An Efficient Method of Constructing Quasi-Cyclic Low-Density Parity-Check Codes

Zhanji Wu, Jiao Cheng School of Information and Telecommunications Beijing University of Posts and Telecommunications Beijing, China, 100876 Email: wuzhanji@bupt.edu.cn, wuzhanji@163.com

Abstract—An efficient method of constructing irregular quasicyclic (QC) low-density parity-check (LDPC) codes is proposed. In order to find the degree distribution with low convergence threshold, the extrinsic information transfer (EXIT) chart is utilized to optimize the degree distribution of LDPC codes. Then, a modified progressive edge growth (PEG) algorithm is used to get the mask matrix with the optimal degree distribution. Finally, the parity-check matrix of QC LDPC code is constructed based on the mask matrix, and the shift values are optimized to eliminate short cycles. Simulation results show that the constructed irregular QC LDPC codes with optimized degree distribution significantly outperform the regular QC LDPC codes in the additive white Gaussion noise (AWGN) channel.

Index Terms—low-density parity-check (LDPC) codes, quasicyclic (QC) LDPC, extrinsic information transfer (EXIT) chart, progressive edge growth (PEG) algorithm

I. Introduction

Low-density parity-check (LDPC) codes were discovered by Gallager in 1962 [1], which have attracted much attention because of its Shannon-limit-approaching performance. One low-complexity low-memory class of LDPC codes is the quasi-cyclic (QC) LDPC code with the simple cyclic-form parity-check matrix [2]. The encoding of a QC LDPC code can be achieved with simple shift-register operations, and the decoding can be done based on the circulant architecture in a parallel manner [3]. Some methods to construct QC LDPC codes were put forward in [4-5], and an algorithm to eliminate short cycles in QC LDPC codes was proposed in [6].

Because the degrees of the checks and variables affect the convergence behavior of the iterative decoder [7], it is important to design the QC LDPC code with good degree distribution. One approach to find the signal-to-noise-ratio (SNR) convergence threshold of iterative decoders is the extrinsic information transfer (EXIT) chart. The EXIT chart was discovered by Brink as an useful tool to analyze the convergence behavior of the iterative decoding [8]. The convergence behavior of the LDPC decoder was analyzed in [9]. In this paper, we investigate the SNR convergence thresholds predicted by EXIT charts, try to find the optimal degree distribution with the low SNR convergence threshold, and then construct the QC LDPC code with the optimal degree distribution.

The mask matrix of QC LDPC code can be made by the progressive edge growth (PEG) algorithm, which is accepted

as an effective algorithm to construct conventional random LDPC codes [10]. In order to construct the mask matrix with the optimal degree distribution, a modified PEG algorithm is proposed. Afterwards, the parity-check matrix of the QC LDPC code is constructed based on the mask matrix.

The rest of this paper is organized as follows. The degree distribution and the EXIT chart of LDPC codes are introduced in Section II. The degree distribution optimization algorithm of LDPC codes is presented in Section III. The modified PEG algorithm is proposed in section IV. The construction method of QC LDPC codes is put forward in section V. Simulation results and EXIT chart analysis are given in Section VI. Finally, the conclusion is reached in section VII.

II. BACKGROUND

In this section, a few basic concepts needed in the next sections are briefly introduced, such as the degree distribution and node distribution of LDPC codes, and the EXIT chart analysis of LDPC codes on the quadrature phase shift keying (OPSK) modulation.

A. Degree Distribution and Node Distribution

The LDPC code is a linear code defined by a sparse parity-check matrix H of size $M \times N$. The degree distribution can be expressed as (λ_i, ρ_j) , where λ_i and ρ_j denote the fraction of edges connected to variable-nodes of degree-i and check-nodes of degree-j in the tanner graph, respectively. The parameters must satisfy the following constraints:

$$0 \le \lambda_i \le 1, i \ge 1$$

$$0 \le \rho_j \le 1, j \ge 1$$

$$\sum_{i=1}^{\infty} \lambda_i = 1$$

$$\sum_{i=1}^{\infty} \rho_j = 1$$
(1)

The node distribution of LDPC code is denoted as (n_i, m_j) , where n_i is the variable-node number of degree-i, m_j is the check-node number of degree-j. The relationship between (λ_i, ρ_j) and (n_i, m_j) is shown as:

$$\lambda_i = \frac{i \times n_i}{\sum_i i \times n_i} \tag{2}$$

$$\rho_j = \frac{j \times m_j}{\sum_j j \times m_j} \tag{3}$$

Moreover, the following linear constraint must be satisfied for a degree distribution in order to be compatible with the given code rate R:

$$\sum_{j=1}^{\infty} \frac{\rho_j}{j} = (1 - R) \sum_{i=1}^{\infty} \frac{\lambda_i}{i}$$
 (4)

Variable-node distribution must fulfill

$$\sum_{i} n_i = N \tag{5}$$

With (2) and (5), the variable-node distribution is:

$$n_i = \frac{N}{1 + \sum_{i \mid i} \frac{i \times \lambda_j}{j \times \lambda_i}} \tag{6}$$

where $j \setminus i$ means j takes values except i.

In the similar way, we can get the check-node distribution:

$$m_j = \frac{M}{1 + \sum_{i \setminus j} \frac{j \times \rho_i}{i \times \rho_j}} \tag{7}$$

Equation (6) and (7) will turn out to be useful in the next section.

B. EXIT Charts of LDPC Codes

The EXIT chart is used to analyze the convergence behavior of the iterative decoding of concatenated codes [8]. By treating the LDPC decoder as the concatenation of the variable-node detectors (VND) and check-node detectors (CND), the convergence behavior of the decoder can be analyzed [9]. The iterative decoding scheme of LDPC code is shown in Fig. 1, where z_k is the soft information sequence received from the additive white Gaussian noise (AWGN) channel, which is supposed to be the Gaussian distribution with zero mean and the variance σ_z^2 .

For each iteration, the extrinsic information is exchanged between variable-nodes and check-nodes. To measure the information, the mutual information $I_A = I(X;A)$ between transmitted systematic bits X and the extrinsic information A is used, as well as the mutual information $I_B = I(X;B)$. In [9], some formulas are given for the computation of VND and CND mutual information on the basis of the Gaussian assumption as follows:

$$I_A = T_1(I_B, \frac{E_b}{N_0})$$

$$= \sum_i \lambda_i J(\sqrt{(i-1)[J^{-1}(I_B)]^2 + \sigma_z^2})$$
(8)

$$I_B = T_2(I_A) = 1 - \sum_j \rho_j J(\sqrt{(j-1)[J^{-1}(1-I_A)]^2})$$
 (9)

For the AWGN channel with the QPSK modulation:

$$\sigma_z^2 = 8R \cdot \frac{E_b}{N_0} \tag{10}$$

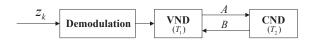


Fig. 1. Iterative decoding model of LDPC codes

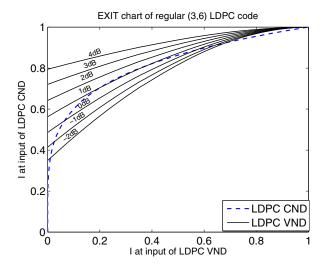


Fig. 2. The EXIT chart of regular (3,6) LDPC code at different E_b/N_0

where E_b/N_0 is the SNR per information bit, and R is the code rate.

 $J(\cdot)$ is a function defined as follows:

$$J(\sigma) = 1 - \int_{-\infty}^{+\infty} \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(\xi - \sigma^2/2)^2}{2\sigma^2}} \cdot \log_2(1 + e^{-\xi}) d\xi$$
 (11)

The EXIT chart of LDPC codes includes two curves: $I_A(I)$ and $I_B^{-1}(I)$, with the mutual information at input of variable-nodes on the abscissa, the mutual information at input of check-nodes on the ordinate. $I_A(I)$ and $I_B^{-1}(I)$ can be drew based on (8) and (9), respectively. Fig. 2 shows the EXIT curves of regular (3,6) LDPC code at different E_b/N_0 from -2dB to 4dB. The cluster of solid lines around the check-node EXIT curve are the variable-node EXIT curves at different E_b/N_0 , which can be obviously observed that the EXIT curve of variable-node ascends gradually as the E_b/N_0 increases. Thus, we can come to the conclusion that $I_A = T_1(I_B, E_b/N_0)$ is an increasing function of E_b/N_0 , while $I_B = T_2(I_A)$ is independent of it.

III. DEGREE DISTRIBUTION OPTIMIZATION ALGORITHM

The decoding process of LDPC codes can be represented as a recursive update of the mutual information I_A and I_B in the EXIT chart. If the mutual information converges to 1, the bit error rate (BER) will converge to zero. For LDPC codes with a given particular SNR, if the EXIT curve $I_A(I)$ is above the EXIT curve $I_B^{-1}(I)$, the tunnel between the two EXIT curves is open (just as shown in Fig. 2), and the convergence of the decoder can be obtained. Thus, the SNR which makes the two EXIT curves tangent is the SNR convergence threshold of the LDPC code. The actual goal of degree distribution

optimization is to find the degree distribution with the lowest SNR convergence threshold.

In order to find the SNR convergence threshold for a given degree distribution, we define a function representative of the tunnel closure:

$$f(\lambda, \rho, E_b/N_0) = \min_{I \in [0,1]} \left\{ I_A(I) - I_B^{-1}(I) \right\}$$
 (12)

When $f(\lambda, \rho, E_b/N_0) > 0$, the tunnel is open, and when $f(\lambda, \rho, E_b/N_0) \leq 0$, the tunnel is closed.

As mentioned above, for a fixed degree distribution (λ, ρ) , increasing the SNR raises the EXIT curve $I_A(I)$, while the EXIT curve $I_B^{-1}(I)$ is always fixed. Thus, when $f(\lambda, \rho, E_b/N_0) > 0$, we can make the degree distribution unchanged and decrease the SNR until $f(\lambda, \rho, E_b/N_0) < 0$, and this smallest SNR is the SNR convergence threshold of the degree distribution (λ, ρ) .

The steps of the proposed optimization algorithm are summarized as follows:

1: Initialization.

Start with a given valid degree distribution (λ, ρ) and an initial SNR E_b/N_0 for a given code rate R. The initial SNR E_b/N_0 is big enough so as to satisfy $f(\lambda, \rho, E_b/N_0) > 0$.

2: Get the convergence threshold of the degree distribution (λ, ρ) .

Calculate the value of $f(\lambda, \rho, E_b/N_0)$. If $f(\lambda, \rho, E_b/N_0) > 0$, decrease E_b/N_0 gradually until $f(\lambda, \rho, E_b/N_0) \leq 0$, then the smallest E_b/N_0 is the SNR convergence threshold of the degree distribution (λ, ρ) .

3: Optimize the degree distribution.

Repeatedly add a Gaussian increment to (λ,ρ) and normalize them until the new degree distribution (λ',ρ') satisfies all inequalities in (1). If the code rate (express as R') of the degree distribution (λ',ρ') , which can be calculated according to (4), is unequal to R, return to step 3 until the degree distribution (λ',ρ') which satisfies R'=R is found.

4: Calculate $f(\lambda', \rho', E_b/N_0)$.

If $f(\lambda', \rho', E_b/N_0) > 0$, substitute (λ, ρ) by (λ', ρ') and return to step 2, otherwise return to step 3. For every E_b/N_0 , if the number of the skips from step 4 to step 3 is bigger than iterNum, then skips to step 5.

5: The degree distribution optimization is stopped. The current (λ,ρ) is the optimal degree distribution, and the current E_b/N_0 is the SNR convergence threshold.

IV. Modified PEG Algorithm

The original PEG algorithm starts with a given variable-node distribution, and builds up a tanner graph on an edge-by-edge basis with a girth as large as possible [10]. For a given variable-node s_k , define its neighbor within depth l, $N_{s_k}^l$, as the set consisting of all check-nodes reached by a tree spreading from variable-node s_k within depth l. Its complementary set $\overline{N_{s_k}^l}$ is defined as the set containing check-nodes don't belong to $N_{s_k}^l$. During the spreading procedure of the tree, when all the check-nodes have been reached by s_k , an edge between s_k and a check-node selected from $\overline{N_{s_k}^l}$ can

be placed. Due to the selected check-node is the one having the smallest number of check-node degree in $\overline{N_{s_k}^l}$, the check-node degree distribution of the parity-check matrix trends to be uniform.

In other words, the parity-check matrix made by the original PEG algorithm can only satisfy the degree distribution of variable-nodes, while the degree distribution of check-nodes can't be satisfied. The purpose of the modified PEG algorithm is to construct the parity-check matrix which can not only satisfy the given variable-node degree distribution, but also the check-node degree distribution.

The modified PEG algorithm starts with the given degree distribution (λ_i, ρ_j) , the variable-node distribution n_i and the check-node distribution m_j can be obtained according to the equations (6) and (7). In order to construct codes under the strict variable-node and check-node degree distribution, we propose the free check-node degree instead of the check-node degree in the edge selection procedure. Define $d(c_r)$ as the current degree, $d_{max}(c_r)$ as the maximum degree, $d_{free}(c_r)$ as the available degree, thus,

$$d_{free}(c_r) + d(c_r) = d_{max}(c_r) \tag{13}$$

In the initialization of the modified PEG algorithm, order the variable-node degree sequences based on the variable-node distribution, randomly choose the maximum check-node degree sequences $d_{max}(c_r)$ for all r according to the check-node distribution, and set $d_{free}(c_r)=d_{max}(c_r)$. During the PEG procedure, place an edge between s_k and the check-node selected from $\overline{N_{s_k}^l}$ which has the maximum $d_{free}(c_r)$, and then set $d_{free}(c_r)=d_{free}(c_r)-1$, $d(c_r)=d(c_r)+1$. However, even if we choose check-nodes through above method, it still often happens that all check-nodes in the set $\overline{N_{s_k}^l}$ have zero free degrees, that is to say, $d_{free}(c_r)=0$. In this case, the maximum check-node degree exchange procedure can be implemented [11]. The main idea is to find a candidate check-node c_r^* with a positive free degree from the set $N_{s_k}^l$ which satisfies:

$$d_{max}(c_r^*) > d_{max}(c_r) = d(c_r) \ge d(c_r^*)$$
 (14)

Thus, if we exchange the maximum check-node degree of c_r and c_r^* , the following functions will be satisfied:

$$d_{free}(c_r) = d_{max}(c_r^*) - d(c_r) > 0,$$

$$d_{free}(c_r^*) = d_{max}(c_r) - d(c_r^*) \ge 0$$
(15)

After the maximum check-node degree exchange procedure, we can choose the check-node c_r from the set $\overline{N_{s_k}^l}$.

Because the check-node degree is not consecutive at the most cases, it is very likely that there are no candidate check-nodes to be found even after the maximum check-node degree exchange procedure in the bottom set. In this case, such maximum check-node degree exchange procedure can be carried out from the upper set $N_{s_k}^{l-1}$ to the top set $N_{s_k}^1$ of the PEG tree until all the edges of variable-node s_k are placed.

In a word, as compared with the original PEG algorithm, the maximum check-node degree exchange procedure is proposed

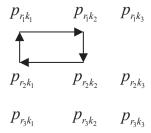


Fig. 3. Girth-4 loop in QC LDPC code basic matrix

to search the available check-nodes from the bottom to the top of the PEG tree, which can satisfy any given variable-node and check-node degree distribution.

V. CONSTRUCTION OF QC LDPC CODE

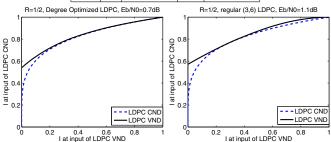
In this section, we propose a generalized construction method of the QC LDPC code with the optimal degree distribution.

The parity-check matrix H of the QC LDPC codes can be characterized with two small matrices, H_m and H_b . The matrix H_m of size $g \times t$ is called the mask matrix, and the matrix H_b of size $g \times t$ is called the basic matrix, just as shown in (16). If a parity-check matrix of size $M \times N$ is required to be constructed with the circulant sub-matrices of size $f \times f$, the parameters g and t can be computed according to the expressing g = M/f and t = N/f.

$$H_{b} = \begin{bmatrix} p_{00} & \cdots & p_{0k} & \cdots & p_{0(t-1)} \\ \vdots & & \vdots & & \vdots \\ p_{r0} & \cdots & p_{rk} & \cdots & p_{r(t-1)} \\ \vdots & & \vdots & & \vdots \\ p_{(g-1)0} & \cdots & p_{(g-1)k} & \cdots & p_{(g-1)(t-1)} \end{bmatrix}$$
(16)

Firstly, for a given code rate R = (N - M)/N, the optimal check-node and variable-node degree distribution can be found by the proposed degree optimization algorithm based on the EXIT chart analysis. Secondly, the mask matrix H_m with the optimal degree distribution can be constructed by the modified PEG algorithm. In the tanner graph with t variable-nodes and g check-nodes made by modified PEG algorithm, if there is an edge between variable-node s_k ($0 \le k < t$) and checknode c_r (0 $\leq r < g$), the element in the rth row and kth column of the mask matrix H_m is "1", otherwise it is "0". If the QC parity-check matrix H is constructed by replacing each element "0" in mask matrix H_m with a full-zero matrix of size $f \times f$, and each element "1" in mask matrix H_m with a cyclic-shift identity matrix of size $f \times f$, then the degree distribution of the parity-check matrix H is the same with that of the mask matrix H_m . Each element p_{rk} $(0 \le p_{rk} < f)$ in the basic matrix H_b represents the right cyclic shift times of the identity matrix in the parity-check matrix H, while each element p_{rk} =-1 in H_b represents a full-zero sub-matrix in the parity-check matrix H.

R	i	λ_i	j	$ ho_j$
1/2	2	0.383562	6	0.904110
	3	0.205479	7	0.095890
	6	0.410959		
3/4	2	0.270270	12	0.648649
	3	0.081081	13	0.351351
	4	0.648649		



(a) EXIT chart of degree optimized (b) EXIT chart of regular (3,6) LDPC LDPC code at $E_b/N_0=0.7 {\rm dB}$ code at $E_b/N_0=1.1 {\rm dB}$

Fig. 4. EXIT charts of code rate 1/2

The shift values p_{rk} are very important to the performance of the QC LDPC code. The short cycles in the QC LDPC code can be eliminated if the p_{rk} s are set reasonably. Thus, we also propose a method to get rid of the girth-4 cycles in the parity-check matrix as follows [12]:

Define all vertex shift values in the girth-4 loop in the basic matrix H_b unequal to "-1" as $p_{r_1k_1}$, $p_{r_1k_2}$, $p_{r_2k_1}$, $p_{r_2k_2}$, respectively, just as shown in Fig. 3, and

$$d = p_{r_1k_1} - p_{r_1k_2} + p_{r_2k_2} - p_{r_2k_1}$$
 (17)

W is an integer set defined as follows:

$$W = \{d|2 < |d| < f - 2\} \cup$$

$$\{d|f + 2 \le |d| \le 2f - 2\} \cup$$

$$\{d|2f - 1 < |d| < 2f\}$$

$$(18)$$

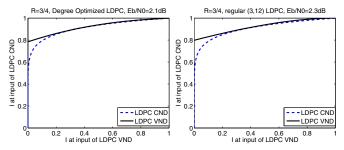
if $d \in W$, then there are no girth-4 cycles in the parity-check matrix. After the basic matrix is constructed, search all girth-4 loops in the basic matrix H_b , if $d \notin W$, change one vertex shift value to make the new $d \in W$, repeat the above procedure until all girth-4 loops in H_b satisfy $d \in W$. Thus, all girth-4 cycles in the parity-check matrix H will be eliminated.

VI. SIMULATION RESULTS

Using the degree distribution optimization algorithm, the optimal degree distributions of code rate 1/2 and 3/4 are shown in Table I.

The EXIT charts of the optimized LDPC code and that of the regular LDPC code for the code rate 1/2 and 3/4 are shown in Fig. 4 and Fig. 5, respectively.

In Fig. 4, for the code rate 1/2, the convergence threshold SNR of the regular (3,6) LDPC code and that of the optimized LDPC code are 1.1dB and 0.7dB, respectively. In Fig. 5, for the code rate 3/4, the corresponding SNRs are 2.3dB and



(a) EXIT chart of degree optimized (b) EXIT chart of regular (3,12) LD-LDPC code at $E_b/N_0=2.1 {\rm dB}$ PC code at $E_b/N_0=2.3 {\rm dB}$

Fig. 5. EXIT charts of code rate 3/4

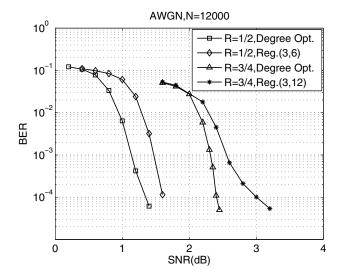


Fig. 6. BER performances of the regular and optimized LDPC codes

2.1dB, respectively. Thus, for both cases, the convergence threshold of the optimized LDPC code is lower than that of the regular LDPC code.

In order to verify the performance of the proposed QC LDPC code, we construct the mask matrices of code rate 1/2 and 3/4 with the size of 12×24 and 6×24 , respectively. The size of the circulant sub-matrices of QC LDPC code are both 500×500 and the shortest girth is 6. The degree distributions of these QC LDPC codes are shown in Table I. For the sake of comparison, we also construct the regular (3,6) and the regular (3,12) QC LDPC codes with the same size and shortest girth for the code rate 1/2 and 3/4, respectively. Computer simulations are carried out on the AWGN channel and the QPSK modulation, as shown in Fig. 6. The belief propagation (BP) LDPC decoding algorithm with maximum iterative number 50 is utilized.

In Fig. 6, the optimized rate-1/2 LDPC code obtains more than 0.33dB SNR gain than the regular (3,6) LDPC code, and the optimized rate-3/4 LDPC code achieves more than 0.5dB gain as compared with the regular (3,12) LDPC code. Hence, simulation results coincide with the analysis of EXIT charts.

VII. CONCLUSION

An efficient method of constructing irregular QC LDPC codes is proposed. Firstly, the degree optimization algorithm

based on EXIT charts is put forward in order to find the optimal degree distribution with the lowest SNR convergence threshold for a given code rate. Then, the modified maximumcheck-degree-swap PEG algorithm is used to construct the mask matrix with the optimal degree distribution. Finally, the parity-check matrix of QC LDPC code is constructed based on the mask matrix, and the shift values are optimized in order to eliminate short cycles. Simulation results turn out that the proposed irregular QC LDPC codes significantly outperform the conventional regular QC LDPC codes in the AWGN channel, which also coincide with our analysis of EXIT charts. Thanks to the QC feature, the proposed QC LDPC codes are low-complexity and low-memory, which is easy to implement for the channel encoding and decoding. In a word, the proposed irregular QC LDPC codes are simple and efficient.

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China (Grant No.61171101) and National Great Science Specific Project of China (Grant No. 2009ZX03003-011-03).

REFERENCES

- R. G. Gallager, "Low-density parity-check codes," *IEEE Trans.Inform. Theory*, vol.IT-8, pp, 21-28, Jan. 1962
- [2] S. Lin, L. Chen, J Xu, I Djurdjevic, "Near Shannon limit quasi-cyclic low-density parity-check codes," *IEEE Global Telecommunications Con*ference, vol.4, pp, 2030-2035, Dec. 2003
- [3] Z. W. Li, L. Chen, L. Q. Zeng, S. Lin, and et al, "Efficent encoding of quasi-cyclic low-density parity-check codes," *IEEE Trans. Commun*, vol.54, pp, 71-81, Jan. 2006
- [4] Y. K. Lin, C. L. Chen, Y. C. Liao, and et al, "Structured LDPC codes with low error floor based on PEG tanner graphs," *ISCAS 2008*, Washington, USA, pp, 1846-1849, May. 2008
- [5] Z. W. Li, B. V. K. V. Kumar, "A class of good quasi-cyclic low-density parity check codes based on progressive edge growth graph," *The 38th ACSSC*, Monterey, California, vol. 2, pp, 1990-1994, Nov. 2004
- [6] J. Lei, J. H. Wang, C. J. Tang, "Quasi-cyclic extension based on PEG algorithm for construction of LDPC codes," *Journal on Communications*, vol. 29, no. 9, pp, 103-110, Nov. 2008
- [7] T. Richardson, A. Shokrollahi, R. Urbanke, "Design of capacity approaching irregular low-density parity-check codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 2, pp, 619-637, Feb. 2001
- [8] S. T. Brink, "Convergence behavior of iteratively decoded parallel concatenated codes," *IEEE Trans. Inform. Theory*, vol. 49, no. 10, pp, 1727-1737, Oct. 2001
- [9] S. T. Brink, G. Kramer, A. Ashikhmin, "Design of low-density parity-check codes for modulation and detection," *IEEE Trans. Commun.*, vol. 52, no. 4, pp, 670-678, Apr. 2004
- [10] X. Y. Xiao, E. Eleftheriou, D. M. Arnold, "Regular and irregular progressive edge-growth tanner graphs," *IEEE Trans. Inform. Theory*, vol. 51, no. 1, pp, 386-398, Jan. 2005
- [11] H. Chen, Z. G. Cao, "A modified PEG algorithm for construction of LDPC codes with strictly concentrated check-node degree distributions," *IEEE Wireless Communications and Networking Conference*, pp, 565-569, Jun. 2007
- [12] T. T. Fu, Z. J. Wu, W. B. Wang, "PEG-based construction method for quasi-cyclic LDPC," *Journal of data acquisition and processing*, vol. 24, no. S, pp, 182-186, Oct. 2009