Determination of the shortest balanced cycles in QC-LDPC codes Matrix

Gao Xiao. and Zhang Nan
Wuhan Maritime Communication Research Institute
Wuhan, 430079, China
gaoxiao1113@sina.com, nan_zhang313@sina.com

***Abstract*—In this paper, we determinate the shortest balanced cycles of quasi-cyclic low-density parity-check (QC-LDPC) codes. We show the structure of balanced cycles and their necessary and sufficient existence conditions. Furthermore, we determine the shortest matrices of balanced cycle. Finally all nonequivalent minimal matrices of the shortest balanced cycles are presented in this paper.**

***Index Terms*—Girth, quasi-cyclic low-density parity-check (QC-LDPC) codes, balanced cycles.**

I. Introduction

Low-density parity-check (LDPC) codes were first discovered by Gallager [1] and rediscovered by MacKay et al. and Sipser et al.. They have created much interest recently since they are shown to have a remarkable performance with iterative decoding that is very close to the Shannon limit over additive white Gaussian noise (AWGN) channels. Also, LDPC codes possess many advantages including parallelizable decoding, self-error-detection capability by syndrome-check, and an asymptotically better performance than turbo codes, etc.

The performance of LDPC codes of finite length may be strongly affected by their cycle property such as girth and stopping sets, etc. Here the girth is the minimum length of cycles in the Tanner graph of a given parity-check matrix. In most cases, it is difficult to analyze explicitly these factors of randomly constructed LDPC codes and predict their performance. One advantage of quasi-cyclic LDPC (QC-LDPC) codes based on circulant permutation matrices is that it is easier to analyze their code properties than in the case of random LDPC codes. Recently, several coding theorists proposed some classes of QC-LDPC codes with algebraically strong restriction on the structure and analyzed their properties more explicitly [2], [3], [4], [5].

The main contribution of this paper is to analyze balanced cycle properties of QC-LDPC codes and we presented all nonequivalent minimal matrices of the shortest balanced cycles Firstly; we analyze necessary and sufficient existence conditions of balanced cycles. Secondly, we determine the shortest balanced cycle in the QC-LDPC codes matrix. According to our results, we presented all nonequivalent minimal matrices of the shortest balanced cycles

The outline of the paper is as follows. In Section II, we review QC-LDPC codes and introduce some definitions for our presentation. In Section III, we analyze necessary and sufficient existence conditions of balanced cycles. In Section IV, we determine the minimal matrices of balanced cycle. In Section V we determinate the shortest balanced cycles of QC-LDPC codes and we presented all nonequivalent minimal matrices of the shortest balanced cycles. Finally we give concluding remarks in Section VI.

II. QUASI-CYCLIC LDPC CODES

A QC-LDPC code is characterized by the parity-check matrix which consists of small square blocks which are the zero matrix or circulant permutation matrices. Let p be the $L \times L$ permutation matrix given by

$$p = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix} \quad (1)$$

Note that p^i is just the circulant permutation matrix which shifts the identity matrix I to the right by i times for any integer i, $0 \le i < L$ .For simple notation, we denote the zero matrix by p^∞ .Let H be the $mL \times nL$ matrix defined by

$$H = \begin{bmatrix} P^{a_{11}} & P^{a_{12}} & \cdots & P^{a_{1n}} \\ P^{a_{21}} & P^{a_{22}} & \cdots & P^{a_{2n}} \\ \vdots & \vdots & \ddots & \vdots \\ P^{a_{m1}} & P^{a_{m2}} & \cdots & P^{a_{mn}} \end{bmatrix} \quad (2)$$

where $a_{ij} \in \{0, 1, ..., L-1, \infty\}$. From now on, the code C with parity-check matrix H will be referred to as a QC-LDPC code. When H has full rank, then its code rate is given by

Manuscript received April 8, 2011. This work was supported by the National Defense Pre-Research Foundation of Chinese Shipbuilding industry.

F. A. Gao Xiao is with the Wuhan Maritime Communication Research Institute (phone: +86 13986022213; e-mail: gaoxiao1113@ sina.com).

S. B. Zhang Nan is with Wuhan Maritime Communication Research Institute. (e-mail: nan_zhang313@sina.com).

$R=1-m/n$ regardless of its code length $N=nL$. If the locations of 1's in the first row of the i th row block are fixed, then those of the other 1's in the block are uniquely determined. Therefore, the required memory for storing the parity-check matrix of a QC-LDPC code can be reduced by a factor $1/L$, as compared with random LDPC codes.

The QC-LDPC code defined in (2) may be regular or irregular depending on the choice of a_{ij}'s of H. When H has no blocks corresponding to the zero matrix, it is a regular LDPC code with column weight m and row weight n. In this case, its code rate is larger than $1-m/n$ since there are at least $m-1$ linearly dependent rows.

For our presentation we introduce the following Lemmas[7][8][9][11][12][13] [14].

Lemma 1.For $\gamma_1,\gamma_2,\gamma_3\in\Gamma(M)$ with $|\gamma_2|\geq 2$, the sequence $\gamma_1\gamma_2\gamma_3$ is a path if and only if $\gamma_1\gamma_2,\gamma_2\gamma_3$ are paths.

Lemma 2. For $e_0,e_1,e,e'\in E(M)$ with $e_0ee_1\in\Gamma(M)$ and $\left|\sigma(e)\cap\sigma(e')\right|=1$, there are integers v and τ in $\{0,1\}$ such that $d_\tau(e_v)=d_\tau(e)=d_\tau(e')$ and $\sigma(e_{1-v})\cap\sigma(e')=\phi$. In particular, $e_{1-v}ee'$ is a path.

Lemma 3. For $\gamma,\gamma_0,\gamma_1\in\{\phi\}/\Gamma(M)$ with $o(\gamma_0)\neq o(\gamma_1)$ and $|\gamma|>1$, if $\gamma\gamma_0$, $\gamma\gamma_1$ are paths, then $\gamma_0^{-1}\gamma_1$ is a path.

Lemma 4. A path γ is a cycle if and only if $|\gamma|>0$ and $\gamma\in\Gamma(M)$.

Lemma 5. For paths γ,γ' of positive lengths, the sequence $\gamma\gamma'$ is a cycle if and only if $|\gamma|+|\gamma'|$ is even and $\gamma\gamma'\gamma$ is a path.

III. NECESSARY AND SUFFICIENT CONDITIONS FOR THE EXISTENCE OF BALANCED-CYCLES

A cycle $e_1e_2...e_{2k}$ of length $2k$ is called a balanced cycle if for any edge $e\in E(M)$ $|\{i:e_{2i}=e,\quad 1\leq i\leq k\}|$ = $|\{i:e_{2i+1}=e,\quad 1\leq i\leq k\}|$ Clearly, in a balanced cycle the number of occurrences of any edge is even. Hence, the length of a balanced cycle is at least twice the number of the distinct edges on the cycle. If M has at least one balanced cycle, the length of the shortest balanced cycles of M is called the $B-girth$ of M, and denoted by $g_B(M)$. If M has no balanced cycle, we say that the $B-girth$ of M is $g_B(M)=\infty$. It is well known that the $B-girth$ of any matrix is not smaller than 12. In particular, the $B-girth$ of M is equal to 12 if and only if the all-one 2×3(or 3×2)matrix is a sub-matrix of M.

For the existence of balanced cycles, The following two lemmas are refinements of Conclusions given in [19,20].

Lemma 6.If γ_1, γ_2 and γ_3 are paths of positive lengths such that $\gamma_1\gamma_2^{-1}$, $\gamma_2\gamma_3^{-1}$ and $\gamma_3\gamma_1^{-1}$ are cycles ,then

$$C=\gamma_1\gamma_2^{-1}\gamma_2\gamma_3^{-1}\gamma_3\gamma_1^{-1} \tag{3}$$

is a balanced cycle of length $2(|\gamma_1|+|\gamma_2|+|\gamma_3|)$. The balanced cycle given by(3) will be called a $(|\gamma_1|,|\gamma_2|,|\gamma_3|)_1$-cycle formed by γ_1, γ_2 and γ_3.

Lemma 7.If $C_1\gamma_0C_2$ is a path, where C_1, C_2 are two cycles without common edges and $\gamma_0=\phi$ or $\gamma_0\neq\phi$ with $o(\gamma_0)\not\subset C_1$ and $t(\gamma_0)\not\subset C_2$,then

$$C=C_1\gamma_0C_2\gamma_0^{-1}C_1^{-1}\gamma_0C_2^{-1}\gamma_0^{-1} \tag{4}$$

is a balanced cycle of length $2(|C_1|+|C_2|)+4\gamma_0$. The balanced cycle given by(4)

will be called a $(|C_1|,|C_2|,|\gamma_0|)_2$ -cycle formed by C_1, C_2 and γ_0.

Theorem 1. If there is at least one cycle $C\in\Theta(M)$ which is not multiple of any simple cycle, then at least one of the following conditions is valid:

1. $\Gamma(M)$ has three acyclic paths γ_1, γ_2, γ_3 such that $\gamma_1\gamma_2^{-1}$, $\gamma_2\gamma_3^{-1}$ and $\gamma_3\gamma_1^{-1}$ are simple cycles.
2. $\Gamma(M)$ has two simple cycles C_1, C_2 and a path γ_0 such that $\gamma_1\gamma_0\gamma_2^{-1}$ is an acyclic path, where, for $i=1,\ 2,$ the path γ_i satisfies $C_i=o(C_i)\gamma_i$.

Now we show some necessary and sufficient conditions for the existence of balanced cycles.

Theorem 2. For any binary matrix M, the followings are equivalent

1. The B-girth of M is finite.
2. There is a cycle which is not a multiple of any simple cycle.
3. There are two connected simple cycles which are not equivalent.
4. There are an acyclic path γ and two different edges f_1, f_2 such that $f_1\gamma$ and γf_2 are cyclic paths.

Proof. "1 $\Longrightarrow$ 2" is obvious.

"2 $\Longrightarrow$ 1" follows from Theorem 1, Lemma 6 and 7.

"2 $\Longrightarrow$ 3" follows from Theorem 1.

"3 $\Longrightarrow$ 1": Assume that there are two connected simple cycles C_0 and C_1 which are not equivalent. If C_0 and C_1 have no common edge, according to Lemma 7, there is a balanced cycle. Now we assume C_0 and C_1 have some common edges, let γ be one of the longest paths such that $\gamma\subseteq C_0$ and $\gamma\subseteq C_1$. For

$i = 0$, 1, let γ_i be the path such that $\gamma^{-1}\gamma_i$ is a cycle equivalent to C_i. Clearly, $|\gamma_0|$ and $|\gamma_1|$ are positive integers with the same parity. If $|\gamma_0| = |\gamma_1| = 1$, then we must have $\sigma(\gamma_0) = \sigma(\gamma_1)$ and thus $\gamma_0 = \gamma_1$. Therefore, C_0 and C_1 are equivalent, contradicts our assumption. Hence, at least one of $|\gamma_0| > 1$ and $|\gamma_1| > 1$ is valid.

If $|\gamma| = 1$, from $\gamma_i\gamma^{-1}\gamma_i \in \Gamma(M)$ for $i = 0$, 1 and Lemma 3, we see that $\gamma_0\gamma_1^{-1}$, $\gamma_0^{-1}\gamma_1$, $\gamma_1\gamma_0^{-1}$ and $\gamma_1^{-1}\gamma_0$ are paths. Then, according to Lemmas 1 and 5, we see $\gamma_0\gamma_1^{-1}$ is a cycle. Thus, according to Lemma 6, there is a balanced cycle.

If $|\gamma| = 1$, then $|\gamma_i| > 1$ for $i = 0$, 1. From $\gamma_i\gamma^{-1}\gamma_i \in \Gamma(M)$ for $i = 0$, Lemma 1 and Lemma 2, we have either $\gamma_0\gamma_1^{-1}, \gamma_1^{-1}\gamma_0 \in \Gamma(M)$ or $\gamma_0\gamma_1, \gamma_1\gamma_0 \in \Gamma(M)$. Then, according to Lemmas 1 and 5, we see that either $\gamma_0\gamma_1^{-1}$ or $\gamma_0\gamma_1$ is a cycle. Thus, according to Lemma 6, there is a balanced cycle.

"2 $\Rightarrow$ 4": Assume that there is a cycle which is not a multiple of any simple cycle. If the condition 1 of Theorem 1 is valid, let γ_1' and γ_3' be the paths such that $\gamma_1 = o(\gamma_1)\gamma'$ and $\gamma_3 = \gamma_3 t(\gamma_3)$. Then, $\gamma = \gamma_1'\gamma_2^{-1}\gamma_3'$ is the desired path. If the condition 2 of Theorem 1 is valid, $\gamma = \gamma_1\gamma_0\gamma_2^{-1}$ is the desired path.

"4 $\Rightarrow$ 3": Assume that there are an acyclic path $\gamma' = e_1e_2\ldots e_k$ of length k and two different edges f_1, f_2 such that $f_1\gamma$ and γf_2 are cyclic paths. Let i be the smallest number such that $i > 1$ and $\sigma(e_1) \cap \sigma(f_1) \neq \phi$. Let j be the largest number such that $j < k$ and $\sigma(e_j) \cap \sigma(f_2) \neq \phi$. Clearly, $C_1 = f_1e_1e_2\ldots e_i$ and $C_2 = e_je_{j-1}\ldots e_kf_2$ are two connected simple cycles. Since f_1 is not on C_2, we see that C_1 and C_2 are not equivalent.

IV. Determination of Minimal Matrices of Balanced Cycles

A matrix W with $g_B(W) < \infty$ is said BC-minimal if $g_B(W') < \infty$ holds for any submatrix W' of W with $W' \neq W$. A matrix W with $g_B(W) < \infty$ is said B_C^*-minimal if any matrix R covered by W with $g_B(R) < \infty$ implies R = W.

Lemma 8. For integers a, b, c with

$$\min\{a,b\} \geq 2, \tag{5}$$

$$\max\{a,b\} \leq \lfloor (a+b+c-1)/2 \rfloor, \tag{6}$$

we define a matrix $S(a,b,c) = (s_{i,j})$ as the following:

1. If $a+b+c = 2n+1$ is odd, $S(a,b,c)$ is an n × n matrix and

$$s_{i,j} = \begin{cases} 1, & \text{if } 0 \leq j-i \leq 1 \text{ or } (i,j) \in \{(a,1),(n,n+1-b)\}; \\ 0, & \text{otherwise.} \end{cases} \tag{7}$$

2. If $a+b+c = 2n+2$ is even, $S(a,b,c)$ is an n × (n + 1) matrix and

$$s_{i,j} = \begin{cases} 1, & \text{if } 0 \leq j-i \leq 1 \text{ or } (i,j) \in \{(a,1),(n+1-b,n+1)\}; \\ 0, & \text{otherwise} \end{cases} \tag{8}$$

then $S(a,b,c)$ is B_C^*-minimal and its B-girth is equal to

$$s(a,b,c) = \begin{cases} 4c, & \text{if } a+b < c; \\ 2(a+b+c), & \text{otherwise.} \end{cases} \tag{9}$$

Lemma 9. For any integers a, b, c with (5) and (6), we have

$$S(a,b,c) \equiv S(b,a,c). \tag{10}$$

If the inequality $a+b > c$ is satisfied further, or equivalently, the integers a, b, c satisfy (5) and

$$\max\{a,b,c\} \leq \lfloor (a+b+c-1)/2 \rfloor, \tag{11}$$

then for any permutation (x,y,z) of (a,b,c), we have

$$S(x,y,z) \equiv S(b,a,c). \tag{12}$$

Proof. For any $n \times m$ matrix W and integer i_1, i_2, j_1, j_2 with $1 \leq i_1 \leq i_2 \leq n$ and $1 \leq j_1 \leq j_2 \leq m$, let W_{i_1,i_2,j_1,j_2} denote the matrix obtained from W by exchanging the (i_1+l)-th and (i_2-l)-th rows for $0 \leq l \leq \lfloor (i_2-i_1)/2 \rfloor$ while exchanging the (j_1+k)-th and (j_2-k)-th columns for $0 \leq k \leq \lfloor (j_2-j_1)/2 \rfloor$. Let $n = \lfloor (a+b+c-1)/2 \rfloor$. Clearly, $a+b+c \in \{2n+1, 2n+2\}$.

If $a+b+c = 2n+2$, then $S(a,b,c) = S(a,b,c)_{1,n;1,n+1}$. If $a+b+c = 2n+1$, then

$S(a,b,c)^T = S(a,b,c)_{1,n;1,n}$, where T denotes the transpose. Hence, we have (10).

Now we assume the integers a, b, c satisfies (5) and (11).. Hence, we have $S(a,c,b) = S(a,b,c)_{1,a-1;1,a}$ and $S(a,c,b) \equiv S(a,b,c)$. Therefore, for any permutation (x,y,z) of (a,b,c), (12) follows from (10).

The following lemma is a simple corollary of Theorem 2.

Lemma 10. Let W be a B_C^*-minimal matrix. There must exist integers a, b, c with

(5) and (6) such that $W \equiv S(a,b,c)$.

Proof. Let $W = (w_{i,j})$ be a B_C^*-minimal matrix. According to Theorem 2, there are an acyclic path γ and two different edges f_1, f_2 such that $f_1\gamma$ and γf_2 are cyclic paths.

If $|\gamma| = 2n$ is even, without loss of generality, we assume that the path γ corresponds the elements $W_{1,1}$. $W_{1,2}$. $W_{2,2}$.

$W_{2,3}$. … $W_{n,n}$.. Clearly, there are integers a, b with 2≤ a, b≤ n such that f1, f2 correspond $W_{a,1}$. $W_{n+1-b,n+1}$., respectively. Let c = 2n + 2 - a - b. Then, the integers a, b, c satisfy (5) and (6), and $W = S(a,b,c)$.

If |γ| = 2n - 1 is odd, without loss of generality, we assume that the path γ corresponds the elements $W_{1,1}$. $W_{1,2}$. $W_{2,2}$. $W_{2,3}$. … $W_{n,n}$. Clearly, there are integers a, b with 2≤ a, b≤ n and a + b<2n such that f1, f2 correspond wa,1, wn,n+1 - b, respectively. Let c = 2n + 1 - a - b. Then, the integers a, b, c satisfy (5) and (6), and $W = S(a,b,c)$.

From Lemmas 8, 9 and 10, one can show the following corollary easily.

Corollary 1. Let k be an integer with k≥ 3.

1. Any B_C^* -minimal matrix W with $g_B(W) = 4k+2$ is equivalent to a matrix $S(a,b,c)$ with

$2 \le a \le b \le c \le a+b$

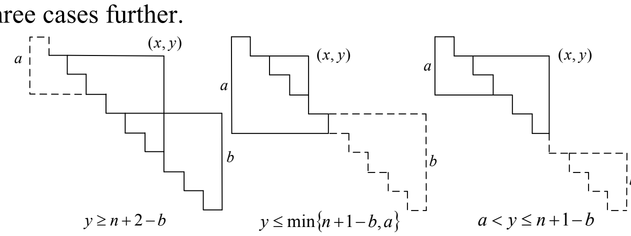
and $a+b+c = 2k+1$

2. Any B_C^* -minimal matrix W with $g_B(W) = 4k$ is equivalent to a matrix $S(a,b,c)$ and $a+b+c = 2k+1$,or with $2 \le a \le b$ and $a+b < k = c$

Theorem 3.Let M be a matrix with $g_B(W) < \infty$ .If R is a B_C^* -minimal matrix covered by M with the least B -girth, then R must be a sub-matrix of M .

Proof. Assume that W is the least sub-matrix of M which covers R .Clearly, the numbers of rows and columns of W are equal to those of R , respectively. According to Lemmas 9 and 10,without loss of generality, we assume that $R = S(a,b,c)$ with $2 \le a \le b \le c$ .Now we want to prove that $W = R$ .If this is not true, let (x, y) be a position of R where the elements of R and W are different. We will show that W must cover a B_C^* -minimal matrix whose B -girth is smaller that $S(a,b,c) = g_B(R)$,which is in conflict with the assumption. This can be realized by distinguishing four cases.

Case 1: $a+b+c = 2n+2$ .Without loss of generality, we assume that $y > x+1$ .As depicted in Figure .4,we distinguish three cases further.



Case $a+b+c = 2n+2$ and $y > x+1$

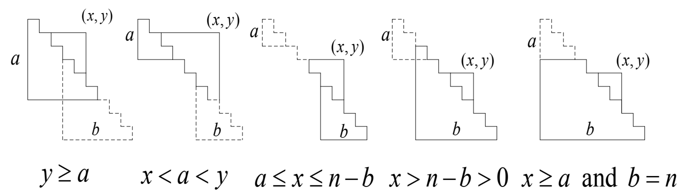
.Case 1.1: $y \ge n+2-b$ .W must cover a matrix which is equivalent to $S(y-x, b, 2n+3-x-y-b)$ whose B -girth is $2(2n+3-2x) < 4n+4 \le s(a,b,c)$.

Case 1.2: $y \le \min\{n+1-b, a\}$ .W must cover a matrix which is equivalent to $S(a, y-x, a+1-y+x)$ whose B -girth is $2(2a+1) < 4n+4 \le s(a,b,c)$.

Case 1.3: $a < y \le n+1-b$ .W must cover a matrix which is equivalent to $S(a, y-x, y+x-a)$ whose B -girth is

$$\begin{cases} 4y & \text{if x} \le \text{a} \\ 4(y+x-a), & \text{otherwise} \end{cases} < 4(2n+2-a-b) = s(a,b,c)$$

Case 2: $a+b+c = 2n+1$ and $y > x+1$ .Clearly, $a < n$ .As depicted in Figure 5, we distinguish five cases further.



Case $a+b+c = 2n+1$ and $y > x+1$

Case 2.1: y≤ a. W must cover a matrix which is equivalent to $S(a, y-x, a+1+x-y)$ whose B-girth is $2(2a+1) < 4n+2 \le s(a,b,c)$.

Case 2.2: x < a < y. W must cover a matrix which is equivalent to $S(a, y-x, y+x-a)$ whose B-girth is $4y < 4n+2 \le s(a,b,c)$.

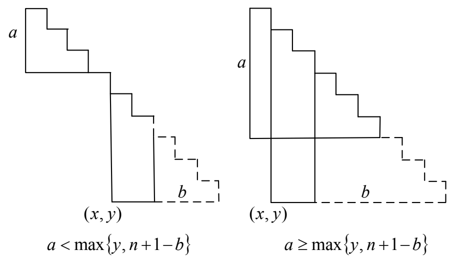
Case 2.3: a≤ x≤ n - b. W must cover a matrix which is equivalent to $S(b, y-x, 2n+2-b-y-x)$ whose B-girth is

$$\begin{cases} 2(2n+2-2x), & \text{if } y > n-b \\ 4(2n+2-b-y-x), & \text{otherwise} \end{cases}.$$
$$\le 4(2n+1-a-b) = s(a,b,c).$$

Case 2.4: x > n - b > 0. W must cover a matrix which is equivalent to $S(b, y-x, b+1+x-y)$ whose B-girth is $2(2b+1) \le 2(2(n-1)+1) < 4n+2 \le s(a,b,c)$.

Case 2.5: x≥ a and b = n. W must cover a matrix which is equivalent to $S(n+1-a, y-x, n+2-a+x-y)$ whose B-girth is $2(2(n+1-a)+1) \le 2(2n+1) < 4n+2 \le s(a,b,c)$.

Case 3: a + b + c = 2n + 1 and y < x = n. Let d = max{y, n + 1 - b} and e =min{y, n + 1 - b}. Clearly, a < n and d < n. As depicted in Figure 5, we distinguish two cases further.



Case $a+b+c=2n+1$ and $y<x=n$

Case 3.1: a < d. W must cover a matrix which is equivalent to $S(a, d-e+1, d+e-a)$

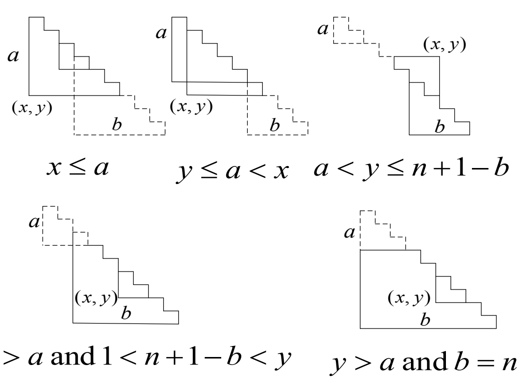
whose B-girth is

$$\begin{aligned}
&S(a, d-e+1, d+e-a) \\
&< S(a, n-e+1, n+e-a) \\
&\leq S(a, b, 2n+1-b-a) = s(a,b,c).
\end{aligned}$$

where, the first inequality is obtained by using n > d and the second inequality is obtained by using n - e + 1 = n + 1 - min{y, n + 1 - b}≥ b.

Case 3.2: a≥ d. W must cover a matrix which is equivalent to $S(a, d-e+1, a+e-d+1)$ whose B-girth is $4a+4 \leq 4n < 4n+2 \leq s(a,b,c)$.

Case 4: a + b + c = 2n + 1 and y < x < n. Clearly, a < n. As depicted in Figure 7, we distinguish five cases further



Case $a+b+c=2n+1$ and $y > x+1$

Case 4.1: x≤ a. W must cover a matrix which is equivalent to $S(a, x-y+1, a-x+y)$ whose B-girth is $2(2a+1) \leq 4n-2 < 4n+2 \leq s(a,b,c)$.

Case 4.2: y≤ a < x. W must cover a matrix which is equivalent to $S(a, x-y+1, y+x-a)$ whose B-girth is $2(2x+1) \leq 4n-2 < 4n+2 \leq s(a,b,c)$.

Case 4.3: a < y ≤ n + 1 - b. W must cover a matrix which is equivalent to $S(x-y+1, b, 2n+2-y-x-b)$ whose B-girth is $2(2n+3-2y) \leq 4n-6 < 4n+2 \leq s(a,b,c)$.

Case 4.4: y > a and 1 < n + 1 - b < y. W must cover a matrix which is equivalent to $S(x-y+1, b, b-x+y)$ whose B-girth is $2(2b+1) \leq 4n-2 < 4n+2 \leq s(a,b,c)$.

Case 4.5: y > a and b = n. W must cover a matrix which is equivalent to $S(x-y+1, n-a+1, n-a-x+y+1)$ whose B-girth is $2(2n-2a+3) \leq 4n-2 < 4n+2 \leq s(a,b,c)$.

V. Determination of the Shortest Balanced Cycles

If a balanced cycle does not contain shorter balanced cycles, it incidence matrix is said B-minimal in this paper. In [8], all the B-minimal matrices whose shortest balanced cycles are of length not exceeding 20 have been determined by an exhaustive search. Since any B_C^*-minimal matrix must be B-minimal, according to Lemmas 9, 10 and the following theorem, we see that a binary matrix is B-minimal if and only if it is equivalent to a matrix of form $S(a,b,c)$. Hence, all the B-minimal matrices are determined in this dissertation.

Theorem 4. Any B_C-minimal matrix is B_C^*-minimal.

Proof. Assume in contrary that W is not a B_C^*-minimal matrix. Let $C_1, C_2, \cdots, C_k$ be the longest list of simple cycles in $\Theta(W)$ with $C_i \neq C_j$ for $1 \leq i \leq j \leq k$. Then, $k \geq 3$ and, for any B_C^*-minimal matrix R covered by W,

$$g_B(R) \geq g_B(W) \geq 2|E(W)| \qquad (13)$$

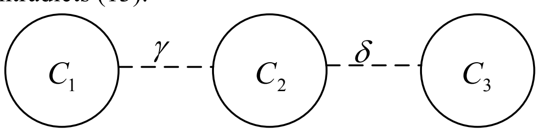
If C_i, C_j have some overlaps for some integers i, j with $1 \leq i < j \leq k$, without loss of generality, we assume that C_1, C_2 have some overlaps and

$$|C_1| + |C_2| - l_{1,2} = \min_{i \neq j, l_{i,j} > 0} (|C_i| + |C_j| - l_{i,j}), \qquad (14)$$

where $l_{i,j}$ is the number of common edges of C_i and C_j. Let γ be one of the longest paths consisting of the common edges of C_1 and C_2. Without loss of generality, we assume that $C_1 = \gamma\delta$ and $C_1 = \gamma\beta$. According to Lemmas 3 and 4, we see that $\gamma\beta^{-1}$ is a cycle. Clearly, there are paths $\delta_1, \delta_2, \beta_1, \beta_2$ with $\delta = \delta_1\delta_2$, $\beta = \beta_1\beta_2$ such that $\delta_1\beta_1^{-1}$ 1is a simple cycle. Then, $\min\{|\delta_1|, |\beta_1|\} > 0$ and $\gamma\delta_1\beta_2$ is also a simple cycle. If $\max\{|\delta_2|, |\beta_2|\} > 0$, then we must have $\delta_2 = \beta_2$. Let i be the integer such that $C_i \equiv \gamma\delta_1\beta_2$. Then, $i \notin \{1,2\}$ and $|C_1| + |C_j| - l_{1,j} = |C_1| + |C_2| - l_{1,2} - |\beta_1|$, contradicts $|\beta_1| > 0$ and (14). Hence, $\delta_1 = \delta$, $\beta_1 = \beta$ and thus the paths $\gamma^{-1}, \delta, \beta$ correspond a B_C^*-minimal matrix R which is covered by W. Since W is not B_C^*-minimal, we see $W \neq R$ and $|E(W)| > |E(R)| = |\gamma| + |\delta| + |\beta|$ Hence, $g_B(W) \le g_B(R) = 2(|\gamma| + |\delta + |\beta||) < 2|E(W)|$,contradicts (13).

Now we assume that C_i, C_j have no overlaps for any integers i, j with $1 \le i < j \le k$.

If there are three simple cycles, say C_1, C_2, C_3 , which are connected by γ and δ in series as depicted as in Figure 5. From the former two cycles, we get a $(|C_1|,|C_2|,|\gamma|)_2$ - cycle and thus $g_B(W) \le 2(|C_1| + |C_2|) + 4|\gamma|$. Similarly, one can get $g_B(W) \le 2(|C_2| + |C_3|) + 4\delta$. Hence, $g_B(W) \le |C_1| + |C_3| + 2|C_2| + 2|\gamma| + 2|\delta| < 2|E(W)|$, contradicts (13).



Three simple cycle are connected in series.

Hence, the simple cycles $C_1, C_2, \cdots, C_k$ are connected by a tree.

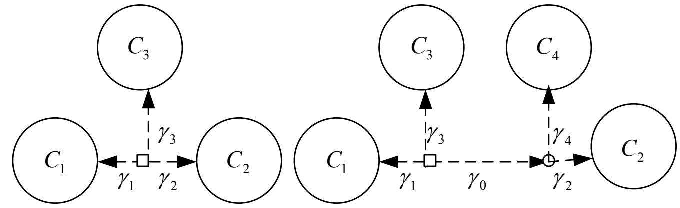
If $k = 3$, then all the edges in $T(W)$ are depicted in (a) of Figure 9. Clearly, $\gamma_1^{-1}\gamma_2$ is the shortest path which touches C_1 and C_2 . Hence, $\gamma_1^{-1}\gamma_2$, C_1 and C_2 correspond a B_C^* - minimal matrix R with $g_B(R) = 2(|C_1| + |C_2|) + 4(|\gamma_1| + |\gamma_2|)$. Clearly, there is a balanced cycle C in $\Theta(W)$ with $|C| = g_B(W)$ such that any edges in $E(W)$ is on C . Since C enters C_i at least two times, it crosses γ_i at least four times. Hence, $g_B(W) = |C| \ge 2(|C_1| + |C_2| + |C_3|) + 4(|\gamma_1| + |\gamma_2| + |\gamma_3|) >$ $2(|C_1| + |C_2|) + 4(|\gamma_1| + |\gamma_2|) = g_B(R)$, contradicts (13).

If $k \ge 4$, without loss of generality, we assume that the cycles C_1, C_2, C_3, C_4 are connected as depicted in (b) of Figure 6. Clearly, $\gamma_1^{-1}\gamma_3$ is the shortest path which touches C_1 and C_3 . Hence,

$$2(|C_1| + |C_3|) + 4(|\gamma_1| + |\gamma_3|) \ge g_B(W) \ge 2|E(W)|. \quad (15)$$

Similarly, we have

$$2(|C_2| + |C_4|) + 4(|\gamma_2| + |\gamma_4|) \ge g_B(W) \ge 2|E(W)|. \quad (16)$$



(a) (b)

Simple cycle are connected by a tree.

Then, from (15), (16) and $|E(W)| \ge |\gamma_0| + \sum_{1 \le i \le 4}(|C_i| + |\gamma_i|)$, we have $2|\gamma_0| + \sum_{1 \le i \le 4}(|C_i|) \le 0$, which is impossible.

The following theorem determines all the shortest balanced cycles in any given binary matrix.

Theorem 5. Let M be a matrix with $g_B(W) < +\infty$. If C is one of the shortest balanced cycles of M , then the least sub-matrix W of M with $C \in \Theta(W)$ is equivalent to a matrix of form $S(a,b,c)$ with $s(a,b,c) = g_B(M)$.

Proof. Suppose that C is one of the shortest balanced cycles of M . Let W be the least matrix covered by M such that $E(W)$ is just the set of edges on C . According to Theorem 4, W is a B_C^* - minimal matrix covered by M with the least B - girth . Then, from Theorem 3, W is a sub-matrix of M . Clearly, W must be the least sub-matrix of M with $C \in \Theta(W)$ and equivalent to a matrix of form $S(a,b,c)$ with $s(a,b,c) = g_B(M)$.

According to Theorem 2, it is of interest to determine all the acyclic paths of any given matrix M . For each edge e in $E(M)$, let $\Upsilon(e)$ be the greatest tree defined by follows:

Each node is marked by an edge in $E(M)$. The mark of the root is e .

For each pair of nodes connected by a branch, their marks e_1 and e_2 satisfy $|\sigma(e_1) \cap \sigma(e_2)| = 1$.

For each node, the marks of its son nodes are distinct.

For each node other than the root, the mark e_1 of any of its son nodes and the mark e_2 of any of its ancestor nodes satisfy $\sigma(e_1) \cap \sigma(e_2) = \phi$.

Clearly, in $\Upsilon(e)$, the marks of the son nodes of the root are just the edges which are directly connected to e in $T(M)$. For each node P other than the root, the mark of P and those of its son nodes are in the same row if the mark of P and that of its parent node are in the same column, and in the same column otherwise.

Obviously, for any edge e in $E(M)$, each acyclic path with

e as the origin can be directly read in the tree $\Upsilon(e)$ from the root. The tree $\Upsilon(e)$ can be easily obtained by recursion. If the tree $\Upsilon(e)$ are employed to determine the shortest balanced cycles of M , some of them are not necessary to be constructed integrally. For example, if a balanced cycle of length $2l$ has been found, according to Corollary 1 and Theorem 5, one needs only to check the acyclic paths of length between 4 and $l-2$.

The following presented all B-minimal matrices with the shortest balanced cycles of length no larger than 30 are given below. S_{2k} denotes a set of all B-minimal matrix with a shortest 2*k*-balanced cycle.

$$S_{12}:\begin{bmatrix}1&1&1\\1&1&1\end{bmatrix} S_{14}:\begin{bmatrix}1&1&0\\1&1&1\\0&1&1\end{bmatrix} S_{16}:\begin{bmatrix}1&1&0&0\\1&1&1&1\\0&0&1&1\end{bmatrix},\begin{bmatrix}1&1&0&1\\1&1&1&0\\0&0&1&1\end{bmatrix}.$$

$$S_{18}:\begin{bmatrix}1&1&0&0\\1&1&1&0\\0&0&1&1\\0&1&0&1\end{bmatrix},\begin{bmatrix}1&1&0&0\\0&1&1&0\\1&0&1&1\\0&1&0&1\end{bmatrix}.$$

$$S_{20}:\begin{bmatrix}1&1&0&0\\1&1&1&0\\0&0&1&1\\0&0&1&1\end{bmatrix},\begin{bmatrix}1&1&0&0&0\\1&1&1&0&1\\0&0&1&1&0\\0&0&0&1&1\end{bmatrix},$$

$$\begin{bmatrix}1&1&0&0&1\\1&1&1&0&0\\0&0&1&1&0\\0&0&0&1&1\end{bmatrix},\begin{bmatrix}1&1&0&0&0\\0&1&1&0&1\\1&0&1&1&0\\0&0&0&1&1\end{bmatrix}.$$

$$S_{22}:\begin{bmatrix}1&1&0&0&0\\1&1&1&0&0\\0&0&1&1&0\\0&0&0&1&1\\0&1&0&0&1\end{bmatrix},\begin{bmatrix}1&1&0&0&0\\0&1&1&0&0\\1&0&1&1&0\\0&0&0&1&1\\0&0&1&0&1\end{bmatrix},\begin{bmatrix}1&1&0&0&0\\0&1&1&0&0\\1&0&1&1&0\\0&0&0&1&1\\0&1&0&0&1\end{bmatrix}.$$

$$S_{24}:\begin{bmatrix}1&1&0&0&0\\1&1&1&0&0\\0&0&1&1&1\\0&0&0&1&1\end{bmatrix},\begin{bmatrix}1&1&0&0&0\\1&1&1&0&0\\0&0&1&1&0\\0&0&0&1&1\\0&0&1&0&1\end{bmatrix},$$

$$\begin{bmatrix}1&1&0&0&0&1\\1&1&1&0&0&0\\0&0&1&1&0&0\\0&0&0&1&1&0\\0&0&0&0&1&1\end{bmatrix},\begin{bmatrix}1&1&0&0&0&0\\1&1&1&0&0&1\\0&0&1&1&0&0\\0&0&0&1&1&0\\0&0&0&0&1&1\end{bmatrix},$$

$$\begin{bmatrix}1&1&0&0&0&0\\0&1&1&0&0&0\\1&0&1&1&0&1\\0&0&0&1&1&0\\0&0&0&0&1&1\end{bmatrix},\begin{bmatrix}1&1&0&0&0&0\\0&1&1&0&0&1\\1&0&1&1&0&0\\0&0&0&1&1&0\\0&0&0&0&1&1\end{bmatrix},\begin{bmatrix}1&1&0&0&0&0\\0&1&1&0&0&1\\0&0&1&1&0&0\\1&0&0&1&1&0\\0&0&0&0&1&1\end{bmatrix}.$$

$$S_{26}:\begin{bmatrix}1&1&0&0&0&0\\1&1&1&0&0&0\\0&0&1&1&0&0\\0&0&0&1&1&0\\0&0&0&0&1&1\\1&0&0&0&0&1\end{bmatrix},\begin{bmatrix}1&1&0&0&0&0\\0&1&1&0&0&0\\1&0&1&1&0&0\\0&0&0&1&1&0\\0&0&0&0&1&1\\0&0&1&0&0&1\end{bmatrix},$$

$$\begin{bmatrix}1&1&0&0&0&0\\0&1&1&0&0&0\\1&0&1&1&0&0\\0&0&0&1&1&0\\0&0&0&0&1&1\\0&1&0&0&0&1\end{bmatrix},\begin{bmatrix}1&1&0&0&0&0\\0&1&1&0&0&0\\0&0&1&1&0&0\\1&0&0&1&1&0\\0&0&0&0&1&1\\0&1&0&0&0&1\end{bmatrix}.$$

$$S_{28}:\begin{bmatrix}1&1&0&0&0\\1&1&1&0&0\\0&0&1&1&0\\0&0&0&1&1\\0&0&0&1&1\end{bmatrix},\begin{bmatrix}1&1&0&0&0&0\\1&1&1&0&0&0\\0&0&1&1&0&1\\0&0&0&1&1&0\\0&0&0&0&1&1\end{bmatrix},$$

$$\begin{bmatrix}1&1&0&0&0&0\\1&1&1&0&0&0\\0&0&1&1&0&0\\0&0&0&1&1&0\\0&0&0&0&1&1\\0&0&1&0&0&1\end{bmatrix},\begin{bmatrix}1&1&0&0&0&0\\0&1&1&0&0&0\\1&0&1&1&0&0\\0&0&0&1&1&0\\0&0&0&0&1&1\\0&0&0&1&0&1\end{bmatrix},$$

$$\begin{bmatrix}1&1&0&0&0&0&1\\1&1&1&0&0&0&0\\0&0&1&1&0&0&0\\0&0&0&1&1&0&0\\0&0&0&0&1&1&0\\0&0&0&0&0&1&1\end{bmatrix},\begin{bmatrix}1&1&0&0&0&0&0\\1&1&1&0&0&0&1\\0&0&1&1&0&0&0\\0&0&0&1&1&0&0\\0&0&0&0&1&1&0\\0&0&0&0&0&1&1\end{bmatrix},$$

$$\begin{bmatrix}1&1&0&0&0&0&1\\0&1&1&0&0&0&0\\1&0&1&1&0&0&0\\0&0&0&1&1&0&0\\0&0&0&0&1&1&0\\0&0&0&0&0&1&1\end{bmatrix},\begin{bmatrix}1&1&0&0&0&0&0\\0&1&1&0&0&0&0\\1&0&1&1&0&0&1\\0&0&0&1&1&0&0\\0&0&0&0&1&1&0\\0&0&0&0&0&1&1\end{bmatrix},$$

$$\begin{bmatrix}1&1&0&0&0&0&1\\0&1&1&0&0&0&0\\0&0&1&1&0&0&0\\1&0&0&1&1&0&0\\0&0&0&0&1&1&0\\0&0&0&0&0&1&1\end{bmatrix},\begin{bmatrix}1&1&0&0&0&0&0\\0&1&1&0&0&0&1\\0&0&1&1&0&0&0\\1&0&0&1&1&0&0\\0&0&0&0&1&1&0\\0&0&0&0&0&1&1\end{bmatrix}$$

$$S_{30}:\begin{bmatrix}1&1&0&0&0&0&0\\1&1&1&0&0&0&0\\0&0&1&1&0&0&0\\0&0&0&1&1&0&0\\0&0&0&0&1&1&0\\0&0&0&0&0&1&1\\1&0&0&0&0&0&1\end{bmatrix},\begin{bmatrix}1&1&0&0&0&0&0\\0&1&1&0&0&0&0\\1&0&1&1&0&0&0\\0&0&0&1&1&0&0\\0&0&0&0&1&1&0\\0&0&0&0&0&1&1\\1&0&0&0&0&0&1\end{bmatrix},$$

$$\begin{bmatrix}1&1&0&0&0&0&0\\0&1&1&0&0&0&0\\1&0&1&1&0&0&0\\0&0&0&1&1&0&0\\0&0&0&0&1&1&0\\0&0&0&0&0&1&1\\0&1&0&0&0&0&1\end{bmatrix},\begin{bmatrix}1&1&0&0&0&0&0\\0&1&1&0&0&0&0\\0&0&1&1&0&0&0\\1&0&0&1&1&0&0\\0&0&0&0&1&1&0\\0&0&0&0&0&1&1\\1&0&0&0&0&0&1\end{bmatrix},$$

$$\begin{bmatrix}1&1&0&0&0&0&0\\0&1&1&0&0&0&0\\0&0&1&1&0&0&0\\1&0&0&1&1&0&0\\0&0&0&0&1&1&0\\0&0&0&0&0&1&1\\0&1&0&0&0&0&1\end{bmatrix},\begin{bmatrix}1&1&0&0&0&0&0\\0&1&1&0&0&0&0\\0&0&1&1&0&0&0\\0&0&0&1&1&0&0\\1&0&0&0&1&1&0\\0&0&0&0&0&1&1\\0&0&1&0&0&0&1\end{bmatrix}.$$

VI. CONCLUDING REMARKS

We discussed the girth limitation of QC-LDPC expanded from a mother matrix is the existence of balanced cycles. We present the necessary and sufficient conditions of balanced cycles and determinate the existence of balanced cycles and the shortest balanced cycles in the QC-LDPC codes matrix. Finally we presented all nonequivalent minimal matrices of the shortest balanced cycles.

ACKNOWLEDGMENT

This work was supported by the National Defense Pre-Research Foundation of Chinese Shipbuilding industry under the supervision of the Wuhan Maritime Communication Research Institute

REFERENCES

[1] C. Di, D. Proietti, I. E. Telatar, T. J. Richardson, and R. Urbanke, " Finitelength analysis of low-density parity-check codes on the binary erasure channel," IEEE Trans. Inform. Theory, vol. 48, pp. 1570-1579, June 2002.

[2] J. L. Fan, " Array codes as low-density parity-check codes," in Proc. 2nd Int. Symp. Turbo Codes, Brest, France, Sept. 4-7, 2000, pp. 543-546.

[3] M. P. C. Fossorier, " Quasi-cyclic low density parity check codes from circulant permutation matrices," IEEE Trans. Inform. Theory, vol. 50, pp.1788-1794, Aug. 2004.

[4] J.-L Kim, U. N. Peled, I. Perepelitsa, V. Pless, and S. Friedland, " Explicit construction of families of LDPC codes with no 4-cycles," IEEE Trans.Inform. Theory, vol. 50, pp. 2378-2388, Oct. 2004.

[5] R. M. Tanner, D. Sridhara, T. Fuja, and D. J. Costello, Jr., " LDPC block and convolutional codes based on circulant matrices," IEEE Trans. Inform.

[6] S.Myung,K.Yang,and J.Kim.Quasi-cyclic ldpc codes for fast encoding. Information Theory,IEEE Transactions on,51(8):2894–2901,Aug.2005.

[7] S.Myung and K.Yang.Extension of quasi-cyclic ldpc codes by lifting.In Information Theory,2005.ISIT 2005.Proceedings.International Symposium on, pages 2305–2309,Sep.2005.

[8] S.Kim,J.S.No,H.Chung,and D.J.Shin.Quasi-cyclic low-density parity-check codes with girth larger than 12.Information Theory,IEEE Transactions on,53(8):2885–2891,Aug.2007.

[9] Z.Li,L.Chen,L.Zeng,S.Lin,and W.H.Fong.E?cient encoding of quasi-cyclic low-density parity-check codes.Communications,IEEE Transactions on, 54(1):71–81,Jan.2006.

[10] M.E.O'Sullivan.Algebraic construction of sparse matrices with large girth.Information Theory,IEEE Transactions on,52(2):718–727,Feb.2006.

[11] S.Myung and K.Yang.Extension of quasi-cyclic ldpc codes by lifting.In Information Theory,2005.ISIT 2005.Proceedings.International Symposium on, pages 2305–2309,Sep.2005

[12] .C.A.Kelley and J.L.Walker.Ldpc codes from voltage graphs.In Information Theory,2008.ISIT 2008.IEEE International Symposium on, pages 792–796,Jul. 2008

[13] Y.Tang,X.Huang and J.Wang,"Determination of the shortest balanced-cycles,"in ISITA2008,Auckland,New Zealand,Dec.2008.

[14] Y.Tang and X.Huang,"A Note on limited-trail Chase-like algorithm achieving bounded-distance decoding,"IEEE Trans.Inform. Theory, vol.55, pp.1047-1050,Mar.2009.

Gao Xiao, Chinese, born in November 1984, received the B.E. degree in computer science, from Central China Normal University, China, in 2006 and the M.S. degree in Ecology form Huazhong Agriculture University, China in 2009.

She currently is an engineer in information and network technology at Wuhan Maritime Communication Research Institute, her interests include information and network technology, wireless communication system, error control coding techniques and applied information theory.