IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received August 29, 2020, accepted November 1, 2020, date of publication November 11, 2020, date of current version November 19, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3037290

New Construction of Low-Density Parity-Check Codes Based on Vector Space Over Finite Fields

XUEMEI LIU AND LIHUA JIA
College of Science, Civil Aviation University of China, Tianjin 300300, China
Corresponding author: Xuemei Liu (xm-liu771216@163.com)

This work was supported by the National Natural Science Foundation of China under Grant 11701558.

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. Two kinds of LDPC codes are constructed based on vector space over finite field. The code length, code rate and minimum distance are given. Moreover, the two kinds of codes are compared with the existing codes, and the constructed codes are better than some existing ones in terms of code rate or minimum distance.

INDEX TERMS Low-density parity-check codes, finite fields, code rate, minimum distance.

I. 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 got the attention of scholars. Tanner [2] studied the codes from the perspective of graph theory until 1981, then Mackay [3] 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 of constructing codes are divided into two kinds: random structure construction and algebraic construction. 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 2001, Kou *et al.* [4] constructed LDPC codes based on Euclidean space and Projective space, and studied the girth, length and minimum distance of this kind of codes. In 2008, Bonello *et al.* [5] constructed a kind of regular Quasi-Cyclic protograph LDPC codes based on the vandermonde matrix. In 2009, Fu *et al.* [6] gave a coding construction method based on the LDPC codes of *PEG* algorithm structure. In 2011, Fang *et al.* [7] *et.al.* proposed a joint optimization algorithm based on the protograph LDPC codes. In 2013, Wang [8] and Deng [9] used algebraic methods to construct LDPC codes based on symplectic space, unitary space and orthogonal space. In 2015, Zhang *et al.* [10] constructed the LDPC codes based on the general protograph. In the same year, Chen and Yuan [11] proposed an improved method of constructing QC-LDPC codes based on *PEG* algorithm.

In this paper, two kinds of LDPC codes are constructed with the inclusive relation of vector space over finite fields, which provides a new method of constructing LDPC codes, and produces a new series of LDPC codes with good performance and practical application value.

II. 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 is $M = N - K$, and the code rate is R.

Definition 2.1 [12]: The parity-check matrix H of binary regular LDPC code satisfies the following four conditions:

(1) Each row cosists of ρ ''ones'';

(2) Each column cosists of γ ''ones'';

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

(4) Both ρ and γ 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 the columns (or rows) of the parity-check

The associate editor coordinating the review of this manuscript and approving it for publication was Yeliz Karaca.

matrix H have different number of "ones", an LDPC code is said to be irregular.

Lemma 2.2 [8]: 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.)

Next, we shall introduce the relative contents of vector space over finite field [13].

Let $\mathbb{F}_q$ be the finite field with q elements, where q is a power of a prime and let n be positive integer. We use $\mathbb{F}_q^n = \{(x_1, x_2, \cdots, x_n) | x_i \in \mathbb{F}_q, i = 1, 2, \cdots, n\}$ to denote the n-dimensional row vector space over the finite field $\mathbb{F}_q$.

Now let P be an m-dimensional vector subspace of $\mathbb{F}_q^n$, then we write $\dim P = m$. Let $v_1, v_2, \cdots, v_m$ be a basis of P. We usually use the $m \times n$ matrix

$$\begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{pmatrix}$$

to represent the vector subspace P, write

$$P = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_m \end{pmatrix},$$

i.e., we use the same letter P to denote a matrix which represents the vector subspace P, and call the matrix P a matrix representation of the vector subspace P.

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 2.3: Let $0 \le m \le n$ 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 2.4: Let $0 \le t \le m \le n$ 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 2.5: Let $0 \le t \le m \le n$. 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 $N'(m-t, n-t)$.

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

III. CONSTRUCTION

In this section, two kinds of LDPC codes based on vector space over finite fields are given, then we compare them with the LDPC codes that have been constructed.

A. FIRST CLASS OF CONSTRUCTION

Definition 3.1.1: Given integers $2 \le m \le \lfloor \frac{n}{2} \rfloor, m_1 = m - 1$. Let H 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 $\mathbb{F}_q^n$. $H(i, j) = 1$ if and only if the i-th m_1-dimensional vector subspace is contained in the j-th m-dimensional vector subspace, otherwise, $H(i, j) = 0$.

By Lemmas 2.3, 2.4 and 2.5, H is an $M \times N$ matrix, whose constant column weight is γ, constant row weight is ρ, where

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

Theorem 3.1.2: Let $2 \le m \le \lfloor \frac{n}{2} \rfloor, m_1 = m - 1$. The matrix H constructed by Definition 3.1.1 is the check matrix of an LDPC code.

Proof: The matrix H is the check matrix of LDPC code; Firstly, by Lemmas 2.4 and 2.5, we know every column of matrix H has γ "ones", where $\gamma = \begin{bmatrix} m \\ m_1 \end{bmatrix}_q$, and every row of matrix H has ρ "ones", where $\rho = \begin{bmatrix} n - m_1 \\ m - m_1 \end{bmatrix}_q$.

Next, let P_1, P_2 be the representation matrices of m_1-dimensional vector subspaces on $\mathbb{F}_q^n$, and let Q_1, Q_2 be the representation matrices of m-dimensional vector subspaces on $\mathbb{F}_q^n$, $P_1 \ne P_2$, $Q_1 \ne Q_2$. Clearly, $\mathrm{rank}(P_1) = \mathrm{rank}(P_2) = m_1$, $\mathrm{rank}(Q_1) = \mathrm{rank}(Q_2) = m$.

Assume that $P_1 \subseteq Q_1, P_1 \subseteq Q_2, P_2 \subseteq Q_1, P_2 \subseteq Q_2$, then $P_1 \cap P_2 \subseteq Q_1, P_1 \cap P_2 \subseteq Q_2$. Since $m = m_1 + 1$, we deduce

rank$(P_1 \cap P_2) = m-2$. Thus we can assume that

$$P_1 = \begin{pmatrix} P_1 \cap P_2 \\ P_{11} \end{pmatrix} \begin{matrix} m_1 - 1 \\ 1 \end{matrix},$$
$$P_2 = \begin{pmatrix} P_1 \cap P_2 \\ P_{22} \end{pmatrix} \begin{matrix} m_1 - 1 \\ 1 \end{matrix},$$

then

$$Q_1 = \begin{pmatrix} P_1 \cap P_2 \\ P_{11} \\ P_{22} \end{pmatrix} \begin{matrix} m-2 \\ 1 \\ 1 \end{matrix},$$
$$sQ_2 = \begin{pmatrix} P_1 \cap P_2 \\ P_{11} \\ P_{22} \end{pmatrix} \begin{matrix} m-2 \\ 1 \\ 1 \end{matrix}.$$

So $Q_1 = Q_2$. It is shown that representation matrices of two m-dimensional vector subspaces are equivalent. Hence, the number of ''ones'' in common between any two rows (or two columns) is no greater than 1.

Lastly, both ρ and γ 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''.

In conclusion, from Definition 2.1, the matrix H is the check matrix of LDPC code.

B. SECOND CLASS OF CONSTRUCTION

Definition 3.2.1: Given integers $3 \le m' \le n', m'_1 = m'-1$. Let V_1 is a 1-dimensional vector subspaces of $\mathbb{F}_q^{n'}$, where base $e_1 = (1, 0, 0, \cdots, 0)$, $V_2 = \{$ all m'_1-dimensional vector subspaces of $\mathbb{F}_q^{n'}\}$, V is a m'-dimensional vector subspaces of $\mathbb{F}_q^{n'}$, and satisfy $V = V_1 \oplus V_2$. Let H' 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 $\mathbb{F}_q^{n'}$. $H'(i,j) = 1$ if and only if the i-th m'-dimensional vector subspace contains in the j-th m'_1-dimensional vector subspace, otherwise, $H'(i,j) = 0$.

Note: The constructed matrix removes duplicate columns in order to ensure the minimum distance at least 3.

By Lemmas 2.3, 2.4 and 2.5, H' is an $M' \times N'$ matrix, where

$$M' = \begin{bmatrix} n'-1 \\ m'-1 \end{bmatrix}_q, \quad N' = \begin{bmatrix} n'-1 \\ m'-1 \end{bmatrix}_q + \begin{bmatrix} n'-1 \\ m'-2 \end{bmatrix}_q.$$

Theorem 3.2.2. Let $3 \le m' \le n', m'_1 = m'-1$. The matrix H' constructed by Definition 3.2.1 is the check matrix of an LDPC code with code length

$$N' = \begin{bmatrix} n'-1 \\ m'-1 \end{bmatrix}_q + \begin{bmatrix} n'-1 \\ m'-2 \end{bmatrix}_q,$$

information length

$$K' = \begin{bmatrix} n'-1 \\ m'-2 \end{bmatrix}_q,$$

minimum distance

$$d' \ge \frac{q^{n'-m'+1}-1}{q-1} + 1,$$

and the code rate

$$R' = \frac{q^{m'-1}-1}{q^{n'-m'+1} + q^{m'-1} - 2}.$$

Proof: (1) The matrix H' is the check matrix of an LDPC code; The proof is the same as the Theorem 3.1.2.

(2)Code length $N' = \begin{bmatrix} n'-1 \\ m'-1 \end{bmatrix}_q + \begin{bmatrix} n'-1 \\ m'-2 \end{bmatrix}_q$;

By the Definition 3.2.1, H' is the binary matrix, whose columns are indexed by the m'_1-dimensional vector subspaces V_2, whose rows are indexed by the m'-dimensional vector subspaces V. Since

$$V = V_1 \oplus V_2, V_1 = \langle (1, 0, 0, \cdots, 0) \rangle,$$

we have $V_1 \subseteq V$, thus row M' is decided by the number of m'-dimensional vector subspaces V containing a given 1-dimensional vector subspace V_1. According to Lemma 2.5,

$$M' = \begin{bmatrix} n'-1 \\ m'-1 \end{bmatrix}_q = \begin{bmatrix} n'-1 \\ m'_1 \end{bmatrix}_q.$$

where $H'(i,j) = 1$ if and only if the i-th m'-dimensional vector subspace is contained in the j-th m'_1-dimensional vector subspace.

Let P'_j be the representation matrix of m'_1-dimensional vector subspaces, where $1 \le j \le \begin{bmatrix} n' \\ m'_1 \end{bmatrix}_q$; and Q'_i be the representation matrix of m'-dimensional vector subspaces, where $1 \le i \le \begin{bmatrix} n'-1 \\ m'_1 \end{bmatrix}_q$. So we can divide the representation matrix of m'_1-dimensional vector subspaces into two situations.

1°: $(1, 0, 0, \cdots, 0) \nsubseteq P'_j$, at this point, to give a P'_j can only be included in a Q'_i, then the matrix H' is 'cogredient' to $\begin{pmatrix} I & T \end{pmatrix}_{M' \times N'}$. Since $M' = \begin{bmatrix} n'-1 \\ m'_1 \end{bmatrix}_q$, we deduce the number of the representation matrix of m'_1-dimensional vector subspaces have $\begin{bmatrix} n'-1 \\ m'_1 \end{bmatrix}_q$.

2°: $(1, 0, 0, \cdots, 0) \subseteq P'_j$, at this point, to give a P'_j can not only be included in a Q'_i. At the time, the number of the representation matrix of m'_1-dimensional vector subspaces is equivalent to the number of columns of the compute matrix T, that is to compute the number of (m'_1-1)-dimensional vector subspaces containing a given 1-dimensional vector subspace V_1. By Lemma 2.5, we obtain

$$N' - M' = \begin{bmatrix} n'-1 \\ m'_1-1 \end{bmatrix}_q = \begin{bmatrix} n'-1 \\ m'-2 \end{bmatrix}_q.$$

In conclusion, $N' = \begin{bmatrix} n'-1 \\ m'-1 \end{bmatrix}_q + \begin{bmatrix} n'-1 \\ m'-2 \end{bmatrix}_q$.

(3)Information length $K' = \begin{bmatrix} n'-1 \\ m'-2 \end{bmatrix}_q$. It is necessary to prove that matrix H' is row full rank.

According to the proof of (2), we can get the matrix H' is cogredient to $\begin{pmatrix} I & T \end{pmatrix}_{M' \times N'}$. Then the matrix H' is row full rank.

(4) Minimum distance $d' \geq \frac{q^{n'-m'+1}-1}{q-1} + 1$.

The code has minimum distance d at least $\gamma + 1$ [2]. From the proof of (2), column weight is maximum when $(1, 0, 0, \cdots, 0) \subseteq P'_j$. Under the circumstances, maximum column weight is equivalent to the number of m'-dimensional vector subspaces V containing a given m'_1-dimensional vector subspace V_2. That is,

$$\begin{bmatrix} n'-m'_1 \\ m'-m'_1 \end{bmatrix}_q = \begin{bmatrix} n'-m'+1 \\ 1 \end{bmatrix}_q.$$

Hence,

$$\begin{aligned} d' &\geq \gamma + 1 \\ &= \begin{bmatrix} n'-m'+1 \\ 1 \end{bmatrix}_q + 1 \\ &= \frac{q^{n'-m'+1}-1}{q-1} + 1. \end{aligned}$$

So, we can deduce

$$R' = \frac{K'}{N'} = \frac{q^{m'-1}-1}{q^{n'-m'+1}+q^{m'-1}-2}.$$

□

Example 3.2.3: From Definition 3.2.1, let $n' = 4, q = 2, m'_1 = 2, m' = 3$, $V_1 = \{(1, 0, 0, 0)\}$, $V_2 = \{$ all 2-dimensional vector subspaces of $\mathbb{F}_2^4\}$, V is a 3-dimensional vector subspace of $\mathbb{F}_2^4$, and satisfies $V = V_1 \oplus V_2$.

Rows of the matrix H' are indexed by the 3-dimensional vector subspaces V of $\mathbb{F}_2^4$. These subspaces are shown as follows,

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

Columns of the matrix H' are indexed by the 2-dimensional vector subspaces V of $\mathbb{F}_2^4$, it has two situations.

1°: $V_1 \nsubseteq V_2$, at this point, to give a 2-dimensional vector subspaces can only be included in a 3-dimensional vector subspaces. By Theorem 3.2.2, the numbers of 2-dimensional vector subspaces have $\begin{bmatrix} 4-1 \\ 2 \end{bmatrix} = 7$. These subspaces are shown as follows,

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

2°: $V_1 \subseteq V_2$, at this point, to give a 2-dimensional vector subspaces can not only be included in a 3-dimensional vector subspaces. By Theorem 3.2.2, the numbers of 2-dimensional vector subspaces have $\begin{bmatrix} 4-1 \\ 2-1 \end{bmatrix} = 7$. These subspaces are shown as follows,

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

From above, we can obtain the check matrix of LDPC code, which parameter is [14, 7, 4]. That is,

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

C. COMPARISON OF TWO KINDS OF LDPC CODES

Example 3.3.1: (1) Suppose H be the binary matrix, which is constructed by Definition 3.1.1. Let $q = 2, n = 4, m_1 = 1, m = 2$. The parameters of the constructed LDPC code are [35, 24, 4]. The constructed code is denoted by $\mathbb{C}_1$, which has code rete $\frac{24}{35}$ and minimum distance 4.

(2) Suppose H' be the binary matrix, which is constructed by Definition 3.2.1. Let $q = 2, n' = 5, m'_1 = 3, m' = 4$. By Theorem 3.2.2, The parameters of the constructed LDPC code are [50, 35, 4]. The constructed code is denoted by $\mathbb{C}_2$, which has code rete $\frac{7}{10}$ and minimum distance 4.

Thus we can get that the rate of code $\mathbb{C}_2$ is larger than code $\mathbb{C}_1$ when the minimum distance is the same.

Next, we shall show the comparison of constructed LDPC codes and known LDPC code, and we can get the minimum distance of constructed code larger than the known code when the code rate is close.

TABLE 1. Parameter comparison of two kinds of LDPC codes.

	N	K	d	R
$\mathbb{C}_1$	35	24	4	$\frac{24}{35}$
$\mathbb{C}_2$	50	35	4	$\frac{7}{10}$

TABLE 2. Parameter comparison of different LDPC codes.

	N	K	d	R
$\mathbb{C}$	15	7	5	$\frac{7}{15}$
$\mathbb{C}_1$	35	24	4	$\frac{24}{35}$
$\mathbb{C}_2$	50	35	4	$\frac{7}{10}$

Example 3.3.2: (1) The parameters of the known LDPC code is $[15, 7, 5]$ [1], we denote this code as $\mathbb{C}$, which has code rate is $\frac{7}{15}$, minimum distance is 5.

(2)Suppose H be the binary matrix, which is constructed by Definition 3.1.1. Let $q = 2, n = 4, m_1 = 1, m = 2$. The parameters of the constructed LDPC code are $[35, 24, 4]$. The constructed code is denoted by $\mathbb{C}_1$, which has code rete $\frac{24}{35}$ and minimum distance 4.

(3) Suppose H' be the binary matrix, which is constructed by Definition 3.2.1. Let $q = 2, n' = 5, m'_1 = 3, m' = 4$. By Theorem 3.2.2, The parameters of the constructed LDPC code are $[50, 35, 4]$. The constructed code is denoted by $\mathbb{C}_2$, which has code rete $\frac{7}{10}$ and minimum distance 4.

Thus we can get that the minimum distance of code $\mathbb{C}_1$ and $\mathbb{C}_2$ is larger than that of the known code $\mathbb{C}$ when the code rate is close.

IV. CONCLUSION

In this paper, we presented two general construction of LDPC codes from vector spaces. Two class of binary codes are constructed based on the subspaces of vector spaces over $\mathbb{F}_q$. We determined and proved the length, coding rate and minimum distance of the LDPC code. In addition, the two kinds of codes constructed are compared with the existing codes, and the constructed codes are better than some existing ones in terms of code rate or minimum distance.

REFERENCES

[1] R. Gallager, "Low-density parity-check codes," *IRE Trans. Inf. Theory*, vol. 8, no. 1, pp. 21–28, Jan. 1962.
[2] R. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inf. Theory*, vol. 27, no. 5, pp. 533–547, Sep. 1981.
[3] D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," *Electron. Lett.*, vol. 33, no. 6, pp. 457–458, 1997.
[4] Y. Kou, S. Lin, and M. P. C. Fossorier, "Low-density parity-check codes based on finite geometries: A rediscovery and new results," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2711–2736, Nov. 2001.
[5] N. Bonello, S. Chen, and L. Hanzo, "Construction of regular quasi-cyclic protograph LDPC codes based on vandermonde matrices," *IEEE Trans. Veh. Technol.*, vol. 57, no. 4, pp. 2583–2588, Jul. 2008.
[6] T. Fu, Z. Wu, and W. Wang, "PEG-based construction method for quasi-cyclic LDPC," *J. Data Acquisition Process.*, vol. 24, pp. 182–186, Jan. 2009.
[7] Y. Fang, L. Wang, P. Chen, and M. Xiao, "Joint optimization algorithm for protograph LDPC codes," *J. Appl. Sci.*, vol. 29, no. 6, pp. 551–558, 2011.
[8] L. Wang, *A Class of LDPC Codes Constructed Based on Symplectic Space*. Shijiazhuang, China: Hebei Normal Univ., 2013.
[9] S. Deng, *A Class of LDPC Codes Constructed Based on Unitary Space and Orthogoal Space*. Shijiazhuang, China: Hebei Normal Univ., 2013.
[10] J. Zhang, G. Han, and Y. Fang, "Deterministic construction of compressed sensing matrices from protograph LDPC codes," *IEEE Signal Process. Lett.*, vol. 22, no. 11, pp. 1960–1964, Nov. 2015.
[11] S. Chen and X. Yuan, "A class of QC-LDPC codes method constructed based on PEG algorithm," *Technol. Outlook*, vol. 22, p. 153, Jun. 2015.
[12] W. Zhexian, *Geometry of Classical Groups Over Finite Fields*, 2nd ed. Beijing, China: Science Press, 2002.

XUEMEI LIU is currently an Associate Professor with the College of Science, Civil Aviation University of China. Her current research interests include algebraic coding and cryptography.

LIHUA JIA is currently pursuing the degree with the College of Science, Civil Aviation University of China. Her current research interests include algebraic coding and cryptography.