Construction of Multiple-Rate Quasi-Cyclic LDPC Codes via the Hyperplane Decomposing

Xueqin Jiang, Yier Yan, and Moon Ho Lee

Abstract: **This paper presents an approach to the construction of multiple-rate quasi-cyclic low-density parity-check (LDPC) codes. Parity-check matrices of the proposed codes consist of $q \times q$ square submatrices. The block rows and block columns of the parity-check matrix correspond to the hyperplanes (μ-flats) and points in Euclidean geometries, respectively. By decomposing the μ-flats, we obtain LDPC codes of different code rates and a constant code length. The code performance is investigated in term of the bit error rate and compared with those of LDPC codes given in IEEE standards. Simulation results show that our codes perform very well and have low error floors over the additive white Gaussian noise channel.**

Index Terms: **Euclidean geometry, low-density parity-check (LD PC) codes, parallel bundle, points, row decomposing, μ-flats.**

I. INTRODUCTION

Low-density parity-check (LDPC) codes, first proposed in the early 1960's [1] and re-discovered in 1996 [2], have recently attracted much attention due to their capacity-approaching performance and low decoding complexity. As an attractive class of LDPC codes, quasi-cyclic (QC)-LDPC codes are well suitable for certain practical applications since they can easily be encoded using simple shift-registers with linear complexity [3].

Communication systems often need to work at different rates. To keep the implementation as simple as possible, the same basic decoder architecture should be able to decode the codes of different code rates. One way to achieve this with LDPC codes is to generate higher-rate codes by puncturing lower-rate codes. However, puncturing reduces the code length, which degrades performance. Another way to achieve this is to generate lower-rate codes by shortening higher-rate codes. As with puncturing, shortening reduces the code length, which degrades performance. The problem is to design a code family of some fixed code length, but varying code rate. The idea that higher-rate effective QC-LDPC codes can be generated from a lower-rate mother QC-LDPC code while maintaining a constant code length by combining rows in the mother matrix was proposed in [4]. The mother and effective matrices consist of cyclic-permutation matrices and zero matrices. Codes of this family support different rates while maintaining the same fundamental decoder architecture. Obviously, the effective matrices, obtained with the row combining method, contain more short cycles than the mother matrix, which also degrades the performance. Furthermore, in the row combining method, we need to consider both of the mother matrix and the effective matrices when we assign the shift values of the cyclic-permutation matrices in the mother matrix.

The motivation of this paper is to find a simple way to construct multiple-rate QC-LDPC codes of a constant code length, which are supported by the same decoder architecture. In our proposed codes, the mother matrix has a block structure that consists of $q \times q$ square submatrices. Each square matrix is also a cyclic-permutation matrix or a zero matrix. The block rows and block columns of a mother matrix correspond to the hyperplanes (μ-flats) and points in Euclidean geometries, respectively. In this paper, the μ-flat decomposing defines the row decomposing and the row decomposing corresponds to the μ-flat decomposing. By decomposing a μ-flat into a parallel bundle of $(\mu - j)$-flats, the corresponding block row of the mother matrix of row weight p^{μ} is decomposed into p^{j} block rows of row weight $p^{\mu-j}$. This is equivalent to decompose a check node of degree p^{μ} into p^{j} check nodes of degree $p^{\mu-j}$. Then, after the decomposing, the result matrix associated with a lower-rate is an effective matrix. The associated mother code and effective codes are supported by the same decoder architecture. Opposite to the row combining method, the row decomposing method makes the effective matrices contain less cycles than the mother matrix. Consequently, there are two advantages of the row decomposing method: 1) It upgrades performance; 2) we do not need to consider the effective matrices when we assign the shift values in the corresponding mother matrix.

In [5] and [6], a different check node splitting method was proposed. This check node splitting method needs to add one more variable node, which means the code length will be increased if the check nodes are splitted with this method. Furthermore, each check node that splitted in this way causes two more ones to appear in the parity check matrix, so the computational complexity also grows. In our proposed row decomposing method (check node splitting method), the number of variable nodes is a constant, which means that the code length is a constant and therefore the computational complexity is a constant.

This paper is organized as follows. Section II explains how to construct the base matrix based on μ-flats and points in Euclidean geometries. The methods to construct the mother and effective matrices are introduced in Section III and Section IV, respectively. Simulation comparisons of our proposed multiple-rate QC-LDPC codes and the QC-LDPC codes given in the IEEE standards are given in Section V. Finally, Section VI concludes this paper.

Manuscript received October 9, 2009; approved for publication by Marco Luise, Division I Editor, February 5, 2011.

This work was supported by World Class University R32-2009-000-20014-0 Fundamental Research 2010-0020942 NRF, Korea.

M. H. Lee is the corresponding author.

X. Jiang is with the School of Information Science and Technology, Donghua University, China, email: xqjiang@dhu.edu.cn.

Y. Yan is with the School of Mechanical and Electrical Engineering, Guangzhou, China, email: year0080@gzhu.edu.cn.

M. H. Lee is with the Division of Electronics and Information Engineering, Chonbuk National University, Korea, email: moonho@jbnu.ac.kr.

II. CONSTRUCTION OF THE BASE MATRIX

Let $EG(d, p^s)$ be a d-dimensional Euclidean geometry over the Galois field $GF(p^s)$, where p is a prime and, d and s are two positive integers. There are p^{ds} points in $EG(d, p^s)$. Let $a_0, a_1, \cdots, a_\mu$ be $\mu+1$ linearly independent points in $EG(d, p^s)$, where $0 \le \mu \le d$. The $p^{\mu s}$ points of the form

$$a_0 + \beta_1 a_1 + \cdots + \beta_\mu a_\mu$$

with $\beta_i \in GF(p^s)$ for $1 \le i \le \mu$, constitute a μ-flat that passes through the point a_0. A point is a 0-flat and a line is a 1-flat.

Definition 1: A μ-flat and the μ-flats parallel to it are called a parallel bundle. The μ-flats in a parallel bundle are parallel to each other.

The points are ordered from 1 to p^{ds}. Let μ_1, μ_2 be two integers and $0 \le \mu_1 < \mu_2 \le d$, there are $N(\mu_2, \mu_1, s, p)$ μ_1-flats contained in a given μ_2-flat and $A(m, \mu_2, \mu_1, s, p)$ μ_2-flats containing a given μ_1-flat [7], where

$$N(\mu_2, \mu_1, s, p) = p^{(\mu_2-\mu_1)s} \prod_{i=1}^{\mu_1} \frac{p^{(\mu_2-i+1)s} - 1}{p^{(\mu_1-i+1)s} - 1} \quad (1)$$

and

$$A(d, \mu_2, \mu_1, s, p) = \prod_{i=\mu_1+1}^{\mu_2} \frac{p^{(d-i+1)s} - 1}{p^{(\mu_2-i+1)s} - 1}. \quad (2)$$

Given a μ-flat F and the incidence vector $v_F = (v_1, v_2, \cdots, v_{p^{ds}})$ of F be a binary p^{ds}-tuple with $v_i = 1$ if the ith point of $EG(d, p^s)$ is in F, and $v_i = 0$ otherwise. The weight of v_F is $p^{\mu s}$, the number of points contained in F.

Lemma 1: Each point in a μ-flat F will appear once and only once in a parallel bundle of $(\mu - j)$-flats contained in F.

Proof: Since a μ-flat F is decomposed into a parallel bundle of $(\mu-j)$-flats, each point in F appears at least once in a parallel bundle of $(\mu-j)$-flats. On the other hand, the $(\mu - j)$-flats in a parallel bundle are disjoint, each point will appear at most once. Hence, each point in F will appear once and only once in a parallel bundle of $(\mu - j)$-flats. □

Lemma 2: A μ-flat F in $EG(d, p^s)$ can be decomposed into

$$K = N(\mu, \mu-j, s, p)/p^{js} = \prod_{i=1}^{(\mu-j)} \frac{p^{(\mu-i+1)s} - 1}{p^{(\mu-j-i+1)s} - 1} \quad (3)$$

parallel bundles of $(\mu - j)$-flats. Denote these parallel bundles of $(\mu - j)$-flats by $P_1, P_2, \cdots, P_K$. For $1 \le l \le K$, P_l consists of p^{js} $(\mu - j)$-flats. Denote the incidence matrix of P_l by v_{P_l}.

Proof: The number of points in a μ-flat is $p^{\mu s}$ and the number of points in a $(\mu - j)$-flat is $p^{(\mu-j)s}$. The $(\mu - j)$-flats in a parallel bundle are disjoint. By Lemma 2, if a parallel bundle of $(\mu - j)$-flats P_l is contained in a μ-flat F, each point in F will appear once and only once in P_l. Therefore, the number of $(\mu - j)$-flats in P_l is

$$\frac{p^{\mu s}}{p^{(\mu-j)s}} = p^{js}.$$

On the other hand, the number of $(\mu - j)$-flats in F is

$$N(\mu, \mu-j, s, p) = p^{js} \prod_{i=1}^{\mu-j} \frac{p^{(\mu-i+1)s} - 1}{p^{(\mu-j-i+1)s} - 1}$$

as given by (1). Then, it is clear that the number of parallel bundles of $(\mu - j)$-flats contained in F is

$$\prod_{i=1}^{(\mu-j)} \frac{p^{(\mu-i+1)s} - 1}{p^{(\mu-j-i+1)s} - 1}$$

which completes the proof. □

In the following, we use one example to illustate the μ-flat decomposing.

Example 1: Consider the Euclidean geometry $EG(3, 2)$ over $GF(2)$. There are eight points $\{a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7\}$, twenty eight 1-flats and fourteen 2-flats. Let $\mu = 2$ and $j = 1$. It follows from (3) that a 2-flat in $EG(3, 2)$ can be decomposed into $K = 3$ parallel bundles of 1-flats. Assume a 2-flat $F = \{a_0, a_1, a_2, a_3\}$, whose incidence vector

$$v_F = (1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0 \quad 0 \quad 0)$$

is decomposed into three parallel bundles, P_1, P_2, and P_3, of 1-flats. Each parallel bundle consists of two 1-flats [3] as

$$P_1 = \{\{a_0, a_1\}, \{a_2, a_3\}\},$$
$$P_2 = \{\{a_0, a_2\}, \{a_1, a_3\}\},$$
$$P_3 = \{\{a_0, a_3\}, \{a_1, a_2\}\}.$$

Their corresponding incidence matrices are

$$v_{P_1} = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix},$$
$$v_{P_2} = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix},$$
$$v_{P_3} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Let $F_1, F_2, \cdots, F_\delta$ be δ μ-flats and $v_{F_1}, v_{F_2}, \cdots, v_{F_\delta}$ be their corresponding incidence vectors. $F_1, F_2, \cdots, F_\delta$ are not necessary to be different. The base matrix is defined by

$$B = \begin{pmatrix} v_{F_1} \\ v_{F_2} \\ \vdots \\ v_{F_\delta} \end{pmatrix} = \begin{pmatrix} v_{1,1} & v_{1,2} & \cdots & v_{1,p^{ds}} \\ v_{2,1} & v_{2,2} & \cdots & v_{2,p^{ds}} \\ \vdots & \vdots & \ddots & \vdots \\ v_{\delta,1} & v_{\delta,2} & \cdots & v_{\delta,p^{ds}} \end{pmatrix} \quad (4)$$

with δ rows and p^{ds} columns.

The row weight of B is $p^{\mu s}$. The column weights of B are variant and at most δ. It is possible that some columns in B have column weight zero or one. In that case, we simply replace some of $v_{F_1}, v_{F_2}, \cdots, v_{F_\delta}$ with other incidence vectors.

III. CONSTRUCTION OF THE QUASI-CYCLIC MOTHER MATRIX

By replacing each '1' in B with a $q \times q$ cyclic-permutation matrix and replacing each '0' with a $q \times q$ zero matrix, each incidence vector v_{F_i} becomes H_{M_i} which is a $1 \times p^{ds}$ array of $q \times q$ submatrices. Then, we obtain the following mother matrix

$$H_M = \begin{pmatrix} H_{M_1} \\ H_{M_2} \\ \vdots \\ H_{M_\delta} \end{pmatrix} = \begin{pmatrix} h^{a_{1,1}} & h^{a_{1,2}} & \cdots & h^{a_{1,p^{ds}}} \\ h^{a_{2,1}} & h^{a_{2,2}} & \cdots & h^{a_{2,p^{ds}}} \\ \cdots & \cdots & \cdots & \cdots \\ h^{a_{\delta,1}} & h^{a_{\delta,2}} & \cdots & h^{a_{\delta,p^{ds}}} \end{pmatrix} \quad (5)$$

where $a_{m,n} \in \{0, 1, \cdots, q-1, \infty\}$ and $h^{a_{m,n}}$ for $1 \le m \le \delta$, $1 \le n \le p^{ds}$ represents a $q \times q$ zero matrix if $a_{m,n} = \infty$ and represents a $q \times q$ cyclic-permutation matrix obtained by cyclically shifting the rows of the identity matrix to the right by $a_{m,n}$ times otherwise. The null space of H_M gives a mother code. The shifting matrix S of H_M is defined by

$$S = \begin{pmatrix} S_1 & S_2 & \cdots & S_{p^{ds}} \end{pmatrix} = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,p^{ds}} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,p^{ds}} \\ \vdots & \vdots & \ddots & \vdots \\ a_{\delta,1} & a_{\delta,2} & \cdots & a_{\delta,p^{ds}} \end{pmatrix} \quad (6)$$

and H_M can be obtained by replacing each entry $a_{m,n}$ of S with $h^{a_{m,n}}$. So, actually, H_M is obtained by replacing each '1' in B first with a shift value $a_{m,n}$ and then with $h^{a_{m,n}}$, and replacing each '0' in B first with ∞ and then with h^{∞}. The code rate associated with H_M is

$$r_M = 1 - \frac{\delta}{p^{ds}}. \quad (7)$$

It is stated in [8] that in a QC-LDPC code, the necessary and sufficient condition for the existence of the cycle of length $2i$ is

$$\sum_{k=0}^{i-1} (a_{m_k,n_k} - a_{m_{k+1},n_k}) \equiv 0 \bmod q \quad (8)$$

where $m_i = m_0$, $m_k \neq m_{k+1}$, $n_k \neq n_{k+1}$, a_{m_k,n_k} is an entry of S, and $a_{m_k,n_k} \neq \infty$.

If we combine the rows of a mother matrix to obtain effective matrices and the rows that will be combined in the mother matrix do not have '1's in the same column, then the corresponding mother and effective codes of different rates have the same fundamental decoder architecture [4]. The row combining method is equivalent to combine a group of check nodes of the mother code into a single check node and keep the variable nodes unchanged. Obviously, the row combining method will make the effective matrix H_E^j contain more short cycles than H_M. Therefore, to prevent short cycles in H_M and H_E^j, we need to consider both of H_M and H_E^j when we assign the shift values in S. On the other hand, the row decomposing method is equivalent to decompose each check node of the mother code into a group of check nodes and keep the variable nodes unchanged. Then, the mother and effective codes of different rates are also supported by the same fundamental decoder structure. It is obvious that the row decomposing method breaks some cycles in H_M and the effective matrix H_E^j will contain less cycles than H_M. Therefore, we only need to consider H_M when we assign the shift values in S. The details of the row decomposing method will be given in the next section.

Techniques used to prevent short cycles have been described in many research works such as [8]–[10]. In this paper, the Algorithm 1 is used in the construction of the shifting matrix S and H_M can be obtained by replacing each entry $a_{m,n}$ of S with a $q \times q$ submatrix $h^{a_{m,n}}$.

Algorithm 1 The shift values assigning algorithm.

procedure SHIFT VALUES ASSIGNING(B, q)
  Initially, entries of $\delta \times p^{ds}$ shifting matrix S are assigned to be ∞.
  for $n \leftarrow 1, p^{ds}$ **do**
    for $m \leftarrow 1, \delta$ **do**
      if $B_{m,n} = 1$ **then**
        $a_{m,n} \leftarrow 0$
        repeat
          $a_{m,n} \leftarrow a_{m,n} + 1$
          if $a_{m,n} = q$ **then** break;
          end if
        until condition (8) is not met.
      end if
    end for
  end for
end procedure

IV. CONSTRUCTION OF THE QUASI-CYCLIC EFFECTIVE MATRICES

The row decomposing method in this paper is based on the following theorem.

Theorem 1: In the Base matrix, if an incidence vector v_F of a μ-flat F is replaced with the incidence matrix v_{P_l} of a parallel bundle of $(\mu - j)$-flats P_l contained in F, the corresponding block row H_{M_i} of row weight $p^{\mu s}$ is decomposed into p^{js} block rows of row weight $p^{(\mu-j)s}$, with the column indices of '1's unchanged.

Proof: By Lemma 3, F contains K parallel bundles of $(\mu - j)$-flats and each of these parallel bundles contains p^{js} parallel $(\mu - j)$-flats. If we replace an incidence vector v_F of weight $p^{\mu s}$ with p^{js} incidence vectors of weight $p^{(\mu-j)s}$. Then, obviously, the corresponding block row H_{M_i} of row weight $p^{\mu s}$ is replaced with p^{js} block rows of row weight $p^{(\mu-j)s}$. By Lemma 2, each point in F will appear once and only once in P_l. Therefore, the column indices of '1's are unchanged. The proof is completed. □

Next, we give one example to illustrate the row decomposing method.

Example 2: We consider the three-dimensional Euclidean geometry $EG(3, 2)$ as in *Example* 1. Assume a 2-flat $F = \{a_0, a_1, a_2, a_3\}$ and $v_F = (11110000)$. Denote the corresponding block row by

$$H_{M_i} = (C_0 \quad C_1 \quad C_2 \quad C_3 \quad 0 \quad 0 \quad 0 \quad 0)$$

where C_i is a $q \times q$ cyclic-permutation matrix and 0 is a $q \times q$ zero matrix. Note that v_F can be decomposed into v_{P_1}, v_{P_2}, and v_{P_3} as explained in *Example* 1. Therefore, using the row decomposing method, H_{M_i} can be decomposed into one of the following three matrices.

$$\begin{pmatrix} C_0 & C_1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & C_2 & C_3 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} C_0 & 0 & C_2 & 0 & 0 & 0 & 0 & 0 \\ 0 & C_1 & 0 & C_3 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} C_0 & 0 & 0 & C_3 & 0 & 0 & 0 & 0 \\ 0 & C_1 & C_2 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

For $j = 1, 2, \cdots, D = (\mu - 1)$, let H_E^j be an effective matrix obtained by decomposing each block row of H_M into p^j block rows, which is defined by

$$H_E^j = \begin{pmatrix} H_{E_1}^j \\ H_{E_2}^j \\ \vdots \\ H_{E_\delta}^j \end{pmatrix} = \begin{pmatrix} h^{a_{1,1}} & h^{a_{1,2}} & \cdots & h^{a_{1,p^{ds}}} \\ h^{a_{2,1}} & h^{a_{2,2}} & \cdots & h^{a_{2,p^{ds}}} \\ \vdots & \vdots & \ddots & \vdots \\ h^{a_{\delta\cdot p^{js},1}} & h^{a_{\delta\cdot p^{js},2}} & \cdots & h^{a_{\delta\cdot p^{js},p^{ds}}} \end{pmatrix} \quad (9)$$

where $H_{E_i}^j$ corresponds to H_{M_i} and has p^{js} block rows and p^{ds} block columns. A concentrated degree distribution is a degree distribution in which every node has the same degree or all the degrees are within one of each other. The check node degree distributions of the mother and effective codes should be concentrated [4]. From Theorem 1, we know that each block row H_{M_i} of row weight $p^{\mu s}$ is decomposed into p^{js} block rows, which are denoted by $H_{E_i}^j$. The rows of H_E^j have the same row weight $p^{(\mu-j)s}$ and therefore have the concentrated check node degree distribution. The QC structure of the mother matrix H_M is also maintained in the effective matrix H_E^j. The null space of H_E^j gives an effective code. The code rate associated with H_E^j is

$$r_j = 1 - \frac{\delta p^{js}}{p^{ds}} = 1 - \frac{\delta}{p^{(d-j)s}}. \quad (10)$$

It can be seen from (7) and (10) that it is possible to adjust the code rate by choosing d, p, s, μ, and δ appropriately. From H_{M_i} to $H_{E_i}^j$, the row decomposing is not unique. By Lemma 3, a μ-flat in $EG(d, p^s)$ consists of K parallel bundles of $(\mu - j)$-flats, $P_1, P_2, \cdots, P_K$. Therefore, H_{M_i} can be decomposed into K different $H_{E_i}^j$'s and replaced with one of them. In the base matrix B, for $1 \le l < t \le \delta$, if $v_{F_l} = v_{F_t}$, their corresponding H_{M_l} and H_{M_t} should be decomposed into $H_{E_l}^j$ and $H_{E_t}^j$ in different ways ($v_{P_l} \ne v_{P_t}$) to reduce the number of cycles between $H_{E_l}^j$ and $H_{E_t}^j$. The mother code and the effective codes have a constant code length

$$L = qp^{ds}. \quad (11)$$

Assume the minimum column weight of W_c, then it is easy to see that for $1 \le l \le L$, each code bit of the mother and effective codes is checked by at least W_c orthogonal check sums. These orthogonal check sums can be used for majority-logic decoding of the code [3]. The code is capable of correcting any error pattern with $\lfloor W_c/2 \rfloor$ or fewer errors using one-step majority-logic decoding [3]. As a result, the minimum distance of the mother and effective codes is at least $W_c + 1$.

Since the row weights of H_M and $H_{E_l}^j$ are $p^{\mu s}$ and $p^{(\mu-j)s}$, respectively, it is clear that the densities of H_M and $H_{E_l}^j$ are $p^{\mu s}/(qp^{ds})$ and $p^{(\mu-j)s}/(qp^{ds})$, respectively.

V. EXAMPLES AND SIMULATIONS

In the following, we first use an example to illustrate the construction method of the mother and effective matrices. The codes in *Example* 3 are by no means good LDPC codes but the we can see them as an example to explain our code construction method.

Example 3: Again we consider the three-dimensional Euclidean geometry $EG(3,2)$. Assume thee 2-flats $F_1 = F_2 = \{a_0, a_1, a_2, a_3\}$ and $F_3 = \{a_4, a_5, a_6, a_7\}$. F_1 and F_2 are analyzed in *Example 1* and *Example 2*. The incidence vector of F_3 is

$$v_{F_3} = (0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 1)$$

which can be decomposed into three incidence matrices

$$v'_{P_1} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix},$$
$$v'_{P_2} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix},$$
$$v'_{P_3} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

Then, we have the following base matrix

$$B = \begin{pmatrix} v_{F_1} \\ v_{F_2} \\ v_{F_3} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

By replacing each '1' in B with a $q \times q$ cyclic-permutation matrix C_{ij} and replacing each '0' with a $q \times q$ zero matrix 0, a mother matrix

$$H_M = \begin{pmatrix} H_{M_1} \\ H_{M_2} \\ H_{M_3} \end{pmatrix} = \begin{pmatrix} C_{11} & C_{12} & C_{13} & C_{14} & 0 & 0 & 0 & 0 \\ C_{21} & C_{22} & C_{23} & C_{24} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & C_{35} & C_{36} & C_{37} & C_{38} \end{pmatrix}$$

is obtained. Now, we consider how to get the effective matrix H_E^1. Since $F_1 = F_2$, H_{M_1} and H_{M_2} are decomposed into $H_{E_1}^1$ and $H_{E_2}^1$ according to different incidence matrices, v_{P_1} and v_{P_2} (given in *Example* 1), respectively. H_{M_3} can be decomposed into

$$\begin{pmatrix} 0 & 0 & 0 & 0 & C_{35} & 0 & C_{37} & 0 \\ 0 & 0 & 0 & 0 & 0 & C_{36} & 0 & C_{38} \end{pmatrix}$$

according to v'_{P_2}. This is one of three possible choices for $H_{E_3}^1$. Finally, we obtain the effective matrix

$$H_E^1 = \begin{pmatrix} H_{E_1}^1 \\ H_{E_2}^1 \\ H_{E_3}^1 \end{pmatrix} = \begin{pmatrix} C_{11} & C_{12} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & C_{13} & C_{14} & 0 & 0 & 0 & 0 \\ C_{21} & 0 & C_{23} & 0 & 0 & 0 & 0 & 0 \\ 0 & C_{22} & 0 & C_{24} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & C_{35} & 0 & C_{37} & 0 \\ 0 & 0 & 0 & 0 & 0 & C_{36} & 0 & C_{38} \end{pmatrix}.$$

Table 1. A list of code parameters.

	Achievable code rates	Submatrix size	Code length
802.16e	1/2, 2/3, 3/4, 5/6	96	2304
Example 4	1/2, 3/4, 7/8	72	2304
802.15	1/2, 3/4, 7/8	21	672
Example 5	1/2, 3/4, 7/8	21	672

Table 2. Comparisons of code densities.

	Code rate 1/2	Code rate 3/4	Code rate 7/8
802.16e	0.0027	0.0063	
Example 4	0.0035	0.0069	0.0139
802.15	0.009	0.022	0.045
Example 5	0.012	0.024	0.048

Next, we give another two examples of our proposed codes and compare them with the LDPC codes given in IEEE 802.16e [11] and IEEE 802.15 [12]. In computing the error performance, in terms of the bit error rate (BER), we assume BPSK transmission over an additive white Gaussian noise (AWGN) channel. The decoding algorithm used here is the log-likelihood belief propagation algorithm and the maximum iteration number is set to be 50.

Example 4: Consider the Euclidean geometry $EG(5,2)$. Let $\mu = 5$, $\sigma = 4$, and $q = 72$. There are 32 points in $EG(5,2)$. We choose 4 incidence vectors and construct a 4×32 base matrix B. Carefully replace each '0' of B with a 72×72 zero matrix and replace each '1' with a 72×72 cyclic-permutation matrix, then we obtain the a 288×2304 mother matrix H_M. Since each 5-flat can be decomposed into parallel bundles of 4-flats or 3-flats, by decomposing the block rows of H_M, we can get effective matrices H_E^1 and H_E^2 of size 576×2304 and 1152×2304, respectively. The null space of H_M, H_E^1, and H_E^2 give QC-LDPC codes of rate $r_M = 7/8$, $r_1 = 3/4$, and $r_2 = 1/2$, respectively. The code length is $L = 2304$. A BER performance comparison of the these codes and the codes given in [11] of the rates 1/2, 3/4 is given in Fig. 1.

Example 5: Again consider the Euclidean geometry $EG(5,2)$. Let $\mu = 5$, $\sigma = 4$ and $q = 21$. There are 32 points in $EG(5,2)$. We choose 4 incidence vectors and construct a 4×32 regular base matrix B. Carefully replace each '0' of B with a 21×21 zero matrix and replace each '1' with a 21×21 cyclic-permutation matrix, then we obtain the a 84×672 mother matrix H_M. Since each 5-flat can be decomposed into parallel bundles of 4-flats or 3-flats, by decomposing the block rows of H_M, we get effective matrices H_E^1 and H_E^2 of size 168×672 and 336×672, respectively. The null space of H_M, H_E^1, and H_E^2 give QC-LDPC codes of rate $r_M = 7/8$, $r_1 = 3/4$, and $r_2 = 1/2$, respectively. The code length is $L = 672$. A BER performance comparison of the these codes and the codes given in [12] of the rates 1/2, 3/4, and 7/8 is given in Fig. 2.

Some parameters of multiple-rate QC-LDPC codes in these two examples and the codes proposed in [11] and [12] are given in Table I. From the Figs. 1 and 2, we can see that our propose codes perform very well over the AWGN channel and have low error floors with the iterative decoding algorithm.

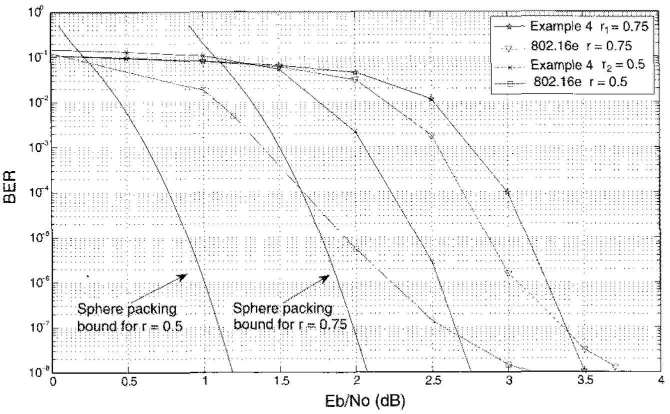


Fig. 1. Performances of LDPC codes in the *Example* 4 and IEEE 802.16e.

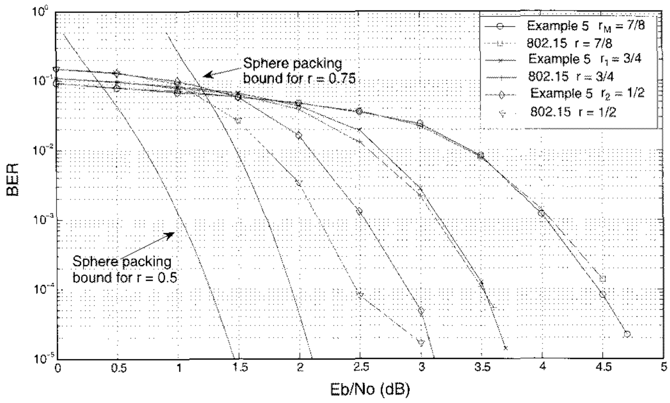


Fig. 2. Performances of LDPC codes in the *Example* 5 and IEEE 802.15.

VI. CONCLUSION

In this paper, a method for the construction of multiple-rate QC-LDPC codes based on Euclidean geometries has been presented. Based on the row decomposing method, we can get lower-rate effective codes from a higher-rate mother code and keep the code length unchanged. The row decomposing method breaks some cycles in the mother matrix. Therefore, the effective matrices has less cycles than the mother matrix. The mother and effective QC-LDPC codes of different code rates are supported by the same fundamental decoder architecture. Simulation results show that our codes perform very well and have low error floor with the iterative decoding over the AWGN channel. This suggests that the new codes have large minimum distances. Their exact computation is an open issue for future research.

REFERENCES

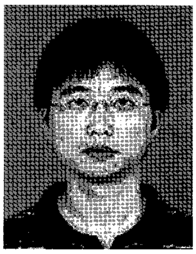
[1] R. G. Gallager, "Low density parity check codes," *IEEE Trans. Inf. Theory*, vol. IT-8, no. 1, pp. 21–28, Jan. 1962.

[2] D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," *IEE Electron. Lett*, vol. 32, no. 18, pp. 1645–1646, Aug. 1996.

[3] S. Lin and D. J. Costello Jr., *Error Control Coding: Fundamentals and Applications*. 2nd ed., Englewood Cliffs, NJ: Prentice-Hall, 2004.

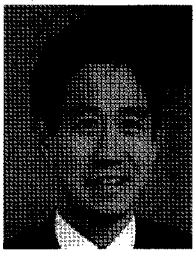
[4] A. I. V. Casado, W. Weng, S. Valle, and R. D. Wesel, "Multiple-rate low-density parity-check codes with constant blocklength," *IEEE Trans. Commun.*, vol. 57, no. 1, pp. 75–83, Jan. 2009.

[5] M. Good and F. R. Kschischang "Incremental redundancy via check splitting," in *Proc. Biennial Symp. Commun.*, 2006.
[6] N. Jacobsen and R. Soni, "Design of rate-compatible irregular LDPC codes based on edge growth and parity splitting," in *Proc. VTC Fall*, 2007.
[7] H. Tang, J. Xu, S. Lin, and K. Abdel-Ghaffar, "Codes on finite geometries," *IEEE Trans. Inf. Theory*, vol. 51, no. 2, pp. 572–596, Feb. 2005.
[8] M. P. C. Fossorier, "Quasi-cyclic low-density parity-check codes from circulant permutation matrices," *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1788–1793, Aug. 2004.
[9] X. Jiang and M. H. Lee, "Large girth quasi-cyclic LDPC codes based on the Chinese remainder theorem," *IEEE Commun. Lett.*, vol. 13, no. 5, pp.342–344, May. 2009.
[10] X. Jiang and M. H. Lee, "Large girth non-binary LDPC codes based on Euclidean geometries and finite fields," *IEEE Signal Process. Lett.*, vol. 16, no. 6, pp. 521–524, June 2009.
[11] IEEE Std. 802.16e 2005, "EEE standard for local and metropolitan area networks - part 16: Air interface for fixed and mobile broadband wireless access systems," Dec. 2005.
[12] IEEE 802.15 WPAN Millimeter Wave Alternative PHY Task Group 3c (TG3c), "Merged proposal: New PHY layer and enhancement of MAC for mmWave system proposal," Nov. 2007.



Xueqin Jiang received the B.S. degree Nanjing Institute of Technology, Nanjing, Jiangsu, P. R. China, in Computer Science. He received the M.S. and Ph.D. degree from Chonbuk National University, Jeonju, Korea, in Communication Engineering. He is currently working at School of Information Science and Technology, Donghua University, China. His research interests include LDPC codes and coding theory.

Yier Yan received the B.S. degree from South-Central Nationality University, Wuhan, Hubei, P. R. China, in Applied Electronics. He received the M.S. and Ph.D. degree from Chonbuk National university, Jeonju, Korea, in Communication Engineering. He is currently working at School of Mechanical and Electrical Engineering of Guangzhou University, China. His research interests include information theory, signal processing, and OFDM in MIMO system.



Moon Ho Lee received his B.S. and M.S. degree in Electrical Engineering from Chonbuk National University, Korea, in 1967 and 1976, respectively, and Ph.D. (I) degree in Electrical Engineering from Chonnam National University in 1984. Also, he received his Ph.D. (II) degree in Information Engineering from the University of Tokyo in 1990. During August 1985 through August 1986, he studied at the University of Minnesota as a Post Doctor. Also, he is Professional Engineer Licensed at 1981, Korea. From 1970–1980, he was a Chief Engineer at the Namyang Moonhwa Broadcasting Company. He was recipient of Paper Prize Awards from Korea Institute of Communication Sciences in 1986 and 1996, from Korea Institute Telematics and Electronics in 1987 and Chonbuk province in 1992, Chonbuk National Engineering in 2000, and Hedong Information Communication in 2007. Also, he received National order of Merits, Doyak Medal in 2007, this month's scientist award by Ministry of Science and Technology (MOST) and Korea Science and Engineering Foundation (KOSEF) in January 2008, respectively. He also studied at the University of Hannover during 1990 summer and at the University of Aachen, 1995 winter, Hannova and at the University of Munchen during 1998 and 2002 summer, Kaiserslautern supported by Germany government. Also, he was invited Professor at Nagaoka Technical University in Japan during 2000 summer, RMIT during 2003 summer and University of Wollongong during 2004 summer in Australia. Currently, he is a Professor of Division of Electronic and Information Engineering and a Head of the Institute of Information and Communication in Chonbuk National University. His research interests include image processing, mobile communication and high speed communication networks, and information and algebra coding theory. He is a Member of Sigma Xi. He is a Korea Engineering Academy Member and Guest Editor of IEEE communication magazine at 2007, "Quality of service based routing algorithm for heterogeneous networks".