Charles Darwin University

Combinatorial design-based Quasi-cyclic LDPC codes with girth eight

Vafi, Sina; Majid, Narges Rezvani

Published in:
Digital Communications and Networks

DOI:
10.1016/j.dcan.2018.01.001

Published: 01/11/2018

Document Version
Publisher's PDF, also known as Version of record

Link to publication

Citation for published version (APA):
Vafi, S., & Majid, N. R. (2018). Combinatorial design-based Quasi-cyclic LDPC codes with girth eight. *Digital Communications and Networks*, *4*(4), 296-300. https://doi.org/10.1016/j.dcan.2018.01.001

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 30. Sep. 2020

Digital Communications and Networks 4 (2018) 296–300

Contents lists available at ScienceDirect

Digital Communications and Networks

journal homepage: www.keaipublishing.com/en/journals/digital-communications-and-networks/

Combinatorial design-based quasi-cyclic LDPC codes with girth eight

Sina Vafi *, Narges Rezvani Majid

College of Engineering, Information Technology and Environment, Charles Darwin University, Ellengowan Drive, NT, 0909, Australia

ARTICLE INFO

Keywords:
Quasi-cyclic LDPC codes
Combinatorial design
Minimum weight
Girth

ABSTRACT

This paper presents a novel regular Quasi-Cyclic (QC) Low Density Parity Check (LDPC) codes with column-weight three and girth at least eight. These are designed on the basis of combinatorial design in which subsets applied for the construction of circulant matrices are determined by a particular subset. Considering the non-existence of cycles four and six in the structure of the parity check matrix, a bound for their minimum weight is proposed. The simulations conducted confirm that without applying a masking technique, the newly implemented codes have a performance similar to or better than other well-known codes. This is evident in the waterfall region, while their error floor at very low Bit Error Rate (BER) is expected.

1. Introduction

Quasi-Cyclic Low-Density Parity Check (QC-LDPC) codes are introduced as a class of structured-type LDPC codes, which are practically applied to the current and next generation of broadband networks. This is because of their less complex encoding and high error-correcting capability formed by a parallel decoding structure. Like other types of LDPC codes, the existence of small trapping sets dominates iterative decoding performance of QC-LDPC codes over the Additive White Gaussian Noise (AWGN) channel at the error floor region. It is well-known that the small size of a trapping set is directly related to the girth of the code. Hence, in order to mitigate the effect of the error floor, the design of a code with large girth and a relatively high minimum weight is recommended.

In general, QC-LDPC codes are designed with girth six. A masking technique is applied on their parity check matrix to prohibit cycle six and form codes with the girth at least eight. This is conventionally applied on the parity check matrix constituted by Circulant Permutation Matrices (CPMs) [1,2].

Similarly, several circulant matrices are used to construct a high performance QC-LDPC code with a shorter length in the waterfall region. This is obtained with the squashing process, which is accomplished on the constructed parity check matrix to achieve girth eight for the QC-LDPC code [3].

Zhang et al. proposed a method for the construction of codes with girth six, whose parity check matrix is formed by two rows of circulant matrices [4]. This work is extended to present criteria for determining codes' parameters, such as rate and length, based on the utilised number of rows and columns of the parity check matrix. An exhaustive search algorithm was also proposed for determining the shortest possible length of regular QC-LDPC codes with girth eight. The algorithm is applied for CPM-based parity check matrices having symmetry in their structure [5].

QC-LDPC codes with large girth and relatively high minimum weight are obtained by Cyclic Difference Families sets (CDFs) in which every specific number of elements defined in the subsets of a group occurs only once [6]. The non-binary shape of these codes with long length and high girth is constructed by using the Singer perfect difference set concept [7]. The parity check matrix of these codes can be modified to demonstrate short-length QC-LDPC codes either in binary or non-binary format with girth eight [8]. In this case, codes with a girth greater than six are designed by parity check matrices with column-weight two. For parity check matrices with column-weight three, their girth is limited to six. Constituent circulant matrices of the parity check matrix with girth six can be designed by using combinatorial design. This means that elements of a subset are determined on the basis of elements of the previous subset. In addition, subsets are defined such that the difference between every two elements of a subset is unique with all other differences [9]. In comparison with codes formed by CDFs, combinatorial design-based codes have more flexibility in their structure as it is not necessary to have the difference of two elements as an element of the subset.

This paper presents a method for constructing combinatorial design-based regular QC-LDPC codes with girth at least eight. The parity check matrix of these codes has column-weight three and is formed by two rows of circulant matrices. In addition to the condition given in Ref. [9], which defines subsets without cycle four, other criteria are applied for the subsets, aiming to remove cycle six from the Tanner graph of the parity check matrix. Based on these specifications, newly designed codes have a

* Corresponding author.
E-mail addresses: Sina.vafi@cdu.edu.au (S. Vafi), Rezvani.narges@gmail.com (N.R. Majid).

https://doi.org/10.1016/j.dcan.2018.01.001
Received 28 May 2017; Received in revised form 19 September 2017; Accepted 2 January 2018
Available online 6 January 2018
2352-8648/© 2018 Chongqing University of Posts and Telecommunications. Production and hosting by Elsevier B.V. on behalf of KeAi. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

high performance in the waterfall region. Moreover, our analysis reveals that codes have a relatively high minimum weight. As a result, it is expected that their error floor occurs at a very low Bit Error Rate (BER). This is confirmed by number of simulations conducted on codes with different rates.

The rest of the paper is organized as follows: Section 2 presents subsets which are applied in the construction of circulant matrices. It demonstrates how elements of subsets are selected to prohibit short cycles in the Tanner graph of the parity check matrix. Section 3 explains the structure of QC-LDPC codes with girth at least eight and also represents a bound for determining the minimum weight of the codes. Section 4 gives the simulation results of the designed codes and their comparison with similar ones. Finally, Section 5 summarizes the paper.

2. Structure of subsets with the unique difference between elements

For given $n \in \mathbb{N}$, we define subsets $S_i \subset \mathbb{N} \cup \{0\}$, $1 \le i \le n$, by strictly increasing sequences $\{\alpha_{i,j}\}_{1 \le j \le 2}$, which satisfy the following conditions:

1) $\alpha_{1,1} \in \mathbb{Z}$ and $\alpha_{1,2} \in \mathbb{Z}$. For $2 \le i \le n$, we choose $m \in \mathbb{N}/\{1\}$, $r \in \mathbb{Z}/\{0\}$ with $m > r$ such that

$$\alpha_{i,2} = m\alpha_{i-1,2} - r. \tag{1}$$

In addition,

$$\alpha_{i,2} - \alpha_{i,1} \neq \alpha_{i',2} - \alpha_{i',1}, \quad \forall i' < i \tag{2}$$

We also define subsets $A_{i_1} \subset \mathbb{N} \cup \{0\}$, $1 \le i_1 \le n$, by $\{\beta_{i_1}\}$, which satisfy the following conditions:

2) $\beta_{i_1} \in \mathbb{Z}$ and for $2 \le i_1 \le n$ we choose $q \in \mathbb{N} \setminus \{1\}$, $d \in \mathbb{Z} \setminus \{0\}$ with $q > d$ such that

$$\beta_{i_1} = q\beta_{i_1-1} - d \tag{3}$$

3) For every $1 \le i \le n$, $1 \le i_1 \le n$,

$$\alpha_{i,2} - \alpha_{i,1} \neq \beta_{i_1} \tag{4}$$

Based on the above-mentioned subsets, an additive group $\mathbb{Z}_\nu = \{0, 1, \cdots, \nu - 1\}$ is defined in such a way that $3(\alpha_{i,2} - \alpha_{i,1})_\nu \neq \nu$ for all $1 \le i \le n$. In addition, for all $1 \le i \le n$ and $1 \le i_1 \le n$, $(\alpha_{i,2} - \alpha_{i,1})_\nu$ and $(\pm\beta_{i_1})_\nu$ are repeated only once in this group and ν is the smallest value, which satisfies the above conditions. For example, consider subsets $S_1 = \{0, 42\}$, $S_2 = \{1, 88\}$, $S_3 = \{2, 180\}$, $A_1 = \{78\}$, and $A_2 = \{155\}$ and $A_3 = \{0, 309\}$ are defined in $\mathbb{Z}_{311}$. The second elements of S_2 and S_3 are obtained from S_1, when $m = 2$ and $r = -4$ are applied in (1). Similarly, A_2 and A_3 are formed from A_1 by using $q = 2$ and $d = 1$ in (3). For these subsets, $\Delta_{S_1} = \{42, 269\}$, $\Delta_{S_2} = \{87, 224\}$, $\Delta_{S_3} = \{178, 133\}$ $\Delta_{A_1} = \{78, 233\}$, $\Delta_{A_2} = \{155, 156\}$ and $\Delta_{A_3} = \{2, 309\}$, which give sets of differences between elements of S_1, S_2, S_3, A_1, A_2 and A_3, respectively. It is concluded that the difference between any two elements of a subset is unique, with other differences obtained from other subsets.

3. Structure of QC-LDPC codes with girth at least 8

Let c be an even value greater than 2, C_i and I_i, $1 \le i \le c$ be $\ell \times \ell$ circulant matrices with column-weight two and one, respectively. For odd values of $\frac{c}{2}$, the parity check matrix of a $(c\ell, (c-2)\ell)$ QC-LDPC code with rate $R = \frac{(c-2)}{c}$ is constructed in the following form:

$$\mathbf{H} = \begin{bmatrix} C_1 & I_1 & I_3 & C_4 & C_5 & I_6 \cdots & C_{c-1} & I_{c-1} \\ I_2 & C_2 & C_3 & I_4 & I_5 & C_6 \cdots & I_c & C_c \end{bmatrix}$$

Similarly, for even values of $\frac{c}{2}$, this matrix is given by:

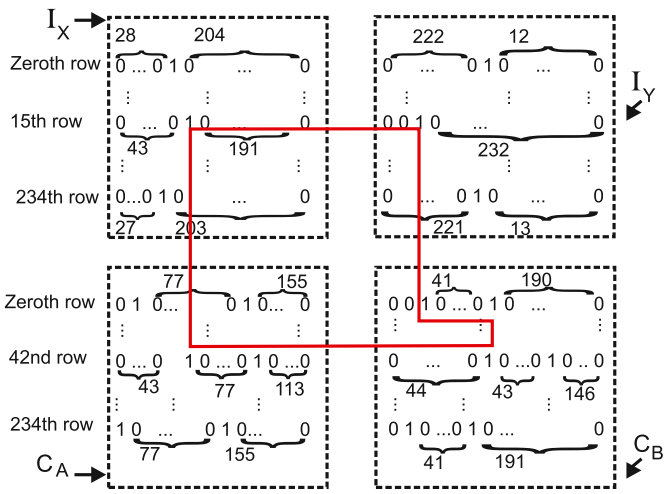

Fig. 1. Existence of a cycle six formed by four circulant matrices.

$$\mathbf{H} = \begin{bmatrix} C_1 & I_1 & I_3 & C_4 & C_5 & I_6 \cdots & I_{c-1} & C_{c-1} \\ I_2 & C_2 & C_3 & I_4 & I_5 & C_6 \cdots & C_c & I_c \end{bmatrix}$$

Positions of 1 in the zeroth row of each circulant matrix will be elements of a subset satisfying conditions represented in Section 2,[1] where $\ell = \nu$ and $c = n$. By $\ell - 1$ cyclic shifts of the zeroth row, other rows of the circulant matrix will be formed. In the constructed parity check matrix, the difference between positions of 1 in a circulant matrix is different from other differences obtained from other circulant matrices. This means that there would not be any two rows or columns in $\mathbf{H}$ having more than one 1 in common [9]. As a result, the given parity check matrix is free of cycle four. In addition, in each of column-weight two circulant matrices, positions of 1 are selected so that their difference multiplied by the value of three is not equal to the value of ℓ. This guarantees that circulant matrices designed with the above conditions are free of cycle six [10].

A cycle six can be obtained, when a combination of circulant matrices positioned in two different columns of $\mathbf{H}$ is considered. For instance, consider I_X and C_A as column-weight one and column-weight two circulant matrices positioned in a column of $\mathbf{H}$. These can be combined with two other circulant matrices, i.e. I_Y and C_B, located at another column of $\mathbf{H}$ to form a $4\ell \times 4\ell$ submatrix of $\mathbf{H}$. Let x and y be the position of 1 in the zeroth row of I_X and I_Y, respectively. Positions of 1 in the zeroth row of C_A and C_B are indicated by $\{a_1, a_2\}$ and $\{b_1, b_2\}$, respectively.

By $(\ell - y + b_1)_\ell$ cyclic shifts of the zeroth row of I_Y, $(\ell - y + b_1)_\ell$ th row of this matrix has a 1 at the b_1th column. With equal number of shifts, the $(\ell - y + b_1)$th row of I_X has a 1 at the $(\ell - y + b_1) + x$th column. By $(b_2 - b_1)$ cyclic shifts of the zeroth row of C_A, the $(b_2 - b_1)$th row of the matrix has a 1 in the b_2th column. This row of C_B is represented as the $\ell + (b_2 - b_1)_\ell$th row of $\mathbf{H}$. Similarly, by $(b_2 - b_1) + a_1$ cyclic shifts of the zeroth row of C_A, its $(b_2 - b_1) + a_1$th row has a 1 at the $(b_2 - b_1) + a_1$th column. A cycle six is obtained when the $(b_2 - b_1) + a_1$th and $(\ell - y + b_1) + x$ th columns of C_A and I_X are interpreted as one column in $\mathbf{H}$. The above analysis can also be used when $(b_2 - b_1) + a_2$ shifts in C_A is considered. In this case, cycle six is made when $(\ell - y + b_1)_\ell$ and $(b_2 - b_1 + a_2 - x)_\ell$ represent one column of $\mathbf{H}$. Therefore, $\mathbf{H}$ is free of cycle six based on the following conditions:

$$\begin{matrix} (\ell - y + b_1)_\ell \neq (b_2 - b_1 + a_1 - x)_\ell \\ (\ell - y + b_1)_\ell \neq (b_2 - b_1 + a_2 - x)_\ell \end{matrix}. \tag{5}$$

Fig. 1 shows the existence of a cycle six formed by four 235×235 circulant matrices. The zeroth row of circulant matrices with column-weight one has a 1 in the 28th ($x = 28$) and 222nd ($y = 222$) columns.

[1] In this paper, rows and columns of circulant matrices are indexed from zero.

Table 1
Cycle-6 conditions based on the combination of circulant matrices applied for the construction of parity check matrix (**H**).

Row of **H**	Shape of combination	Cycle-6 condition
1st	$I_X \quad I_Y$	$(b_2-b_1+a_1-x)_\ell=(\ell-y+b_1)_\ell$
2nd	$C_A \quad C_B$	$(b_2-b_1+a_2-x)_\ell=(\ell-y+b_1)_\ell$
1st	$C_A \quad I_Y$	$(b_2-b_1+x-a_2)_\ell=(\ell-y+b_1)_\ell$
2nd	$I_X \quad C_B$	$(b_2-b_1+x-a_1)_\ell=(\ell-y+b_1)_\ell$
1st	$I_X \quad C_A$	$(a_1-a_2+x-b_1)_\ell=(x-b_2)_\ell$
2nd	$C_B \quad I_Y$	$(a_1-a_2+x-b_2)_\ell=(x-b_2)_\ell$
1st	$C_A \quad C_B \quad I_Y$	$(a_2-a_1+b_2)_\ell=(y-e_1+x)_\ell$ $(a_2-a_1+b_1)_\ell=(y-e_1+x)_\ell$
2nd	$I_X \quad C_E$	$(a_2-a_1+b_2)_\ell=(y-e_2+x)_\ell$ $(a_2-a_1+b_1)_\ell=(y-e_2+x)_\ell$

C_A and C_B, which represent circulant matrices with column-weight two, have a 1 at $(a_1=1,\ a_2=79)$ and $(b_1=2,\ b_2=44)$. By $\ell-y+b_1=15$ cyclic shifts of the first row of I_Y, the 15th row of the matrix has a 1 in the second column. The $b_2-b_1+1=43$rd rows of C_A and C_B have a 1 in $b_2=44$th column. On the other hand, by 15 cyclic shifts of the zeroth row of I_X, the 15th row of the matrix has a 1 at the 43rd column. Therefore, at three different rows of **H**, every two rows have one 1 in common, which is different from two other 1 positions. This concludes a cycle six in **H**.

By the same argument, there are other combinations of circulant matrices, which form a cycle six in the parity check matrix. Cycle six can also be obtained from circulant matrices positioned in three different columns of **H**. Table 1 gives the possibilities of the cycle six and their correspondence conditions. In this table, C_E represents a column-weight two circulant matrix, whose zeroth row has 1 in e_1 and e_2 positions.

In order to have a parity check matrix with girth eight, it is necessary that constituent circulant matrices satisfy conditions given in Section 2. First, circulant matrices with column weight 2 without cycles four and six are formed. Then, circulant matrices with column weight 1 are constructed, which also satisfy conditions given in Section 2 and prohibit the existence of cycle six in **H**. Steps for constructing such a parity check matrix are given in Algorithm 2.

Algorithm 1 Procedure for construction of parity check matrix with girth eight.

1 Determine $\ell=\frac{k}{c-2}$.
2 For arbitrary values of m and r, determine subsets S_i, $1\le i\le c$, which satisfy conditions mentioned in Section 2.
3 Construct column-weight-two circulant matrices (C_is, $1\le i\le c$) from S_is.
4 $i_1=1$ and three arbitrary integer values for β_1, q and d.
5 $i_1\rightarrow i_1+1$.
6 If $i_1=2$, then $t=i_1$.
7 if $i_1>2$, then $t=tt$.
8 $\beta_t=q\beta_{t-1}-d$. If $\beta_t<\ell$ and satisfies conditions given in Section 2, construct the column-weight-one I_{i_1} based on β_t. If $\beta_t\ge\ell$, repeat the algorithm from Step 4.
9 If the combination of all I_xs, $1\le i\le i_1$s with C_is, $1\le i\le c$ satisfies one of the conditions of Table 1, $t\rightarrow t+1$ and repeat the algorithm from Step 8.
10 If the combination of all I_xs, $1\le i\le i_1$s with C_is, $1\le i\le c$ does not satisfy all conditions of Table 1, $tt=t$ and $\beta_{i_1}=\beta_t$.
11 If $i_1<c$, repeat the algorithm from Step 5. Otherwise, stop the algorithm.

Table 2 gives the details of subsets applied for the construction of the parity check matrix of QC-LDPC codes with girth eight and rates $\frac{1}{2}$ and $\frac{2}{3}$. As expected, for the fixed value of ℓ, the complexity in the design of **H** is proportional to the number of circulant matrices. It is possible to consider a common element for S_is, $1\le i\le c$, while the second element of the subsets is determined by (1). In addition, the number of A_{i_1}s can be determined by particular values of q and d, which are different from those considered for the rest of column-weight one circulant matrices.

3.1. A bound for the minimum weight of proposed codes

The constructed parity check matrix can be considered as two submatrices. The first $2\ell\times(c-2)\ell$ submatrix corresponds to message bits, whereas the second one with size $2\ell\times2\ell$ is relevant to parity bits. Each of the $2\ell\times2\ell$ matrices obtained from the first submatrix can be combined with the second submatrix to demonstrate a parity check matrix for the half rate $(4\ell,2\ell)$ QC-LDPC code. Let $W_i^{(w_{in})}$ be the low weight of the i-th $(4\ell,\ 2\ell)$ code, $1\le i\le\binom{c-2}{2}$, obtained from messages with weight w_{in}, where $\binom{c-2}{2}$ gives number of codes and is defined as the combination of $(c-2)$ and 2. Let $(W^{(w_{in})})_{\min}=\min(W_i^{(w_{in})})$ as the lowest weight of these codes based on the fixed weight w_{in}. The minimum weight of $(c\ell,(c-2)\ell)$ QC-LDPC code is upper bounded by:

$$(W_{min})_{QC-LDPC}\le\min\left\{\left(W^{(w_{in})}\right)_{min}\right\} \tag{6}$$

The constructed **H** has three 1s in its columns. Hence, a set of low weights of designed codes is obtained from three checksums of a message bit with parity bit 1's. Based on girth eight, some conditions should be considered in checksums of each message bit. Fig. 2(a) shows a possibility of cycle six, when positions of 1s in two rows of the matrix are related to the checksum of the message bit (M_0) with two parity bits (P_0 and P_1). In this figure, columns are labeled by the message and parity bits applied in the checksums. In order to have a cycle six, P_0 and P_1 should be multiplied by the common 1 located at the second submatrix of **H**, which concludes $P_0+P_1=0$. As **H** does not have cycle six, parity bit 1's involved in checksums of the message bit will not form a checksum with each other. Alternatively, a cycle six is obtained when checksums of two message bits have two parity bits in common. Fig. 2(b) shows the possibility of this cycle. Since **H** is free of the cycle six and differences between the positions of 1s in the zeroth row of each circulant matrix are

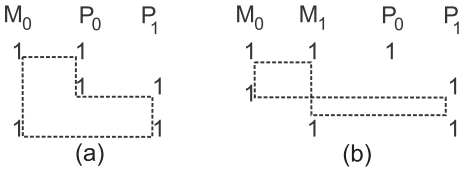

Fig. 2. Conditions of cycle 6 formed by checksums of message bits.

Table 2
Specifications of subsets applied for the parity check matrix of QC-LDPC codes with rates $\frac{1}{2}$ and $\frac{2}{3}$.

Code	First subsets	$m(q)$	$r(d)$	ν	Other subsets
(668,334)	{0,4},{9}	3(2)	3(5)	167	{0,15},{1,45},{2138} {23},{51},{107}
(1710,1140)	{0,2},{12}	3(2)	2(1)	285	{0,4},{0,10},{0,28},{0,82},{0,254} {23},{45},{89},{177},{253}

Table 3
Minimum weights of (200,100) QC-LDPC code on the basis of messages with weight no greater than 6.

Subsets	w_{in}	$(W^{(w_{in})})_{\min}$
{0,2},{12},{23},{0,28}{45},{0,10},{0,4},{32}	1	48
	2	38
	3	26
	4	20
	5	28
	6	22

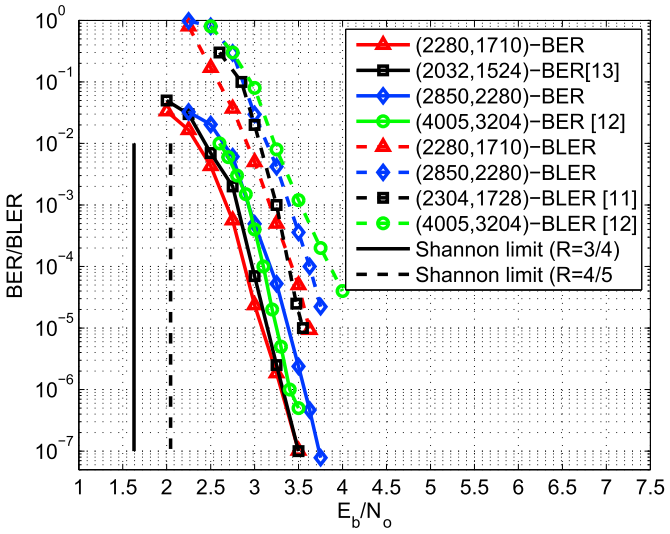

Fig. 3. Performance of QC-LDPC codes with rates $\frac{3}{4}$ and $\frac{4}{5}$.

unique, checksums of two message bits do not have more than one parity bit in common.

Considering the above-mentioned conditions, for messages with weight 4 ($w_{in}=4$), checksums with the minimum number of parity bits are formed as follows:

$$M_0+M_1=0, M_0+P_0=0, M_0+P_5=0, M_1+P_3=0, M_2+P_4=0,$$
$$M_2+M_1=0, M_2+P_5=0, M_3+P_6=0, M_3+P_{15}=0, M_3+P_1=0, P_0+P_3=0,$$
$$P_0+P_7=0, P_2+P_8=0, P_2+P_9=0, P_2+P_5=0, P_3+P_6=0, P_4+P_{10}=0,$$
$$P_6+P_8=0, P_7+P_{11}=0, P_7+P_{12}=0, P_8+P_{13}=0, P_9+P_{13}=0, P_9+P_{14}=0,$$
$$P_{10}+P_{14}=0, P_{10}+P_{11}=0, P_{11}+P_{15}=0, P_{12}+P_1=0, P_{12}+P_4=0, P_{13}+P_{15}=0, P_1+P_{14}=0.$$

These give a codeword with weight 20. Similarly, for messages with weight 3, checksums with minimum number of parity bits will be as follows:

$$M_0+\acute{P}_0=0, M_0+\acute{P}_1=0, M_0+\acute{P}_2=0, M_1+\acute{P}_3=0, M_1+\acute{P}_4=0,$$
$$M_1+\acute{P}_5=0, M_2+\acute{P}_0=0, M_2+\acute{P}_6=0 M_2+\acute{P}_7=0, P_1+\acute{P}_4=0,$$
$$P_1+\acute{P}_6=0, P_2+\acute{P}_{14}=0, P_2+\acute{P}_{15}=0, P_3+\acute{P}_{14}=0, P_3+\acute{P}_9=0,$$
$$P_4+\acute{P}_{10}=0, P_5+\acute{P}_{11}=0, P_5+\acute{P}_2=0, P_6+\acute{P}_8=0, P_7+\acute{P}_{12}=0, P_7+\acute{P}_{13}=0,$$
$$P_{14}+\acute{P}_{10}=0, P_9+\acute{P}_{15}=0, P_9+\acute{P}_{16}=0, P_{10}+\acute{P}_{12}=0, P_{11}+\acute{P}_{17}=0,$$
$$P_{11}+\acute{P}_{13}=0, P_8+\acute{P}_{18}=0, P_{12}+\acute{P}_{19}=0, P_{15}+\acute{P}_{18}=0, P_{15}+\acute{P}_{17}=0,$$
$$P_{16}+\acute{P}_{20}=0, P_{16}+\acute{P}_{13}=0, P_{17}+\acute{P}_{20}=0, P_{18}+\acute{P}_{22}=0, P_{19}+\acute{P}_{21}=0,$$
$$P_{18}+\acute{P}_{19}=0, P_{19}+\acute{P}_{20}=0, P_{20}+\acute{P}_{21}=0, P_{22}+\acute{P}_{21}=0, P_{22}+\acute{P}_{19}=0,$$

This concludes a codeword with weight 26. Similar analysis can be done for messages with other weights, which return codewords greater than 20 calculated by $w_{in}=4$. Table 3 gives the minimum weight of the

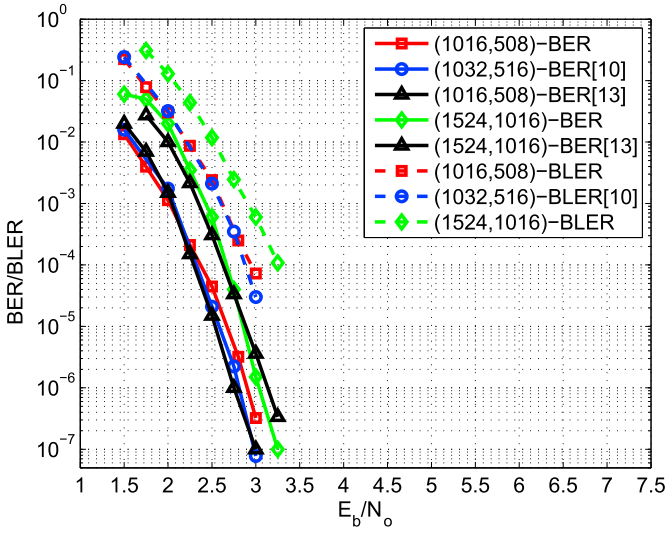

Fig. 4. Performance of QC-LDPC codes with rates $\frac{1}{2}$ and $\frac{2}{3}$.

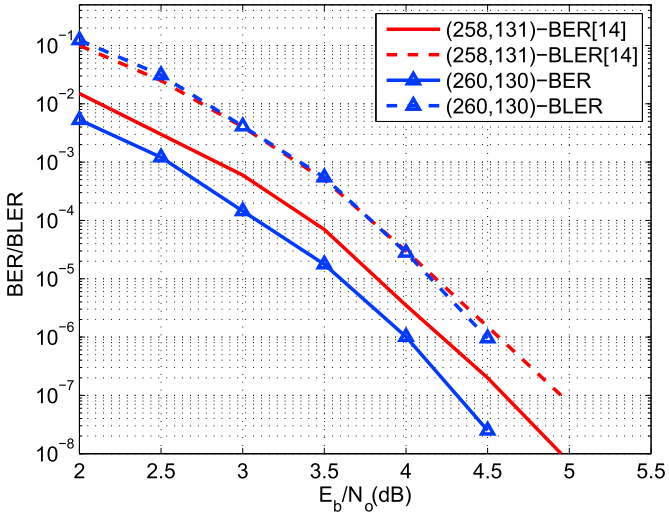

Fig. 5. Performance of (260,130) QC-LDPC code and its comparison with (258,131) QC-LDPC code given in Ref. [14].

half rate (200,100) QC-LDPC code on messages with weight no greater than 6. The initial subsets applied for the construction of circulant matrices are $S_1=\{0,2\}$ and $A_1=\{12\}$. Other subsets with two elements are obtained using $m=3$ and $r=2$. Alternatively, for subsets with one element, $q=2$ and $d=1$ are used. Subset $A_4=\{32\}$ is found by exhaustive search so that it guarantees the existence of no cycle-4 and 6 in the structure of **H**.

4. Simulation results

The performance of different codes constructed by using parity check matrices proposed in Section 2 is verified for the AWGN channel. Codes are modulated by using Binary Phase Shift Keying (BPSK) and decoded by using Sum Product Algorithm (SPA). Maximum 100 iterations are considered for the iterative decoding. Fig. 3 shows the performance of (2280,1710) and (2850,2280) QC-LDPC codes. Both codes demonstrate high error-correcting capability. At $BER=10^{-6}$, they are 1.5 dB away from their Shannon limit. The Block Error Rate (BER) performances of

these codes are very similar to those of other well known codes with the same rate presented in Ref. [11, 12]. This is mainly evident for (2850, 2280) QC-LDPC code as it has a behaviour similar to that of the (4005, 3204) QC-LDPC code, while it is implemented with a shorter length and its error floor occurs at a lower *BER*. The performance of newly designed QC-LDPC codes with rates $\frac{1}{2}$ and $\frac{2}{3}$ is shown in Fig. 4. The codes demonstrate close performance to those presented in Ref. [13], while they do not apply a masking technique to form the girth 8 in the structure of their parity check matrix. Moreover, no error floor is observed for $BER \leq 10^{-5}$.

Fig. 5 shows performance of (260,130) QC-LDPC code. With similar length and rate, this code has a block error rate performance similar to that of the (258,131) QC-LDPC code in Ref. [14]. However, it provides better bit error rate performance. The improvement is observed to be 0.25 dB at $BER = 2{*}10^{-8}$.

5. Conclusion and future work

This paper presented a new scheme of QC-LDPC codes with girth eight. These were mainly designed on the basis of proper definition of subsets in which the difference between elements of a subset is unique. In addition, appropriate conditions were considered to ensure that the parity check matrix of the code is free of cycle six. This provided high-performance codes without utilizing a masking technique. The design of codes with higher girth and an optimum length will be carried out in further research.

References

[1] S. Lin, D. Costello, Error Control Coding: Fundamentals and Applications, Prentice Hall, second ed.
[2] W. Ryan, S. Lin, Channel Codes: Classical and Modern, Cambridge University Press.
[3] Y. Wang, S. Draper, J. Yedidia, Hierarchical and high-girth QC LDPC codes, IEEE Trans. Inf. Theor. 59 (7) (2013) 4553–4582.
[4] J. Zhang, G. Zhang, Deterministic girth-eight QC-LDPC codes with large column weight, IEEE Commun. Lett. 18 (4) (2014) 656–659.
[5] A. Tasdighi, A.H. Banihashemi, M.R. Sadeghi, Symmetrical constructions for regular girth-8 QC-LDPC codes, IEEE Trans. Commun. 14 (8) (2016) 1–9.
[6] H. Fujisawa, S. Sakata, A class of Quasi-Cyclic regular LDPC codes from cyclic difference families with girth 8, in: International Symp.on Information Theory, 2005, pp. 2290–2294.
[7] C. Chen, B. Bai, X. Wang, Construction of nonbinary quasicyclic LDPC cycle codes based on singer perfect difference set, IEEE Commun. Lett. 14 (2) (2010) 181–183.
[8] M. Gholami, M. Samadieh, Design of binary and nonbinary codes from lifting of girth-8 cycle codes with minimum lengths, IEEE Commun. Lett. 17 (4) (2014) 777–780.
[9] S. Vafi, N. Majid, A new scheme of high performance quasi-cyclic LDPC codes with girth 6, IEEE Commun. Lett. 19 (10) (2015) 1666–1669.
[10] S. Vafi, N. Majid, Half rate quasi cyclic low density parity check codes based on combinatorial designs, J. Comput. Commun. 04 (1) (2016) 39–49.
[11] I. standard for broadband wireless metropolitan area networks, Air interface for broadband wireless access systems, IEEE std 802.16.
[12] I. Bocharova, F. Hug, R. Johannesson, B.D. Kudryashov, High-rate QC LDPC codes of short and moderate length with good girth profile, in: c7th International Symposium on Turbo Codes and Iterative Information Processing (ISTC), 2012, pp. 150–154.
[13] J. Li, K. Liu, S. Lin, K. Abdel-Ghaffar, Algebraic Quasi-Cyclic LDPC codes: construction, low error-floor, large girth and a reduced-complexity decoding scheme, IEEE Trans. Commun. 62 (4) (2014) 2626–2637.
[14] C. Sun, H. Xu, D. Feng, B. Bai, Non-isomorphic (3,L) Quasi-Cyclic LDPC codes: simplified exhaustive search and designs, in: 9th International Symposium on Turbo Codes and Iterative Information Processing (ISTC), 2016, pp. 271–275.