Binary LDPC Codes Constructed Based on Symplectic Spaces over Finite Fields *

Shangdi Chen[†] Junying Liang

College of Science, Civil Aviation University of China, Tianjin, 300300, China

Abstract This paper mainly presents a construction of LDPC codes based on symplectic spaces. By two subspaces of type (m,r) to produce a subspace of type $(m+1,r)$ or $(m+1,r+1)$ in $\mathbb{F}_q^{(2\nu)}$, we use all subspaces of type (m,r) to mark rows and all subspaces of type $(m+1,r)$ and $(m+1,r+1)$ to mark columns of check matrix H. A construction of LDPC codes has been given based on symplectic spaces. As a special case, we use all subspaces of type $(1,0)$ to mark rows and all subspaces of type $(2,0)$ and $(2,1)$ to mark columns of check matrix H_1 in $\mathbb{F}_q^{(4)}$, the cycles of length 6 of H_1 is further discussed.

Keywords LDPC codes; symplectic spaces; totally isotropic subspaces; non-isotropic subspaces

MSC 2010 94A60; 94A62

1 Introduction

In 1962, Gallager proposed LDPC codes. In 1963, Gallager published "Low-Density Parity-Check Code" which began to mark the birth of LDPC codes. However, LDPC codes were limited to the technical conditions at that time and lacked a feasible decoding algorithm, which was largely ignored in the next 35 years. The rediscovery of LDPC codes[2] in the late 1990's showed that the performance of LDPC codes based on irregular bidirectional graphs is better than that of Turob codes. K. Yu, et al.[3] constructed four classes of LDPC codes based on points and lines of finite geometrices and gave the lower bounds of the minimum distance. R. Tanner[4] gave a method that described for constructing long error-correcting codes from one or more shorter error-correcting codes, referred to as subcodes,

[*]Supported by the National Natural Science Foundation of China (No. 61179026)

[†]Corresponding author. E-mail address: 11csd@163.com

and a bipartite graph. H. Tang, et al.[5] presented new algebraic methods for constructing codes based on hyperplanes of two different dimensions in finite geometries. L. Zeng, et al.[7] introduced five methods for constructing nonbinary LDPC codes based on finite geometrices. These methods result in five classes of nonbinary LDPC codes, one class of cyclic LDPC codes, three classes of quasi-cyclic LDPC codes and one class of structured regular LDPC codes. S. Myung, et al.[6] presented a special class of quasi-cyclic low-density parity-check (QC-LDPC) codes, called block-type LDPC (B-LDPC) codes, which have an efficient encoding algorithm due to the simple structure of their parity-check matrices. D.Chandler, et al.[8] studied the permutation action of a finite symplectic group of characteristic 2 on the set of subspaces of its standard module which are either totally isotropic or else complementary to totally isotropic subspaces with respect to the alternating form. A general formula is obtained for the 2-rank of the incidence matrix for the inclusion of one-dimensional subspaces in the distinguished subspaces of a fixed dimension.

In recent years, the well-constructed LDPC codes based on matrix geometry, finite geometry, graph theory and combinatorial designs are studied. Many researchers have made greatly contribution to this area. C. Ma and his students[9] presented three families of low-density parity-check (LDPC) codes are constructed based on the totally isotropic subspaces of symplectic, unitary, and orthogonal spaces over finite fields, respectively. The minimum distances of the three families of LDPC codes in some special cases are settled. X. Wang and Y. Hao[10] gave two constructions of LDPC codes with larger grith based on the pseudo-symplectic geometry over finite fields. At present, LDPC codes are considered to be the best performance codes so far, LDPC codes are of great importance both in theory and in practical applications. Therefore, LDPC codes have become a hot topic to research .

The structure of the paper is following: In section 2 we give some preliminaries. The main body of the paper are section 3. By two subspaces of type (m,r) to produce a subspace of type $(m+1,r)$ or $(m+1,r+1)$ in $\mathbb{F}_q^{(2\nu)}$, we use all subspaces of type (m,r) to mark rows and all subspaces of type $(m+1,r)$ and $(m+1,r+1)$ to mark columns of check matrix H. A construction of LDPC codes based on symplectic spaces has been given. As a special case, consider $\mathbb{F}_q^{(4)}$, the cycles of length 6 of H_1 is discussed.

2 Preliminaries

LDPC codes are a class of linear block codes.

Definition 2.1 [3] *An LDPC code is defined as the null space of a parity check matrix H with the following structural properties:*

(1) *each row consists of* ρ *"ones";*

(2) *each column consists of* γ *"ones";*

(3) *the number of "ones" in common between any two columns, denote* λ, *is not greater than 1;*

(4) *both* ρ *and* γ *are small compared to the length of the code and the number of rows in H.*

Since ρ and γ are small, H has a small density of "one" and hence is a sparse 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"(or weights), an LDPC code is said to be irregular.

Let $\mathbb{F}_q$ be the finite field with q element, where q is a power of a prime, and ν a positive integer. We use

$$\mathbb{F}_q^{(2\nu)} = \{(x_1, x_2, \cdots, x_{2\nu}) | x_i \in \mathbb{F}_q, i = 1, 2, \cdots, 2\nu\}$$

to denote the 2ν-dimensional row vector space over $\mathbb{F}_q$.

Theorem 2.1 [1] *Let K be an* $n \times n$ *alternate matrix over* $\mathbb{F}_q$. *The rank of K is necessarily even. Furthermore, if K is of rank* $2\nu (\leq n)$, *then K is cogredient to*

$$\begin{bmatrix} 0 & I^{(\nu)} & \\ -I^{(\nu)} & 0 & \\ & & 0^{(n-2\nu)} \end{bmatrix}.$$

Let K be a $2\nu \times 2\nu$ nonsingular alternate matrix over $\mathbb{F}_q$. A $2\nu \times 2\nu$ matrix T over $\mathbb{F}_q$ is called a symplectic matrix with respect to K if

$$TKT^t = K.$$

Clearly, $2\nu \times 2\nu$ symplectic matrix with respect to nonsingular alternate matrix K are nonsingular and they form a group with respect to matrix multiplication, called the symplectic group of degree 2ν with respect to K over $\mathbb{F}_q$ and denoted by $Sp_{2\nu}(\mathbb{F}_q, K)$.

Without loss of generality, we take

$$K = \begin{bmatrix} 0 & I^{(\nu)} \\ -I^{(\nu)} & 0 \end{bmatrix}$$

denote the symplectic group with respect to K over $\mathbb{F}_q$ simply by denoted by $Sp_{2\nu}(\mathbb{F}_q)$, called it the symplectic group of degree 2ν over $\mathbb{F}_q$.

Clearly, $Sp_{2\nu}(\mathbb{F}_q)$ is a subgroup of $GL_{2\nu}(\mathbb{F}_q)$ and the action of $GL_{2\nu}(\mathbb{F}_q)$ on $\mathbb{F}_q^{(2\nu)}$ induces an action of $Sp_{2\nu}(\mathbb{F}_q)$ on $\mathbb{F}_q^{(2\nu)}$ as follow:

$$\mathbb{F}_q^{(2\nu)} \times Sp_{2\nu}(\mathbb{F}_q) \to \mathbb{F}_q^{(2\nu)}$$

$$((x_1, x_2, \cdots, x_{2\nu}), T) \mapsto (x_1, x_2, \cdots, x_{2\nu})T.$$

The elements of $Sp_{2\nu}(\mathbb{F}_q)$ are also called symplectic transformations. The vector space $\mathbb{F}_q^{(2\nu)}$ together with the above group action of the symplectic group $Sp_{2\nu}(\mathbb{F}_q)$, ia called the 2ν-dimensional symplectic space over $\mathbb{F}_q$.

Let P be an m-dimensional vector subspace of $\mathbb{F}_q^{(2\nu)}$. We use the same letter P to denote a matrix representation of the vector subspace P, i.e., P is an $m \times 2\nu$ matrix of rank m whose rows form a basis of P. It is easy to see that PKP^t is an alternate matrix. By Theorem 2.1, let the rank of PKP^t be $2s$, then we call the vector subspace P a subspace of type (m, s). Clearly $s \leq \nu$ and $2s \leq m$. In particular, subspaces of type $(m, 0)$ are called m-dimensional totally isotropic subspaces, and subspaces of type $(2s, s)$ are called $2s$-dimensional non-isotropic subspaces. It is clear that a subspace P is a totally isotropic if and only if $PKP^t = 0$, and it is non-isotropic if and only if PKP^t is nonsingular.

Theorem 2.2 [1] *Let $2s \leq m \leq \nu + s$. Then the number of subspaces of type (m, s) in the 2ν-dimensional symplectic space over $\mathbb{F}_q$ is given by*

$$N(m, s; 2\nu) = q^{2s(\nu+s-m)} \frac{\prod\limits_{i=\nu+s-m+1}^{\nu} (q^{2i} - 1)}{\prod\limits_{i=1}^{s} (q^{2i} - 1) \prod\limits_{i=1}^{m-2s} (q^i - 1)}.$$

Theorem 2.3 [1] *Subspaces of type (m, s) exist in the 2ν-dimensional symplectic space if and only if $2s \leq m \leq \nu + s$.*

Theorem 2.4 [1] *$\mathcal{M}(m_1, s_1; m, s; 2\nu)$ is non-empty if and only if*

$$2s \leq m \leq \nu + s,$$

$$2s_1 \leq m_1 \leq \nu + s_1,$$

and

$$0 \leq s - s_1 \leq m - m_1,$$

and these three conditions are equivalent to

$$2s \leq m \leq \nu + s$$

and

$$max\{0, m_1 - s - s_1\} \leq min\{m - 2s, m_1 - 2s_1\}.$$

Theorem 2.5 [1] *Let*

$$2s \leq m \leq \nu + s$$

and

$$max\{0, m_1 - s - s_1\} \leq \{minm - 2s, m_1 - 2s_1\}.$$

Then the number $N(m_1, s_1; m, s; 2\nu)$ of subspaces of type (m_1, s_1) contained in a given subspace of type (m, s) in the 2ν-dimensional symplectic space over $\mathbb{F}_q$ is

$$N(m_1, s_1; m, s; 2\nu) \quad = \quad \sum_{k=max\{0, m_1-s-s_1\}}^{min\{m-2s, m_1-2s_1\}} q^{2s_1(s+s_1-m_1+k)+(m_1-k)(m-2s-k)}$$
$$\times \frac{\prod_{i=s+s_1-m_1+k+1}^{s}(q^{2i}-1) \prod_{i=m-2s-k+1}^{m-2s}(q^i-1)}{\prod_{i=1}^{s_1}(q^{2i}-1) \prod_{i=1}^{m_1-2s_1-k}(q^i-1) \prod_{i=1}^{k}(q^i-1)}.$$

Theorem 2.6 [1] *Let*

$$2s \leq m \leq \nu + s$$

and

$$max\{0, m_1 - s - s_1\} \leq \{minm - 2s, m_1 - 2s_1\}.$$

Then the number $N'(m_1, s_1; m, s; 2\nu)$ of subspaces of type (m, s) containing a given subspace of type (m_1, s_1) in the 2ν-dimensional symplectic space over $\mathbb{F}_q$ is

$$N'(m_1, s_1; m, s; 2\nu)$$
$$= \sum_{k=max\{0, m_1-s-s_1\}}^{min\{m-2s, m_1-2s_1\}} q^{2(\nu+s-m)(s+s_1-m_1+k)+(2\nu-m-k)(m_1-2s_1-k)}$$
$$\times \frac{\prod_{i=s+s_1-m_1+k+1}^{\nu+s_1-m_1}(q^{2i}-1) \prod_{i=m_1-2s_1-k+1}^{m_1-2s_1}(q^i-1)}{\prod_{i=1}^{\nu+s-m}(q^{2i}-1) \prod_{i=1}^{m-2s-k}(q^i-1) \prod_{i=1}^{k}(q^i-1)}.$$

Theorem 2.7 [11] *Take any 3 column vectors l_m, l_n and l_k, $m, n, k \in \{1, 2, \cdots, N\}$, $m \neq n \neq k$ in H, if there is free of cycles of length 4 in H, then the necessary and sufficient condition for H to have cycles of length 6 is that every two column vector has 1 on the same line, i.e., $l_m^T l_n = 1$, $l_m^T l_k = 1$, $l_n^T l_k = 1$.*

Theorem 2.8 [11] *If there is free of cycles of length 4 in H, then the necessary and sufficient condition for H to have free cycles of length 6 is that the condition of Theorem 2.7 is dissatisfied.*

3 Main Results

In this paper we assume that $\mathbb{F}_q$ is a finite field of characteristic 2.

Theorem 3.1 *Let V_1 and V_2 be two subspaces of type (m,r) of $\mathbb{F}_q^{(2\nu)}$. If $dim(V_1+V_2)=m+1$, then V_1+V_2 is a subspace of type $(m+1,r)$ of $\mathbb{F}_q^{(2\nu)}$, where $2r\le m\le \nu+r-1$, or a subspace of type $(m+1,r+1)$ of $\mathbb{F}_q^{(2\nu)}$, where $2r+1\le m\le \nu+r$.*

Proof. Since V_1 and V_2 are two subspaces of type (m,r) of $\mathbb{F}_q^{(2\nu)}$, by *Theorem* 2.3, $2r\le m\le \nu+r$. We can suppose that V_1+V_2 is a subspace of type $(m+1,s)$, then $2s\le m+1\le \nu+s$. Since $V_1\subseteq V_1+V_2$, by Theorem 2.4, $0\le s-r\le 1$.

If $s=r$, then $2r\le m\le \nu+r-1$, V_1+V_2 is a subspace of type $(m+1,r)$. If $s=r+1$, then $2r+1\le m\le \nu+r$, V_1+V_2 is a subspace of type $(m+1,r+1)$. □

It is always assumed that $2r+1\le m\le \nu+r-1$ is established, we can construct check matrix H.

Let V be the set of all subspaces of type (m,r) of $\mathbb{F}_q^{(2\nu)}$ that are called points. Let L be the set of all subspaces of type $(m+1,r)$ and $(m+1,r+1)$ of $\mathbb{F}_q^{(2\nu)}$ that are called lines. Let $M=N(m,r;2\nu)$, $N=N(m+1,r;2\nu)+N(m+1,r+1;2\nu)$.

Using points to mark rows of H, using lines to mark columns of H. We construct an $M\times N$ matrix H as follow:

$$h_{i,k}=\begin{cases}1 & v_i\in l_k\\ 0 & v_i\notin l_k\end{cases}$$

where $v_i\in V, i=1,2,\cdots,M, l_k\in L, k=1,2,\cdots,N$.

H has the following structural properties:

(1) The column and row weights $\gamma=N(m,r;m+1,r;2\nu)$ or $\gamma=N(m,r;m+1,r+1;2\nu)$ and $\rho=N'(m,r;m+1,r;2\nu)+N'(m,r;m+1,r+1;2\nu)$, respectively.

(2) The null space of $HX=0$ over $\mathbb{F}_q$ gives a LDPC code C of length $n=N(m+1,r;2\nu)+N(m+1,r+1;2\nu)$.

(3) The code rate is at least $\frac{N(m+1,r;2\nu)+N(m+1,r+1;2\nu)-N(m,r;2\nu)}{N(m+1,r;2\nu)+N(m+1,r+1;2\nu)}$.

Lemma 3.1 *For $1\le i,j\le M$ and $i\neq j$, the rows v_i and v_j of H have at most one position where they both are 1.*

Proof. Suppose there exist $v_i,v_j\in V$ and $l_k,l_l\in L(k\neq l)$ so that $h_{ik}=h_{il}=h_{jk}=h_{jl}=1$, that is to say, $v_i,v_j\in l_k$ and $v_i,v_j\in l_l$. Further, $v_i+v_j\in l_k$ and $v_i+v_j\in l_l$. Since $\dim v_i=\dim v_j=m$ and $\dim l_k=\dim l_l=m+1$, then there always exists

$l_k = v_i + v_j = l_l$ which contradict to the assumptions that $k \neq l$. This prove the Lemma. □

Let us consider 4-dimensional symplectic space over $\mathbb{F}_q$. Since $2r+1 \leq m \leq v+r-1$, then we choose $m=1, r=0$. Let V_1 be the set of all subspaces of type $(1,0)$ of $\mathbb{F}_q^{(4)}$. Let L_1 be the set of all subspaces of type $(2,0)$ and $(2,1)$ of $\mathbb{F}_q^{(4)}$. Construct a check matrix H_1 of LDPC code C_1, H_1 is an $M_1 \times N_1$ matrix, where $M_1 = q^3+q^2+q+1$ and $N_1 = q^4+q^3+2q^2+q+1$. The weights of row and column of H_1 are q^2+q+1 and $q+1$, respectively.

According to Theorem 2.7 and Theorem 2.8, we take any 3 column vectors l_m, l_n and l_k, $m,n,k \in \{1,2,\cdots,N_1\}, m \neq n \neq k$ in H_1. Now let's discuss the cycles of H_1.

Lemma 3.2 *If l_m, l_n, and l_k are subspaces of type $(2,0)$ of $\mathbb{F}_q^{(4)}$, then the girth of H_1 is 8.*

Proof. Let v_{i_1}, v_{i_2} and $v_{i_3} \in V_1$ that are pairwise collinear and $v_{i_1}, v_{i_2}, v_{i_3}$ are not-collinear, i.e.,

$$l_m = \begin{bmatrix} v_{i_1} \\ v_{i_2} \end{bmatrix}, l_n = \begin{bmatrix} v_{i_1} \\ v_{i_3} \end{bmatrix}, \text{ and } l_k = \begin{bmatrix} v_{i_2} \\ v_{i_3} \end{bmatrix}.$$

Since l_m, l_n and l_k are subspaces of type $(2,0)$ of $\mathbb{F}_q^{(4)}$, then $l_m K l_m^t = 0$, $l_n K l_n^t = 0$ and $l_k K l_k^t = 0$. We conclude that $v_{i_1} K v_{i_1}^t = v_{i_2} K v_{i,2}^t = v_{i_3} K v_{i_3}^t = v_{i_1} K v_{i_2}^t = v_{i_2} K v_{i_1}^t = v_{i_1} K v_{i_3}^t = v_{i_3} K v_{i_1}^t = v_{i_2} K v_{i_3}^t = v_{i_3} K v_{i_2}^t = 0$. Further,

$$\begin{bmatrix} v_{i_1} \\ v_{i_2} \\ v_{i_3} \end{bmatrix} K \begin{bmatrix} v_{i_1} \\ v_{i_2} \\ v_{i_3} \end{bmatrix}^t = \begin{bmatrix} v_{i_1} K v_{i_1}^t & v_{i_1} K v_{i_2}^t & v_{i_1} K v_{i_3}^t \\ v_{i_2} K v_{i_1}^t & v_{i_2} K v_{i_2}^t & v_{i_2} K v_{i_3}^t \\ v_{i_3} K v_{i_1}^t & v_{i_3} K v_{i_2}^t & v_{i_3} K v_{i_3}^t \end{bmatrix} = 0.$$

Hence

$$\begin{bmatrix} v_{i_1} \\ v_{i_2} \\ v_{i_3} \end{bmatrix}$$

is a subspace of type $(3,0)$ of $\mathbb{F}_q^{(4)}$. By Theorem 2.3, the subspaces of type $(3,0)$ don't exist in $\mathbb{F}_q^{(4)}$. Therefore, the length of the circles is at least 8.

There is a cycles of length 8, such as

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

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

□

Lemma 3.3 *If l_m and l_n are two subspaces of type $(2,0)$ of $\mathbb{F}_q^{(4)}$, l_k is a subspace of type $(2,1)$ of $\mathbb{F}_q^{(4)}$, then the length of the circles of H_1 is at least 6.*

Proof. By Theorem 2.3, the subspaces of type $(3,1)$ exist in $\mathbb{F}_q^{(4)}$. Let v_{i_1}, v_{i_2} and $v_{i_3} \in V_1$ that $\begin{bmatrix} v_{i_1} \\ v_{i_2} \\ v_{i_3} \end{bmatrix}$ is a subspace of type $(3,1)$ of $\mathbb{F}_q^{(4)}$. Hence,

$$\begin{bmatrix} v_{i_1} \\ v_{i_2} \\ v_{i_3} \end{bmatrix} K \begin{bmatrix} v_{i_1} \\ v_{i_2} \\ v_{i_3} \end{bmatrix}^t = \begin{bmatrix} v_{i_1}Kv^t_{i_1} & v_{i_1}Kv^t_{i_2} & v_{i_1}Kv^t_{i_3} \\ v_{i_2}Kv^t_{i_1} & v_{i_2}Kv^t_{i_2} & v_{i_2}Kv^t_{i_3} \\ v_{i_3}Kv^t_{i_1} & v_{i_3}Kv^t_{i_2} & v_{i_3}Kv^t_{i_3} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

We conclude that $v_{i_1}Kv^t_{i_1} = v_{i_2}Kv^t_{i2} = v_{i_3}Kv^t_{i_3} = v_{i_1}Kv^t_{i_2} = v_{i_2}Kv^t_{i_1} = v_{i_1}Kv^t_{i_3} = v_{i_3}Kv^t_{i_1} = 0$, $v_{i_2}Kv^t_{i_3} = 1$, and $v_{i_3}Kv^t_{i_2} = -1$. Since l_m and l_n are two subspaces of type $(2,0)$ of $\mathbb{F}_q^{(4)}$, l_k is a subspace of type $(2,1)$ of $\mathbb{F}_q^{(4)}$, then $l_mKl_m^T = 0, l_nKl_n^T = 0$ and $l_kKl_k^T = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. It is obviously that

$$l_m = \begin{bmatrix} v_{i_1} \\ v_{i_2} \end{bmatrix}, l_n = \begin{bmatrix} v_{i_1} \\ v_{i_3} \end{bmatrix}, \text{ and } l_k = \begin{bmatrix} v_{i_2} \\ v_{i_3} \end{bmatrix}.$$

Therefore, the length of the circles of H_1 is at least 6. □

Lemma 3.4 *If l_m and l_n are subspaces of type $(2,1)$ of $\mathbb{F}_q^{(4)}$, l_k is a subspace of type $(2,0)$ of $\mathbb{F}_q^{(4)}$, then the length of the circles of H_1 is at least 6.*

Proof. By Theorem 2.3, the subspaces of type $(3,1)$ exist in $\mathbb{F}_q^{(4)}$. Let v_{i_1}, v_{i_2} and $v_{i_3} \in V$ that $\begin{bmatrix} v_{i_1} \\ v_{i_2} \\ v_{i_3} \end{bmatrix}$ is a subspace of type $(3,1)$ of $\mathbb{F}_q^{(4)}$.

Let $P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$, then

$$\begin{aligned} P \begin{bmatrix} v_{i_1} \\ v_{i_2} \\ v_{i_3} \end{bmatrix} K (P \begin{bmatrix} v_{i_1} \\ v_{i_2} \\ v_{i_3} \end{bmatrix})^t &= P \begin{bmatrix} v_{i_1} \\ v_{i_2} \\ v_{i_3} \end{bmatrix} K \begin{bmatrix} v_{i_1} \\ v_{i_2} \\ v_{i_3} \end{bmatrix}^t P^t \\ &= P \begin{bmatrix} v_{i_1}Kv^t_{i_1} & v_{i_1}Kv^t_{i_2} & v_{i_1}Kv^t_{i_3} \\ v_{i_2}Kv^t_{i_1} & v_{i_2}Kv^t_{i_2} & v_{i_2}Kv^t_{i_3} \\ v_{i_3}Kv^t_{i_1} & v_{i_3}Kv^t_{i_2} & v_{i_3}Kv^t_{i_3} \end{bmatrix} P^t \\ &= \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \end{aligned}$$

We conclude that $v_{i_1}Kv^t_{i_1} = v_{i_2}Kv^t_{i,2} = v_{i_3}Kv^t_{i_3} = v_{i_2}Kv^t_{i_3} = v_{i_3}Kv^t_{i_2} = 0$, $v_{i_1}Kv^t_{i_2} = v_{i_1}Kv^t_{i_3} = 1$ and $v_{i_2}Kv^t_{i_1} = v_{i_3}Kv^t_{i_1} = -1$. Since l_m and l_n are two subspaces of type $(2,1)$ of $\mathbb{F}_q^{(4)}$, l_k is a subspace of type (2,0) of $\mathbb{F}_q^{(4)}$, then $l_mKl^t_m = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $l_nKl^t_n = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and $l_kKl^t_k = 0$. It is obviously that

$$l_m = \begin{bmatrix} v_{i_1} \\ v_{i_2} \end{bmatrix}, l_n = \begin{bmatrix} v_{i_1} \\ v_{i_3} \end{bmatrix}, \text{ and } l_k = \begin{bmatrix} v_{i_2} \\ v_{i_3} \end{bmatrix}.$$

Therefore, the length of the circles of H_1 is at least 6. □

Lemma 3.5 *If l_m, l_n and l_k are subspaces of type $(2,1)$ of $\mathbb{F}_q^{(4)}$, then the length of the circles of H_1 is at least* 6.

Proof. By Theorem 2.3, the subspace of type $(3,1)$ exist in $\mathbb{F}_q^{(4)}$. Let v_{i_1}, v_{i_2} and $v_{i_3} \in V$ that $\begin{bmatrix} v_{i_1} \\ v_{i_2} \\ v_{i_3} \end{bmatrix}$ is a subspace of type $(3,1)$ of $\mathbb{F}_q^{(4)}$.

Let $P = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$, then

$$\begin{aligned} P\begin{bmatrix} v_{i_1} \\ v_{i_2} \\ v_{i_3} \end{bmatrix} K(\begin{bmatrix} v_{i_1} \\ v_{i_2} \\ v_{i_3} \end{bmatrix})^t &= P\begin{bmatrix} v_{i_1} \\ v_{i_2} \\ v_{i_3} \end{bmatrix} K \begin{bmatrix} v_{i_1} \\ v_{i_2} \\ v_{i_3} \end{bmatrix}^t P^t \\ &= P\begin{bmatrix} v_{i_1}Kv^t_{i_1} & v_{i_1}Kv^t_{i_2} & v_{i_1}Kv^t_{i_3} \\ v_{i_2}Kv^t_{i_1} & v_{i_2}Kv^t_{i_2} & v_{i_2}Kv^t_{i_3} \\ v_{i_3}Kv^t_{i_1} & v_{i_3}Kv^t_{i_2} & v_{i_3}Kv^t_{i_3} \end{bmatrix} P^t \\ &= \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \end{aligned}$$

We conclude that $v_{i_1}Kv^t_{i_1} = v_{i_2}Kv^t_{i,2} = v_{i_3}Kv^t_{i_3} = 0$, $v_{i_1}Kv^t_{i_2} = v_{i_1}Kv^t_{i_3} = v_{i_2}Kv^t_{i_3} = 1$ and $v_{i_2}Kv^t_{i_1} = v_{i_3}Kv^t_{i_1} = v_{i_3}Kv^t_{i_2} = -1$ Since l_m, l_n and l_k are subspaces of type $(2,1)$ of $\mathbb{F}_q^{(4)}$, then $l_mKl^t_m = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, $l_nKl^t_n = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and $l_kKl^t_k = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. It is obviously that

$$l_m = \begin{bmatrix} v_{i_1} \\ v_{i_2} \end{bmatrix}, l_n = \begin{bmatrix} v_{i_1} \\ v_{i_3} \end{bmatrix}, \text{ and } l_k = \begin{bmatrix} v_{i_2} \\ v_{i_3} \end{bmatrix}.$$

Therefore, the length of the circles of H_1 is at least 6. □

From the above lemmas and Theorem 2.7, we have

Theorem 3.2 *H_1 has cycles of length 6.*

Example 3.1 In $\mathbb{F}_2^{(4)}$, $M_1 = N(1,0;4) = 2^3+2^2+2+1 = 15$, $N_1 = N(2,0;4) + N(2,1;4) = 2^4+2^3+2\times 2^2+2+1 = 35$. We can get

$$\begin{aligned}
V_1 = \{ \quad & v_1 = \begin{bmatrix}1 & 0 & 0 & 0\end{bmatrix}, v_2 = \begin{bmatrix}0 & 1 & 0 & 0\end{bmatrix}, v_3 = \begin{bmatrix}0 & 0 & 1 & 0\end{bmatrix}, \\
& v_4 = \begin{bmatrix}0 & 0 & 0 & 1\end{bmatrix}, v_5 = \begin{bmatrix}1 & 1 & 0 & 0\end{bmatrix}, v_6 = \begin{bmatrix}1 & 0 & 1 & 0\end{bmatrix}, \\
& v_7 = \begin{bmatrix}1 & 0 & 0 & 1\end{bmatrix}, v_8 = \begin{bmatrix}0 & 1 & 1 & 0\end{bmatrix}, v_9 = \begin{bmatrix}0 & 1 & 0 & 1\end{bmatrix}, \\
& v_{10} = \begin{bmatrix}0 & 0 & 1 & 1\end{bmatrix}, v_{11} = \begin{bmatrix}1 & 1 & 1 & 0\end{bmatrix}, v_{12} = \begin{bmatrix}1 & 1 & 0 & 1\end{bmatrix}, \\
& v_{13} = \begin{bmatrix}1 & 0 & 1 & 1\end{bmatrix}, v_{14} = \begin{bmatrix}0 & 1 & 1 & 1\end{bmatrix}, v_{15} = \begin{bmatrix}1 & 1 & 1 & 1\end{bmatrix}\}.
\end{aligned}$$

$$\begin{aligned}
L_1 = \{ \quad & l_1 = \begin{bmatrix}1 & 0 & 1 & 0\\0 & 1 & 0 & 0\end{bmatrix}, l_2 = \begin{bmatrix}0 & 0 & 0 & 1\\1 & 0 & 1 & 0\end{bmatrix}, l_3 = \begin{bmatrix}0 & 1 & 0 & 1\\1 & 0 & 1 & 0\end{bmatrix}, \\
& l_4 = \begin{bmatrix}1 & 0 & 0 & 1\\0 & 1 & 1 & 0\end{bmatrix}, l_5 = \begin{bmatrix}1 & 0 & 0 & 1\\0 & 1 & 1 & 1\end{bmatrix} l_6 = \begin{bmatrix}1 & 0 & 1 & 1\\0 & 1 & 1 & 0\end{bmatrix}, \\
& l_7 = \begin{bmatrix}1 & 1 & 0 & 1\\0 & 0 & 1 & 1\end{bmatrix}, l_8 = \begin{bmatrix}1 & 0 & 1 & 1\\0 & 1 & 1 & 1\end{bmatrix}, l_9 = \begin{bmatrix}0 & 1 & 0 & 1\\1 & 0 & 0 & 0\end{bmatrix}, \\
& l_{10} = \begin{bmatrix}0 & 0 & 1 & 0\\0 & 1 & 0 & 1\end{bmatrix}, l_{11} = \begin{bmatrix}0 & 1 & 0 & 0\\1 & 0 & 0 & 0\end{bmatrix}, l_{12} = \begin{bmatrix}0 & 0 & 1 & 0\\0 & 1 & 0 & 0\end{bmatrix}, \\
& l_{13} = \begin{bmatrix}0 & 0 & 0 & 1\\1 & 0 & 0 & 0\end{bmatrix}, l_{14} = \begin{bmatrix}0 & 0 & 1 & 0\\0 & 0 & 0 & 1\end{bmatrix}, l_{15} = \begin{bmatrix}1 & 1 & 0 & 0\\0 & 0 & 1 & 1\end{bmatrix}, \\
& l_{16} = \begin{bmatrix}1 & 0 & 0 & 0\\0 & 0 & 1 & 0\end{bmatrix}, l_{17} = \begin{bmatrix}1 & 0 & 0 & 0\\0 & 1 & 1 & 0\end{bmatrix}, l_{18} = \begin{bmatrix}1 & 0 & 0 & 1\\0 & 0 & 1 & 0\end{bmatrix}, \\
& l_{19} = \begin{bmatrix}1 & 0 & 1 & 0\\0 & 1 & 1 & 0\end{bmatrix}, l_{20} = \begin{bmatrix}1 & 0 & 0 & 1\\1 & 0 & 1 & 0\end{bmatrix}, l_{21} = \begin{bmatrix}1 & 0 & 0 & 0\\0 & 0 & 1 & 1\end{bmatrix}, \\
& l_{22} = \begin{bmatrix}1 & 0 & 0 & 0\\0 & 1 & 1 & 1\end{bmatrix}, l_{23} = \begin{bmatrix}1 & 0 & 1 & 0\\0 & 1 & 1 & 1\end{bmatrix}, l_{24} = \begin{bmatrix}1 & 1 & 0 & 0\\0 & 0 & 1 & 0\end{bmatrix}, \\
& l_{25} = \begin{bmatrix}1 & 1 & 0 & 1\\0 & 0 & 1 & 0\end{bmatrix}, l_{26} = \begin{bmatrix}0 & 1 & 0 & 0\\0 & 0 & 0 & 1\end{bmatrix}, l_{27} = \begin{bmatrix}0 & 1 & 1 & 0\\0 & 0 & 0 & 1\end{bmatrix}, \\
& l_{28} = \begin{bmatrix}0 & 1 & 1 & 0\\0 & 1 & 0 & 1\end{bmatrix}, l_{29} = \begin{bmatrix}0 & 1 & 0 & 0\\1 & 0 & 0 & 1\end{bmatrix}, l_{30} = \begin{bmatrix}1 & 1 & 0 & 0\\0 & 0 & 0 & 1\end{bmatrix}, \\
& l_{31} = \begin{bmatrix}1 & 1 & 0 & 0\\0 & 1 & 0 & 1\end{bmatrix}, l_{32} = \begin{bmatrix}1 & 1 & 1 & 0\\0 & 0 & 0 & 1\end{bmatrix}, l_{33} = \begin{bmatrix}1 & 1 & 1 & 0\\0 & 1 & 0 & 1\end{bmatrix}, \\
& l_{34} = \begin{bmatrix}0 & 1 & 0 & 0\\0 & 0 & 1 & 1\end{bmatrix}, l_{35} = \begin{bmatrix}0 & 1 & 0 & 0\\1 & 0 & 1 & 1\end{bmatrix}\}.
\end{aligned}$$

We construct a 15×35 matrix H_1 as follow:

$$H_1 = \left[\begin{array}{ccccccccccccccccccccccccccccccccccc}
0&0&0&0&0&0&0&0&1&0&1&0&1&0&0&1&1&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
1&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&1&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0\\
0&1&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&1&0&1&0&0&0\\
0&0&0&0&0&0&0&1&0&0&1&0&0&0&1&0&0&0&1&0&0&0&0&1&0&0&0&0&0&1&1&0&0&0&0\\
1&1&1&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&1&1&0&0&0&0&0&0&0&1&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&1&0&1&0&0&0&0\\
0&0&0&1&0&1&0&0&0&0&0&1&0&0&0&0&1&0&1&0&0&0&0&0&0&0&1&1&0&0&0&0&0&0&0\\
0&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&1&0&1&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&0&0&0&1&1&0&0&0&0&0&0&1&0&0&0&0&0&1&0\\
1&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&1&0&0\\
0&0&0&0&0&1&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&0&1&1&0&0&0&0&0\\
0&1&0&0&0&1&0&1&0&0&0&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&0&1&0&1\\
0&0&0&0&1&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&1&0&0&0&0&0&0&1&0\\
0&0&1&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&0&0&1&0&0&0&0&0&0&1&0&0&1
\end{array}\right].$$

It is clearly to obtain that

(1) each row has weight $\rho_1 = N'(1,0;2,0;4) + N'(1,0;2,1;4) = 7$.

(2) each column has weight $\gamma_1 = N(1,0;2,0;4) = N(1,0;2,1;4) = 3$.

(3) H_1 has cycles of length 6.

The null space in $\mathbb{F}_2^{(4)}$ gives a regular LDPC C_1 of length 35 with the code rate 0.571428 and minimum distance is at lest 4.

4 Conclusion

In this work we introduce a construction of LDPC codes based on symplectic spaces. By two subspaces of type (m,r) to produce a subspace of type $(m+1,r)$ or $(m+1,r+1)$ in $\mathbb{F}_q^{(2v)}$, we use all subspaces of type (m,r) to mark rows and all subspaces of type $(m+1,r)$ and $(m+1,r+1)$ to mark columns of check matrix H. A construction of LDPC codes based on symplectic spaces has been given. As a special case, we choose $m = 1$ and $r = 0$ to construct check matrix H_1 in $\mathbb{F}_q^{(4)}$ and the cycles of length 6 of H_1 is further discussed.

References

[1] Z. Wan. Geometry of classical groups over finite fields. Science Press, Beijing, New York, 2002.

[2] D. J. C. MacKay and R. M. Neal. Near shannon limit performance of low density parity check codes. Electronices Letters, 1996, 32:1645-1646.

[3] K. Yu, S. Lin and M. Fossorier. Low density parity check codes based on finite geometries: a rediscovery and new results. IEEE Transactions Information Theory, 2001, 47:2711-2736.

[4] R. Tanner. A recursive approach to low complexity codes. IEEE Transactions on Information Theory, 1981, 27:533-547.

[5] H. Tang, J. Xu and S. Lin. Codes on finite geometries. IEEE Transactions on Information Theory, 2005, 51:572-596.

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

[7] L. Zeng, L. Lan, Y. Y. Tai, B. Zhou and S. Lin. Construction of nonbinary cylic, quasi-cyclic and regular LDPC codes: a finite geometry approach. IEEE Transactions on Communications, 2008, 56:378-387.

[8] D. Chandler, P. Sin and Q. Xiang. Incidence modules for symplectic spaces in characteristic two. Journal of Algebra. 2008, 323:3157-3181.

[9] Y. Feng, S. Deng, L. Wang and C. Ma. Minimum distances of three families of low-density parity-check codes based on finite geometries. Frontiers of Mathematics in China, 2016, 11(2):279-289.

[10] X. Wang and Y. Hao. Two constructions of LDPC codes based on pseudo-symplectic geometry over finite fields. The Journal of China Universities of Posts and Telecommunications, 2018, 25:49-59.

[11] Y. Xiao. Turbo and LDPC encode and decode and its application. Pepole Posts and Telecommunications Press. 2010.