# The Construction of Low-Density Parity-Check Codes Based on Protograph

Xuemei Liu *, Qianyu Fan
*College of Science, Civil Aviation University of China, Tianjin, 300300, P.R.China*

**Abstract** Low-Density Parity-Check (LDPC) codes have low linear decoding complexity, which is a kind of good codes with excellent performance. Therefore, LDPC codes have great research value. This article is based on vector space over finite field as a theoretical tool by the inclusive relation of vector subspaces to construct protograph, and then constructs the LDPC codes with larger girth based on protograph by the modified progressive edge growth(M-PEG) algorithm, and utilize the related knowledge, such as Anzahl theorem in vector space, determines the code length, code rate and code word number of the LDPC codes. Moreover, the LDPC codes constructed are compared with the existing codes, and the constructed codes are better than some existing ones.

***Keywords:*** Low-Density Parity-Check codes, Code rate, Protograph, Modified Progressive Edge Growth Algorithm.

***AMS*** *classification*: 20G40 51D25

## 1. Introduction

The error correction coding theory is an important part of digital communication system and computer system, and LDPC codes channel coding technology is one of the important achievements in the coding field. As early as 1962, Gallager[1] proposed the LDPC codes, but has not received the attention of the coding community. Tanner[2] studied the codes from the perspective of graph theory until 1981, then, Mackay, Spielman and Wiberg "rediscovered" the LDPC codes almost at the same time. In recent years, how to construct a code with excellent performance and simple encoding and decoding has always been a hot topic.

The methods for constructing codes are divided into two kinds: random structure and algebraic structure. Different construction methods are designed to achieve the following goals: enlarging the ring in the graph, optimizing the node distribution of non-regular code, and reducing the coding complexity. In this paper, the LDPC codes are constructed by

*Correspondence : College of Science, Civil Aviation University of China,Tianjin,300300, P.R.China; E-mail: xm-liu771216@163.com.

the modified progressive edge growth. In 2005, Xiao-Yu Hu[3] proposed the PEG algorithm in the article "Regular and Irregular Progressive Edge Growth Tanner Graphs"; In 2008, Nicholas Bonello, Sheng Chen and Lajos Hanzo[4] constructed a kind of regular Quasi-Cyclic protograph LDPC codes based on the vandermonde matrix; In 2009, Tingting Fu, Zhanji Wu and Bowen Wang[5] gave a coding construction method based on the LDPC codes of PEG algorithm structure; In 2011, Yi Fang and Lin Wang[6] et al. proposed a joint optimization algorithm based on the protograph LDPC codes; In 2013, Lu Wang and Shuo Deng[7][8] used algebraic methods to construct LDPC codes based on symplectic space, unitary space and orthogonal space; In 2015, Jun Zhang, Guojun Han and Yi Fang[9] constructed the LDPC codes based on the general protograph. In the same year, Shu Chen and Xinqi Yuan[10]proposed an improved method of constructing QC-LDPC codes based on *PEG* algorithm.

This article utilize inclusion relation of vector subspaces to structure protograph, and then constructs the LDPC codes with larger girth based on protograph by the modified progressive edge growth(M-PEG) algorithm, which provides a new method for constructing LDPC codes, and gets a new series of LDPC codes with good performance with important theoretical significance and practical application value.

## 2. Preliminaries

In this section, we shall introduce the contents of LDPC codes and vector sapce over finite fields.

Firstly, the definition of LDPC codes is introduced.

LDPC codes are a class of linear block codes, defined by their parity-check matrices. The parity-check matrix $H$ is a matrix of size $M \times N$, then the code length is $N$, the length of information bits is $K$, the length of check bits $M = N - K$, the code word number $D = q^k$, and the code rate $R = \frac{K}{N}$.

**Definition 2.1.**[11] The parity-check matrix $H$ of binary LDPC code satisfies the following four condition:

(1) Each row cosists of $\rho$ "ones";

(2) Each column cosists of $\gamma$ "ones";

(3) The number of "one" in common between any two rows (or two columns) is no greater than 1;

(4) Both $\rho$ and $\gamma$ are small compared to the length of the code and the number of rows in $H$. That is, $H$ has a small density of "ones" and hence is a spare matrix.

For this reason, the code specified by $H$ is called an LDPC code. The LDPC code defined above is known as a regular LDPC code. If not all the columns or all the rows of the parity-check matrix $H$ have the same

number of "ones", an LDPC code is said to be irregular.

**Lemma 2.2.**[11]Let $\mathbb{C}$ be a linear code with check matrix $H$. Let $d$ be the largest integer such that any $d$ of the columns of $H$ are linearly independent. Then $\mathbb{C}$ has minimum distance $d+1$. (Conversely, if $\mathbb{C}$ has minimum distance $d+1$ then any $d$ columns of $H$ are linearly independent.)

The Tanner graph is a graph that shows the constraint relationship between codeword bit and parity bits, each coded bit (corresponding to a column in the check matrix) corresponds to a vertex, called variable node, and each check bit (corresponding to a row in the check matrix) also corresponds to a vertex, called check node. If a coded bit participates in a check bit, the corresponding position in the check matrix is not zero. Whereupon match the corresponding variable node and the check node by drawing a line. After connecting all the graphs, the obtained graph is the Tanner graph corresponding to the check matrix. The check matrix of each LDPC code can be represented by the Tanner graph.

**Definition 2.3.**[2]Several definitions of the Tanner graph:

(1)Degree refers to the number of edges that are connected to a vertex, that is, the degree of the variable node is equal to the weight of the column of the parity check matrix that correspond to the node, the degree of the check node is equal to the weight of the row of the parity check matrix corresponding to the node;

(2)Ring refers to a closed loop consisting of variable node, check node and side;

(3)Girth refers to the length of the shortest ring in the Tanner graph.

**Lemma 2.4.**[2]Any rings of LDPC code that length is L, satisfying $L \geq 4$, and is a multiple of 2.

Next, we shall introduce the relative contents of vector space over finite field.

Let $\mathbb{F}_q$ be the finite field with $q$ elements, where $q$ is a power of a prime and $n$ be a positive integer. We use $\mathbb{F}_q^n$ to denote the $n$-dimensional row vector space over the finite field $\mathbb{F}_q$.

The set of $n \times n$ nonsingular matrices over $\mathbb{F}_q$ forms a group under matrix multiplication, called the general linear group of degree $n$ over $\mathbb{F}_q$ and denoted by $GL_n(\mathbb{F}_q)$. In fact, $GL_n(\mathbb{F}_q)$ is transitive on the set of all subspaces of the same dimension in $\mathbb{F}_q^n$.

Let $s_1$, $s_2$ be two integers. Then the Gaussian coefficient

$$\begin{bmatrix} s_2 \\ s_1 \end{bmatrix}_q = \frac{\prod_{i=s_2-s_1+1}^{s_2} (q^i - 1)}{\prod_{i=1}^{s_1} (q^i - 1)}.$$

In particular, $\begin{bmatrix} s_2 \\ 0 \end{bmatrix}_q = 1$ for all integer $s_2$, and $\begin{bmatrix} s_2 \\ s_1 \end{bmatrix}_q = 0$ whenever $s_1 < 0$ or $s_2 < s_1$.

**Lemma 2.5.**[12]Let $0 \leq m \leq n$ and $N(m,n)$ be the number of $m$-dimensional vector subspaces of $\mathbb{F}_q^n$. Then

$$N(m,n) = \begin{bmatrix} n \\ m \end{bmatrix}_q = \frac{\prod_{i=n-m+1}^{n} (q^i - 1)}{\prod_{i=1}^{m} (q^i - 1)}.$$

**Lemma 2.6.**[12]Let $0 \leq t \leq m \leq n$ and $N(t,m,n)$ be the number of $t$-dimensional vector subspaces contained in a given $m$-dimensional vector subspace of $\mathbb{F}_q^n$. Then

$$N(t,m,n) = N(t,m) = \begin{bmatrix} m \\ t \end{bmatrix}_q = \frac{\prod_{i=m-t+1}^{m} (q^i - 1)}{\prod_{i=1}^{t} (q^i - 1)}.$$

**Lemma 2.7.**[12]Let $0 \leq t \leq m \leq n$. Then the number $N'(t,m,n)$ of $m$-dimensional vector subspaces containing a given $t$-dimensional vector subspace of $\mathbb{F}_q^n$ is equal to

$$N'(t,m,n) = N'(m-t,n-t) = \frac{\prod_{i=n-m+1}^{n-t} (q^i - 1)}{\prod_{i=1}^{m-t} (q^i - 1)}.$$

## 3. Protograph and LDPC codes based on protograph

### 3.1.Protograph

A protograph $\mathbb{G} = (V, C, \varepsilon)$ is a Tanner graph, which consists of $V, C$ being the set of variable and check nodes, respectively, and $\varepsilon$ being the set of undirected edges. The Tanner graph and its matrix are one-to-one correspondence, thus, the protograph can be represented by matrices.

Note: The number of nodes included in the protograph are relatively small, and parallel edges are allowed in the graph.

**Definition 3.1.1.** Given integers $1 \leq m_1 \leq m \leq n$. Let $\mathbb{G}$ be the binary matrix, whose rows are indexed by the $m_1$-dimensional vector subspaces of $\mathbb{F}_q^n$, and whose columns are indexed by the $m$-dimensional vector subspaces of $\mathbb{F}_q^n$. $\mathbb{G}(i,j) = 1$ if and only if the $i$-th $m_1$-dimensional vector subspace is contained in the $j$-th $m$-dimensional vector subspace, otherwise, $\mathbb{G}(i,j) =$

0.

By Lemmas 2.5, 2.6 and 2.7, $\mathbb{G}$ is an $M \times N$ matrix, whose constant column weight is $\gamma$, constant row weight is $\rho$, where

$$M = \begin{bmatrix} n \\ m_1 \end{bmatrix}_q, N = \begin{bmatrix} n \\ m \end{bmatrix}_q,$$

$$\gamma = \begin{bmatrix} m \\ m_1 \end{bmatrix}_q, \rho = \begin{bmatrix} n - m_1 \\ m - m_1 \end{bmatrix}_q.$$

From this, a protograph can be constructed.

**Definition 3.1.2.** Given integers $2 \leq m' \leq n'$. Let $V_1$ is a $(m' - m'_1)$-dimensional vector subspaces of $\mathbb{F}_q^{n'}$, where base

$$e_1 = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 & \cdots & 0 \\ & & & \cdots & & & \\ 0 & 0 & 0 & \cdots & 1 & \cdots & 0 \end{pmatrix}_{(m'-m'_1)\times N},$$

$V_2 = \{$all $m'_1$-dimensional vector subspaces of $\mathbb{F}_q^{n'}\}$, $V$ is a $m'$-dimensional vector subspaces of $\mathbb{F}_q^{n'}$, and satisfies $V = V_1 \oplus V_2$. Let $\mathbb{G}'$ be the binary matrix, whose rows are indexed by the $m'$-dimensional vector subspaces $V$ of $\mathbb{F}_q^{n'}$, and whose columns are indexed by the $m'_1$-dimensional vector subspaces $V_2$ of $\mathbb{F}_q^{n'}$. $\mathbb{G}'(i,j) = 1$ if and only if the $i$-th $m'$-dimensional vector subspace contains in the $j$-th $m'_1$-dimensional vector subspace, otherwise, $\mathbb{G}'(i,j) = 0$.

By Lemmas 2.5, 2.6 and 2.7, $\mathbb{G}'$ is an $M' \times N'$ matrix, where

$$M' = \begin{bmatrix} n' - (m' - m'_1) \\ m' - (m' - m'_1) \end{bmatrix}_q, N' = \begin{bmatrix} n' \\ m' \end{bmatrix}_q.$$

From this, a protograph can be constructed.

### 3.2.LDPC codes based on protograph

After expansion operation on a given protograph, an expanded protograph, namely derived graph, is obtained, which corresponds to the protograph LDPC code. Among them, the expansion operation is implemented by the PEG algorithm.

The PEG algorithm is a simple and effective method for constructing Tanner graphs, which aim to keep the large girth as much as possible, and increase the edges of variable nodes and check nodes one by one. The existing PEG algorithm first gives the number of variable nodes, the number

of check nodes and the distribution sequence of variable nodes, and then select the program starts and place new edges. After the new edges are placed, continue searching for the next edge until the end. In this paper, the modified PEG(M-PEG) algorithm aims to increase the girth, remove the small ring, and construct LDPC code with better performance.

**Algorithm:**

Initial value: The protograph $\mathbb{G}$ is a matrix of $M \times N$, define a $m \times n$ order all-one matrix, where $m \leq M, n \leq N$. Let $i, j = s, \cdots, 3, 2$, where $s \leq m$.

(1)If $i = s, j = s$, find all s-order all-one matrices in the protograph $\mathbb{G}$ in turn, that is,

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ & & & \cdots & & & \\ 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 1 & 1 & \cdots & 1 & 1 \end{pmatrix}_{s \times s},$$

keep 1 of its $a_{11}, a_{n1}, a_{12}, a_{22}, a_{23}, a_{33}, a_{34}, a_{44}, \cdots, a_{(n-1)n}, a_{nn}$ position, replace at the remaining position with 0, that is,

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ & & & \cdots & & & \\ 1 & 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 1 & 1 & 1 & \cdots & 1 & 1 \end{pmatrix}_{s \times s}$$

$$\longrightarrow \begin{pmatrix} 1 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 \\ & & & \cdots & & & \\ 0 & 0 & 0 & 0 & \cdots & 1 & 1 \\ 1 & 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}_{s \times s};$$

the transformed matrix is denoted as $\mathbb{G}_1$;

(2)If $i = s-1, j = s-1$, repeat the above step for all $s-1$ order all-one matrices in $\mathbb{G}_1$;

(3)Continue in order until $i = 3, j = 3$, at this time, find all 3 order

all-one matrices in the transformed matrix, repeat step (1), that is

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix};$$

the transformed matrix is denoted as $\mathbb{G}_2$;

(4)If $i = 2, j = 3$, find all $2 \times 3$ order all-one matrices in $\mathbb{G}_2$, that is $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$. Replace 1 at the $a_{21}$, $a_{23}$ positions with 0, that is

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix};$$

the transformed matrix is denoted as $\mathbb{G}_3$;

(5)If $i = 3, j = 2$, find all $3 \times 2$ order all-one matrices in $\mathbb{G}_3$, that is $\begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{pmatrix}$. Replace 1 at the $a_{11}$, $a_{31}$ positions with 0, that is

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 1 \\ 0 & 1 \end{pmatrix};$$

the transformed matrix is denoted as $\mathbb{G}_4$;

(6)If $i = 2, j = 2$, find all 2 order all-one matrices in $\mathbb{G}_4$, that is $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$. Replace 1 at the $a_{12}$ positions with 0, that is

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix};$$

the transformed matrix is denoted as $\mathbb{G}_5$;

(7)At this time, redefine a null matrix $\mathbb{G}_a$, compare $\mathbb{G}_5$ with $\mathbb{G}$, hold position of 1 which transformed in $\mathbb{G}$ and add it to $\mathbb{G}_a$. The transformed $\mathbb{G}_a$ is $\mathbb{G}_{a'}$, then combine $\mathbb{G}_5$ and $\mathbb{G}_{a'}$ into a new one matrix;

(8)Repeat (1) – (7) steps until no (1) – (6) steps appear;

(9)Check the resulting matrix and remove the duplicate column in the matrix.

In summary, the final matrix is the check matrix of the LDPC code constructed based on protograph.

Note: In (7), let $\mathbb{G} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$, $\mathbb{G}_5 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$, compare $\mathbb{G}_5$ with $\mathbb{G}$, the position of the change is $a_{21}$, $a_{32}$, $a_{13}$. Hold position of 1 which

transformed in $\mathbb{G}$ and add it to $\mathbb{G}_a$. the transformed $\mathbb{G}_a$ is $\mathbb{G}_{a'}$, at this time, $\mathbb{G}_{a'} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$, and then combine $\mathbb{G}_5$ with $\mathbb{G}_{a'}$ to obtain

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

### 3.3.Example

**Example 3.3.1.**Suppose $\mathbb{G}$ be the protograph, which is constructed by Definition 3.1.1. Let $n = 4, q = 2, m_1 = 1, m = 3$. Rows of the matrix $\mathbb{G}$ are indexed by the 1-dimensional vector subspaces, (0001), (0010), (0011), (0100), (0101), (0110), (0111), (1000), (1001), (1010), (1011), (1100), (1101), (1110), (1111). Columns of the matrix $\mathbb{G}$ are indexed by the 3-dimensional vector subspaces,

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

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

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

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

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

$\mathbb{G}(i, j) = 1$ if and only if the $i$-th 1-dimensional vector subspace is contained in the $j$-th 3-dimensional vector subspace. Thus, a $15 \times 15$ matrix $\mathbb{G}$ can

be obtained as the protograph.

$$\mathbb{G} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Extended the protograph $\mathbb{G}$ by the M-PEG algorithm, a LDPC code based on protograph with a girth of 6 and a parameter of $[39, 24, 3]$ can be obtained, and the extended protograph LDPC code is recorded as $\mathbb{C}$, where the code rate is $\frac{8}{13}$, the number of codewords is $2^{24}$.

We compare it with the existed LDPC code and the constructed LDPC code based on vector space;

The parameters of the known LDPC code is $[15, 7, 5]$[11], denoted by $\mathbb{C}_1$, code rate is $\frac{7}{15}$, girth is 6, and codeword number is $2^7$. The parameters of constructed LDPC code based on vector sapce is $[35, 24, 4]$, denoted by $\mathbb{C}_2$, code rate is $\frac{24}{35}$, girth is 6, and codeword number is $2^{24}$. Thus we can get that the length of code $\mathbb{C}$ is larger than code $\mathbb{C}_1$ and $\mathbb{C}_2$ when the girth is the same. Moreover, the codewords and code rate of $\mathbb{C}$ are larger than that of the known code $\mathbb{C}_1$.

| | N | K | L | R | D |
|---|---|---|---|---|---|
| $\mathbb{C}$ | 39 | 24 | 6 | $\frac{8}{13}$ | $2^{24}$ |
| $\mathbb{C}_1$ | 15 | 7 | 6 | $\frac{7}{15}$ | $2^7$ |
| $\mathbb{C}_2$ | 35 | 24 | 6 | $\frac{24}{35}$ | $2^{24}$ |

**Example 3.3.2.**Suppose $\mathbb{G}'$ be the protograph, which is constructed by Definition 3.1.2. let $n' = 4, q = 2, m'_1 = 1, m' = 3$, $V_1 = \{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}\}$, $V_2 = \{$ all 1-dimensional vector subspaces of $\mathbb{F}_2^4\}$, $V$ is a 3-dimensional vector subspaces of $\mathbb{F}_2^4$, and satisfies $V = V_1 \oplus V_2$. Rows of the matrix $\mathbb{G}'$ are

indexed by the 3-dimensional vector subspaces $V$,

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix};$$

Columns of the matrix $\mathbb{G}'$ are indexed by the 1-dimensional vector subspaces $V_2$. Where $\mathbb{G}'(i,j) = 1$ if and only if the $i$-th 3-dimensional vector subspace contains in the $j$-th 1-dimensional vector subspace. Thus, a $3 \times 15$ matrix $\mathbb{G}'$ can be obtained as the protograph. That is

$$\mathbb{G}' = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

Extended the protograph $\mathbb{G}'$ by the M-PEG algorithm, a LDPC code based on protograph with a girth of 6 and a parameter of $[6, 3, 3]$ can be obtained, and the extended protograph LDPC code is recorded as $\mathbb{C}'$, where the code rate is $\frac{1}{2}$.

$$\mathbb{C}' = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}.$$

We compare it with the existed LDPC code;

The parameters of the known LDPC code is $[15, 7, 5]$[11], we denote this code as $\mathbb{C}_1$, which has code rate $\frac{7}{15}$ and girth 6. Thus we can get that the rate of code $\mathbb{C}'$ is larger than that of code $\mathbb{C}_1$ when the girth is the same.

| | N | K | L | R |
|---|---|---|---|---|
| $\mathbb{C}'$ | 6 | 3 | 6 | $\frac{1}{2}$ |
| $\mathbb{C}_1$ | 15 | 7 | 6 | $\frac{7}{15}$ |

**Acknowledgements** This work is supported by the National Natural Science Foundation of China under Grant No. 11701558.

# References

[1] Gallager. *Low density parity check codes*[J], IRE Transactions on Information Theory, 1962, 8: 21-28.

[2] Tanner. *A recursive approach to low complexity codes*[J], IEEE Trans Inform Theory, 1981, 27: 533-547.

[3] Xiao-Yu Hu. *Regular and Irregular Progressive Edge-growth Tanner Graphs*[J], IEEE Transactions on Information Theory, 2005, 57(11): 386-398.

[4] Bonello N, Chen Sheng and Hanzo L. *Construction of regular quasi-cyclic protograph LDPC codes based on vandermonde matrices*[J], IEEE Transactions on Vehicular Technology, 2008, 57(04): 2583-2588.

[5] Tingting Fu, Zhanji Wu and Wenbo Wang. *PEG-Based Construction Method for Quasi-Cyclic LDPC*[J], Journal of Date Acquisition and Processing, 2009, 24: 182-186.

[6] Yi Fang, Lin Wang, Pingping Chen and Min Xiao. *Joint Optimization Algorithm for Protograph LDPC codes*[J], Journal of Applied Sciences, 2011, 29(6): 551-558.

[7] Lu Wang. *A class of LDPC codes constructed based on symplectic space*[D], Hebei Normal University, 2013.

[8] Shuo Deng. *A class of LDPC codes constructed based on unitary space and orthogoal space*[D], Hebei Normal University, 2013.

[9] Jun Zhang, Guojun Han and Yi Fang. *Deterministic Construction of Compressed Sensing Matrices from Protograph LDPC codes*[J], IEEE Signal processing letters, 2015, 22(11): 1960-1964.

[10] Shu Chen, Xinqi Yuan. *A class of QC-LDPC codes method constructed based on PEG algorithm*[J], Technology Outlook, 2015, 22: 153.

[11] Yu kou, Shu Lin and Marc P.C.Fossorier. *Low-Density Parity-Check Codes Based on Finite Geometries: A Rediscovery and New Results*[J], IEEE Transactions on Information Theory, 2001, 47(07): 2711-2736.

[12] Wan Zhexian. *Geometry of classical groups over finite fields (second edition)*[J], Beijing: Science Press, 2002.