Journal of Computer and Communications, 2016, 4, 39-49
http://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Half Rate Quasi Cyclic Low Density Parity Check Codes Based on Combinatorial Designs

Sina Vafi, Narges Rezvani Majid

School of Engineering and Information Technology, Charles Darwin University, Darwin, Australia
Email: sina.vafi@cdu.edu.au, narges.rezvanimajid@cdu.edu.au

How to cite this paper: Vafi, S. and Majid, N.R. (2016) Half Rate Quasi Cyclic Low Density Parity Check Codes Based on Combinatorial Designs. *Journal of Computer and Communications*, **4**, 39-49.
http://dx.doi.org/10.4236/jcc.2016.412002

Received: August 15, 2016
Accepted: October 15, 2016
Published: October 18, 2016

Copyright © 2016 by authors and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/
Open Access

Abstract

This paper presents new half rate Quasi Cyclic Low Density Parity Check (QC-LDPC) codes formed on the basis of combinatorial designs. In these codes, circulant matrices of the parity check matrix are formed on the basis of subsets in which the difference between any two elements of a subset is unique with all differences obtained from the same or different subsets. This structure of circulant matrices guarantees non-existence of cycle-4 in the Tanner graph of QC-LDPC codes. First, an irregular code with girth 6 constituted by two rows of circulant matrices is proposed. Then, more criteria will be considered on the structure of subsets with the mentioned feature aiming to represent a new scheme of regular QC-LPDC codes with girth at least 8. From simulations, it is confirmed that codes have similar to or better performance than other well-known half rate codes, while require lower complexity in their design.

Keywords

Quasi-Cyclic LDPC Codes, Combinatorial Designs, Circulant Matrix

1. Introduction

Quasi-Cyclic Low Density Parity Check (QC-LDPC) codes are represented as reputable structured-type LDPC codes, which are considered in the current and next generations of broadband transmission and storage systems [1] [2]. This is mainly because of their high error correcting performance in different channels, low-complex encoding and parallel iterative decoding conducted on the constituted circulant matrices. QC-LDPC codes are conventionally implemented as high rate and long length codes, while short cycles (in particular cycle-4) are prohibited in structure of their parity check matrix[1]. On the other hand, half rate of these codes with girth 6 and short lengths has been in-

[1] In this letter, codes with rates greater than half and length greater than 1000 are categorized as high rate and long-length codes.

terested in some applications such as multirate transmission systems affected by fading phenomenon [3]. For short to medium block length codes, an algorithm was proposed, which removes harmful structures of the code's graph and improves the performance at the medium to high signal to noise ratios. Indeed, this improvement provides a lower error floor for the code.

It is also possible to have half rate of QC-LDPC codes with girth greater than 6 to produce the error floor at lower bit error rates (BERs). These codes are initially designed as a regular code with girth 6 based on approximate cycle extrinsic message degree (ACE) algorithm [4] or arithmetic progression (AP) sequence [5]. Then, a masking technique is accomplished on their parity check matrix to prohibit existence of cycle-6 and form an irregular code with girth at least 8. QC-LDPC codes can be implemented based on progressive edge growth algorithm (PEG). In PEG algorithm, check nodes are formed so as to produce the maximum distance possible from the considered variable code [6]. This structure will lead to construct cycles with the long length and consequently provides a code with the high girth. Error correcting capability of these codes can be improved by selecting those edges that provide the best performance for its iterative decoder [7].

Alternatively, half-rate QC-LDPC codes with the high performance are constructed based on circulant permutation matrices (CPMs). In one method, CPMs with an arbitrary column and row weights are designed based on greatest common divisor (GCD) concept. In addition, a proper masking technique is applied to construct a code with girth at least 8 [8]. A modification on the GCD-based structure of CPMS was proposed aiming to reduce the encoding complexity. In this case, information part of parity check matrix is only formed by the greatest common divisor concept [9]. A criterion is defined for construction of this part of the parity check matrix to prohibit existence of cycles 4 and 6. Then, a quasi-diagonal structure is applied on the parity check matrix to maintain girth 8 for the code. Similarly, a suitable masking technique is applied to increase girth of the code.

CPM-based parity check matrix of QC-LDPC codes is possibly formed by combination of finite fields and combinatorial designs. In this case, circulant matrices are obtained by combination of two arbitrary subsets of elements from a defined field. Finally, an appropriate masking technique is applied on the obtained CPM-based matrix to construct QC-LDPC codes with girth 8 or higher [10].

QC-LDPC codes can also be designed on the basis of cyclic difference sets (CDF) in which every specific number of elements defined in the subsets of a group occurs only once [11] [12]. Subsets with this feature conventionally define constituent circulant matrices of the parity check matrix with the girth 6. Despite CDF, it is not necessary to have difference of elements in a subset as an element of the subsets. This simplifies formation of subsets and consequently provides more flexibility in design of codes. Recently, new QC-LDPC codes with girth 6 and rates greater than half were proposed by difference sets concept [13]. In this method, the elements of the first subset are optionally selected so as the difference between any two elements is unique. Then, elements of other subsets are determined based on elements of the first subset, while the difference between any two elements of a subset is also unique. This guarantees non-existence of cycle-4 in Tanner graph of the code. Codes implemented by this technique demonstrate high error correcting performance so as they are compared by QC-LDPC codes with girth 8.

In this letter, we apply concept of difference sets in constructing two new schemes of QC-LDPC codes. Despite the method presented in [13], codes have half rate and subsets are defined by unequal lengths. Based on this feature of circulant matrices, an irregular QC-LDPC code with girth 6 is proposed. Subsets defined with the abovementioned structure will also apply to represent a regular QC-LDPC code with girth 8. For the regular code, instead of utilizing a masking technique, circulant matrices are interactively designed with each other to prohibit existence of cycles with lengths 4 and 6 in the Tanner graph of the parity check matrix. Simulation results express that the newly proposed codes have low error floors. In addition, these demonstrate performances similar to or better than other well-known half-rate QC-LDPC codes, while a lower complexity in their design is applied.

The rest of paper is organised as follows: Section 2 explains how subsets with unique differences between their elements are formed. Section 3 presents structure of an irregular QC-LDPC code based on subsets defined in section 2. Moreover, it explains how subsets with different lengths are applied to form a regular QC-LDPC code with column weight 3 and girth 8. Section 4 gives simulation results of the newly designed codes and compares their performance with half-rate QC-LDPC codes constructed by other methods and masking techniques. Finally, Section 5 summarises the paper and gives suggestions for the further work.

2. Subsets with Different Lengths and Unique Differences between Elements

For given $n,t \in \mathbb{N}$, we define sets $S_i \subset \mathbb{N} \cup \{0\}$, $1 \le i \le n$, by strictly increasing sequences $\{\alpha_{i,j}\}_{1\le j\le t}$, which satisfy the following conditions:

1) $\alpha_{1,1} = 0$ and for every $1 \le j, j', k, k' \le t$ we have

$$\alpha_{1,j} - \alpha_{1,k} \ne \alpha_{1,j'} - \alpha_{1,k'} \tag{1}$$

where $(j,k) \ne (j',k')$, $j > k$ and $j' > k'$.

2) For $2 \le i \le n$, $\alpha_{i,1} = 0$ and there exist $p \in \mathbb{N} \setminus \{1\}$ and $r \in \mathbb{Z} \setminus \{0\}$ with $p > r$ such that

$$\alpha_{i,j} := p\alpha_{i-1,j} - r \tag{2}$$

for every $j \le 2 \le t$.

Based on this condition, non-zero elements of S_i, $2 \le i \le n$ can be directly determined from non-zero elements of S_1. The relationship between *j*th element of *i*th subset and its correspondence at subset S_1, is obtained by:

$$\alpha_{i,j} = p^{i-1}\alpha_{1,j} - \sum_{w=0}^{i-2} p^w \cdot r \tag{3}$$

where $p \in \mathbb{N} \setminus \{1\}$, $r \in \mathbb{Z} \setminus \{0\}$.

3) For every $1 \le j, j', k, k' \le t$, which $j > k$, $j' > k'$

$$\alpha_{i,j} - \alpha_{i,k} \ne \alpha_{i',j'} - \alpha_{i',k'}, \tag{4}$$

where $1 \le i, i' \le n$ and $i' \ne i$.

For the given $m \in \mathbb{N}$, we define sets $A_{i_1} \subset \mathbb{N} \cup \{0\}$, $1 \le i_1 \le m$, by $\{\beta_{i_1}\}$, where $\beta_1 \in \mathbb{Z}$ and there exist $q \in \mathbb{N} \setminus \{1\}$ and $d \in \mathbb{Z} \setminus \{0\}$ with $q > d$ such that

$$\beta_{i_1} := q\beta_{i_1 - 1} - d, \tag{5}$$

for all $2 \le i_1 \le m$.

For every $1 \le i \le n$, $1 \le i_1 \le m$ and $1 \le j, k \le t$, which $j > k$

$$\alpha_{i,j} - \alpha_{i,k} \ne \beta_{i_1}. \tag{6}$$

Based on the above constructions, there exists an additive group

$$\mathbb{Z}_\nu = \{0, 1, \cdots, \nu - 1\}, \tag{7}$$

such that for all $1 \le i \le n$, $1 \le i_1 \le m$ and $1 \le j, k \le t$, $j \ne k$, $(\alpha_{i,j} - \alpha_{i,k})_\nu$ and $(\pm\beta_{i_1})_\nu$ are repeated only once in this group and ν is the minimum value, which satisfies this property[2].

For example, let $S_1 = \{0, 3, 10\}$, $S_2 = \{0, 5, 19\}$, $S_3 = \{0, 9, 37\}$, $S_4 = \{20\}$ and $S_5 = \{17\}$ defined in $\mathbb{Z}_{41}$ $(\nu = 41)$. Non-zero elements of S_2 and S_3 can be obtained from (3), where $p = 2$ and $r = 1$. In this case, $\delta_{S_1} = \{3, 7, 10, 38, 34, 31\}$, $\delta_{S_2} = \{5, 14, 19, 36, 27, 22\}$, $\delta_{S_3} = \{9, 28, 37, 32, 13, 4\}$, $\delta_{S_4} = \{20, 21\}$ and $\delta_{S_5} = \{17, 24\}$ are sets of differences between elements of S_1, S_2, S_3, S_4 and S_5, respectively. It is concluded that difference between any two elements of a subset is unique with other differences obtained from the same or other subsets. Note that $\nu = 41$ is the minimum value that provides this condition for the given subsets.

3. Construction of Half Rate QC-LDPC Codes Based on Subsets with Different Lengths

In this section, two new schemes of half rate QC-LDPC codes are presented. In the first method, an irregular code with girth 6 is constructed based on two rows of circulant matrices. In the second method, structure of a regular code with girth 8 formed by more than three rows of circulant matrices is discussed.

3.1. Irregular Half Rate QC-LDPC Codes with Girth 6

Irregular half rate $(2\ell, \ell)$ QC-LDPC code is constructed by the parity check matrix having the below form:

$$\mathbf{H} = \begin{bmatrix} C_1 & I_1 & | & C_3 & O \\ I_2 & C_2 & | & O & C_4 \end{bmatrix}, \tag{8}$$

where ℓ is an even value, C_i, $1 \le i \le 4$ are $\frac{\ell}{2} \times \frac{\ell}{2}$ circulant matrices with column

[2] It is possible to have greater ν and provide all given conditions.

weight 3, I_1 and I_2 are $\frac{\ell}{2}\times\frac{\ell}{2}$ circulant matrices with column weight 1 and O represents the $\frac{\ell}{2}\times\frac{\ell}{2}$ zero matrix.

The above matrix can be viewed as two $\ell\times\ell$ matrices and one of these matrices should be full rank to obtain the generator matrix of the code.

Positions of 1 in circulant matrices are based on elements of subsets defined in Equations (1)-(7), where $\ell=\nu$. Indeed, elements of each subset give positions of 1 in the first row of a circulant matrix. Other elements of the first row of circulant matrices are zero. By $\ell-1$ cyclic shifts of the first row, other rows of the circulant matrix will be obtained. That means, there exist $S_i=\{0,\alpha_i,p\alpha_i-r\}$, $1\le i\le 4$, which define C_is. Similarly, there exist $A_1=\{\beta_1\}$ and $A_2=\{q\beta_1-d\}$, which define I_1 and I_2, respectively. In the given parity check matrix, $A_1=\{0\}$ is considered.

As differences between position of 1s in a circulant matrix with column weight 3 are unique, a cycle-4 will not be obtained from C_is, $1\le i\le 4$ [13]. Based on $A_1=\{0\}$ and $A_2=\{q\beta_1-d\}$, position of one 1 in I_1 and I_2 does not lead a cycle-4 in these circulant matrices. Similarly, combination of C_1, C_3 and I_1 will not produce more than one common 1 in every two rows or two columns of $\boldsymbol{H}$. In order not to have cycle-4 from circulant matrices positioned in two rows of $\boldsymbol{H}$, position of 1 in I_2, should be different with differences between position of any two 1s of C_1 and C_2 as well as position of 1 in I_1. Note that existence of zero matrices will also conclude no cycle-4 from combination of C_3 or C_4 with the left $\ell\times\ell$ submatrix of $\boldsymbol{H}$.

3.2. Regular Half Rate QC-LDPC Codes with Girth 8

As another scheme of half rate QC-LDPC code, the parity check matrix is formed by more than two rows of circulant matrices. This matrix is generally expressed by:

$$\boldsymbol{H}=\begin{bmatrix}H_0 & H_1\end{bmatrix}, \tag{9}$$

where H_γ, $0\le\gamma\le 1$, are $\ell\times\ell$ matrices defined by:

$$H_\gamma:=\begin{bmatrix} C_{\gamma,1} & I_{\gamma,1} & O & \cdots & O & O \\ O & C_{\gamma,2} & I_{\gamma,2} & \cdots & O & O \\ O & O & C_{\gamma,3} & \cdots & O & O \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ O & O & O & \cdots & C_{\gamma,u-1} & I_{\gamma,u-1} \\ I_{\gamma,u} & O & O & \cdots & O & C_{\gamma,u} \end{bmatrix}. \tag{10}$$

$C_{\gamma,a}$, $0\le\gamma\le 1$, $1\le a\le u$, and $I_{\gamma,b}$, $1\le b\le u$, are $\frac{\ell}{u}\times\frac{\ell}{u}$ sparse circulant matrices with column weights 2 and 1, respectively. Moreover, O presents $\frac{\ell}{u}\times\frac{\ell}{u}$ zero matrix. Note that, ℓ is a multiple of *u*.

Similar to our first scheme, elements of $\left\{0,\alpha^{(\gamma)}_{(i+1)_u,2}\right\}$ and $\left\{\beta^{(\gamma)}_i\right\}$, $1\le i\le u$, give positions of 1 in $C_{\gamma,(i+1)_u}$ and $I_{\gamma,i}$, respectively. All these subsets follow the properties defined in Equations (1)-(7) with $\ell = \nu$. Other elements in the first row of these circulant matrices are zero. By construction, at least one of H_γ s is full rank to achieve code's generator matrix from $\boldsymbol{H}$. The matrix given in (9) expresses existence of two circulant matrices in its every column. This introduces a regular LDPC code with column weight 3.

Lemma 1 *The parity check matrix given in Equation* (9) *with* $\beta_i^{(0)} < \alpha_{(i+1)_u,2}^{(0)}$, $\beta_i^{(1)} > \alpha_{(i+1)_u,2}^{(1)}$ *and* $\beta_i^{(1)} > \beta_i^{(0)}$ *has cycle-*4 *if the below condition is satisfied*:

$$\beta_i^{(0)} = \beta_i^{(1)} - \alpha_{(i+1)_u,2}^{(1)}$$

Proof. $C_{0,(i+1)_u}$ has 1 at its zeroth column of the zeroth row. Hence, by $\beta_i^{(0)}$ cyclic shifts of the zeroth row of $C_{0,(i+1)_u}$, the $\beta_i^{(0)}$ th row of this matrix has 1 at $\beta_i^{(0)}$ th column. Similarly, the $\beta_i^{(1)} - \alpha_{(i+1)_u,2}^{(1)}$ th row of $C_{1,(i+1)_u}$ has 1 at $\beta_i^{(1)}$ th column. As $\beta_i^{(0)} = \beta_i^{(1)} - \alpha_{(i+1)_u,2}^{(1)}$, the $\beta_i^{(0)}$ th row of $C_{0,(i+1)_u}$ and $C_{1,(i+1)_u}$ has 1 at the $\beta_i^{(0)}$ th and $\beta_i^{(1)} - \alpha_{(i+1)_u,2}^{(1)}$ th columns, respectively. On the other hand, the zeroth rows of $I_{0,i}$ and $I_{1,i}$, which represent $(i-1)\ell$ th row of $\boldsymbol{H}$, also have 1 at the $\beta_i^{(0)}$ th and $\beta_i^{(1)} - \alpha_{(i+1)_u,2}^{(1)}$ th columns, respectively. This means that two rows of $\boldsymbol{H}$ have two common 1 and consequently a cycle-4 is formed for the given $\boldsymbol{H}$.

By the same argument presented in Lemma 1, it is possible to have other conditions for the existence of a cycle-4, which are dependent on elements of subsets applied in construction of parity check matrix of QC-LDPC code. Table 1 gives criteria for the existence of cycle-4 based on the relationships existed between elements of different subsets.

Table 1. Cycle-4 condition based on definition of subsets applied for construction of parity check matrix given in (9).

Structure of subsets	Cycle-4 condition
$\beta_i^{(0)} < \alpha_{(i+1)_u,2}^{(0)}$	$\beta_i^{(1)} - \alpha_{(i+1)_u,2}^{(1)} = \beta_i^{(0)}$
$\beta_i^{(1)} > \alpha_{(i+1)_u,2}^{(1)}$	
$\beta_i^{(1)} > \beta_i^{(0)}$	
$\beta_i^{(0)} > \alpha_{(i+1)_u,2}^{(0)}$	$\beta_i^{(1)} - \alpha_{(i+1)_u,2}^{(1)} = \beta_i^{(0)} - \alpha_{(i+1)_u,2}^{(0)}$
$\beta_i^{(1)} > \alpha_{(i+1)_u,2}^{(1)}$	
$\beta_i^{(0)} < \alpha_{(i+1)_u,2}^{(0)}$	$\alpha_{(i+1)_u,2}^{(1)} - \beta_i^{(1)} = \alpha_{(i+1)_u,2}^{(0)} - \beta_i^{(0)}$
$\beta_i^{(1)} < \alpha_{(i+1)_u,2}^{(1)}$	
$\beta_i^{(0)} > \alpha_{(i+1)_u,2}^{(0)}$	$\beta_i^{(0)} - \alpha_{(i+1)_u,2}^{(0)} = \beta_i^{(1)}$
$\beta_i^{(1)} < \alpha_{(i+1)_u,2}^{(1)}$	
$\beta_i^{(0)} > \beta_i^{(1)}$	

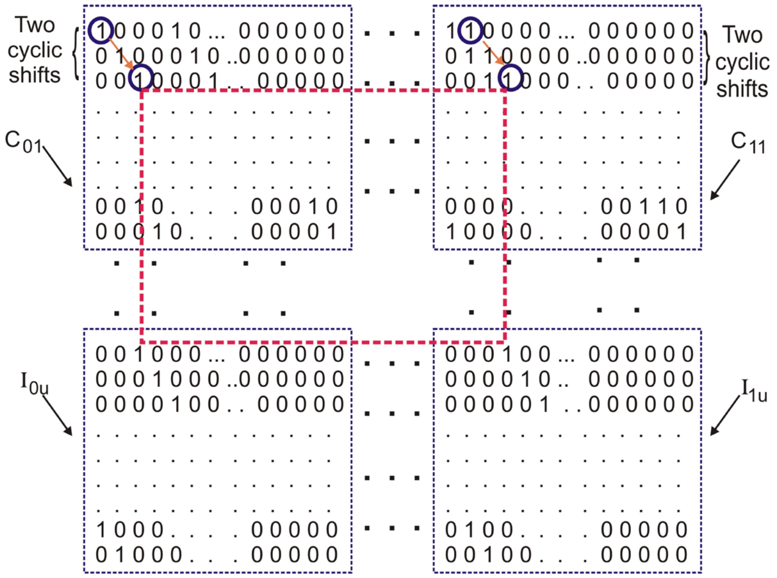

Figure 1. Existence of a cycle-4 based on combination of four circulant matrices.

As an example, Figure 1 shows structure of $\boldsymbol{H}$ constituted by u rows of $\ell \times \ell$ circulant matrices $(u \geq 3)$. In this $\boldsymbol{H}$, $C_{0,1}$, $C_{1,1}$, $I_{0,1}$ and $I_{1,1}$ are formed by $S_1 = B_{0,1} = \{0,4\}$, $S_2 = B_{1,1} = \{0,1\}$, $A_1 = B_{0,u} = \{2\}$ and $A_2 = B_{1,u} = \{3\}$, respectively. In this case, ℓ is an arbitrary value, which satisfies conditions in (1)-(7). The second column of $C_{0,1}$ has 1 in its second row obtained from two cyclic shifts of the zeroth row. By equal number of shifts conducted on the zeroth row of $C_{1,1}$, its third column of the second row is also 1. In the zeroth row of $I_{0,u}$ and $I_{1,u}$, the second and third columns are 1. This means that the second and zeroth rows of $C_{0,1}$ and $I_{0,u}$ have common 1 in their second column, respectively. Existence of common 1 also exists in the second and zeroth rows of $C_{1,1}$ and $I_{1,u}$. As a result, combination of the mentioned circulant matrices will conclude a cycle-4 for the matrix constructed by the utilized circulant matrices.

Lemma 2 *In a circulant matrix with length* λ *and column weight* 2, *let* 0 *and* ρ *be positions of 1 in the zeroth row, where* $0 < \rho \leq \lambda - 1$. *The matrix has cycle*-6 *if and only if*

$$\begin{cases} \lambda = 3\rho, & 2\rho < \lambda \\ 2\lambda = 3\rho, & 2\rho \geq \lambda \end{cases} \tag{11}$$

Proof. By [10], a circulant matrix has cycle-6, if a 3×3 submatrix of the main matrix includes two identical terms in its determinant expansion. This means, in every three rows of the circulant matrix, any row pair should have one and only one 1 in common and position of this common-1 must be different with positions of common-1 in other row pairs. Figure 2(a) shows all possible shapes of cycle-6 in a circulant matrix.

At ρth row of a circulant matrix with column weight 2 and length λ, positions of 1 will be at ρth and $(2\rho)_\lambda$ th columns. Similarly, by $(\lambda - \rho)$ cyclic shifts of the zeroth row, positions of 1 will be at $(\lambda - \rho)$ th and zeroth columns. Considering structure of

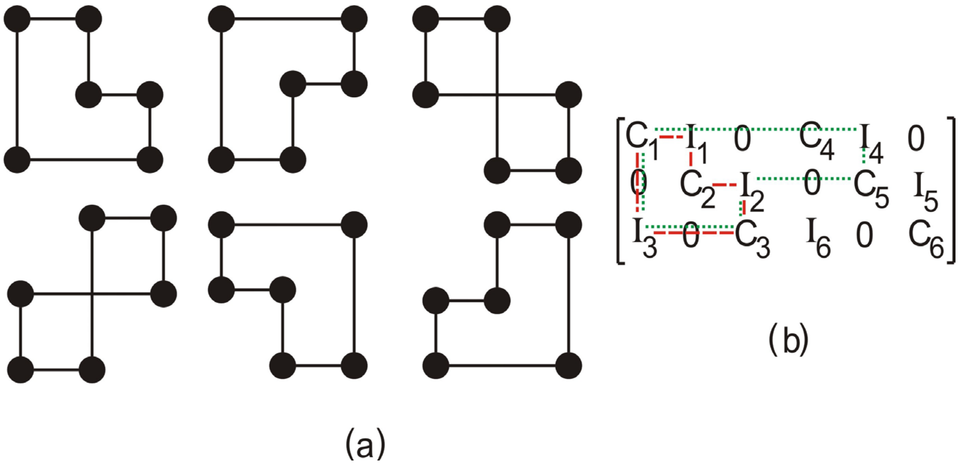
$\begin{bmatrix} C_1 & I_1 & 0 & C_4 & I_4 & 0 \\ 0 & C_2 & I_2 & 0 & C_5 & I_5 \\ I_3 & 0 & C_3 & I_6 & 0 & C_6 \end{bmatrix}$
(b)
(a)

Figure 2. Expression of cycle-6. (a) All possible shapes of cycle-6 (b) existence of cycle-6 in the parity check matrix given in 9.

cycle-6 mentioned in above, the first and ρth rows with $(\lambda-\rho)$ th row can form a cycle-6 if $(2\rho)_{\lambda}=(\lambda-\rho)$. This means $\lambda=3\rho$ for $2\rho<\lambda$ and $2\lambda=3\rho$ for $2\rho\geq\lambda$.

Proposition 1 *The girth of parity check matrix given in* (9) *with* $\frac{\ell}{u}\neq 3\alpha_{a,2}^{(\gamma)}$ *for* $2\alpha_{a,2}^{(\gamma)}<\frac{\ell}{u}$ *and* $\alpha_{a,2}^{(\gamma)}$ *for* $2\alpha_{a,2}^{(\gamma)}\geq\frac{\ell}{u}$, $u>3$, *is at least 8.*

Proof. In the given $\boldsymbol{H}$, each $C_{\gamma,a}$, $0\leq\gamma\leq1$, $1\leq a\leq u$, has two 1s in every row and column. This matrix is free of cycle-4 because circulant matrices are formed on the basis of conditions given in (1)-(7). In addition, in circulant matrices with column weight 2, position of 1s in their first row do not provide the condition mentioned in Lemma 1.

By the same argument in Lemma 2, in the structure of every $C_{\gamma,a}$, in every three rows, any row pair does not have one common 1 in a unique position as differences between positions of 1 are unique and length of circulant matrices does not satisfy conditions of the lemma. This structure is not even observed in $I_{\gamma,b}$ s because in their every row or column only one 1 exists.

The given $\boldsymbol{H}$ can also have cycle-6, when combination of circulant matrices forms one of the shapes shown in Figure 2(a). Indeed, circulant matrices in these graphs are interpreted as nodes of graph. Hence, in order to have cycle-6, it is essential to have six non-zero circulant matrices positioned in three different rows and columns of $\boldsymbol{H}$, while in every row and column, there are exactly two of these circulant matrices. Figure 2(b) shows two possible cycle-6 formed by combination of six circulant matrices. Considering structure of $\boldsymbol{H}$, cycle-6 is prohibited, when $\boldsymbol{H}$ is constructed by more than three rows of circulant matrices $(u>3)$. It is observed that in every three rows, any row pair does not have two non-zero matrices in one column. Thus, combination of circulant matrices will also not produce cycle-6 and the girth of the given $\boldsymbol{H}$ is at least 8.

4. Simulation Results

The performance of proposed QC-LDPC codes is verified for additive white gaussian noise (AWGN) channel. Codes are modulated by Binary Phase Shift Keying (BPSK) modulation and decoded by Sum Product Algorithm (SPA). Maximum 100 iterations are considered for iterative decoding. Figure 3 shows performance of codes with lengths 128 and 255.

Parity check matrix of the irregular (256, 128) QC-LDPC code is formed by two rows of circulant matrices given in Equation (8). For $\frac{E_b}{N_o} < 4.5\,\text{dB}$ proposed code with girth 6 has close performance to two other (256, 128) codes having girth 8. However, for $\frac{E_b}{N_o} \geq 4.5\,\text{dB}$, it outperforms them. This is evident at $BER \approx 10^{-7}$, when it shows 0.25 dB improvement compared to PEG QC-LDPC code [6]. It is also concluded that the error floor of the proposed irregular code will be occurred at $BER \leq 10^{-9}$. For code with and length $L = 255$, parity check matrix is constructed by five rows of the circulant matrices and satisfies conditions of the proposition 1. This concludes a half-rate regular code with girth at least 8. Again, results express that the new code outperforms PEG code, while it has very similar performance to the QC-LDPC code with girth 8 and an optimised iterative decoding performance. Result of regular (1032, 516) QC-LDPC code is shown in Figure 4. The parity check matrix of this code is formed by six rows of circulant matrices. This code has very similar performance with (1016, 508) and (1010, 505) codes, which require more steps in construction of their parity check matrix as masking technique is applied. In comparison with irregular code, regular codes demonstrate better performance than PEG code. This is because of

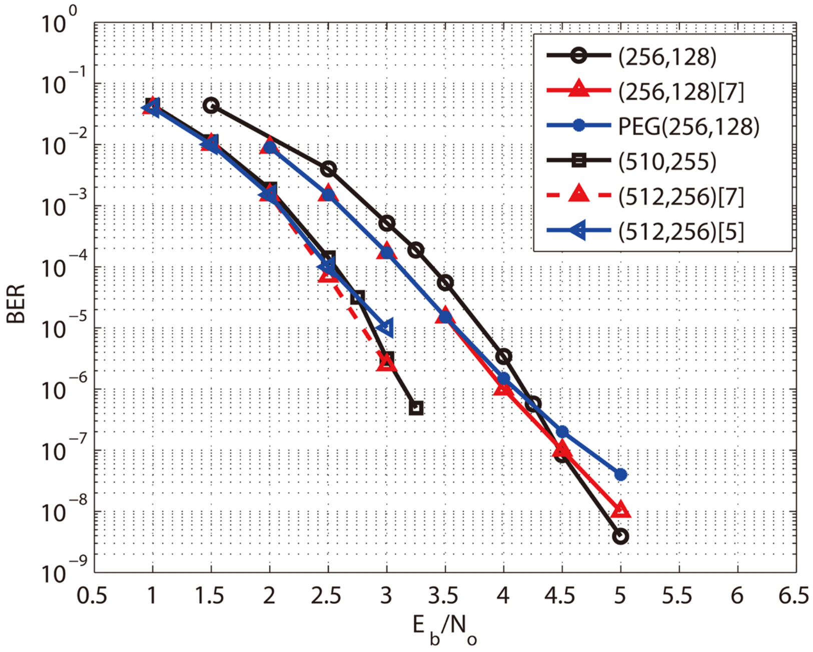

Figure 3. Performance of the half rate QC-LDPC codes with lengths 128 and 255.

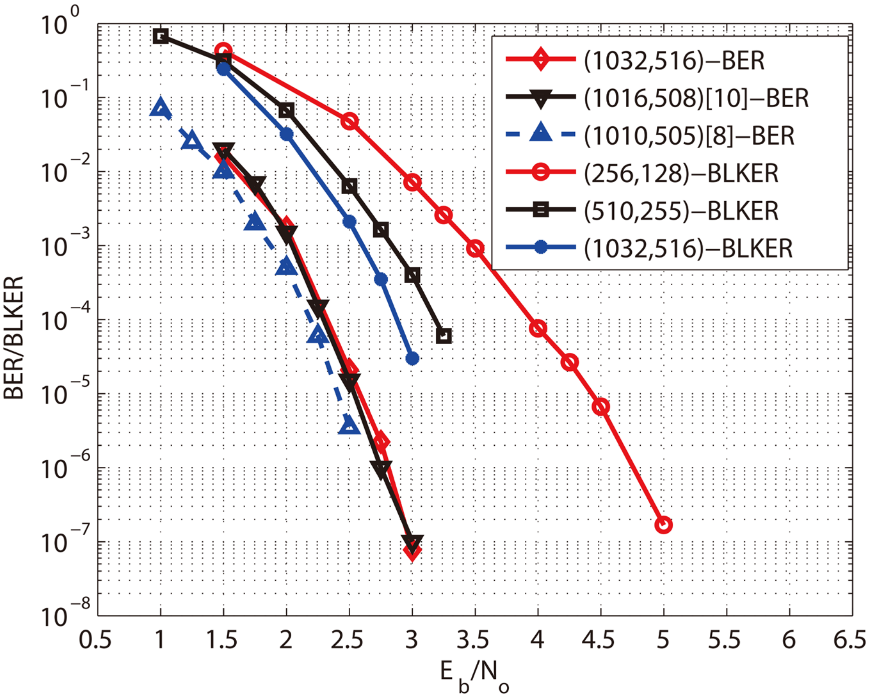

Figure 4. Bit error rate (BER) and block error rate (BLKER) performance of the half rate QC-LDPC codes with lengths 128, 255 and 516.

non-existence of cycle-6 in structure of regular code, which deteriorates effect of harmful trapping sets on the error correcting performance of codes. The results obtained from simulations demonstrate that the error floor of the newly designed codes with girth 8 will be for $BER \le 10^{-8}$.

The figure also gives the block error rate (BLKER) performance of the constructed QC-LDPC codes. In general, no error floor is observed for $BLKER \ge 10^{-5}$.

5. Conclusions and Future Work

The paper presented new schemes of half rate QC-LDPC codes with girth 6 or 8. They are designed on the basis of difference set property of subsets, which determine structure of constituent circulant matrices. Based on defining new criteria in structure of subsets and proper combination of circulant matrices, regular QC-LDPC codes with girth 8 were obtained. This concluded a high girth code without applying a masking technique. Simulation results confirmed that newly proposed codes have similar performance to other well-known half rate codes, while are designed with the lower complexity. In future work, the performance of constructed codes in the error floor region will be verified by trapping sets analysis and determining their minimum weight.

References

[1] ETSI EN 302 307-1:1, Digital Video Broadcasting (DVB); Second Generation Framing Structure, Channel Coding and Modulation Systems for Broadcasting, Interactive Services, News Gathering and Other Broadband Satellite Applications. ETSI Standard, Part 1: DVB-

S2, Vol. 4, No. 1, 2014.

[2] IEEE Standard for Broadband Wireless Metropolitan Area Networks\Air Interface for Broadband Wireless Access Systems. IEEE std 802.16, August 2012.

[3] Li, Y. and Salehi, M. (2010) Quasi-Cyclic LDPC Code Design for Block-Fading Channels. 44*th Annual Conference on Information Sciences and Systems* (*CISS*), 17-19 March 2010, 1-5. http://dx.doi.org/10.1109/ciss.2010.5464729

[4] Han, G., Guan, Y.L. and Kong, L. (2014) Construction of Irregular QC-LDPC Codes via Masking with ACE Optimization. *IEEE Communications Letters*, **18**, 348-351.

[5] Zhang, Y. and Da, X.Y. (2015) Construction of Girth-Eight QC-LDPC Codes from Arithmetic Progression Sequence with Large Column Weight. *IET Electronics Letters*, **51**, 1257-1259.

[6] Eleftheriou, E., Hu, X.-Y. and Arnold, D.-M. (2001) Progressive Edge-Growth Tanner Graphs. *IEEE GLOBECOM*, 995-1001.

[7] Healy, C.T. and de Lamare, R.C. (2011) Decoder Optimised Progressive Edge Growth Algorithm. *IEEE Vehicular Technology Conference* (*VTC Spring*), 1-5.

[8] Zhang, G.H., Sun, R. and Wang, X.M. (2013) Construction of Girth-Eight QC-LDPC Codes from Greatest Common Divisor. *IEEE Communications Letters*, **17**, 369-372.

[9] Zhao, H., Qin, L., Wang, R., Li, Y. and Zhang, H. (2016) Construction of Girth-Eight Quasi-Cyclic Low-Density Parity-Check Codes with Low Encoding Complexity. *IET Communications Journal*, **10**, 148-153.

[10] Li, J., Liu, K., Lin, S. and Abdel-Ghaffar, K. (2014) Algebraic Quasi-Cyclic LDPC Codes: Construction, Low Error-Floor, Large Girth and a Reduced-Complexity Decoding Scheme. *IEEE Transactions on Communications*, **62**, 2626-2637.

[11] Vasic, B. and Milenkovic, O. (2004) Combinatorial Constructions of Low-Density Parity-Check Codes for Iterative Decoding. *IEEE Transactions on Information Theory*, **50**, 1156-1176.

[12] Park, H., Hong, S.B., No, J.S. and Shin, D.J. (2013) Construction of High-Rate Regular Quasi-Cyclic LDPC Codes Based on Cyclic Difference Families. *IEEE Transactions on Communications*, **61**, 3108-3113.

[13] Vafi, S. and Rezvani Majid, N. (2015) A New Scheme of High Performance Quasi-Cyclic LDPC Codes with Girth 6. *IEEE Communications Letters*, **19**, 1666-1669.

Scientific Research Publishing

Submit or recommend next manuscript to SCIRP and we will provide best service for you:

Accepting pre-submission inquiries through Email, Facebook, LinkedIn, Twitter, etc.
A wide selection of journals (inclusive of 9 subjects, more than 200 journals)
Providing 24-hour high-quality service
User-friendly online submission system
Fair and swift peer-review system
Efficient typesetting and proofreading procedure
Display of the result of downloads and visits, as well as the number of cited articles
Maximum dissemination of your research work

Submit your manuscript at: http://papersubmission.scirp.org/
Or contact jcc@scirp.org