Cycle Analysis in Expanded QC LDPC Codes

Gao Xiao, and Zhang Nan

***Abstract*—A quasi-cyclic (QC) low-density parity-check (LDPC) code can be viewed as the protograph code with circulant permutation matrices. In this paper, we use permutation matrices to form protograph LDPC codes. In protograph LDPC codes, we present cycle relationships of the mother matrix and the protograph LDPC code. It is derived that the girth of a protograph LDPC code is no smaller than its mother matrix .And cycles in the protograph LDPC codes are uniquely induced by the cycles in its mother matrix.**

***Index Terms*—QC-LDPC, protograph code, permutation matrices, cycles.**

I. Introduction

QC-LDPC codes as efficient encodable and small memory requirement codes can be constructed by methods proposed by Gallager[6]in the early 1960s.More recently, they have been investigated by various researchers in[1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12],.Many of the methods are based on constructing parity-check matrices that are arrays of circulant permutation matrices. Since cycles of length four in the Tanner graph have a very negative effect on decoding[23]and matrices with larger girth yield much lower error floors[19],the code designer must be careful in the choice of the circulant permutation matrices in order to avoid short cycles in the code's Tanner graph. Thorpe [20]introduced the concept of protograph codes, a class of LDPC codes constructed from a protograph. QC-LDPC code whose parity-check matrices are arrays of circulant permutation matrices is a class of protograph codes. While analyzing the cycle properties of QC-LDPC codes expanded by circulant permutation matrices, we would like to consider QC-LDPC codes as protograph codes to get more general results.

II. Expanded LDPC Codes

A. Permutation and Permutation Matrix

We give the definition of permutation and permutation matrix, and present some properties of them [21][25][26].

We denote a permutation $f : \mathrm{Z}_n \to \mathrm{Z}_n$ by a $2 \times n$ array:

$$f : \begin{bmatrix} 1 & 2 & \Lambda & n \\ f_1 & f_2 & \Lambda & f_n \end{bmatrix}$$

where $f_1, f_2, \Lambda\ , f_n$ is simply a linear rearrangement of the integers 1,2,...,n.

The notation means that $f_1 = f(1)$, $f_2 = f(2)$,Λ , $f_n = f(n)$ .We see that there is a 1-1 correspondence between the linear rearrangements of the integers 1,2,...,n and permutations.

Let $f : \mathrm{Z}_n \to \mathrm{Z}_n$ be a permutation. We call j a fixed point, if $j = f(j)$,where $j \in \{1, 2, \Lambda\ n\}$.

Let $f : \mathrm{Z}_n \to \mathrm{Z}_n$ and $g : \mathrm{Z}_n \to \mathrm{Z}_n$ be two permutations. We can compose them to get another permutation, the composition, denoted $fg : \mathrm{Z}_n \to \mathrm{Z}_n$

$$k\ \alpha\ \ f(k)\ \alpha\ \ g(f(k))$$

$$Z_n \to\ \ Z_n \to\ \ \ Z_n$$

The inverse of a permutation $f = \begin{bmatrix} 1 & 2 & \Lambda & n \\ f(1) & f(2) & \Lambda & f(n) \end{bmatrix}$ is denoted as f^{-1}, and

$$f^{-1} = \begin{bmatrix} f(1) & f(2) & \Lambda & f(n) \\ 1 & 2 & \Lambda & n \end{bmatrix}$$

To a permutation $f : \mathrm{Z}_n \to \mathrm{Z}_n$, given by

$$f = \begin{bmatrix} 1 & 2 & \Lambda & n \\ f(1) & f(2) & \Lambda & f(n) \end{bmatrix}$$

we associate to it the $n \times n$ matrix $P(f)$ of 0's and 1's defined as follows: the ij -th entry of $P(f)$ is 1 if $j = f(i)$ and is 0 otherwise. $P(f)$ is called a permutation matrix. We also know the ij -th entry of $P(f)$ is 1 if $i = f^{-1}(j)$ and is 0 otherwise.

Example The matrix of the permutation f given by

$$f = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}$$

is

Manuscript received May 3, 2011. This work was supported by National Defense Pre-Research Foundation of Chinese Shipbuilding industry.

Gao Xiao is with Wuhan Maritime Communication Research Institute China. He is now a engineer in digital communication at Wuhan Maritime Communication Research Institute, China (e-mail: gaoxiao1113@sina.com).

Zhang Nan is with Wuhan Maritime Communication Research Institute China. He is now a engineer in digital communication at Wuhan Maritime Communication Research Institute, China (e-mail:nan_zhang313@sina.com).

$$P(f)=\begin{bmatrix}0&1&0\\1&0&0\\0&0&1\end{bmatrix}$$

Proposition 1.If $f:\mathrm{Z}_n\to\mathrm{Z}_n$ is a permutation, then

1、$P(f)=\begin{bmatrix}1\\2\\\vdots\\n\end{bmatrix}=\begin{bmatrix}f(1)\\f(2)\\\vdots\\f(n)\end{bmatrix}$

2、Furthermore, the inverse of the matrix of the permutation is the matrix of the inverse of the permutation. $P(f)^{-1}=P(f^{-1})$,

3、And the matrix of the product is the product of the matrices $P(fg)=P(f)P(g)$

For simple notation, we express the $L\times L$ circulant permutation matrix as P^i which shifts the identity matrix I to the right by i times for any integer i , $0\le i<L$ And we denote the zero matrix by P^∞ .The set of $L\times L$ circulant permutation matrices together with P^∞ denotes by P_L .

B. *Expanded LDPC Codes*

In an expanded LDPC code, the parity-check matrix H consists of binary square matrices .It can be written as

$$H=\begin{bmatrix}A_{1,1}&A_{1,2}&\cdots&A_{1,n}\\A_{2,1}&A_{2,2}&\cdots&A_{2,n}\\\vdots&\vdots&\ddots&\vdots\\A_{m,1}&A_{m,2}&\cdots&A_{m,n}\end{bmatrix}\qquad(1)$$

where $A_{i,j}(1\le i\le m,\ 1\le j\le n)$ is a $L\times L$ square matrix.

The $m\times n$ binary matrix $M(H)$ can be uniquely obtained by replacing zero matrix and nonzero square matrices by‘0’and‘1’,respectively, from the parity-check matrix H of the expanded LDPC code in(1).Then $M(H)$ is called the mother matrix(or base matrix)of H .

If all the nonzero binary square matrices in the parity-check matrix H of an expanded LDPC code are circulant matrices, this expanded LDPC code is called a quasi-cyclic LDPC code(QC-LDPC code for short).Whether a QC-LDPC code is a regular LDPC code, depends on the weight distribution of $A_{i,j}$ and the column and row weights of the mother matrix $M(H)$ .If H has constant column and row weight, then the QC-LDPC code is a regular LDPC code. Otherwise, it is a irregular LDPC code. For example, let $n=3$, $m=2$,and the weights of $A_{1,1}$, $A_{1,2}$, $A_{1,3}$ are 1,2,3,while the weights of $A_{2,1}$, $A_{2,2}$, $A_{2,3}$ are 3,2,1.Then H has constant row weight 6 and constant column weight 4,thus C is a regular QC-LDPC code in this condition.

If all the nonzero binary square matrices in the parity-check matrix H of an expanded LDPC code are permutation matrices, then this expanded LDPC code is called a protograph LDPC code. If the mother matrix has constant row and column weight, the protograph LDPC code is a regular LDPC code. Otherwise, it is a irregular LDPC code.

Here, protograph LDPC codes are defined by the parity-check matrix which is the same as Thorpe’s definition[20]in Tanner graph.

Researches of expanded LDPC codes are focus on LDPC codes whose parity-check matrices consist of permutation matrices, especially circulant permutation matrices.

Protograph LDPC codes formed by permutation matrices can also be written as:

$$H=\begin{bmatrix}P(f_{1,1})&P(f_{1,2})&\cdots&P(f_{1,n})\\P(f_{2,1})&P(f_{2,2})&\cdots&P(f_{2,n})\\\vdots&\vdots&\ddots&\vdots\\P(f_{m,1})&P(f_{m,2})&\cdots&P(f_{m,n})\end{bmatrix}\qquad(2)$$

Where $P(f_{i,j})\,(1\le i\le m,1\le j\le n)$ is a $L\times L$ permutation matrix. The exponent matrix of H , denoted as $E(H)$,is defined by

$$E(H)=\begin{bmatrix}f_{1,1}&f_{1,2}&\cdots&f_{1,n}\\f_{2,1}&f_{2,2}&\cdots&f_{2,n}\\\vdots&\vdots&\ddots&\vdots\\f_{m,1}&f_{m,2}&\cdots&f_{m,n}\end{bmatrix}\qquad(3)$$

Note that H in (1)can be obtained by extending the $m\times n$ exponent matrix $E(H)$ into an $m\times n$ matrix over all the permutations. This procedure will be called an exponent extension denoted by $H=\varepsilon_L(E(H))$ .We also call this procedure lifting.

If a $2l$ -cycle in $M(H)$ corresponds to an ordered sequence of $2l$ permutation matrices $P(f_1),P(f_2),\cdots,P(f_{2l})$ in H , then($f_1,\cdots f_{2l}$)is called its exponent chain. Here both $P(f_i)$ and $P(f_{i+1})$ are located in either the same column blocks or the same row block of H ,and both $P(f_i)$ and $P(f_{i+2})$ are located in the distinct column and row blocks. Note that the $P(f_i)$ ’s are not necessarily distinct blocks located in the distinct places.

III. CYCLE RELATIONSHIPS IN PROTOGRAPH LDPC CODES

Let $M(m_{i,j})$ be a $m \times n$ mother matrix,

$$H = \begin{bmatrix} P(f_{1,1}) & P(f_{1,2}) & \Lambda & P(f_{1,n}) \\ P(f_{2,1}) & P(f_{2,2}) & \Lambda & P(f_{2,n}) \\ M & M & O & M \\ P(f_{m,1}) & P(f_{m,2}) & \Lambda & P(f_{m,n}) \end{bmatrix}$$ be its expander matrix, each $P(f_{i,j})$ in H is a $L \times L$ permutation matrix or zero matrix. We define a natural projection mapping $\phi : H \to M, \phi(P(f_{i,j})) = m_{i,j}$.

From the definition of the natural projection mapping, we can obtain the following Lemma.

*Lemma 2.*Each cycle in a expanded matrix H projects to a unique cycle in its mother matrix M by the natural projection mapping.

Proof. Assume C be a cycle in the expanded matrix H with length $2k$ .From the definition of permutation matrix, we know that two consecutive points in the cycle C are in the two different permutation matrix of the expander matrix H .Without loss of generality, we assume the permutation matrices which cycle C traverse in H be $P(f_{i_1,j_1}), P(f_{i_2,j_2}), \Lambda , P(f_{i_{2k},j_{2k}})$ where $P(f_{i_t,j_t}) \neq P(f_{i_{t+1},j_{t+1}}) \neq P(f_{i_{t+2},j_{t+2}})$,for $1 \leq t \leq 2k$ We use the convention that subscripts are computed modulo $2k$ using least positive residues, so that the latter statement includes $P(f_{i_{2k-1},j_{2k-1}}) \neq P(f_{i_{2k},j_{2k}}) \neq P(f_{i_1,j_1})$ and $P(f_{i_{2k},j_{2k}}) \neq P(f_{i_2,j_2}) \neq P(f_{i_1,j_1})$ .By the natural projection mapping, we get an ordered sequence of points $m_{i_1,j_1}, m_{i_2,j_2}, m_{i_{2k},j_{2k}}$,which forms a cycle in the mother matrix M .

From Lemma 2,we can have the following result easily.

*Theorem 3.*The girth of a expanded matrix is not smaller than its mother matrix.

Cycles in a mother matrix and its Expander matrix have the following relationship.

*Theorem 4.*Let M be a $m \times n$ mother matrix. H be the $mL \times nL$ matrix obtained by the extension of a $m \times n$ exponent matrix $E(H)$ with $L \times L$ permutation matrices. Let C be a cycle of length $2k$ in the mother matrix, its exponent chain is $(f_1, f_2, \Lambda , f_{2k})$. Then, cycle C brings a cycle of length $2k$ in matrix H if and only if $f_1^{-1} f_2, \Lambda , f_{2k-1}^{-1} f_{2k}$ has a fixed point. And the number of cycles induced by C equal to the number of fixed point of $f_1^{-1} f_2, \Lambda , f_{2k-1}^{-1} f_{2k}$

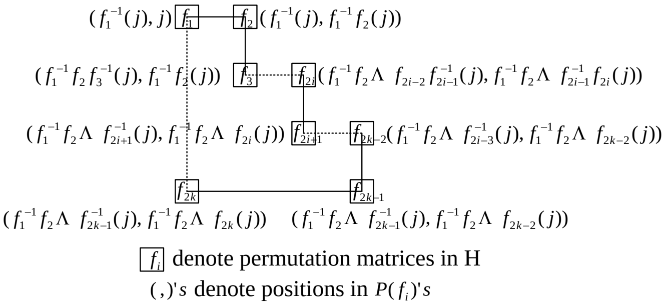
$(f_1^{-1}(j), j)$
$\boxed{f_1}$
$\boxed{f_2}$
$(f_1^{-1}(j), f_1^{-1} f_2(j))$
$(f_1^{-1} f_2 f_3^{-1}(j), f_1^{-1} f_2(j))$
$\boxed{f_3}$
$\boxed{f_{2i}}$
$(f_1^{-1} f_2 \Lambda \ f_{2i-2} f_{2i-1}^{-1}(j), f_1^{-1} f_2 \Lambda \ f_{2i-1}^{-1} f_{2i}(j))$
$(f_1^{-1} f_2 \Lambda \ f_{2i+1}^{-1}(j), f_1^{-1} f_2 \Lambda \ f_{2i}(j))$
$\boxed{f_{2i+1}}$
$\boxed{f_{2k-2}}$
$(f_1^{-1} f_2 \Lambda \ f_{2i-3}^{-1}(j), f_1^{-1} f_2 \Lambda \ f_{2k-2}(j))$
$\boxed{f_{2k}}$
$\boxed{f_{2k-1}}$
$(f_1^{-1} f_2 \Lambda \ f_{2k-1}^{-1}(j), f_1^{-1} f_2 \Lambda \ f_{2k}(j))$
$(f_1^{-1} f_2 \Lambda \ f_{2k-1}^{-1}(j), f_1^{-1} f_2 \Lambda \ f_{2k-2}(j))$
$\boxed{f_i}$ denote permutation matrices in H
$(,)'s$ denote positions in $P(f_i)'s$

Figure 1 A point in $P(f_1)$ traverses through $P(f_2), \Lambda , P(f_{2k})$

Proof. Without loss of generality, we assume f_1 and f_2 are in the same row of $E(H)$. It is obviously f_{2i-1} and f_{2i} are in the same row, f_{2i} and f_{2i+1} are in the same column, for $i = 1,2,\Lambda , k$ From the definition of permutation, we can get easily that consecutive points of a cycle in H are in different permutation matrices. Then, we can denote the points of a cycle in matrix H by their positions in the permutation matrices.

To prove the theorem, we only need to consider whether the path, starting from the point of the j -th column of the permutation matrix $P(f_1)$, passing by $P(f_2), P(f_3), \Lambda , P(f_{2k})$, forms a cycle ,i.e., whether the point is still in the j -th column of the permutation matrix $P(f_{2k})$.

By the definition of permutation matrix, the position of 1's in the j -th column of

$P(f_1)$ is $(f_1^{-1}(j), j)$,denote this point A_1 .Since f_1 and f_2 are in the same row, assume

the point in the same row of A_1 in permutation matrix $P(f_2)$ is A_2 .Then the position of

A_2 in $P(f_2)$ is $(f_1^{-1}(j), f_1^{-1} f_2(j))$. f_3 and f_2 are in the same row of the exponent matrix,

we assume the point A_3 in $P(f_3)$ is in the same column of A_2 ,the position of A_3 in

$P(f_3)$ is $(f_1^{-1} f_2 f_3^{-1}(j), f_1^{-1} f_2(j))$ .Iteratively, we have f_{2k-1} and f_{2k} are in the same row,

the position of A_{2k-1} in $P(f_{2k-1})$ is $(f_1^{-1} f_2 \Lambda \ f_{2k-2} f_{2k-1}^{-1}(j), f_1^{-1} f_2 \Lambda \ f_{2k-3}^{-1} f_{2k-2}(j))$ .We

assume the point in the same column of A_{2k-1} in $P(f_{2k})$ is A_{2k} .The position of A_{2k} is $(f_1^{-1} f_2 \Lambda \ f_{2k-1}^{-1}(j), f_1^{-1} f_2 \Lambda \ f_{2k-1}^{-1} f_{2k}(j))$.

If cycle C brings a cycle in matrix H , A_{2k} is in the j -th column of $P(f_{2k})$,i.e., $(f_1^{-1} f_2 \Lambda \ f_{2k-1}^{-1} f_{2k}(j)) = j$,it means j is the fix point of the permutation $f_1^{-1} f_2 \Lambda\ f_{2k-1}^{-1} f_{2k}$.

If $f_1^{-1} f_2 \Lambda\ f_{2k-1}^{-1} f_{2k}$ has fixed points, from the definition of cycle, there are cycles in H of length $2k$.And each fix point of the permutation will induce a $2k$-cycle in H. Thus, the number of the cycles in H induced by C is the number of the fixed points of $f_1^{-1} f_2 \Lambda\ f_{2k-1}^{-1} f_{2k}$.

When the permutation matrices are all circulant permutation matrices, i.e., a protograph LDPC code is also a QC-LDPC code, the above theorem can be described as the following corollary:

Corollary 5.Let M be a $m \times n$ mother matrix. H be the $mL \times nL$ matrix obtained by the extension of a $m \times n$ exponent matrix $E(H)$ with $L \times L$ circulant permutation matrices. Let C be a cycle of length $2k$ in the mother matrix, its exponent chain is $(a_1, a_2, \Lambda\ , a_{2k})$.Then, cycle C brings a cycle of length $2k$ in matrix H if and only if

$$\sum_{i=1}^{2k} (-1)^{-i} a_i \equiv 0 \mod L \qquad (4)$$

Fossorier, in[70,16],presented essentially the same results on the necessary and sufficient condition under which there are cycles in the QC-LDPC codes. Myung, in [4]expressed the cycles of QC-LDPC codes into simple equations. Both these results are special case of Theorem

IV. Limitation of Lifting QC-LDPC Codes

QC-LDPC codes are getting more attention due to their linear-time encodability and small size of required memory. Cycles in the Tanner graph lead to correlations in the marginal probabilities passed by the sum-product decoder; the smaller the cycles the fewer the number of iterations that are correlation free. Thus cycles in the Tanner graph affect decoding convergence, and the smaller the code girth, the larger the negative effect. From Theorem 3,we know the girth of QC-LDPC codes is no smaller than its mother matrix. Thus, lifting methods of QC-LDPC codes to get large girth are considered by many coding theorists.

There are two classes of lifting problems in QC-LDPC codes.

Class 1 Give a mother matrix and the order of circulant permutation matrix, search for an exponent matrix which make the girth of the QC-LDPC codes as large as possible.

Class 2 Give a mother matrix and the girth of a QC-LDPC codes, look for a minimal order of circulant permutation matrices which ensure the QC-LDPC codes achieve the given girth.

Now, we show some results of QC-LDPC codes by lifting.

A. *Some Results of Lifting in QC-LDPC Codes*

Myung, in[5],[22],presented two simple methods called floor and modulo lifting to construct QC-LDPC codes of larger length. We will describe one of the two methods in the following.

Consider a given QC-LDPC code C_0 with $mL_0 \times nL_0$ parity-check matrix H_0 and $m \times n$ exponent matrix $E(H_0) = (a_{ij})$.Our goal here is to construct a QC-LDPC code C_1 with $mL_1 \times nL_1$ parity-check matrix H_1 and $m \times n$ exponent matrix $E(H_1) = (b_{ij})$, where $L_1 = qL_0$ for an integer $q > 1$.Assume that both codes have the same $m \times n$ mother matrix, i.e., $M(H_0) = M(H_1)$ for simplicity. Then it suffices to specify how to lift $E(H_1)$ from $E(H_0)$,since H_1 can be obtained by exponent extension $\varepsilon_{L_1}(E(H_1))$.

Floor-lifting Procedure:

Step 1:Initialize: $E(H_1)$ is the zero matrix.

Step 2:For each‘1’at the i-th row and the j-th column among the columns with lowest degree $\omega_{\min}$ in $M(H_1)$,replace the corresponding block of H_1 by $P^{b_{ij}}$ list the girth and the number of the shortest cycles in the replaced matrix. Here, b_{ij} runs through the q exponents $qa_{ij}, qa_{ij} + 1, qa_{ij} + 2, \Lambda\ , qa_{ij} + (q-1)$

Step 3:Among all the possibilities for $P^{b_{ij}}$ Step 2,select a circulant permutation matrix at the position of‘1’in $M(H_1)$ such that the corresponding girth is maximized and then the number of the shortest cycles is minimized. Update H_1 and $E(H_1)$ by applying the chosen circulant permutation matrix and the corresponding exponent at the selected position, respectively.

Step 4:Repeat Steps 2 and 3 until each‘1’in the degree-$\omega_{\min}$ columns of $M(H_1)$ is assigned to a circulant permutation matrix.

Step 5:Repeat Steps 2,3 and 4 for each degree $\omega > \omega_{\min}$ in turn.

Modulo lifting is similar to floor lifting, only in step 2 let b_{ij} run through the q exponents $a_{ij}, a_{ij} + L_0, a_{ij} + 2L_0, \Lambda\ , a_{ij} + (q-1)L_0$.

Applying the lifting methods recursively, it is possible to generate a sequence of QC-LDPC codes.

Fossorier, in[1],showed some smallest value p(the order of circulant permutations)by computer searching. Hagiwara, in [24],investigated the smallest value p (the order of circulant permutations)for a (J, L, p) QC-LDPC code with girth 6 exists for $J = 3$ and $J = 4$.

Define $p_{\min}$ as the minimum value of p for which $a(J,L)$-regular LDPC code with $g \geq 6$ exists. Then

$$p_{\min} \geq \begin{cases} L, & if\ L\ is\ odd; \\ L+1, & if\ L\ is\ even. \end{cases} \tag{5}$$

*Proposition 6.*If L has no divisor q with $2 \leq q \leq J-1$, then $a(J,L)$-regular QC-LDPC code with $g \geq 6$ and $p = L$ exists.

*Proposition 7.*For an arbitrary J ,if $a(J,L_i)$ -regular QC-LDPC code with $g \geq 6$ and $p = L_i$ exists for each $i = 1,2,$ then for $L = L_1L_2$, $a(J,L)$ -regular QC-LDPC code with $g \geq 6$ and $p = L$ exists.

For $J = 3$, $p_{\min}$ for any value of L had been obtained. For $J = 4$, $p_{\min}$ for any $L \leq 31$ and for any $(J,L) = (4,6m),(4,6m+1),(4,6m_2),(4,6m-1)$ had been acquired.

In [17], conditions for cycles of lengths 4, 6, 8, and 10 in Tanner (3, 5) QC-LDPC codes are expressed as simple polynomial equations in a primitive 15th root of unity in F_p. By checking the existence of solutions for these equations, their girths are derived. When the shift value L is 31, the girth of the code is 8, and when the shift value L is 61 or 151, the girth of the code is 10. For the remaining values L in $P_{15} \setminus \{31,61,151\}$, the girth becomes 12.

B. Limitation of QC-LDPC Codes

We have presented the relationship of the cycles in the expanded codes and its mother matrix. QC-LDPC codes as a class of expanded LDPC codes, have efficient encoding algorithm. The girth of QC-LDPC codes are upper bounded, because of the structure of the mother matrix.

From the definition of cycle, we know the points in a cycle maybe appear more than once. If a cycle in the mother matrix of a QC-LDPC code, whose all points appear the same times in the odd positions as in the even positions, and the exponent chain of the cycle satisfies (4), there will be a cycle inevitably in the QC-LDPC code with the same length of the cycle in the mother matrix.

Example 1. Let $M_1 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ be a mother matrix. Let $H_1 = \begin{bmatrix} P(a_{11}) & P(a_{12}) & P(a_{13}) \\ P(a_{21}) & P(a_{22}) & P(a_{23}) \end{bmatrix}$ denote the expanded matrix which replace the 1's in the mother matrices by $L \times L$ circulant permutation matrices. There is inevitably a cycle of length 12 in the matrix H_1. Such a cycle is depicted in Figure 2. The cycle in Figure 2 satisfies (4),

$$a_{11} - a_{13} + a_{23} - a_{22} + a_{12} - a_{11} + a_{21} - a_{23}$$
$$+ a_{13} - a_{12} + a_{22} - a_{21} \equiv 0 \bmod \mathrm{L}$$

for any value L. Then, this cycle will bring cycles of length 12 in H_1.

Here, every points in the cycle appear two times in the cycle. And the set of points in the odd positions of the cycle is the same as the set in the even positions.

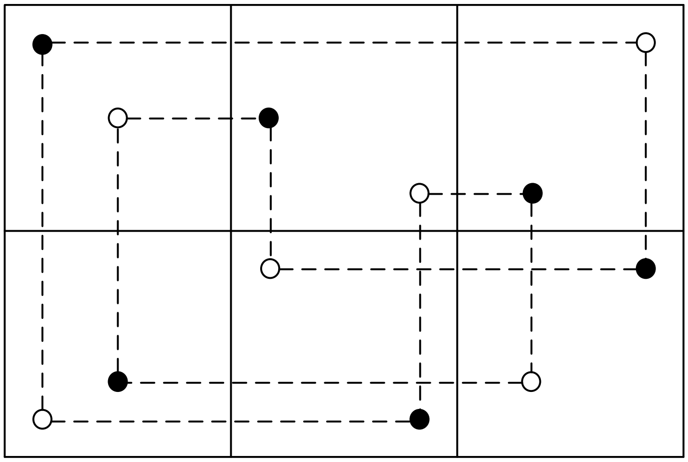

Figure 2: An inevitable cycle of length 12 in QC LDPC codes.

Example 2. Let $M_2 = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$ be a mother matrix.

Let

$$H_2 = \begin{bmatrix} P(a_1) & P(a_2) & 0 & 0 \\ P(a_3) & P(a_4) & P(a_5) & 0 \\ 0 & 0 & P(a_6) & P(a_7) \\ 0 & 0 & P(a_8) & P(a_9) \end{bmatrix}$$

denote the expanded matrix which replace the 1's in the mother matrices by $L \times L$ circulant permutation matrices and 0'a by $L \times L$ zero matrix. There is inevitably a cycle of length 20 in the matrix H_2. Since the exponent chain of the cycle is

$$\begin{pmatrix} a_1, a_2, a_4, a_5, a_6, a_7, a_9, a_8, a_5, a_4, \\ a_2, a_1, a_3, a_5, a_8, a_9, a_7, a_6, a_5, a_3 \end{pmatrix}.$$

And the exponent chain of the cycle satisfies (4),

$$a_1 - a_2 + a_4 - a_5 + a_6 - a_7 + a_9 - a_8 + a_5$$
$$- a_4 + a_2 - a_1 + a_3 - a_5 + a_8 - a_9 + a_7 - a_6 + a_5 - a_3 \equiv 0 \bmod \mathrm{L}$$

for any value L.

Here, except a_5 appear four times, the other points all appear two times. And the set of points in the odd positions of the cycle is the same as the set in the even positions.

V. CONCLUSION

We discussed cycle in expanded QC-LDPC codes. First, we consider QC-LDPC codes with circulant permutation matrices as protograph LDPC codes. And we reveal the relationship of cycles in a protograph LDPC code and its mother matrix. Second, we showed the limitation of the lifting QC-LDPC codes and give some results. Finally We have proved that the girth of a protograph LDPC code is not smaller than the girth of its mother matrix.

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] M.P.C.Fossorier.Quasicyclic low-density parity-check codes from circulant permutation matrices.Information Theory,IEEE Transactions on, 50(8): 1788–1793, Aug.2004.

[2] R.M. Tanner, D. Sridhara, and T.E. Fuja. A class of group structured ldpc codes. In Int. Conf. Inf. Syst. Technol. Its Appl., Jun .2001.

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

[4] 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.

[5] 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.

[6] 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.

[7] L.Chen,J.Xu,I.Djurdjevic,and S.Lin. Near shannon limit quasi-cyclic low-density parity-check codes. Communications, IEEE Transactions on, 52(7):1038–1042,Jul.2004.

[8] Y.Kou,S.Lin,and M.P.C.Fossorier.Low-density parity-check codes based on finite geometries:a rediscovery and new results.Information Theory,IEEE Transactions on,47(7):2711–2736,Nov.2001.

[9] B.Vasic and O.Milenkovic.Combinatorial constructions of low-density parity-check codes for iterative decoding.Information Theory,IEEE Transactions on, 50(6):1156–1176,Jun.2004.

[10] B.Ammar,B.Honary,Y.Kou,Jun Xu,and S.Lin.Construction of low-density parity-check codes based on balanced incomplete block designs. Information Theory, IEEE Transactions on,50(6):1257–1269,Jun.2004.

[11] R.M.Tanner.Spectral graphs for quasi-cyclic ldpc codes.In Information Theory, 2001.Proceedings.2001 IEEE International Symposium on,pages 226–,2001.

[12] J.L.Fan.Array codes as low-density parity-check codes.In 2nd Int.Symp. Turbo Codes,Brest,France,Sep.2000.

[13] H.Tang,J.Xu,Y.Kou,S.Lin,and K.Abdel-Gha?ar.On algebraic construction of gallager and circulant low-density parity-check codes.Information Theory, IEEE Transactions on,50(6):1269–1279,Jun.2004.

[14] L.Chen,I.Djurdjevic,and J.Xu.Construction of quasicyclic ldpc codes based on the minimum weight codewords of reed-solomon codes.In Information Theory,2004.ISIT 2004.Proceedings.International Symposium on,page 239,Jun.-2 Jul.2004.

[15] L. Chen, I. Djurdjevic, S. Lin, and K. Abdel Ghar. An algebraic method for constructing quasi-cyclic ldpc codes.In Int. Symp. Inform. Theory and Its Applications, pages 535–539,Oct.10–13 2004.

[16] J. Xu, L. Chen, L. Zeng, L. Lan, and S.Lin. Construction of low-density parity-check codes by superposition. Communications, IEEE Transactions on, 53(2):243–251,Feb.2005.

[17] S. Kim, J. S. No, H. Chung, and D.J .Shin. On the girth of tanner(3,5)quasi- cyclic ldpc codes. Information Theory, IEEE Transactions on, 52 (4):1739–1744, Apr.2006.

[18] S. Myung and K. Yang. A combining method of quasi-cyclic ldpc codes by the Chinese remainder theorem. Communications Letters, IEEE, 9(9):823–825, Sep. 2005.

[19] M.E.O' Sullivan, J. Brevik, and R. Wolski. The performance of ldpc codes with large girth. In 43rd Annu.Allerton Conf. Communication, Control, and Computing,Monticello,IL,Sep.2005.

[20] J. Thorpe. Low-density parity-check codes constructed from protographs. IPN Progress Report,42,Aug.2003.

[21] D. Joyner, R. Kreminski, and J. turisco. Applied Abstract Algebra. The Johns Hopkins University Press,Cambridge.Mass.,2004.

[22] S. Myung, K. Yang, and Y. Kim. Lifting methods for quasi-cyclic ldpc codes. Communications Letters,IEEE,10(6):489–491,Jun.2006.

[23] D.J.C. Mac Kay. Good error-correcting codes based on very sparse matrices. Information Theory, IEEE Transactions on,45(2):399–431,Mar.1999.

[24] M. Hagiwara, K. Nuida, and T. Kitagawa. On the minimal length of quasi-cyclic ldpc codes with girth greater than or equal to 6.In International Symposium on Information Theory and its Applications, ISITA 2006.,Oct.29-Nov.1 2006.

[25] Zhang Nan, Gao Xiao, "Jointly Iterative Decoding of Low-Density Parity Check codes (LDPC) coded Continues Phase Modulation (CPM)" Multidisciplinary Journals in Science and Technology. JSAT, Vol. 2, No. 3, pp. 25-31, March 2011

[26] Gao Xiao, Zhang Nan, "Determination of the shortest balanced cycles in QC-LDPC codes Matrix" Multidisciplinary Journals in Science and Technology. JSAT,, pp. 15-22, April 2011

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.

Zhang Nan

He received the B.E. degree in electronical information engineering, from Henan University of Technology, China, in 2006 and the M.S. degree in electrical engineering form China Ship Research and Development Academy , in 2009. He currently is a engineer in digital communication at Wuhan Maritime Communication Research Institute, his interests include wireless communication system, error control coding techniques and applied information theory.