Double Cylinder Cycle codes of Arbitrary Girth

Mehdi Samadieh* and Mohammad Gholami†

March 5, 2014

Abstract

A particular class of low-density parity-check codes referred to as cylinder-type BC-LDPC codes is proposed by Gholami and Eesmaeili. In this paper we represent a double cylinder-type parity-check matrix $H$ by a graph called the block-structure graph of $H$ and denoted by $\text{BSG}(H)$. Using the properties of $\text{BSG}(H)$ we propose some mother matrices with column-weight two such that the rate of corresponding cycle codes are greater than cycle codes constructed by Gholami with same girth.

Keywords: LDPC codes, tanner graph, girth, closed walk.

1 Introduction

Low-density parity-check (LDPC) codes are a class of linear block codes represented by sparse parity-check matrices [2], capable of performing very close to the Shannon capacity limits when they are decoded under simple iterative decoders [3], [4], such as Sum-product algorithm [5]. LDPC codes can be constructed into two methods: random codes [3]-[6] and structured codes [7]-[8]. Quasi-cyclic(QC) LDPC codes are the most promising class of structured LDPC codes due to their ease of implementation and excellent performance over noisy channels when decoded with message-passing algorithms as extensive simulation studies have shown. Compared with randomly constructed codes, QC-LDPC codes can be encoded in linear time with shift registers and require small memory space to store the code graphs for decoding. LDPC codes are specified by a sparse parity check matrix and its corresponding Tanner graph [7].

*Corresponding author: Mehdi Samadieh is the Researcher of Isfahan Mathematics House, Isfahan, IRAN, e-mail: samadieh.m@gmail.com, m.samadieh@mathhouse.org
†Mohammad Gholami is with the Department of Mathematics, Shahrekord University, 115, Shahrekord, IRAN, e-mail: gholami-m@sci.sku.ac.ir, gholamimoh@gmail.com.
Tanner determined a lower bound on the minimum distance that grows exponentially with the girth of the code. The extension of LDPC codes to non-binary Galois field GF(q) was first investigated empirically by Davey and MacKay over the binary-input AWGN channel [9].

Cycle codes [10] are a special class of binary LDPC codes with the property that each column of the parity-check matrix contains exactly two nonzero elements. Gallager [1] has shown that the minimum distance of cycle codes increases logarithmically with code length, while this increment is linear for the codes with column-weight greater than two. In spite of this weakness which causes to have poor performance, cycle codes have their own advantages: 1) Their encoding and decoding operations have lower computation and storage complexity, 2) They have better block error statistics when applied on partial response channels [11]-[12], 3) Non-binary cycle codes are among the most promising non-binary codes and for q = 64, 128, 256, the best q-ary LDPC codes decoded with belief propagation (BP) algorithm are cycle codes [13]-[14]. This makes non-binary cycle codes good candidates for both optimum maximum likelihood (ML) and iterative decoding, 4) Compared with other LDPC codes, the girth of the Tanner graph plays more important roles for cycle codes [15, 16], since it affects not only the message dependence of iterative decoding but also the minimum distance of the code [14].

Accordingly we propose a new method to construct mother matrices in order to construction of cycle codes with high girts and various lengths.

2 Preliminaries and Notations

A graph $G$ is a triple consisting of a vertex set $V(G)$, an edge set $E(G)$, and a relation of incidence that associates with each edge two vertices (not necessarily distinct), called its endpoints.

A bipartite graph is a graph $G = (V, E)$ that $V$ can be divided into two disjoint sets $A$ and $B$, such that every edge $e \in E$ connects a vertex in $A$ to one in $B$.

A length-$l$ walk is a successive series of edges $e_i$ and vertices $v_j$, such as $v_1e_1v_2e_2\cdots v_le_lv_{l+1}$, forming a continuous curve, i.e. each $e_i$ connects $v_i$ to $v_{i+1}$. A walk is closed if the initial and
terminal vertices be same, i.e. \( v_1 = v_{l+1} \). A closed walk where the only end vertices are the same is a \textit{cycle}, i.e. \( v_i \neq v_j \) for each \( 1 \leq i < j \leq l+1 \) except \( i = 1, j = l+1 \). Also the \textit{girth} of a graph can be defined as the length of the shortest cycle.

To the LDPC code with the parity-check matrix \( H \), we can associate a graph referred to as its \textit{Tanner graph} (TG), which is a bipartite graph where the two disjoint sets collect the check nodes and the bit nodes associated to the rows and columns of \( H \), respectively. An edge connects a check node to a bit node if a nonzero entry exists in the intersection of the corresponding row and column of \( H \).

Let \( m, s \) be nonnegative integers with \( 0 \leq s \leq m - 1 \). The \( m \times m \) circulant permutation matrix shifted by \( s \), \( I_m^s \), is the matrix obtained from \( m \times m \) identity matrix \( I_m \) by shifting rows \( s \) positions to the bottom, that is \( I_m^s = (e_{i,j})_{m \times m} \) where \( e_{i,j} = 1 \), if \( i - j = s \mod m \); and \( e_{i,j} = 0 \), otherwise. It is clear that \( I_m^0 = I \). For simplicity, \( I_m^s \) is denoted by \( I^s \) when \( m \) is known.

The definition of block-structure graph, given in [1], is as the following.

\section*{2.1 Block-Structure Graph}

Let \( m, b \) and \( \gamma \) be some positive integers and \( b < \gamma \). Let \( H = (H_{i,j})_{b \times \gamma} \), where each \( H_{i,j} \) is a \( m \times m \) circulant permutation matrix or the \( m \times m \) zero matrix. Considering \( H \) as a \( b \times \gamma \) matrix with \( m \times m \) entries, we refer to \( H \) as a matrix having \( b \) block-rows and \( \gamma \) block-columns. For simplicity, the matrix \( H \) and the quasi-cyclic LDPC code with the parity-check matrix \( H \) are called as \( m \)--circulant matrix and \( m \)--circulant code, respectively. Then we can define the block-structure graph associated to \( H \), denoted by \( \text{BSG}(H) \), as the following:

\textbf{Definition 2.1} Let \( G \) be a graph with the vertex set \( V(G) = \{v_1, v_2, ..., v_b\} \), where \( v_i \) represents the \( i \)th block-row of \( H \). For each \( i, j \in \{1, \ldots, b\} \) and \( k \in \{1, \ldots, \gamma\} \), where \( H_{i,k} = I_{s_1}^i \) and \( H_{j,k} = I_{s_2}^j \) for some \( 0 \leq s_1, s_2 \leq m - 1 \), two vertices \( v_i, v_j \in V \) are joined by two directed edges labeled with \((k, s)\), from \( v_i \) to \( v_j \), and \((k, s')\), from \( v_j \) to \( v_i \), where \( s = -s' = s_2 - s_1 \mod m \). For each edge of \( G \), the first and second component of its label \((k, s)\) are referred to as the \textit{column}
index and slope of that edge, respectively. The resulting graph $G$ is called the block-structure graph of $H$, and is denoted by $\text{BSG}(H)$.

**Definition 2.2** Let $G$ be $\text{BSG}(H)$, where $H$ is a $m$-circulant matrix. A length-$l$ closed walk in $G$ is given by a sequence of vertices $v_{i_1}, v_{i_2}, \ldots, v_{i_l}, v_{i_{l+1}}$, where $i_{l+1} = i_1$, with edges $e_1, e_2, \ldots, e_l$ such that for each $1 \leq j \leq l$ edge $e_j$ connect vertex $v_{i_j}$ to vertex $v_{i_{j+1}}$ and if $(k_j, s_j)$ denotes the label $e_j$ from $v_{i_j}$ to vertex $v_{i_{j+1}}$ then the following conditions are hold:

1. Each edge $e_j$ in the sequence $e_1, e_2, \ldots, e_l$ is repeated at most $m$ times;

2. For each $1 \leq j \leq l$, $k_j \neq k_{j+1}$, where $k_{l+1} := k_1$, i.e. the index columns of successive edges are different;

3. $\sum_{j=1}^{l} s_j \equiv 0 \pmod{m}$, i.e. the sum of slopes of edges are zero in modulus of $m$.

For simplicity, we can show this length-$l$ closed walk, or briefly $l$ closed walk, in $G$ with the following chain:

$$v_{i_1} \xrightarrow{(k_1, s_1)} v_{i_2} \xrightarrow{(k_2, s_2)} v_{i_3} \ldots \xrightarrow{(k_{l-1}, s_{l-1})} v_{i_l} \xrightarrow{(k_1, s_l)} v_{i_1}.$$ 

**Definition 2.3** Let $a, b$ and $c$ be some non-negative integers such that $a \geq 2$, $b \geq 1$ and $c \geq 0$. By $(a, b, c)$-double-cylinder LDPC (DC-LDPC) codes, we mean QC LDPC codes having the
Figure 1: a) Overall diagram of BSG($H(a, b, c)$) b) BSG($H(3, 2, 2)$) of Example 2.4.

Mother matrix $H(a, b, c)$ as follows:

$$H(a, b, c) = egin{pmatrix}
1 & \cdots & 1 & 1 & 1 & 1 & \cdots & 1
\end{pmatrix}$$

Where, the number of blocks $\begin{bmatrix} 1 & 1 \\ \end{bmatrix}$ between each two consecutive blocks $\mathcal{I} + \mathcal{I}^1$ is exactly $c$, and the number of blocks $\mathcal{I} + \mathcal{I}^1$ in $H(a, b, c)$ is $b$.

In fact, $H(a, b, c) = (h_{i,j})$ is a $(a + c - 1)b \times (a + c)b$ binary matrix, where $h_{i,j} = 1$, if and only if one of two following conditions is hold:

1. $\lfloor \frac{i-1}{a+c-1} \rfloor = \lfloor \frac{j-1}{a+c} \rfloor$, and if $i1 = i - 1 \mod (a + c - 1)$, and $j1 = j - 1 \mod (a + c)$, then one of the following conditions is hold:
(a) $i1 < a$, $j1 < a$ and $i1 - j1 \equiv 0, 1$.

(b) $i1 \geq a - 1$, $j1 \geq a$ and $j1 - i1 = 0, 1$.

2. $i = (a + c - 1) \times k + 1 \pmod{(a + c - 1) \times b}$, $j = (a + c) \times k$, for some $1 \leq k \leq b$.

So, the design rate of the cycle code with the parity-check matrix $H(a, b, c)$ is $\mathcal{R} = 1 - \frac{(a+c-1)b}{(a+c)b} = \frac{1}{a+c}$; whereas the following lemma states the the maximum-achievable girth $g_{\text{max}}$ of QC LDPC codes having the mother matrix $H(a, b, c)$, for $b$ large enough, is $8(a + c)$. This shows that larger rates yields more less maximum-achievable girths.

**Example 2.4** Let $a = 3$ and $b = c = 2$. The parity-check matrix of $H(3, 2, 2)$ is

$$H(3, 2, 2) = \begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}$$

**Theorem 2.5** Let $a \geq 2$, $b \geq 1$ and $c \geq 0$ be some integers and $g_{\text{max}}$ be the maximum achievable girth of QC LDPC codes having mother matrix $H(a, b, c)$. If $b \geq \left\lceil \frac{a+c-1}{c+1} \right\rceil + 2$, then $g_{\text{max}} = 8(c + a)$, else $g_{\text{max}} = 4(bc + b + a - 1)$.

**Proof.** Let $H$ be the $(H(a, b, c))$, as shown in Figure 2.1. Let $P_1$ be the following chain from $v_a$ to itself:

$$v_a \xrightarrow{(a,s_a)} v_1 \xrightarrow{(1,s_1)} v_2 \xrightarrow{(2,s_2)} v_3 \cdots v_{a-1} \xrightarrow{(a-1,s_{a-1})} v_a,$$

$P_2$ be the following chain from $v_a$ to $v_{a+c}$:

$$v_a \xrightarrow{(a+1,s_{a+1})} v_{a+1} \xrightarrow{(a+2,s_{a+2})} v_{a+2} \cdots v_{a+c-1} \xrightarrow{(a+c-1,s_{a+c-1})} v_{a+c},$$

and $P_3$ be the following chain from $v_{a+c}$ to itself:

$$v_{a+c} \xrightarrow{(a+c,s_{a+c})} v_{a+c+1} \cdots v_{2a+c-1} \xrightarrow{(2a+c-1,s_{2a+c-1})} v_{a+c}.$$
It is clear that $P_1$, $P_2$ and $P_3$ have length $a$, $c$ and $a$, respectively. Hence, the chain $P = P_1P_2P_3^{-1}P_2^{-1}P_2^{-1}P_2^{-1}$ is an inevitable walk with length $l(P) = 2l(P_1) + 4l(P_2) + 2l(P_3) = 4(a + c)$ from $v_a$ to itself, which is equivalent to an inevitable length-$8(a + c)$ in the Tanner graph. So, $g_{\text{max}} \leq 8(a + c)$. On the other hand, let $P'_1$ be the chain from $v_1$ to $v_a$ as follows.

$$v_1 \rightarrow (1,s_1) \rightarrow v_2 \rightarrow (2,s_2) \rightarrow v_3 \cdot \cdot \cdot \rightarrow v_{a-1} \rightarrow (a-1,s_{a-1}) \rightarrow v_a,$$

and $P'_i$, $2 \leq i \leq b + 1$, be the following chains from $v_{(i-1)a+(i-2)(c-1)}$ to $v_{ia+(i-1)(c-1)}$:

$$v_{(i-1)a+(i-2)(c-1)} \rightarrow ((i-1)a+(i-2)(c-1)+1,s_{(i-1)a+(i-2)(c-1)+1}) \rightarrow v_{(i-1)a+(i-2)(c-1)+1} \rightarrow \cdots \rightarrow v_{ia+(i-1)(c-1)},$$

where we accept that $v_{(b+1)a+b(c-1)-1} = v_1$ and $v_{(b+1)a+b(c-1)} = v_a$. It is clear that $P'_1$ and $P'_i$, $2 \leq i \leq b + 1$, have length $a - 1$, $c + 1$, respectively. Hence, the chain

$$P' = P'_1P'_2 \cdots P'_{i+1}P'_{b+1}P'_{b+1}^{-1} \cdots P'_{b+1}^{-1}$$

is an inevitable walk with length $l(P') = 2 \sum_{i=1}^{b+1} l(P'_i) = 2((a-1)+b(c+1)) = 2(bc+b+a-1)$ from $v_a$ to itself, which is equivalent to an inevitable length-$4(bc+b+a-1)$ in the Tanner graph. So, $g_{\text{max}} \leq 4(bc+b+a-1)$. However $4(a + c) = l(P) \geq l(P') = 2(bc+b+a-1)$, if and only if $b \geq \frac{a-1}{c+1} + 2$, which is hold iff $b \geq \lceil \frac{a-1}{c+1} \rceil + 2$. □

Figure 2.1 shows maximum-achievable girth for different $a$, $b$ and $c$ values. In the following we propose construction of QC-LDPC codes.

### 2.2 Construction of DC-LDPC codes

Given positive integers $a$, $b$ and $c$, let $H(a,b,c)$ be the parity check matrix of a double-cylinder LDPC (DC-LDPC), by code-generating algorithm given in [?] we can obtain suitable shift sequence values by select an enough large $m$ as size of circulate permutation matrices and in order to construct double-cylinder LDPC (DC-LDPC) code with desire girth. In table some DC-LDPC codes various length $n$ rate $r$ and girth $2g$. 


Figure 2: The maximum-achievable girth of \( DC(a, b, c) \) codes for \( c = 1, 2, 3 \), from left to right, respectively.

References

[1] M. Gholami, and M. Esmaeili, *Maximum-girth Cylinder-type Block-circulant LDPC Codes*, IEEE Trans. on Commun., vol. 60, no. 4, pp. 952–962, April 2012.

[2] R. G. Gallager, “Low-density parity-check codes,” IRE Trans. Inf. Theory, vol. IT-8, no. 1, pp. 21-28, Jan. 1962. D. J. C.

[3] D. J. C. MacKey, “Good error-correcting codes based on very sparse matrices,” IEEE Trans. Inf. Theory, vol. 45, no. 2, pp. 399432, Mar. 1999.

[4] S. Y. Chung, G. D. Forney, T. J. Richardson, and R. L. Urbanke, “On the design of low-density parity-check codes within 0.0045 dB of the Shannon limit,” IEEE Commun. Lett., vol. 5, no. 2, pp. 5860, Feb. 2001.

[5] F. R. Kschischang, B. J. Frey and H. -A. Loeliger, “Factor graphs and the sum-product algorithm,” IEEE TIT: IEEE Trans. on Inf. Theory, vol 47, 2001.

[6] N. Bonello, S. Chen, and L. Hanzo, *Design of low-density parity-check codes*, an overview, IEEE Vehicular Technology Magazine, Dec. 2011.
Table 1: FSS(m, B, S) codes with girth 2g and length n constructed from FSS(v, b, 2)

| m | n | v | B | S | g | 2g |
|---|---|---|---|---|---|---|
| 1/5 | 40 | 30 | 40 | 50 | 12 | 24 |
| 2/5 | 48 | 32 | 48 | 60 | 12 | 24 |
| 3/5 | 56 | 40 | 56 | 70 | 12 | 24 |
| 4/5 | 64 | 48 | 64 | 80 | 12 | 24 |
| 5/5 | 72 | 56 | 72 | 90 | 12 | 24 |

[7] R.M. Tanner, D. Sridhara, A. Sridharan, T.E. Fuja, and D.J. Costello, “LDPC block and convolutional codes based on circulant matrices,” IEEE Trans. Inform. Theory, vol. 50, no. 12, pp. 2966-2984, Dec. 2004.

[8] Sunghwan Kim, Jong-Seon No, Habong Chung, and Dong-Joon Shin, “Quasi-cyclic low-density parity-check codes with girth larger than 12,” IEEE Trans. Inform. Theory, vol. 53, no. 8, pp. 2885-2891, Aug. 2007.

[9] M. C. Davey and D. J. C. MacKay, “Low-density parity check codes over GF(q),” IEEE Commun. Lett., vol. 2, no. 6, pp. 165–167, June 1998.

[10] T. D. Souza, *Cycle Codes*, EPFL / ALGO-LMA, SSC 6th semester, June. 2005.
[11] H. Song, J. Liu, B. V. K. V. Kumar, “Low complexity LDPC codes for magnetic recording,” in IEEE Globecom 2002, Taipei, Taiwan, R.O.C., Nov. 2002.

[12] H. Song, J. Liu, B. V. K. V. Kumar, “Large girth cycle codes for partial response channels,” IEEE Trans. Magn., vol. 40, no. 4, part 2, pp. 3084-3086, 2004.

[13] X.-Y. Hu, and E. Eleftheriou, “Binary representation of cycle Tannergraph codes,” in Proc. IEEE Intern. Conf. on Commun., Paris, France, pp. 528–532, June 2004.

[14] C. Poulliat, M. Fossorier, and D. Declercq, “Design of regular $(2, d_c)$ LDPC codes over $\mathbb{F}_q$ using their binary images,” IEEE Trans. Commun., vol. 56, pp. 1626–1635, Oct. 2008.

[15] M. Esmaeili, and M. Gholami, Geometrically-structured maximum-girth LDPC block and convolutional codes, IEEE journal of selected area of commun., vol. 27, no. 6, Aug. 2009.

[16] M. Esmaeili, and M. Gholami, Maximum-girth Slope-based Quasi-cyclic $(2, k \geq 5)$-LDPC Codes, IET commun., vol. 2, no. 10, Aug. 2008.