices, CPMs and circulant matrices with weight of 2 (W2CMs)[2]. Compared with a type-I QC-LDPC code, a type-II QC-LDPC code generally has a higher upper bound of the minimum distance[6]. The minimum distance is directly related to the error-correction performance of the code, and the larger minimum distance makes the code have the better anti-interference performance, as well as the error-detection and error-correction performance. Type-II QC-LDPC codes with the medium/short block lengths can also perform better than randomly constructed LDPC codes under the sum-product algorithm (SPA) iterative decoding[7,8]. However, the existence of the W2CMs in parity check matrix inevitably makes the Tanner graph more prone to have the girth-4, which affects the convergence speed of iterative decoding to some extent and thus degrades the decoding performance. The influence of W2CMs in the parity check matrices of type-II QC-LDPC codes on the minimum distance upper bound and error-correction performance has been showed in Ref.[8]. The parity check matrices of type-II QC-LDPC codes constructed in Refs.[9] and [10] only include the arrays of W2CMs, which are more likely to introduce into the short cycle in Tanner graphs, and parity check matrices are not full rank. Although the above proposed QC-LDPC codes can reduce the storage complexity to a certain extent, the problem that its encoding complexity is high has not yet solved effectively. The encoding

* This work has been supported by the National Natural Science Foundation of China (No.61472464), the Research Foundation of Education Bureau of Hunan Province in China (No.16C0686), and the Key Discipline Construction Project Funding for Hunan University of Science and Engineering (Electrical systems).
** E-mail: lilingxiang2013@hotmail.com

calculation amount of the traditional QC-LDPC code is proportional to the square of the code length[11-15], namely it is about $O(n^2)$. For QC-LDPC codes with larger block lengths, its larger encoding calculation amount can not be underestimated. Therefore, how to reduce the encoding complexity of QC-LDPC codes has become a research hotspot in the coding field.

In view of the above problems, the new irregular type-II QC-LDPC codes with fast encoding based on perfect cyclic difference sets (CDSs) are presented, whose parity check matrices consist of zero matrices, CPMs and W2CMs. The new type-II QC-LDPC code can achieve the fast encoding by directly using the parity check matrix, and its encoding complexity is linearly proportional to the code length, namely it is $O(n)$. In addition, the specific fast encoding algorithm of type-II QC-LDPC codes is also given in this paper.

Suppose L and p are two positive integers, and the structure of parity check matrix $\boldsymbol{H}$ of a type-II QC-LDPC code with code length $N=Lp$ is shown as

$$\boldsymbol{H}=\begin{bmatrix} \boldsymbol{I}(p_{0,0}^{(1)})+\boldsymbol{I}(p_{0,0}^{(2)}) & \boldsymbol{I}(p_{0,1}^{(1)})+\boldsymbol{I}(p_{0,1}^{(2)}) & \cdots & \boldsymbol{I}(p_{0,L-1}^{(1)})+\boldsymbol{I}(p_{0,L-1}^{(2)}) \\ \boldsymbol{I}(p_{1,0}^{(1)})+\boldsymbol{I}(p_{1,0}^{(2)}) & \boldsymbol{I}(p_{1,1}^{(1)})+\boldsymbol{I}(p_{1,1}^{(2)}) & \cdots & \boldsymbol{I}(p_{1,L-1}^{(1)})+\boldsymbol{I}(p_{1,L-1}^{(2)}) \\ \vdots & \vdots & \ddots & \vdots \\ \boldsymbol{I}(p_{J-1,0}^{(1)})+\boldsymbol{I}(p_{J-1,0}^{(2)}) & \boldsymbol{I}(p_{J-1,1}^{(1)})+\boldsymbol{I}(p_{J-1,1}^{(2)}) & \cdots & \boldsymbol{I}(p_{J-1,L-1}^{(1)})+\boldsymbol{I}(p_{J-1,L-1}^{(2)}) \end{bmatrix}, \quad (1)$$

where $J\le L$, and $p_{j,l}^{(i)}$ is the times of cyclically shifting to the right for each row of the identity matrix for arbitrary $0\le j\le J-1$ and $0\le l\le L-1$ with $i\in\{1,2\}$, $p_{j,l}^{(i)}\in\{\infty,0,1,p-1\}$. If $p_{j,l}^{(i)}=\infty$, the circulant $\boldsymbol{I}(\infty)$ represents a $p\times p$ zero matrix $\boldsymbol{0}$; if $p_{j,l}^{(i)}=0$, the circulant $\boldsymbol{I}(0)$ is a $p\times p$ identity matrix $\boldsymbol{I}_p$; otherwise, the circulant $\boldsymbol{I}\left(p_{j,l}^{(i)}\right)$ represents the CPM obtained by shifting right each row of a $p\times p$ identity matrix by $p_{j,l}^{(i)}$ places. From Eq.(1), it is observed that weight-0 circulant $\boldsymbol{0}$, weight-1 circulant $\boldsymbol{I}\left(p_{j,l}^{(i)}\right)$ and weight-2 circulant $\boldsymbol{I}\left(p_{j,l}^{(1)}\right)+\boldsymbol{I}\left(p_{j,l}^{(2)}\right)$ are included in parity check matrix $\boldsymbol{H}$, where $p_{j,l}^{(1)}<p_{j,l}^{(2)}$. A type-II QC-LDPC code can also be expressed by the shift matrix $\boldsymbol{S}(\boldsymbol{H})$ of parity check matrix $\boldsymbol{H}$, namely

$$\boldsymbol{S}(\boldsymbol{H})=\begin{bmatrix} (p_{0,0}^{(1)},p_{0,0}^{(2)}) & (p_{0,1}^{(1)},p_{0,1}^{(2)}) & \cdots & (p_{0,L-1}^{(1)},p_{0,L-1}^{(2)}) \\ (p_{1,0}^{(1)},p_{1,0}^{(2)}) & (p_{1,1}^{(1)},p_{1,1}^{(2)}) & \cdots & (p_{1,L-1}^{(1)},p_{1,L-1}^{(2)}) \\ \vdots & \vdots & \ddots & \vdots \\ (p_{J-1,0}^{(1)},p_{J-1,0}^{(2)}) & (p_{J-1,1}^{(1)},p_{J-1,1}^{(2)}) & \cdots & (p_{J-1,L-1}^{(1)},p_{J-1,L-1}^{(2)}) \end{bmatrix}. \quad (2)$$

It is known that the parity check matrix $\boldsymbol{H}$ of a (J, L)-regular type-I QC-LDPC code with $J>2$ has rank at most $pJ-(J-1)$[2]. Similarly, since the p binary rows within each row of circulants in $\boldsymbol{H}$ sum to the all-zero rows, that is there are at least $p-1$ linearly independent rows within each row of circulants in $\boldsymbol{H}$. So it can be easily deduced that the parity check matrix $\boldsymbol{H}$ of a (2J, 2L)-regular type-II QC-LDPC code has rank at most $pJ-J$. Therefore, a (2J, 2L)-regular type-II QC-LDPC code has code rate at least $\frac{Lp-(Jp-J)}{Lp}=1-\frac{J(p-1)}{Lp}$. However, for most of type-II QC-LDPC codes, the weight configurations of circulants in $\boldsymbol{H}$ are non-uniform (even while maintaining regularity), which can make a wider range of rates for a given $J\times L$ array. But if the parity check matrix $\boldsymbol{H}$ of $J\times L$ array has full rank pJ, the null space of this $\boldsymbol{H}$ is defined as a type-II QC-LDPC code, which has code rate of $1-J/L$.

Let $d_{j,l}=p_{j,l}^{(2)}-p_{j,l}^{(1)}$, where $d_{j,l}$ is always a positive integer, since $p_{j,l}^{(1)}<p_{j,l}^{(2)}$. It is considered that the value $d_{j,l}$ is undefined for weight-0 circulants and weight-1 circulants. Theorem 1 gives the necessary and sufficient conditions for a type-II QC-LDPC matrix $\boldsymbol{H}$ to have girth at least 6.

Theorem 1[6]: The corresponding Tanner graph of the parity check matrix $\boldsymbol{H}$ given in Eq.(1) has girth at least 6 if and only if each of the following inequalities holds true for all j_0 and j_1 with $0\le j_0\ne j_1\le J-1$, all l_0 and l_1 with $0\le l_0\ne l_1\le L-1$, all $i_t\in\{1,2\}$ with $0\le t\le 3$, and all values in following inequalities are defined.

(1) $d_{j_0,l_0}\ne -d_{j_0,l_0} \bmod p$;

(2) $d_{j_0,l_0}\ne \pm d_{j_0,l_1} \bmod p$;

(3) $d_{j_0,l_0}\ne \pm d_{j_1,l_0} \bmod p$;

(4) $p_{j_0,l_0}^{(i_0)}-p_{j_1,l_0}^{(i_1)}\ne p_{j_0,l_1}^{(i_2)}-p_{j_1,l_1}^{(i_3)} \bmod p$.

For the Abelian additive group $Z_v=\{0,1,2,\ldots,v-1\}$ of order v, a k-element subset $D=\{d_1, d_2,\ldots, d_k\}$ of Z_v forms a (v, k, λ)-cyclic difference set (CDS) if every nonzero element of Z_v occurs precisely λ times among the differences $(d_i-d_j)\bmod v$ in terms of elements of D. From the definition of CDS, it is known that the relation among parameters v, k and λ is $\lambda=k(k-1)/(v-1)$. If $\lambda=1$, then $v=k^2-k+1$, such a (v, k, 1)-CDS is called as a perfect CDS, and the differences $(d_i-d_j)\bmod v$ is distinct for arbitrary two elements d_i and d_j from D in a perfect CDS. For a (v, k, 1)-perfect CDS, its difference table, where the row and the column indexes are both the arrangement of k elements from D in an ascending order, can be built. Each element in the difference table is the modulo v difference between the index values of the corresponding row and column. The difference table of a (7, 3, 1)-perfect CDS $D=\{1, 2, 4\}$ is shown in Tab.1. It can be seen from the Tab.1 that all differences between different elements in a perfect CDS are distinct except 0 elements.

Tab.1 Difference table of the perfect CDS D={1, 2, 4} mod 7

	1	2	4
1	0	1	3
2	6	0	2
4	4	5	0

Theorem 2[16]: For any prime power $q=p^m$, p is a prime and m is an arbitrary positive integer, and there exists a $(q^2+q+1,\ q+1,\ 1)$-perfect CDS for the additive group Z_{q2+q+1}.

The first three conditions of Theorem 1 can be reformulated as

(1) $p_{j_0,l_0}^{(2)} - p_{j_0,l_0}^{(1)} \neq p_{j_0,l_0}^{(1)} - p_{j_0,l_0}^{(2)} \bmod p$;

(2) $p_{j_0,l_0}^{(2)} - p_{j_0,l_0}^{(1)} \neq p_{j_0,l_1}^{(2)} - p_{j_0,l_1}^{(1)} \bmod p$ and

$p_{j_0,l_0}^{(2)} - p_{j_0,l_0}^{(1)} \neq p_{j_0,l_1}^{(1)} - p_{j_0,l_1}^{(2)} \bmod p$;

(3) $p_{j_0,l_0}^{(2)} - p_{j_0,l_0}^{(1)} \neq p_{j_1,l_0}^{(2)} - p_{j_1,l_0}^{(1)} \bmod p$ and

$p_{j_0,l_0}^{(2)} - p_{j_0,l_0}^{(1)} \neq p_{j_1,l_0}^{(1)} - p_{j_1,l_0}^{(2)} \bmod p$.

At the same time, considering the condition (4) in Theorem 1, we can learn that all the conditions in Theorem 1 will be met if none of the differences between any two different elements $p_{j_0,l_0}^{i_0}$ and $p_{j_1,l_1}^{i_1}$ in $\boldsymbol{S}(\boldsymbol{H})$ are identical, where $i_0, i_1 \in \{1,2\}$, $0 \le j_0,j_1 \le J-1$ and $0 \le l_0,l_1 \le L-1$. It should be noted that if $j_0=j_1$ and $l_0=l_1$, then $i_0 \neq i_1$. Thus, combining perfect CDS with the property of different differences under modulo p operation, the parity check matrices of type-II QC-LDPC codes with girth at least 6 can be constructed. The specific construction steps are as follows.

(1) Design a $J\times L$ weight configuration matrix $\boldsymbol{A}_{wt}$. Each value of a_{jl} ($1\le j\le J$, $1\le l\le L$) in $\boldsymbol{A}_{wt}$ represents the weight of corresponding circulant in parity check matrix $\boldsymbol{H}$ of type-II QC-LDPC codes. In this paper, we decide to construct the parity check matrix $\boldsymbol{H}$ with three rows circulants, namely J=3. The designed weight configuration matrix $\boldsymbol{A}_{wt}$ is shown as

$$\boldsymbol{A}_{wt} = \left[\begin{array}{cccc|ccc} (1^2+1^2)\bmod 3 & [(1^2+2^2)+w_1]\bmod 3 & \cdots & [(1^2+k_b^2)+w_1]\bmod 3 & 2 & 1 & 0 \\ (2^2+1^2)\bmod 3 & [(2^2+2^2)+w_2]\bmod 3 & \cdots & [(2^2+k_b^2)+w_2]\bmod 3 & 2 & 1 & 1 \\ (3^3+1^2)\bmod 3 & [(3^2+2^2)+w_3]\bmod 3 & \cdots & [(3^2+k_b^2)+w_3]\bmod 3 & 1 & 0 & 1 \end{array}\right]. \quad (3)$$

Obviously, the entry of the first column on the left part of $\boldsymbol{A}_{wt}$ separated by dashed line is (x^2+y^2)mod 3, and the entry of remaining columns is $[(x^2+y^2)+w_1/w_2/w_3]$mod 3, where x and y are the row index and column index of the corresponding entry, respectively. Let w_1=2 when the column index is $3i_b$ ($2\le i_b\le k_b$) for the entries in the first row, otherwise let w_1=0. Then let w_2=1 for all entries in the second row, and let w_3=1 for all entries in the third row. The sub-matrix on the right part of $\boldsymbol{A}_{wt}$ separated by dashed line in Eq.(3) has the form of quasi-dual diagonal structure, which make $\boldsymbol{A}_{wt}$ have full rank. Thus, the corresponding parity check matrix $\boldsymbol{H}$ of this $\boldsymbol{A}_{wt}$ also has form of quasi-dual diagonal structure and full rank, namely rank($\boldsymbol{H}$)=pJ. The null space of this full rank $\boldsymbol{H}$ defines a code C with the code rate of $R=1-J/L$.

(2) Assign the number of elements in each entry of $\boldsymbol{S}(\boldsymbol{H})$ according to $\boldsymbol{A}_{wt}$ in Eq.(3). The value of nonzero element in $\boldsymbol{A}_{wt}$ represents the number of elements in each entry of $\boldsymbol{S}(\boldsymbol{H})$, and the value 0 in $\boldsymbol{A}_{wt}$ corresponds to the element ∞ in $\boldsymbol{S}(\boldsymbol{H})$.

(3) Set the entry including only one element to "0" excepting ∞, namely, let all weight-1 circulants in $\boldsymbol{H}$ be identity matrices with the same size.

(4) According to the property of perfect CDS, let $p=v=k^2-k+1$, and arrange the elements of a perfect CDS in the entries of shift matrix $\boldsymbol{S}(\boldsymbol{H})$ excepting 0 and ∞, in an ascending order from left to right and from top to bottom.

(5) Transform shift matrix $\boldsymbol{S}(\boldsymbol{H})$ to parity check matrix $\boldsymbol{H}$ according to Eq.(1), that's to say "0" in $\boldsymbol{H}$ is replaced by a $p\times p$ identity matrix, ∞ in $\boldsymbol{H}$ is replaced by a $p\times p$ zero matrix, and other each element in $\boldsymbol{H}$ is the permutation of a $p\times p$ CPM. The designed $3p\times(3+k_b)p$ parity check matrix $\boldsymbol{H}$ in this paper has the form of $\boldsymbol{H}=[\boldsymbol{H}_1\ \boldsymbol{H}_2]$, where the $3p\times k_bp$ $\boldsymbol{H}_1$ is termed as information sub-matrix and the $3p\times 3p$ $\boldsymbol{H}_2$ is termed as check sub-matrix. The quasi-dual diagonal structure of $\boldsymbol{H}_2$ is the base of achieving fast encoding. Suppose code vector $\boldsymbol{c}=[\boldsymbol{s}_1\ \boldsymbol{s}_2 \ldots \boldsymbol{s}_{k_b}\ \boldsymbol{p}_1\ \boldsymbol{p}_2\ \boldsymbol{p}_3]$, where $[\boldsymbol{s}_1\ \boldsymbol{s}_2 \ldots \boldsymbol{s}_k]$ is the information code vector and $[\boldsymbol{p}_1\ \boldsymbol{p}_2\ \boldsymbol{p}_3]$ is the check code vector. According to the parity check equation $\boldsymbol{Hc}^{\mathrm{T}}=\boldsymbol{0}$, it can be obtained that

$$\begin{bmatrix} \boldsymbol{H}_{1,1} & \boldsymbol{H}_{1,2} & \cdots & \boldsymbol{H}_{1,k_b} & \boldsymbol{\Phi}_1 \oplus \boldsymbol{\Phi}_2 & \boldsymbol{I} & \boldsymbol{0} \\ \boldsymbol{H}_{2,1} & \boldsymbol{H}_{2,2} & \cdots & \boldsymbol{H}_{2,k_b} & \boldsymbol{\Phi}_3 \oplus \boldsymbol{\Phi}_4 & \boldsymbol{I} & \boldsymbol{I} \\ \boldsymbol{H}_{3,1} & \boldsymbol{H}_{3,3} & \cdots & \boldsymbol{H}_{3,k_b} & \boldsymbol{I} & \boldsymbol{0} & \boldsymbol{I} \end{bmatrix} \cdot$$

$$[\boldsymbol{s}_1\ \ \boldsymbol{s}_2\ \ \cdots\ \ \boldsymbol{s}_{k_b}\ \ \boldsymbol{p}_1\ \ \boldsymbol{p}_2\ \ \boldsymbol{p}_3]^{\mathrm{T}} = \boldsymbol{0}\ . \quad (4)$$

Then, Eq.(4) can be expressed by the form of linear equations, which is shown as

$$\begin{cases} \boldsymbol{H}_{1,1}\cdot\boldsymbol{s}_1^{\mathrm{T}} + \boldsymbol{H}_{1,2}\cdot\boldsymbol{s}_2^{\mathrm{T}} + \cdots + \boldsymbol{H}_{1,k_b}\cdot\boldsymbol{s}_{k_b}^{\mathrm{T}} + \boldsymbol{X}_1\cdot\boldsymbol{p}_1^{\mathrm{T}} + \\ \boldsymbol{p}_2^{\mathrm{T}} = 0 \\ \boldsymbol{H}_{2,1}\cdot\boldsymbol{s}_1^{\mathrm{T}} + \boldsymbol{H}_{2,2}\cdot\boldsymbol{s}_2^{\mathrm{T}} + \cdots + \boldsymbol{H}_{2,k_b}\cdot\boldsymbol{s}_{k_b}^{\mathrm{T}} + \boldsymbol{X}_2\cdot\boldsymbol{p}_1^{\mathrm{T}} + \\ \boldsymbol{p}_2^{\mathrm{T}} + \boldsymbol{p}_3^{\mathrm{T}} = 0 \\ \boldsymbol{H}_{3,1}\cdot\boldsymbol{s}_1^{\mathrm{T}} + \boldsymbol{H}_{3,2}\cdot\boldsymbol{s}_2^{\mathrm{T}} + \cdots + \boldsymbol{H}_{3,k_b}\cdot\boldsymbol{s}_{k_b}^{\mathrm{T}} + \boldsymbol{p}_1^{\mathrm{T}} + \\ \boldsymbol{p}_3^{\mathrm{T}} = 0 \end{cases}, \quad (5)$$

where $\boldsymbol{X}_1=\boldsymbol{\Phi}_1+\boldsymbol{\Phi}_2$ and $\boldsymbol{X}_2=\boldsymbol{\Phi}_3+\boldsymbol{\Phi}_4$.

Let $\boldsymbol{q}_1 = \sum_{j=1}^{k_b} \boldsymbol{H}_{1,j}\cdot\boldsymbol{s}_j^{\mathrm{T}}$, $\boldsymbol{q}_2 = \sum_{j=1}^{k_b} \boldsymbol{H}_{2,j}\cdot\boldsymbol{s}_j^{\mathrm{T}}$, and $\boldsymbol{q}_3 =$

$\sum_{j=1}^{k_b} \boldsymbol{H}_{3,j} \cdot \boldsymbol{s}_j^{\mathrm{T}}$. Eq.(5) can be simplified as

$$\begin{cases} \boldsymbol{q}_1 + \boldsymbol{X}_1 \cdot \boldsymbol{p}_1^{\mathrm{T}} + \boldsymbol{p}_2^{\mathrm{T}} = 0 \\ \boldsymbol{q}_2 + \boldsymbol{X}_2 \cdot \boldsymbol{p}_1^{\mathrm{T}} + \boldsymbol{p}_2^{\mathrm{T}} + \boldsymbol{p}_3^{\mathrm{T}} = 0 \\ \boldsymbol{q}_3 + \boldsymbol{p}_1^{\mathrm{T}} + \boldsymbol{p}_3^{\mathrm{T}} = 0 \end{cases} . \quad (6)$$

The vectors of the check code can be obtained by elimination method as

$$\boldsymbol{p}_1^{\mathrm{T}} = (\boldsymbol{X}_1 + \boldsymbol{X}_2 + \boldsymbol{I})^{-1} \cdot (\boldsymbol{q}_1 + \boldsymbol{q}_2 + \boldsymbol{q}_3) , \quad (7)$$

$$\boldsymbol{p}_2^{\mathrm{T}} = \boldsymbol{q}_1 + \boldsymbol{X}_1 \cdot \boldsymbol{p}_1^{\mathrm{T}} , \quad (8)$$

$$\boldsymbol{p}_3^{\mathrm{T}} = \boldsymbol{q}_3 + \boldsymbol{p}_1^{\mathrm{T}} . \quad (9)$$

Eqs.(7)—(9) are the fast iterative encoding algorithm for the proposed type-II QC-LDPC codes in this paper. If the information code vector and the parity check matrix are given, we can obtain the code vector $\boldsymbol{c}=[\boldsymbol{s}_1 \ \boldsymbol{s}_2 \ \dots \boldsymbol{s}_{k_b} \ \boldsymbol{p}_1 \ \boldsymbol{p}_2 \ \boldsymbol{p}_3]$ by Eqs.(7)—(9).

Encoding complexity analysis is mainly concerned with the amount of computation, computational complexity and the required storage for parameters in the encoding process. The amount of computation refers to the calculation amount of multiplication and addition, and the computational complexity refers to the relation between the amount of computation and the code length. Due to all the sub-matrices in fast iterative encoding algorithm of the proposed type-II QC-LDPC codes in this paper are sparse matrices, computing in accordance with sparse matrix pattern can greatly reduce the amount of computation. Tab.2 shows the exact values of the computation of Eqs.(7)—(9).

Tab.2 The computation amount of the fast encoding algorithm for type-II QC-LDPC codes

	The calculation amount of multiplication	The calculation amount of addition
$\boldsymbol{P}_1$	$3Rn/p$	$3Rn+2p^2-p$
$\boldsymbol{P}_2$	$Rn+p$	Rn
$\boldsymbol{P}_3$	Rn	Rn

It is clear from Tab.2 that the computational complexity of calculating parity check code vector $\boldsymbol{P}$ is $O(n)$, namely, computational complexity is linearly proportional to code length, because this encoding algorithm of LDPC codes has the advantages of sparse matrix and iteration. However, the traditional encoding algorithm of QC-LDPC codes is indirectly achieved by parity check matrix $\boldsymbol{H}$, that is, the parity check matrix $\boldsymbol{H}$ is transformed into the generating matrix $\boldsymbol{G}$ firstly, then encoding is achieved by generating matrix $\boldsymbol{G}$. And the computational complexity is $O(n^2)$, namely it is linearly proportional to the square of the code length. Thus, compared with the traditional encoding algorithm used by Refs.[4] and [9], the fast encoding algorithm in this paper can greatly reduce the computational complexity of encoding when the code length is large. In terms of the storage, since the quasi-cyclic extension method is adopted for the design of the presented type-II QC-LDPC codes in this paper, and the parity check matrix $\boldsymbol{H}$ can be determined by the corresponding shift matrix $\boldsymbol{S}(\boldsymbol{H})$, the storage amount is less because the elements in the shift matrix $\boldsymbol{S}(\boldsymbol{H})$ are only stored. So it is concluded that the fast encoding algorithm in this paper can effectively reduce the encoding complexity.

Two examples are given to illustrate and analyze the performance of the proposed regular type-II CDS-QC-LDPC codes. Binary phase shift keying (BPSK) modulation over an AWGN channel is assumed. The SPA is used for decoding, and the maximum iteration times of is set as 50. Regular type-II QC-LDPC codes[9] constructed by the construction method based on CDS and type-I QC-LDPC codes[4] constructed by the construction method based on arithmetic progression sequence (APS) are included for comparison.

Example 1: Considering a (183, 14, 1)-perpect CDS D={1, 2, 4, 25, 42, 53, 58, 67, 71, 97, 103, 150, 165, 177}, and let $p=v=183$, $k_b=3$, then a 3×6 weight configuration matrix $\boldsymbol{A}_{wt}$ is obtained by Eq.(3), which is shown as

$$\boldsymbol{A}_{wt} = \left[\begin{array}{ccc|ccc} 2 & 2 & 1 & 2 & 1 & 0 \\ 2 & 0 & 2 & 2 & 1 & 1 \\ 1 & 2 & 1 & 1 & 0 & 1 \end{array}\right] . \quad (10)$$

According to the (183, 14, 1)-perfect CDS and configuration matrix $\boldsymbol{A}_{wt}$ in Eq.(10), we can obtain a shift matrix $\boldsymbol{S}(\boldsymbol{H})$, and the null space of parity check matrix $\boldsymbol{H}$ obtained by extending this $\boldsymbol{S}(\boldsymbol{H})$ defines a type-II irregular QC-LDPC(1 098, 549) code with the code rate of 0.5. The simulation results are shown in Fig.1. It is easily seen from Fig.1 that at the bit error rate (*BER*) of 10^{-6}, the net coding gain (*NCG*) of the proposed type-II irregular QC-LDPC (1 098, 549) code with the code rate of 0.5 in this paper is respectively improved by 0.42 dB and 0.68 dB than those of the type-II regular CDS QC-LDPC(1 092, 546) code in Ref.[9] and the type-I APS-QC-LDPC (1 096, 548) code in Ref.[4]. In addition, *BER* of the proposed type-II irregular QC-LDPC(1 098, 549) code can reach 10^{-7} at the signal-to-noise ratio (*SNR*) of 2.8 dB, which shows that the proposed code has excellent decoding convergence properties, and there is no occurrence of the error floor at *BER* down to 10^{-7}.

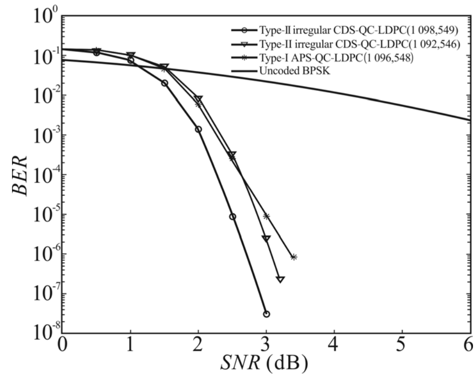

Fig.1 The comparison of the error correction performance among the type-II irregular CDS QC-LDPC(1 098, 549) code and other codes with the code rate of 0.5

Example2: Considering a (553, 24, 1)-perfect CDS D={1, 2, 4, 18, 37, 43, 65, 94, 132, 150, 162, 194, 205, 215, 220, 228, 265, 274, 314, 401, 449, 453, 473, 480}, and let p=v=553, k_b=6, then a 3×9 weight configuration matrix $\boldsymbol{A}_{wt}$ is obtained according to Eq.(3), which is shown as

$$\boldsymbol{A}_{wt}=\begin{bmatrix}2&2&1&2&2&0&2&1&0\\2&0&2&0&0&2&2&1&1\\1&2&1&2&2&1&1&0&1\end{bmatrix}. \quad (11)$$

According to the (553, 24, 1)-perfect CDS and configuration matrix $\boldsymbol{A}_{wt}$ in Eq.(11), we can obtain a shift matrix $\boldsymbol{S}(\boldsymbol{H})$, and the null space of parity check matrix $\boldsymbol{H}$ obtained by extending this $\boldsymbol{S}(\boldsymbol{H})$ defines a type-II irregular QC-LDPC(4 977, 3 318) code with the code rate of 0.67. The simulation results are shown in Fig.2. Fig.2 shows that compared with the type-II regular CDS QC-LDPC(5 226, 3 486) code in Ref.[9] and the type-I APS-QC-LDPC (4 980, 33 208) code in Ref.[4], the *NCG* of type-II irregular QC-LDPC (4 977, 3 318) code with the code rate of 0.67 proposed in this paper is improved by 0.38 dB and 0.28 dB at *BER* of 10^{-6}, respectively. Furthermore, there is no error floor phenomenon when *BER* is close to 10^{-7}.

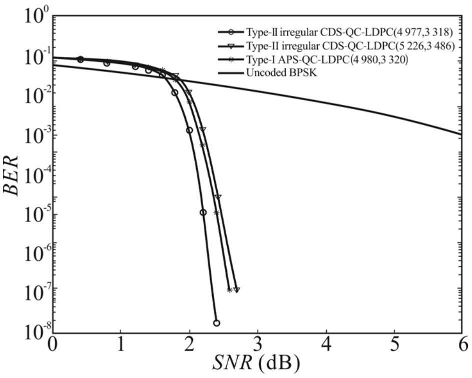

Fig.2 The comparison of the error correction performance between the Type-II irregular CDS QC-LDPC (4 977,3 318) code and other codes with the code rate of 0.67

The new irregular type-II QC-LDPC codes with the fast encoding based on perfect CDS are proposed in this paper. The Tanner graphs of these type-II QC-LDPC codes have no girth-4, and they can achieve the fast encoding by directly using the parity check matrices with the quasi-dual diagonal structure, so it has the lower encoding complexity. Simulation results show that the new type-II QC-LDPC codes have the more excellent error-correction performance and no occurrence of the error floor at *BER* of 10^{-7}. Under the same conditions, the new irregular type-II CDS-QC-LDPC codes can perform better in comparison with the type-II irregular CDS-QC-LDPC code in Ref.[9] and type-I APS-QC-LDPC code in Ref.[4].

References

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

[2] R Smarandache and P O Vontobel, On Regular Quasi-Cyclic LDPC Codes from Binomials, IEEE International Symposium on Information Theory, 274 (2004).

[3] Zhang G H, Sun R and Wang X M, IEEE Communications Letters **17**, 369 (2013).

[4] Zhang Y and Da X, Electronics Letters **51**, 1257 (2015).

[5] Wang J, Zhang G, Zhou Q, Yang Y and Sun R, Explicit Constructions for Type-1 QC-LDPC Codes with Girth at Least Ten, IEEE Information Theory Workshop, 436 (2014).

[6] Lally K, Explicit Construction of Type-II QC-LDPC Codes with Girth at Least 6, IEEE International Symposium on Information Theory, 2371 (2007).

[7] O'Sullivan M E, IEEE Transactions on Information Theory **52**, 718 (2006).

[8] Smarandache R and Vontobel P O, IEEE Transactions on Information Theory **58**, 585 (2012).

[9] Zhang L, Li B and Cheng L, Chinese Journal of Electronics **24**, 146 (2015).

[10] Zhang G H, Electronics Letters **52**, 367 (2016).

[11] Richardson T J and Urbanke R L, IEEE Transactions on Information Theory **47**, 638 (2001).

[12] Johnson S J and Weller S R, IEEE Transactions on Communications **56**, 1201 (2008).

[13] Yuan Jian-guo, Zhou Guang-xiang, Gao Wen-chun, Wang Yong, Lin Jin-zhao and Pang Yu, Optoelectronics Letters **12**, 61 (2016).

[14] Peng L, Zhu G and Wu X, Acta Electronica Sinica **35**, 950 (2007). (in Chinese)

[15] YUAN Jian-guo, Liang Meng-qi, Wang Yong, Lin Jin-zhao and Pang Yu, Optoelectronics Letters **12**, 208 (2016).

[16] Esmaeili M and Javedankherad M, IEEE Transactions on Communications **60**, 3579 (2012).