# A Novel Construction Method of QC-LDPC Based on BIBD and Protograph 

Sheng Huang ${ }^{1, \mathrm{a}}$, Rui Zhang ${ }^{2, \mathrm{~b}}$, Xueting Jia ${ }^{3, \mathrm{c}}$, Xiang Ao ${ }^{4, \mathrm{~d}}$, Jianguo Yuan ${ }^{5, \mathrm{e}}$<br>${ }^{1}$ School of Chongqing University of Posts and Telecommunications, Chongqing, 400065, China.<br>${ }^{2}$ School of Chongqing University of Posts and Telecommunications, Chongqing, 400065, China.<br>${ }^{3}$ School of Chongqing University of Posts and Telecommunications, Chongqing, 400065, China.<br>${ }^{4}$ School of Chongqing University of Posts and Telecommunications, Chongqing, 400065, China.<br>${ }^{5}$ School of Chongqing University of Posts and Telecommunications, Chongqing, 400065, China.<br>${ }^{\text {ahuangs } @ c q u p t . e d u . c n, ~}{ }^{\text {b }}$ cquptzr@163.com, ${ }^{\text {c}}$ cquptjxt@163.com, ${ }^{\text {d }} \mathrm{ax}$ _cqupt@163.com, ${ }^{\mathrm{e}}$ yuanjg@c qupt.edu.cn

Keywords: BIBD; Protograph; QC-LDPC; Extension Method;


#### Abstract

A novel construction method of Quasi-Cyclic Low-Density Parity-Check (QC-LDPC) code is proposed in this paper, which is based on protograph and Balanced Block Design (BIBD) in combinational mathematics. The method is to fill the base matrix of protograph with the base set elements of BIBD in accordance with certain mathematical rules. And the base matrix of protograph proposed in the paper has special double diagonal structure, which overcomes the low weight code words in general structure and achieves rapid encoding at the same time. The QCLDPC code in this paper possesses lower encoding complexity and less memory occupation; therefore it is easy for hardware implementation. In addition, it effectively avoids girth 4 . Simulation results show that when the Bit Error Rate (BER) is $10^{-7}$, QC-LDPC codes based on Protograph and BIBD (PBIBD-LDPC) proposed in this paper has 0.5 dB Net Coding Gain (NCG) compared with the protograph QC-LDPC codes that based on Vander monde matrix and PEG algorithm structure, and has 0.15 dB NCG compared with the excellent code QC-LDPC that based on the lifting structure.


## 1. Introduction

LDPC code was first proposed by Gallager in 1963[1]. It was proved to be a kind of excellent code that approaches the Shannon limit later and was adopted by several international communication standards [2, 3]. It is well known that LDPC code has a sparse check matrix, bur the generator matrix of LDPC code usually does not possess sparsity, and the nonzero elements in the generator matrix are randomly arranged with high density, so the encoder needs a large amount of chip area to store nonzero element of the generator matrix, which leads to a higher coding complexity of LDPC. J.Thorpe proposed LDPC code based on protograph to solve the high encoding complexity problem[4], and then the code was studied deeply[5, 6]. This kind of code expands the Tanner graph that has lesser nodes to a derived graph of any size. Therefore, it possesses the advantages of high speed decoding, low error floors and the low iterative decoding threshold[7-9].

The two extension methods of protograph LDPC code are computer random search method [10] that whose disadvantage is long searching time and PEG method [11] that has high coding complexity. BIBD in combinatorial mathematics is used to construct a high-performance LDPC code with girth length of at least six [12-14]. A novel construction method of QC-LDPC code is proposed in the paper, which is based on protograph and BIBD in combinational mathematics. The elements in the base matrix of protograph that we proposed are derived by mathematical relationships, and they have double diagonal structure [15]. As we all know that LDPC codes that can encode efficiently need to be no low weight code words, while general double diagonal structures will cause low weight code words. However, for the double diagonal structure in the
paper, we specially designed three circular permutation matrixes with codes weight $2,2,1$ in the first left column, which overcomes the low weight code words in general structure and achieves rapid encoding at the same time. In addition, the girth length of the code is at least 6 , and simulation results show that the method possesses excellent performance to adopt the AWGN channel and BP decoding algorithm.

## 2. The Extension of Protograph QC-LDPC Code Based on BIBD The extension method based on BIBD

Here is a base matrix of simple protograph shown below:

$$
\boldsymbol{H}_{\text {base }}=\left[\begin{array}{ccccc}
a_{0,0} & a_{0,1} & a_{0,2} & \cdots & a_{0, l}  \tag{1}\\
a_{1,0} & a_{1,1} & a_{1,2} & \cdots & a_{1, l} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
a_{p, 0} & a_{p, 1} & a_{p, 2} & \cdots & a_{p, l}
\end{array}\right]
$$

The $a_{p, l}, p$ and $l$ are integers $\left(a_{p, l} \geq 0,0 \leq p \leq 4, l \geq 0\right)$. Here we do the extension to the BIBD based on Bose - II type as an example:
(1) Copy each node of the simple protograph for $N$ times, $N=q=20 t+1$.
(2) Do the replacement operation to the protograph got from (1) according to the following rules:

The circular permutation matrix $\Phi_{k}$ is got by shifting the q-dimension position vector of $L(k)(k$ $\in\{1,2, \ldots, \infty\})$ :

$$
L(k)=\left\{\begin{array}{l}
L(1+5 i)=\partial^{2 i} \bmod q  \tag{2}\\
L(2+5 i)=\partial^{2 i+4 t} \bmod q \\
L(3+5 i)=\partial^{2 i+8 t} \bmod q \quad i=0,1,2,3, \ldots p p \\
L(4+5 i)=\partial^{2 i+12 t} \bmod q \\
L(5+5 i)=\partial^{2 i+16 t} \bmod q
\end{array}\right.
$$

(3) We will extend a circle permutation matrix with size of $q * q=(20 t+1) *(20 t+1)$ by XOR operations of the circular permutation matrix got from step (2), according to the value of $a_{p, l}$. The row and column weight are all equal to $a_{p, l}$. In particular, if $a_{p, l}$ is equal to zero, the extension is a all-zeros matrix $O_{q}$, its size is $q * q=(20 t+1) *(20 t+1)$;

Here is an example of expanding the protograph based on the Bose - II of BIBD.
As shown in the following graph with 6 BN and 3 CN :


Fig. 1 A simple protograph
We can get the base matrix of protograph from graph 4:

$$
H_{\text {base }}=\left[\begin{array}{llllll}
2 & 1 & 2 & 2 & 1 & 0  \tag{3}\\
1 & 3 & 0 & 2 & 2 & 1 \\
2 & 1 & 1 & 1 & 0 & 2
\end{array}\right]
$$

According to the step (1) (2) (3), we replace the element 0 to all-zeros matrix Oq, which size is $q$ * q , and replace the $\mathrm{r}(\mathrm{r} \geq 1)$ to X-OR operations of r circular permutation matrix $\Phi \mathrm{k}$, then we get the following check matrix of PBIBD-LDPC.

$$
H_{1 / 2}=\left(\begin{array}{cccccc}
\Phi_{1} \oplus \Phi_{2} & \Phi_{6} & \Phi_{11} \oplus \Phi_{12} & \Phi_{16} \oplus \Phi_{17} & \Phi_{21} & O_{q}  \tag{4}\\
\Phi_{3} & \Phi_{7} \oplus \Phi_{8} \oplus \Phi_{9} & O_{q} & \Phi_{18} \oplus \Phi_{19} & \Phi_{22} \oplus \Phi_{23} & \Phi_{26} \\
\Phi_{4} \oplus \Phi_{5} & \Phi_{10} & \Phi_{13} & \Phi_{20} & O_{q} & \Phi_{27} \oplus \Phi_{28}
\end{array}\right)
$$

## 3. Fast encoding characteristics of matrix

A base matrix of protograph LDPC which code rate is $\mathrm{a} /(\mathrm{a}+3)$ is designed as shown below:

$$
H_{\text {basel }}=\left[\begin{array}{llll|lll}
\left(1^{2}+1^{2}\right) \bmod 4 & {\left[\left(1^{2}+2^{2}\right)+0\right] \bmod 4} & \cdots & {\left[\left(1^{2}+a^{2}\right)+0\right] \bmod 4} & 2 & 1 & 0  \tag{5}\\
\left(2^{2}+1^{2}\right) \bmod 4 & {\left[\left(2^{2}+2^{2}\right)+3\right] \bmod 4} & \cdots & {\left[\left(2^{2}+a^{2}\right)+3\right] \bmod 4} & 2 & 1 & 1 \\
\left(3^{2}+1^{2}\right) \bmod 4 & {\left[\left(3^{2}+2^{2}\right)+4\right] \bmod 4} & \cdots & {\left[\left(3^{2}+a^{2}\right)+4\right] \bmod 4} & 1 & 0 & 1
\end{array}\right]
$$

As the three elements, which are $(12+12) \bmod 4=2, \quad(22+12) \bmod 4=1, \quad(32+12) \bmod 4=2$, shown in the first column in the left half, they are all calculated by ( $\mathrm{x} 2+\mathrm{y} 2$ ) $\bmod 4=2$. And the value of x and $y$ are related to their position of the row and column. For example, if its position is in the row 1 and column 1 , then $\mathrm{x}=1, \mathrm{y}=1,(12+12) \bmod 4=2$. The extension of the rest columns are all extended based on $[(x 2+y 2)+w 1 / \mathrm{w} 2 / \mathrm{w} 3] \bmod 4$. The value of w 1 corresponding to the 1 th row is equal to 0 . The value of w 2 corresponding to the 2 th row is equal to 3 . The value of w 3 corresponding to the 3th row is equal to 4 .

According to the extension method of protograph based on BIBD is proposed in the paper, we can obtain the check matrix of Protograph-LDPC code whose rate is $\mathrm{a} /(\mathrm{a}+3)$ as follows:

$$
H_{a /(a+3)}=\left[\begin{array}{ll}
H_{a} & H_{d} \tag{6}
\end{array}\right]
$$

Ha corresponds to the check matrix extended from left half part of formula (9) and Hd corresponds to the check matrix extended from right half part.

Here:

$$
H_{a}=\left[\begin{array}{cccc}
H_{1,1} & H_{1,2} & \cdots & H_{1, a}  \tag{7}\\
H_{2,1} & H_{2,2} & \cdots & H_{2, a} \\
H_{3,1} & H_{3,2} & \cdots & H_{3, a}
\end{array}\right]_{3 \times a}
$$

$H_{1,1}, H_{1,2}, \cdots, H_{3, a}$ are the X-OR operation of the circular permutation matrix or all-zeros matrix.

$$
H_{d}=\left[\begin{array}{ccc}
\Phi_{1} \oplus \Phi_{2} & I_{1} & O  \tag{8}\\
\Phi_{3} \oplus \Phi_{4} & I_{2} & I_{3} \\
\Phi_{5} & O & I_{4}
\end{array}\right]
$$

The double diagonal structure of Hd is the most basic part of the fast encoding. But the double diagonal structure will inevitably lead to low weight code, because the double diagonal structure will cause a low column weight of some rows or columns. And the low weight code will make the minimum hamming distance smaller and influence decoding performance. While the novel double diagonal structure of Hd proposed in this paper designs three circular permutation matrixes, and their codes weight respectively are $2,2,1$, in the first left column of the double diagonal structure. Thus we can achieve rapid encoding and avoid low weight code at the same time.

So the structure of $\mathrm{Ha} /(\mathrm{a}+3)$ can be summarized as shown below:

$$
H_{a /(a+3)}=\left[\begin{array}{ll}
H_{a} & H_{d}
\end{array}\right]=\left[\begin{array}{ccccccc}
H_{1,1} & H_{1,2} & \cdots & H_{1, a} & \Phi_{1} \oplus \Phi_{2} & I_{1} & O  \tag{9}\\
H_{2,1} & H_{2,2} & \cdots & H_{2, a} & \Phi_{3} \oplus \Phi_{4} & I_{2} & I_{3} \\
H_{3,1} & H_{3,2} & \cdots & H_{3, a} & \Phi_{5} & O & I_{4}
\end{array}\right]
$$

In order to test the PBIBD - LDPC code proposed in this paper whether has the fast encoding features, we assume that a code vector $\mathrm{c}=[\mathrm{T} 1 \mathrm{~T} 2 \cdots \mathrm{TaS} 1 \mathrm{~S} 2 \mathrm{~S} 3], \mathrm{T} 1 \mathrm{~T} 2 \cdots \mathrm{Ta}$ is the information bit vector and S1S2S3 is the parity vector. According to the standard principle of coding algorithm $\mathrm{HcT}=0$, we can get:

$$
\left[\begin{array}{ccccccc}
\boldsymbol{H}_{1,1} & \boldsymbol{H}_{1,2} & \cdots & \boldsymbol{H}_{1, a} & \Phi_{1} \oplus \Phi_{2} & \boldsymbol{I}_{1} & \boldsymbol{O}  \tag{10}\\
\boldsymbol{H}_{2,1} & \boldsymbol{H}_{2,2} & \cdots & \boldsymbol{H}_{2, a} & \Phi_{3} \oplus \Phi_{4} & \boldsymbol{I}_{2} & \boldsymbol{I}_{3} \\
\boldsymbol{H}_{3,1} & \boldsymbol{H}_{3,2} & \cdots & \boldsymbol{H}_{3, a} & \Phi_{5} & \boldsymbol{O} & \boldsymbol{I}_{4}
\end{array}\right] \cdot\left[\boldsymbol{T}_{1} \boldsymbol{T}_{2} \cdots \boldsymbol{T}_{h} \boldsymbol{S}_{1} \boldsymbol{S}_{2} \boldsymbol{S}_{3}\right]^{T}=\mathbf{0}
$$

The system of linear equations of form (10) is expressed as follows:

$$
\left\{\begin{array}{c}
\boldsymbol{H}_{1,1} \cdot \boldsymbol{T}_{1}^{\mathrm{T}} \oplus \boldsymbol{H}_{1,2} \cdot \boldsymbol{T}_{2}^{\mathrm{T}} \oplus \cdots \oplus \boldsymbol{H}_{1, \mathrm{a}} \cdot \boldsymbol{T}_{a}{ }^{\mathrm{T}} \oplus \boldsymbol{F}_{1} \cdot \boldsymbol{S}_{1}{ }^{\mathrm{T}} \oplus \boldsymbol{S}_{2}{ }^{\mathrm{T}}=0  \tag{11}\\
\boldsymbol{H}_{2,1} \cdot \boldsymbol{T}_{1}^{\mathrm{T}} \oplus \boldsymbol{H}_{2,2} \cdot \boldsymbol{T}_{2}{ }^{\mathrm{T}} \oplus \cdots \oplus \boldsymbol{H}_{2, a} \cdot \boldsymbol{T}_{a}^{\mathrm{T}} \oplus \boldsymbol{F}_{2} \cdot \boldsymbol{S}_{1}^{\mathrm{T}} \oplus \boldsymbol{S}_{2}{ }^{\mathrm{T}} \oplus \boldsymbol{S}_{3}{ }^{\mathrm{T}}=0 \\
\boldsymbol{H}_{3,1} \cdot \boldsymbol{T}_{1}^{\mathrm{T}} \oplus \boldsymbol{H}_{3,2} \cdot \boldsymbol{T}_{2}^{\mathrm{T}} \oplus \cdots \oplus \boldsymbol{H}_{3, a} \cdot \boldsymbol{T}_{a}^{\mathrm{T}} \oplus \boldsymbol{F}_{3} \cdot \boldsymbol{S}_{1}{ }^{\mathrm{T}} \oplus \boldsymbol{S}_{3}{ }^{\mathrm{T}}=0
\end{array}\right.
$$

Here:

$$
\boldsymbol{F}_{1}=\Phi_{1} \oplus \Phi_{2}, \quad \boldsymbol{F}_{2}=\Phi_{3} \oplus \Phi_{4}, \quad \boldsymbol{F}_{3}=\Phi_{5}
$$

Then w1, w2, w3 are expressed as follows:

$$
\begin{aligned}
& w_{1}=\boldsymbol{H}_{1,1} \cdot \boldsymbol{T}_{1}^{\mathrm{T}} \oplus \boldsymbol{H}_{1,2} \cdot \boldsymbol{T}_{2}^{\mathrm{T}} \oplus \cdots \oplus \boldsymbol{H}_{1, a} \cdot \boldsymbol{T}_{\mathrm{a}}^{\mathrm{T}} \\
& w_{2}=\boldsymbol{H}_{2,1} \cdot \boldsymbol{T}_{1}^{\mathrm{T}} \oplus \boldsymbol{H}_{2,2} \cdot \boldsymbol{T}_{2}^{\mathrm{T}} \oplus \cdots \oplus \boldsymbol{H}_{2, a} \cdot \boldsymbol{T}_{a}^{\mathrm{T}} \\
& w_{3}=\boldsymbol{H}_{3,1} \cdot \boldsymbol{T}_{1}^{\mathrm{T}} \oplus \boldsymbol{H}_{3,2} \cdot \boldsymbol{T}_{2}^{\mathrm{T}} \oplus \cdots \oplus \boldsymbol{H}_{3, a} \cdot \boldsymbol{T}_{a}^{\mathrm{T}}
\end{aligned}
$$

Thus the system of linear equations can be simplified as below:

$$
\left\{\begin{array}{c}
w_{1} \oplus \boldsymbol{F}_{1} \cdot \boldsymbol{S}_{1}{ }^{\mathrm{T}} \oplus \boldsymbol{S}_{2}{ }^{\mathrm{T}}=0  \tag{12}\\
w_{2} \oplus \boldsymbol{F}_{2} \cdot \boldsymbol{S}_{1}^{\mathrm{T}} \oplus \boldsymbol{S}_{2}{ }^{\mathrm{T}} \oplus \boldsymbol{S}_{3}{ }^{\mathrm{T}}=0 \\
w_{3} \oplus \boldsymbol{F}_{3} \cdot \boldsymbol{S}_{1}{ }^{\mathrm{T}} \oplus \boldsymbol{S}_{3}{ }^{\mathrm{T}}=0
\end{array}\right.
$$

The check code vector can be obtained by elimination method:

$$
\begin{gather*}
\boldsymbol{S}_{1}^{\mathrm{T}}=\left(w_{1} \oplus w_{2} \oplus w_{3}\right) \cdot\left(\boldsymbol{F}_{1} \oplus \boldsymbol{F}_{2} \oplus \boldsymbol{F}_{3}\right)^{-1}  \tag{13}\\
\boldsymbol{S}_{2}{ }^{\mathrm{T}}=w_{1} \oplus \boldsymbol{F}_{1} \cdot \boldsymbol{S}_{1}^{\mathrm{T}}  \tag{14}\\
\boldsymbol{S}_{3}{ }^{\mathrm{T}}=w_{3} \oplus \boldsymbol{F}_{3} \cdot \boldsymbol{S}_{1}{ }^{\mathrm{T}} \tag{15}
\end{gather*}
$$

Thus we can obtain the code vector: $\mathrm{c}=[\mathrm{T} 1 \mathrm{~T} 2 \cdots \mathrm{TaS} 1 \mathrm{~S} 2 \mathrm{~S} 3]$.

## 4. Simulation and Performance Analysis

Case 1: The base matrix of protograph based on $G F(20 t+1), t=12, q=20 t+1=241$, is extended using the BIBD extension method proposed in this paper. $\mathrm{a}=3$, the corresponding Hbase 1 is:

$$
H_{\text {basel }}=\left[\begin{array}{lll|lll}
2 & 1 & 2 & 2 & 1 & 0  \tag{16}\\
1 & 3 & 0 & 2 & 1 & 1 \\
2 & 1 & 2 & 1 & 0 & 1
\end{array}\right]
$$

Then Ha is a matrix with size of $3 q^{*} 3 q$ :

$$
H_{a}=\left[\begin{array}{ccc}
\Phi_{1} \oplus \Phi_{2} & \Phi_{6} & \Phi_{11} \oplus \Phi_{12}  \tag{17}\\
\Phi_{3} & \Phi_{7} \oplus \Phi_{8} \oplus \Phi_{9} & O_{q} \\
\Phi_{4} \oplus \Phi_{5} & \Phi_{10} & \Phi_{13} \oplus \Phi_{14}
\end{array}\right]
$$

Then Hd is a matrix with size of $3 q * 3 q$ too:

$$
H_{d}=\left[\begin{array}{ccc}
\Phi_{16} \oplus \Phi_{17} & I_{1} & O_{q}  \tag{18}\\
\Phi_{18} \oplus \Phi_{19} & I_{2} & I_{3} \\
\Phi_{20} & O_{q} & I_{4}
\end{array}\right]
$$

And:

$$
H_{1 / 2}=\left[\begin{array}{cccccc}
\Phi_{1} \oplus \Phi_{2} & \Phi_{6} & \Phi_{11} \oplus \Phi_{12} & \Phi_{16} \oplus \Phi_{17} & I_{1} & O_{q}  \tag{19}\\
\Phi_{3} & \Phi_{7} \oplus \Phi_{8} \oplus \Phi_{9} & O_{q} & \Phi_{18} \oplus \Phi_{19} & I_{2} & I_{3} \\
\Phi_{4} \oplus \Phi_{5} & \Phi_{10} & \Phi_{13} \oplus \Phi_{14} & \Phi_{20} & O_{q} & I_{4}
\end{array}\right]
$$

$\mathrm{H} 1 / 2$ is obtained by having a particular value to refuse girth 4 in the Tanner graph. Let I1 be a q * q identity matrix shifted to the right by 81 , noted $\mathrm{I} 1=\mathrm{I}$ ( 81 ) , $\mathrm{I} 2=\mathrm{I}$ (141) , $\mathrm{I} 3=\mathrm{I}$ (29) , I4=I (113) . A PBIBD-LDPC $(1446,723)$ code with a code rate of 0.5 is constructed by the check matrix H1/2 based on Gaussian elimination method. In order to fully illustrate the error correction performance of the proposed code, we compare the PBIBD - LDPC code $(1446,723)$ with the protograph QC-LDPC code having same code rate constructed based on Vander monde matrix and PEG algorithm [16] , and good QC-LDPC constructed based on lifting [17]. In the simulation, we adopt the AWGN channel, BPSK modulation and BP decoding algorithm for 100 iterations. The simulation results are shown in figure 5. When the BER=10-7, the proposed PBIBD - LDPC code $(1446,723)$ gains 0.5 dB of NCG compared with protograph QC-LDPC codes constructed based on Vander monde matrix and PEG algorithm[16]. And it gains 0.15 dB of NCG compared with QCLDPC constructed based on lifting [17]. And the proposed PBIBD - LDPC code $(1446,723)$ has special double diagonal structure, thus it has lower coding complexity.


Fig. 2 PBIBD - LDPC code and other code error correction performance comparison
Case 2: The base matrix of protograph based on $G F(20 t+1), t=14, q=20 t+1=281$, is extended by the BIBD extension method proposed in this paper. It is assumed that $\mathrm{a}=12$ and the corresponding Hbase2 is:

$$
H_{\text {base } 2}=\left[\begin{array}{llllll|lll}
2 & 1 & 2 & 1 & \cdots & 1 & 2 & 1 & 0  \tag{20}\\
1 & 3 & 0 & 3 & \cdots & 3 & 2 & 1 & 1 \\
2 & 1 & 2 & 1 & \cdots & 1 & 1 & 0 & 1
\end{array}\right]
$$

Ha is a matrix with size of $3 \mathrm{q}^{*} 12 \mathrm{q}$ :

$$
H_{a}=\left[\begin{array}{cccccc}
\Phi_{1} \oplus \Phi_{2} & \Phi_{6} & \Phi_{11} \oplus \Phi_{12} & \Phi_{16} & \cdots & \Phi_{56}  \tag{21}\\
\Phi_{3} & \Phi_{7} \oplus \Phi_{8} \oplus \Phi_{9} & O_{q} & \Phi_{17} \oplus \Phi_{18} \oplus \Phi_{19} & \cdots & \Phi_{57} \oplus \Phi_{58} \oplus \Phi_{59} \\
\Phi_{4} \oplus \Phi_{5} & \Phi_{10} & \Phi_{13} \oplus \Phi_{14} & \Phi_{20} & \cdots & \Phi_{60}
\end{array}\right]
$$

And Hd is a matrix with size of $3 q^{*} 3 q$ too:

$$
H_{d}=\left[\begin{array}{ccc}
\Phi_{61} \oplus \Phi_{62} & I_{1} & O_{q}  \tag{22}\\
\Phi_{63} \oplus \Phi_{64} & I_{2} & I_{3} \\
\Phi_{65} & O_{q} & I_{4}
\end{array}\right]
$$

Then:

$$
H_{455}=\left[\begin{array}{cccccc:ccc}
\Phi_{1} \oplus \Phi_{2} & \Phi_{6} & \Phi_{11} \oplus \Phi_{12} & \Phi_{16} & \ldots & \Phi_{56} & \Phi_{61} \oplus \Phi_{62} & I_{1} & O_{q}  \tag{23}\\
\Phi_{3} & \Phi_{7} \oplus \Phi_{8} \oplus \Phi_{9} & O_{q} & \Phi_{17} \oplus \Phi_{18} \oplus \Phi_{19} & \cdots & \Phi_{57} \oplus \Phi_{58} \oplus \Phi_{59} & \Phi_{63} \oplus \Phi_{64} & I_{2} & I_{3} \\
\Phi_{4} \oplus \Phi_{5} & \Phi_{10} & \Phi_{13} \oplus \Phi_{14} & \Phi_{20} & \cdots & \Phi_{60} & \Phi_{65} & O_{q} & I_{4}
\end{array}\right]
$$

$H_{4 / 5}$ is obtained by having a particular value to refuse girth 4 in the Tanner graph. $I_{1}=I$ (111), $I_{2}=I$ (181) , $I_{3}=I(76), I_{4}=I(42)$. A PBIBD-LDPC $(4215,3372)$ code with a code rate of 0.8 is constructed by the check matrix $H_{4 / 5}$ based on Gaussian elimination method. In order to fully illustrate the error correction performance of the proposed code, we compare the PBIBD - LDPC code $(4215,3372)$ with the code having same code rate, DS LDPC code $(5100,4083)$ constructed based on difference set[18]. In the simulation, we adopt the AWGN channel, BPSK modulation and BP decoding algorithm for 50 iterations. The simulation results are shown in figure 6. When the $\operatorname{BER}=10^{-7}$, the distance to Shanon is just 1.1 dB , and the decoding performance increases 0.1 dB than the DS LDPC $(5100,4083)$.


Fig. 3 Error correction performance of PBIBD - LDPC code and other codes

## 5. Conclusion

A novel construction method of QC-LDPC based on protograph and BIBD is proposed in combinatorial mathematics in the paper. The girth length of the proposed code is at least 6. Especially the elements in the base matrix of protograph proposed in this paper are derived by mathematical relation and it has double diagonal structure. And it has lower encoding complexity. The simulation result shows that the proposed code has a better error correction performance compared with protograph LDPC code constructed based on Vandermonde matrix, QC - LDPC code constructed by lifting and LDPC code based on difference set.

## Acknowledgments

This work is supported by the National Natural Science Foundation of China (61171158, 61571072 ) , the Natural Science Foundation Project of CQ CSTC (cstc2015jcyjA40015, cstc2013jcyjA40052), the Scientific and Technological Research Program of Chongqing Municipal Education Commission (Grant No.KJ130515).

## References

[1] Gallager R G. Low-density parity-check codes[J]. Information Theory, IRE Transactions on, 1962, 8(1): 21-28.
[2] DVB-S2 standard draft ETSI EN 302307 V1.1.1[S].2004.
[3] IEEE P802.16e/D8 [S]. 2005.
[4] Thorpe J. Low-density parity-check (LDPC) codes constructed from protographs[J]. IPN progress report, 2003, 42(154): 42-154.
[5] Van Nguyen T, Nosratinia A, Divsalar D. Rate-compatible protograph-based LDPC codes for inter-symbol interference channels[J]. Communications Letters, IEEE, 2013, 17(8): 1632-1635.
[6] Nguyen T V, Nosratinia A, Divsalar D. The design of rate-compatible protograph LDPC codes[J]. Communications, IEEE Transactions on, 2012, 60(10): 2841-2850.
[7] Mitchell D, Smarandache R, Costello D J. Quasi-cyclic LDPC codes based on pre-lifted protographs[J]. Information Theory, IEEE Transactions on, 2014, 60(10): 5856-5874.
[8] Divsalar D, Dolinar S, Jones C. Short protograph-based LDPC codes[C]. Military Communications Conference, 2007. MILCOM 2007. IEEE. IEEE, 2007: 1-6.
[9] Wang K, Hu S, Xiao Y, et al. Construction of protograph LDPC codes based on Jacket matrices[C]. Signal Processing (ICSP), 2010 IEEE 10th International Conference on. IEEE, 2010: 1604-1607.
[10] Wang K, Xiao Y, Kim K. Construction of protograph LDPC codes with circular generator matrices[J]. Systems Engineering and Electronics, Journal of, 2011, 22(5): 840-847.
[11]Bonello N, Chen S, Hanzo L. Construction of regular quasi-cyclic protograph LDPC codes based on Vandermonde matrices[J]. Vehicular Technology, IEEE Transactions on, 2008, 57(4): 2583-2588.
[12]Stinson D R. Combinatorial designs: constructions and analysis[M]. Springer Science \& Business Media, 2007.
[13]Zhao S M, Zhu X L, Xiao Y. A novel construction of quantum LDPC codes based on balanced Incomplete Block Designs[J]. Dianzi Yu Xinxi Xuebao(Journal of Electronics and Information Technology), 2011, 33(1): 218-222.
[14]Lan L, Tai Y Y, Lin S, et al. New constructions of quasi-cyclic LDPC codes based on special classes of BIBD's for the AWGN and binary erasure channels[J]. IEEE transactions on communications, 2008, 56(1): 39-48.
[15]Zhao X, Zhu L, Guo Y, et al. An effective puncturing algorithm for QC-LDPC codes with dualdiagonal structure[C]. Millimeter Waves (GSMM), 2012 5th Global Symposium on. IEEE, 2012: 38-42.
[16]Bonello N, Chen S, Hanzo L. Construction of regular quasi-cyclic protograph LDPC codes based on Vandermonde matrices[J]. Vehicular Technology, IEEE Transactions on, 2008, 57(4): 2583-2588.
[17]Asvadi R, Banihashemi A H, Ahmadian-Attari M. Design of finite-length irregular protograph codes with low error floors over the binary-input AWGN channel using cyclic liftings[J]. Communications, IEEE Transactions on, 2012, 60(4): 902-907.
[18]Esmaeili M, Javedankherad M. 4-Cycle free LDPC codes based on difference sets[J]. Communications, IEEE Transactions on, 2012, 60(12): 3579-3586.

