# DETERMINATION OF MINIMAL MATRICES OF SIMPLE CYCLES IN LDPC CODES

Zhang Nan[1] and Gao Xiao[2]

[1, 2] Wuhan Maritime Communication Research Institute, Wuhan, 430079, China
[1]nan_zhang313@sina.com , [2]gaoxiao1113@sina.com

## ABSTRACT

*Simple cycles are the easiest cycles to reveal in Low-Density Parity Check (LDPC) codes. All minimum matrices of simple cycles with the same length will be equivalent after row or column permutations .In this paper，we analysis the structure of simple cycles and show all figures of minimal matrices of simple cycles. Firstly, we introduce a more general definition of cycle and investigate simple cycles in LDPC codes. Secondly, we present the number of simple cycles of arbitrary length and all the minimal matrices of simple cycles. Finally, we have proved that the number of all minimal matrices of 2k-simple cycles is* $\frac{(k-1)!}{2}.P_k^k,\ for\ k \geq 3.$

## KEYWORDS

*Minimal matrices, cycles &LDPC codes*

## 1. INTRODUCTION

The performance of Low-density parity-check (LDPC) codes of finite length may be strongly affected by their cycle property such as girth and stopping sets [1], 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 [5], [6], [7], [8]. Gao Xiao and Zhang Nan had analyzed balanced cycle properties of QC-LDPC codes and propose a method to determine the B-girth of a QC-LDPC code in its mother matrix and presented cycle relationships of the mother matrix and the protograph LDPC code [16],[17].

While decoding cycle-free LDPC codes with the sum-product algorithm, the performance converges to the optimal solution. If the Tanner graph of an LDPC code has cycles, very little is known regarding the convergence of iterative decoding methods.

On the other hand, it is known that cycle-free Tanner graphs do not support good codes, as the code minimum distance is asymptotically upper bounded by [3]

$$d_{\min} \leq 2\left\lfloor \frac{1}{R} \right\rfloor$$

DOI : 10.5121/ijwmn.2011.3313

where $R$ is the code rate. Therefore, the engineering practice is to construct codes with limited number of short cycles and live with long cycles. In this paper, we will give a more general definition of cycles which is a little different from the definition of cycles in graph theory.

The outline of the paper is as follows. In Section 2, reviews on the quasi-cyclic LDPC codes studies followed by description of QC-LDPC and the definition of the path and cyclic. In Section 3, we analyze Cycle Effects on the error Performance of LDPC Code. In Section 4, we determine the Minimal Matrices of Simple Cycles and all RN minimal matrices of $2k-simple$ cycles and we give concluding in Section 5.

## 2. 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

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

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 $p^\infty$ .Let $H$ be the $mL\times nL$ matrix defined by

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

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 $R=1-m/n$ 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.

## 2.1. PATHS

Suppose that $M$ is a binary matrix. Let $T(M)$ denote the Tanner graph of $M$. The set of edges of $T(M)$ is denoted by $E(M)$. For $e \in E(M)$, let $d_0(e)$ and $d_1(e)$ denote the check and bit nodes connected by $e$, respectively. Let $\sigma(e) = \{d_0(e), d_1(e)\}$. Clearly, two edges $e$, $e'$ are equal if and only if $\sigma(e) = \sigma(e')$. Here, we will mainly work on the paths in $T(M)$. However, differing from in literature, we will despise the nodes on the paths to some extent. Let $\Omega$ be a nonempty subset of $E(M)$. For $\tau \in \{0,1\}$, let $\Gamma_\tau(\Omega)$ denote the set of sequences $\gamma = e_1 e_2 \cdots e_k$ with $e_1, e_2, \cdots, e_k \in \Omega$ and

$$d_{1-\tau}(e_{2i-1}) = d_{1-\tau}(e_{2i}), \quad \text{for } 1 \le i \le \lfloor k/2 \rfloor, \tag{3}$$

$$d_\tau(e_{2i}) = d_\tau(e_{2i+1}), \quad \text{for } 1 \le i \le \lfloor (k-1)/2 \rfloor, \tag{4}$$

$$e_i \ne e_{i+1}, \quad \text{for } 1 \le i \le k, \tag{5}$$

where $k$, $e_1$, $e_k$ are called the length, origin, terminal of $\gamma$ and also denoted by $|\gamma|$, $o(\gamma)$, $t(\gamma)$, respectively. The edges $o(\gamma)$ and $t(\gamma)$ are also called ends of $\gamma$. By convention, $\Gamma_\tau(\Omega)$ contains the null sequence $\phi$. Clearly, $\Gamma_0(\Omega) \cap \Gamma_1(\Omega) = \Omega \cup \{\phi\}$. We write $\Gamma(\Omega) = \Gamma_0(\Omega) \cup \Gamma_1(\Omega)$. A sequence of edges is called a path over $\Omega$ if it is in $\Gamma(\Omega)$. The null sequence is also called a path of length $0$. $\Gamma_0(E(M))$, $\Gamma_1(E(M))$ and $\Gamma(E(M))$ are also abbreviated as $\Gamma_0(M)$, $\Gamma_1(M)$ and $\Gamma(M)$, respectively. For any path $\gamma$, let $\Gamma(\gamma)$ denote the set of paths consisting of edges on $\gamma$. For any sequence $e_1, e_2, \cdots, e_k$ of edges, let $(e_1, e_2, \cdots, e_k)^{-1} = (e_k e_{k-1} \cdots e_1)$. Clearly, for any $\gamma \in E(M) \cup \{\phi\}$, we have $\gamma^{-1} = \gamma$. According to the definitions, we can show the following five lemmas easily.

Lemma 1. A sequence $\gamma$ of edges is a path if and only if $\gamma^{-1}$ is a path. For $\tau \in \{0,1\}$ and $\gamma \in \Gamma_\tau(M)$ with $|\gamma| > 1$, the path $\gamma^{-1}$ is also in $\Gamma_\tau(M)$ if and only if $|\gamma|$ is even.

Lemma 2. For $e_1, e_2 \in E(M)$, $\tau \in \{0,1\}$ and $\gamma \in \Gamma_\tau(M)$ with $|\gamma| > 1$, if $e_1\gamma$, $e_2\gamma$ are paths, then we have $d_\tau(e_1) = d_\tau(e_2) = d_\tau(o(\gamma))$.

Lemma 3. For $\tau \in \{0,1\}$ and $\gamma_1\gamma_2\gamma_3 \in \Gamma_\tau(M)$, we have $\gamma_2 \in \Gamma_\tau(M)$ if $|\gamma_1|$ is even, and $\gamma_2 \in \Gamma_{1-\tau}(M)$ otherwise.

Lemma 4. For $\gamma_1, \gamma_2, \gamma_3 \in \Gamma(M)$ with $|\gamma_2| \ge 2$, the sequence $\gamma_1\gamma_2\gamma_3$ is a path if and only if $\gamma_1, \gamma_2, \gamma_3$ are paths.

Lemma 5. For $e \in E(M)$ and $\gamma_1, \gamma_2 \in \Gamma(M) \setminus \{\phi\}$, the sequence $\gamma_1 e \gamma_2$ is a path if and only if there is a $\tau \in \{0,1\}$ such that $e\gamma_1^{-1} \in \Gamma_\tau(M)$ and $e\gamma_2^{-1} \in \Gamma_{1-\tau}(M)$.

The following lemma can also serve as another definition for paths.

Lemma 6. A sequence $e_1, e_2, \cdots, e_k$ of edges is a path if and only if

$$\left|\sigma(e_i) \cap \sigma(e_{i+1})\right| = 1, \quad \text{for } 1 \le i < k, \tag{6}$$

$$\sigma(e_{j-1}) \cap \sigma(e_{j+1}) = \phi, \quad \text{for } 1 < j < k. \tag{7}$$

Proof. Only-if-part: Assume that $e_1, e_2, \cdots, e_k$ is a path of length $k$. Clearly, (6) follows from (3) to (5). To show (7), assume in contrast that $\sigma(e_{j-1}) \cap \sigma(e_{j+1}) \ne \phi$ for some $j$ with $1 < j < k$ Let $\tau$ be the integer in $\{0,1\}$ such that $d_\tau(e_{j-1}) = d_\tau(e_j)$ and $d_{1-\tau}(e_{j+1}) = d_{1-\tau}(e_j)$. If $d_\tau(e_{j-1}) = d_\tau(e_{j+1})$, then we have $e_j = e_{j+1}$, which contradicts (5). If $d_{1-\tau}(e_{j-1}) = d_{1-\tau}(e_{j+1})$, then we have $e_j = e_{j-1}$, which contradicts (5) too. Hence, (7) is valid.

If-part: Assume that (6) and (7) are valid. Clearly, (5) follows from (6). For any given $j$ with $1 < j < k$, let $\tau'$ and $\tau''$ be integers in $\{0,1\}$ such that $d_{\tau'}(e_{j-1}) = d_{\tau'}(e_{j+1})$ and $d_{\tau''}(e_{j+1}) = d_{\tau''}(e_j)$. Then, from (7) we see $\tau' = 1 - \tau''$. Hence, (3) and (4) are valid for some integer $\tau \in \{0,1\}$.

According to Lemma 6, we can show the following two lemmas.

**Lemma 7.** For $e_0, e_1, e, e' \in E(M)$ with $e_0 e e_1 \in \Gamma(M)$ and $\left|\sigma(e) \cap \sigma(e')\right| = 1$, there are integers $v$ and $\tau$ 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, $e_{1-v} e e'$ is a path.

Proof. Let $\tau \in \{0,1\}$ be the integer such that $d_\tau(e) = d_\tau(e')$. Clearly, $d_{1-\tau}(e) \ne d_{1-\tau}(e')$. Since $e_0 e e_1$ is a path, there is an integer $\gamma \in \{0,1\}$ such that $d_\tau(e_v) = d_\tau(e)$ and $d_{1-\tau}(e_{1-v}) = d_{1-\tau}(e)$. Hence, we have $d_\tau(e') = d_\tau(e) = d_\tau(e_v)$ and $d_{1-\tau}(e_{1-v}) \ne d_{1-\tau}(e')$. From Lemma 6, we see $d_\tau(e_{1-v}) \ne d_\tau(e_v) = d_\tau(e')$. Then, we have $\sigma(e_{1-v}) \cap \sigma(e') = \phi$.

**Lemma 8.** For $\gamma, \gamma_0, \gamma_1 \in \Gamma(M) \setminus \{\phi\}$ with $o(\gamma_0) \ne o(\gamma_1)$ and $|\gamma| > 1$, if $\gamma\gamma_0$, $\gamma\gamma_1$ are paths, then $\gamma_0^{-1}\gamma_1$ is a path.

Proof. According to Lemma 2, we see $\left|\sigma(o(\gamma_0)) \cap \sigma(o(\gamma_1))\right| = 1$. For $v \in \{0,1\}$, let $\gamma_v'$ denote the path with $\gamma_v = o(\gamma_v)\gamma_v'$. If $\gamma_v' \ne \phi$, from $t(\gamma)o(\gamma_v)o(\gamma_v') \in \Gamma(M)$, $\left|\sigma(o(\gamma_{1-v})) \cap \sigma(o(\gamma_v))\right| = 1$, $\left|\sigma(o(\gamma_{1-v})) \cap \sigma(t(\gamma))\right| = 1$ and Lemma 7, we see $\sigma(o(\gamma_{1-v})) \cap \sigma(o(\gamma_v')) \ne \phi$. Then, from Lemma 6, we see that

$$\gamma_0^{-1}\gamma_1 = (\gamma_0')^{-1} o(\gamma_0) o(\gamma_1) \gamma_1'$$

is a path.

**Lemma 9.** Assume that $\Omega$ is a nonempty subset of $E(M)$. If there is at least one path in $\Gamma(M)\setminus\Gamma(\Omega)$ with ends in $\Omega$, let $e_1e_2\cdots e_k$ be a such path with the least length, then

$$e_i \notin \Omega, \text{ for } 1 < i < k, \tag{8}$$

$$\sigma(e_i)\cap\sigma(e) = \phi, \text{ for } 3 \le i \le k-2, e \in \Omega. \tag{9}$$

Proof. (8) is obvious. If there is an edge $e \notin \Omega$ and integer $i$ with $3 \le i \le k-2$ such that $\sigma(e_i)\cap\sigma(e) \ne \phi$, according to Lemma 4 and 7, we see that either $e_1e_2\cdots e_ie$ or $ee_ie_{i+1}\cdots e_k$ is a path connecting $\Omega_1$ and $\Omega_2$, contradicts our assumption. Hence, we have (9).

### 2.2. Cycle

For $\tau \in \{0,1\}$, a path $\gamma \in \Gamma_\tau(M)\setminus\{\phi\}$ of even length is called a cycle if $o(\gamma) \ne t(\gamma)$ and

$$d_\tau(o(\gamma)) = d_\tau(t(\gamma)). \tag{10}$$

Clearly, the length of any cycle is even and at least 4. Let $\Theta(M)$ denote the set of cycles. Clearly, $C \in \Theta(M)$ if and only if $C^{-1} \in \Theta(M)$. If $\Theta(M) \ne \phi$, the length of the shortest cycles in $\Theta(M)$ is called the girth of $M$, and denoted by $g(M)$. If $\Theta(M) = \phi$, we say that the girth of $M$ is $g(M) = \infty$. The following lemma can also serve as another definition for cycles.

**Lemma 10.** A path $\gamma$ is a cycle if and only if $|\gamma| > 0$ and $\gamma\gamma \in \Gamma(M)$.

Proof. If-part: Assume that $|\gamma|$ is positive and $\gamma\gamma$ is a path in $\Gamma_\tau(M)$ for some $\tau \in \{0,1\}$. Clearly, we have $\gamma \in \Gamma_\tau(M)$, $|\gamma| > 1$ and $t(\gamma) \ne o(\gamma)$. Furthermore, from Lemma 3 and $\Gamma_0(M)\cap\Gamma_1(M) = E(M)\cap\{\phi\}$, we see that $|\gamma|$ is even and therefore $d_\tau(t(\gamma)) = d_\tau(o(\gamma))..$ Hence, $\gamma$ is a cycle.

Only-if part: Assume that $\gamma$ is a cycle of length $2k$. For $1 \le i \le 2k$, let $e_i$ denote the $i-th$ edge on $\gamma$. Then, $e_1 \ne e_{2k}$ and $e_i \ne e_{i+1}$ for $1 \le i < 2k$. Furthermore, for the integer $\tau \in \{0,1\}$ with $\gamma \in \Gamma_\tau(M)$, we have $d_\tau(e_{2k}) = d_\tau(e_1)$ and

$$d_{1-\tau}(e_{2i-1}) = d_{1-\tau}(e_{2i}), \text{ for } 1 \le i \le k, \tag{11}$$

$$d_\tau(e_{2i}) = d_\tau(e_{2i+1}), \text{ for } 1 \le i < k. \tag{12}$$

Hence, $\gamma\gamma = e_1e_2\cdots e_{2k}e_1e_2\cdots e_{2k}$ is a path by definition.

**Lemma 11.** For paths $\gamma$, $\gamma'$ 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.

Proof. If-part: Assume that $|\gamma|+|\gamma'|$ l is even and $\gamma\gamma'\gamma$ is a path in $\Gamma_\tau(M)$ for some $\tau\in\{0,1\}$. Clearly, we have $o(\gamma)\neq t(\gamma')$, $d_\tau(o(\gamma))=d_\tau(t(\gamma'))$ and $\gamma\gamma'\in\Gamma_\tau(M)$. Hence, $\gamma\gamma'$ is a cycle.

Only-if-part: Assume that $\gamma\gamma'$ is a cycle. According to Lemma 10, $\gamma\gamma'\gamma\gamma'$ is a path. Thus, we see that $\gamma\gamma'\gamma$ is a path.

**Remark:** We note that the condition "$|\gamma|+|\gamma'|$ is even" in Lemma 11 can be dropped if the length of $\gamma$ is at least 2.

The following lemma is a simple corollary of Lemmas 10 and 11.

Lemma 12. For any two paths $\gamma,\gamma'\in\Gamma_\tau(M)\backslash\{\phi\}$, $\gamma\gamma'$ is a cycle if and only if $\gamma\gamma'$ is a cycle.

Proof. Assume that $\gamma\gamma'$ is a cycle. Clearly, we have $2\,|\,(|\gamma|+|\gamma'|)$. From Lemma 10, we see $\gamma\gamma'\gamma\gamma'\in\Gamma(M)$. Then, we have $\gamma'\gamma\gamma'\in\Gamma(M)$ and thus, from Lemma 11, $\gamma\gamma'$ is a cycle.

A path $\gamma\in\Gamma_\tau(M)\backslash\{\phi\}$ is said acyclic if $\Gamma(\gamma)$ has no cycle.

Lemma 13. Let $\gamma=e_1e_2\cdots e_k$ be a path in $\Gamma(M)$. Then, $\gamma$ is a acyclic if and only if $k\geq 1$ and $\sigma(e_i)\cap\sigma(e_j)=\phi$ for all $i, j$ with $|i-j|\geq 3$.

Proof. Only-if-part: Assume $\gamma$ is acyclic. Clearly, we have $k\geq 1$. If $\sigma(e_i)\cap\sigma(e_j)\neq\phi$

for some $i, j$ with $|i-j|\geq 3$, according to $\sigma(e_i)\cap\sigma(e_{i+2})=\phi$ and $\sigma(e_j)\cap\sigma(e_{j-2})=\phi$, we can assume further, without loss of generality, that $\sigma(e_i)\cap\sigma(e_{j-1})=\phi$ and $\sigma(e_j)\cap\sigma(e_{i+1})=\phi$. From $|\sigma(e_i)\cap\sigma(e_{i+1})|=1$ and $\sigma(e_j)\cap\sigma(e_{i+1})=\phi$, we see $e_i\neq e_j$. Hence, $e_ie_{i+1}\cdots e_j$ is a cycle in $\Gamma(\gamma)$, contradicts our assumption. Thus, $\sigma(e_i)\cap\sigma(e_j)=\phi$ for all $i, j$ with $|i-j|\geq 3$.

If-part: Assume $k\geq 1$ and $\sigma(e_i)\cap\sigma(e_j)=\phi$ for all $i, j$ with $|i-j|\geq 3$. Let $\gamma'$ be

an arbitrary path in $\Gamma(\gamma)$. One can show easily that there are some integers $i$ and $j$ with $1\leq i\leq j\leq k$ such that

$$\gamma'=e_ie_{i+1}\cdots e_j \text{ or } e_je_{j-1}\cdots e_i.$$

Clearly, we have $\gamma'\notin\Theta(M)$. Hence, $\gamma$ is a cyclic.

According to Lemma 6 and 13 we can get the following corollary easily.

Corollary 1. A sequence $e_1e_2\cdots e_k$ of edges is an acyclic path if and only if it satisfies (6) and

$$\sigma(e_{i-1}) \cap \sigma(e_{j+1}) = \phi, \quad \text{for } 1 < i \leq j \leq k. \tag{13}$$

Two cycles $C$ and $C'$ are said equivalent if there are paths $\gamma_1$, $\gamma_2$ such that $C = \gamma_1\gamma_2$ and $C' = \gamma_2\gamma_1$ or $\gamma_1^{-1}\gamma_2^{-1}$. For cycle $C$ and path $\gamma$, we write $\gamma \subseteq C$ if there is a path $\gamma'$ such that $\gamma\gamma'$ is a cycle equivalent to $C$, such path $\gamma'$ is called the complementary of $\gamma$ in $C$. A cycle $C$ is said simple if any path $\gamma \subseteq C$ with $0 < |\gamma| < |C|$ is acyclic.

Lemma 14. For $\gamma \in \Gamma(M)$ and $e_0 \in E(M)$, the sequence $e_0\gamma$ is a simple cycle if and

only if $\gamma$ is acyclic and $e_0\gamma e_0 \in \Gamma(M)$.

Proof. The only-if-part is obvious. Now we consider the if-part. Assume $\gamma = e_1e_2 \cdots e_k$ is acyclic and $e_0\gamma e_0 \in \Gamma_\tau(M)$ for some $\tau$ in $\tau \in \{0,1\}$. From $e_0\gamma e_0 \in \Gamma(M)$, we see $k \geq 3$, $|\sigma(e_0) \cap \sigma(e_1)| = |\sigma(e_0) \cap \sigma(e_k)| = 1$ and

$$\sigma(e_0) \cap \sigma(e_2) = \sigma(e_0) \cap \sigma(e_{k-1}) = \phi$$

Since $\gamma$ is acyclic, we see $\sigma(e_1) \cap \sigma(e_k) = \phi$. Then, $e_0\gamma e_0\gamma$ is a path and thus, from Lemma 10, $e_0\gamma$ is a cycle. From $\sigma(e_0) = \{d_{1-\tau}(e_1), d_\tau(e_k)\}$ and (13), we see $\sigma(e_0) \cap \sigma(e_i) = \phi$ for any $i$ with $3 \leq i \leq k-2$. Hence, for any $j$ with $1 \leq j \leq k$, $e_{j+1} \cdots e_k e_0 e_1 \cdots e_{j-1}$ is an acyclic path. Thus, $e_0\gamma$ is a simple cycle.

According to Corollary 1 and Lemma 14, one can show the following corollary easily.

Corollary 2. A necessary and sufficient condition for a sequence $e_1e_2 \cdots e_k$ of different edges to be a simple cycle is

$$|\sigma(e_i) \cap \sigma(e_j)| = 1 \quad \text{if and only if } i - j \equiv \pm 1 \bmod k. \tag{14}$$

A path in $\Gamma(M) \setminus \{\phi\}$ is said cyclic if it is not acyclic. We note that the null sequence $\phi$ is neither acyclic nor cyclic according to our definitions.

**Lemma 15.** Suppose that $\gamma$ is a cyclic path. Then, there are a simple cycle $C_0$ and paths $\gamma_1$, $\gamma_2$ such that $\gamma = \gamma_1 C_0 \gamma_2$.

Proof. Suppose $\gamma = e_1e_2 \cdots e_k$ is a cyclic path of length $k$. According to Lemma 13, there are integers $i$ and $j$ with $|i - j| \geq 3$ such that $\sigma(e_i) \cap \sigma(e_j) \neq \phi$. Without loss of

generality, we assume further $i < j$ and $\sigma(e_{i'}) \cap \sigma(e_{j'}) = \phi$ for any $i'$, $j'$ with $i + 3 \leq i' + 3 \leq j' \leq j$ and $(i', j') \neq (i, j)$. From $\sigma(e_j) \cap \sigma(e_{j-1}) \neq \phi$ and $\sigma(e_i) \cap \sigma(e_{j-1}) = \phi$, we have $e_i \neq e_j$. Hence, from Corollaries 1 and 2, $e_i e_{i+1} \cdots e_j$ is a simple cycle and $\gamma = \gamma_1 e_i e_{i+1} \cdots e_j \gamma_2$ for $\gamma_1 = e_1 e_2 \cdots e_{i-1}$ and $\gamma_2 = e_{j+1} e_{j+2} \cdots e_k$.

A cycle $C$ is called a sub-cycle of another cycle $C'$ if $C \subseteq C'$. Clearly, two cycles are equivalent if and only if they are sub-cycles of each other. Furthermore, according to Lemma 15, the shortest sub-cycles of a given cycle C must be simple. We note that, even if $C_1$ is a sub-cycle of $C_2$ and $C_2$ is a sub-cycle of $C_3$, $C_1$ is not necessary to be a sub-cycle of $C_3$. However, if $C$ and $C'$ are equivalent cycles, then any sub-cycle of $C$ is a sub-cycle of $C'$.

If $C$ and $C'$s are equivalent cycles, for any given integer t, the cycle

$$C^t = \underbrace{CC \ldots C}_{t}$$

is called a multiple of $C'$.

**Lemma 16.** Let $C$ be a simple cycle. Then any cycle in $\Gamma(C)$ is a multiple of $C$. In particular, any sub-cycle of $C$ is equivalent to $C$.

Proof. Let $C = e_1 e_2 \cdots e_{2k}$ be a simple cycle and $C' = f_1 f_2 \cdots f_{2l}$ a cycle in $\Gamma(C)$. According to Corollary 2, $|\sigma(e_i) \cap \sigma(e_j)| = 1$ if and only if $i - j \equiv \pm 1 \bmod 2k$. Without loss of generality, we assume that $f_1 = e_1$. From $|\sigma(f_1) \cap \sigma(f_2)| = 1$, we have

$$f_2 \in \{e_2, e_{2k}\}.$$

If $f_2 = e_2$, according to $|\sigma(f_2) \cap \sigma(f_3)| = 1$, we have $f_3 \in \{e_1, e_3\}$. From $\sigma(f_1) \cap \sigma(f_3) = \phi$ and $f_1 = e_1$, we have $f_3 = e_3$. By induction, one can show easily that $f_i \bmod 2l = e_i \bmod 2k$ for any positive integer $i$. By taking i as the least common multiple of $2l$ and $2k$, we get $f_{2l} = e_{2k}$. Since $e_1, e_2, \cdots, e_{2k}$ are distinct, $k$ must divide $l$. Hence $C' = C^t$ for some positive integer $t$.

If $f_2 = e_{2k}$, one can show similarly that $f_i \bmod 2l = e_{2k+2-i} \bmod 2k$ for any positive integer $i$. Hence, $k$ must divide $l$ and there is some positive integer $t$ such that $C' = C_0^t$, where $C_0 = e_1 e_{2k} e_{2k-1} \cdots e_2$ is a cycle equivalent to $C$.

## 3. Cycle Effects on the Performance of LDPC Code

The error performance of an LDPC code with iterative decoding such as SPA depends on a number of structural properties besides its minimum distance. One such structural property is the girth of the code.

By proving the convergence of the sum-product algorithm for codes whose graphs are free of cycles, Tanner was the first to formally recognize the importance of cycle free graphs in the context of iterative decoding. The effect of cycles on the practical performance of LDPC codes was demonstrated by simulation experiments by MacKay and Neal [1] in the mid-1990s, and the beneficial effects of using graphs free of short cycles were shown [2]. Given the detrimental effects of cycles on the convergence of iterative decoders, it is natural to seek strong codes whose Tanner graphs are free of cycles. An important negative result in this direction was established by Etzion et al. [3], who showed that for linear codes of rate $k/n \geq 0.5$ which can be represented by a Tanner graph without cycles, the minimum distance is at most 2. Therefore, we should construct codes with long cycles. The shortest possible cycle in a Tanner graph is a cycle of length 4. A length 4 cycle results if two columns of parity check matrix $H$ have more than one check positions in common. We are interested in knowing and controlling short cycles, since they have a negative impact on the decoding algorithm. Short cycles in LDPC codes cause successive iterations of the sum-product decoding algorithm to be highly correlated after only small number of iterations, thus prevent the iterative sum-product decoding from converging to the optimal solution. One commonly applied constraint in constructing parity check matrix is that the maximum overlap between any two columns in the matrix should be one, which ensures that the code has no 4-cycles.

In LDPC decoding, the sum-product algorithm assumes that the reliability information gathered by the variable or check nodes at each iteration is statistically independent. This assumption is valid for the initial number of iterations equal to $\lfloor (g-1)/4 \rfloor$, as the information has not been propagated around the shortest cycle in the graph, and the messages arriving at any node are indeed statistically independent. Therefore, it is desirable for a Tanner graph to have a large girth. In deriving the bounds on the maximum number of decoding iterations for regular LDPC codes. Gallager [6] established a simple lower bound on the code length of an LDPC code give the girth of the associated Tanner graph. It shows it is difficult to construct high-rate regular LDPC codes with moderate block length (i.e. N = 5000) and large girth (i.e. g = 10).

## 4. Determination of Minimal Matrices of Simple Cycles

It is obviously the most ordinary cycle in LDPC codes is the simple cycle. We will analysis the property of simple cycles in this section.

For two matrices $W$ and $R$, we say that $W$ covers $R$ if $R$ can be obtained from some sub-matrix of $W$ by changing some nonzero elements to zero. Clearly, $R$ is covered by $W$ if and only if the Tanner graph of $R$ can be obtained from that of $W$ by deleting some nodes and edges.

A matrix $M$ is called a minimal matrix of a simple cycle $C$ if the following two conditions are valid:

- any sub-matrix of $M$ does not contain the simple cycle $C$,
- any covered matrix of $M$ does not contain the simple cycle $C$.

Two matrices $M$ and $M'$ are said equivalent, and denoted $M \equiv M'$, if $M$ itself or its transpose is equal to $M'$ after some permutations of rows and columns.

When we construct LDPC codes with large girth, it is obviously that the shortest cycles are simple cycles. We will present all the minimal matrix of 2k-simple cycles $(k \geq 2)$ in the following.

From the definitions of simple cycle and minimal matrix of a simple cycle, we get the following lemma.

Lemma 17. The minimal matrix of a $2k-simple$ cycle is equivalent to a $k \times k$ matrix expressed as follows:

$$\begin{bmatrix} 1 & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & 0 & \dots & 1 & 1 \\ 1 & 0 & 0 & 0 & \dots & 0 & 1 \end{bmatrix}_{k \times k} \tag{15}$$

It is obviously every minimal matrix of a $2k-simple$ cycle is a $k \times k$ matrix with row and column weights 2. We can get all minimal matrices of a $2k-simple$ cycle after some row or column permutations of (15).

We say a matrix $M$ is row non-equivalent (RN for short) to another matrix $M'$ , if $M$ can not be obtained only by row permutations of $M'$.

Let $(i, j)$ denote the position which is in the $i-th$ row and $j-th$ column of a matrix.

We will find all figures of $2k-simple$ cycles into two steps. First, find all RN minimal matrices of $2k-simple$ cycle. Then, make exhausted row permutations to each RN minimal matrices. All these RN minimal matrices and their row permutation matrices are matrices we look for.

### 4.1. Determine all RN minimal matrices of $2k-simple$ cycles

For $k=2$, it is obviously the minimal matrix of a $4-simple$ cycle is $\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$.

Now, for $k \geq 3$ determine all RN minimal matrices of $2k-simple$ cycles.

Let $M$ be a minimal matrix of $2k-simple$ cycle. Then $M$ is a $k \times k$ matrix, each column and each row of $M$ have weights 2, and $M$ does not contain cycles shorter than $2k$.

Assume two 1's in the first column of $M$ are in the $i_1-th$ and $i_2-th$ rows, where $i_1 \neq i_2$. The positions of two 1's in the first column are $(i_1,1)$, $(i_1, j_1)$. Assume the 1 in the same row of $(i_2,1)$ is in position $(i_1, j_1)$, and the 1 in the same row of $(i_2,1)$ is in position $(i_2, j_2)$, where $j_1 \in \{2,3,\cdots,k\}$, $j_2 \in \{2,3,\cdots,k\} \setminus \{j_1\}$.

Since a matrix, whose 1's in the $i_1-th$ and $i_2-th$ rows are in positions $(i_1,1)$, $(i_1, j_1)$, $(i_2,1)$, $(i_2, j_2)$, are row equivalent to matrix whose 1's in the $i_1-th$ and $i_2-th$ rows are in positions $(i_1,1)$, $(i_1, j_2)$, $(i_2,1)$, $(i_2, j_1)$. We only reserve one of them to obtain all RN minimal matrices.

Assume the position of the 1, which is in the same column of the 1 in position $(i_1, j_1)$, is $(i_3, j_1)$, where $i_3 \neq i_1$, $i_3 \neq i_2$. Assume the position of the 1, which is in the same row of the 1 in position (i3, j1), is (i3, j3), where $j_3 \in \{2,3,\cdots,k\} \setminus \{j_1, j_2\}$.

Iteratively, assume the position of the 1, which is in the same column of the 1 in position $(i_l, j_{l-2})$, is $(i_l, j_l)$, where $3 \leq l < k$, $j_1 \in \{2,3,\cdots,k\} \setminus \{j_1, j_2, \cdots, j_{l-1}\}$, and $i_l \neq i_1, \cdots i_l \neq i_{l-1}$.

Assume the position of the 1, which is in the same column of the 1 in position $(i_{k-2}, j_{k-2})$, is $(i_k, j_{k-2})$, where $i_k \neq i_1, \cdots i_k \neq i_{k-1}$. Then the position of the 1, which is in the same row of the 1 in position $(i_k, j_{k-2})$, is $(i_k, j_{k-1})$.

Then, all the 1's in $M$ are in positions:

$$\{(i_1,1),(i_1, j_1),(i_2,1),(i_2, j_2),(i_3, j_1),(i_3, j_3),\cdots,$$
$$(i_l, j_{l-2}),(i_l, j_l),\cdots(i_k, j_{k-2}),(i_k, j_{k-1})\},$$

where $(i_1, i_2, \cdots, i_k)$ is a permutation of $\{1,2,\cdots,k\}$, $j_1 \in \{2,3,\cdots,k\} \setminus \{j_1, j_2, \cdots, j_{l-1}\}, 1 \leq l < k$.

Take $(i_1, i_2, \cdots, i_k)$ one permutations of $\{1,2,\cdots,k\}$. Take all the possible values of $j_1, j_2, \cdots, j_{k-1}$ described above. We can get all RN minimal matrices of $2k - simple$ cycles.

For each RN minimal matrix, make row permutation of it, we will have $p_k^k$ different minimal matrices.

The number of all minimal matrices of $2k - simple$ cycles can be easily obtained.

Theorem 1. Let $N_{2k}$ be the number of all minimal matrices of $2k - simple$ cycles. Then,

$$N_{2k} = \begin{cases} 1, & \mathrm{k} = 2 \\ \dfrac{(k-1)!}{2} \cdot k!, & \mathrm{k} \geq 3. \end{cases}$$

Proof. It is obviously there is only one minimal matrix of $4 - simple$ cycle.

For simple cycles of length $2\mathrm{k}$, $\mathrm{k} \geq 3$, we prove the number of all figures of minimal matrices is $\frac{(k-1)!}{2} \cdot k!$. The number of all minimal matrices of $2k - simple$ cycles is equal to the number of all RN minimal matrices multiple the number of all row permutations. For a $k \times k$ matrix, the number of all row permutations is $p_k^k$, which is equal to the number of all permutations of $\{1,2,\cdots,k\}$. Now, we calculate the number of all RN minimal matrices. Since $j_1$ can choose from $k-1$ possible values, $j_2$ can choose from $k-2$ possible values, All possible chosen of $j_1, j_2, \cdots, j_{k-1}$ is $(k-1)!$. Since exchanging the values of $j_1$ and $j_2$ results in row equivalent minimal matrices, the number of all RN minimal matrices is $\frac{(k-1)!}{2}$. Then, the number of all minimal matrices is obtained.

**Example** All row non-equivalent matrices of 8-simple cycles are as follows:

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

For each row non-equivalent matrix, we can obtain all figures of $8-simple$ cycles after all rows permutations. There are $4!=24$ row permutations, hence the number of all minimal matrices of $8-simple$ cycles are $3\times 24=72$

## 5. CONCLUSIONS

Simple cycles are the easiest cycles to reveal in LDPC codes. All minimum matrices of simple cycles with the same length will be equivalent after row or column permutations. We know the number of all minimal matrices of 2k-simple cycles is $\frac{(k-1)!}{2}.P_k^k,\ for\ k\geq 3$ we introduce a more general definition of cycle and investigate simple cycles in LDPC codes. We present a number of simple cycles of arbitrary length and all the minimal matrices of simple cycles. Future studies include research other cycles different from simple cycles and balanced cycles. For example, a cycle formed by a simple cycle twice will induce a cycle in the expanded matrix for some circulant permutation matrices.

## ACKNOWLEDGEMENTS

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] D.J.C. MacKay and R.M. Neal. Near shannon limit performance of low density parity check codes. Electronics Letters,32(18):1645–,Aug.1996.

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

[3] T. Etzion, A. Trachtenberg, and A. Vardy. Which codes have cycle-free tanner graphs Information Theory, IEEE Transactions on,45(6):2173–2181,Sep.1999.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

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

[9] 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.

[10] 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.

[11] 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.

[12] 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.

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

[14] 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

[15] .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

[16] 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

[17] Gao Xiao, Zhang Nan, "Determination of the shortest balanced cycles in QC-LDPC codes Matrix" Multidisciplinary Journals in Science and Technology. JSAT, Vol.2, No. 4 , pp. 15-22, April 2011

[18] Najoua Achoura, Riaha Bouallegue, "Impact of feedback on MIMO-OFDM system using joint beamforming " International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 2, pp. 39-45 April 2011

## Authors

Zhang Nan 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.

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.