Design of Quasi-Cyclic Low-Density Parity Check Codes with Large Girth

Long-Jiang Jing, Jing-Li Lin, and Wei-Le Zhu

In this paper we propose a graph-theoretic method based on linear congruence for constructing low-density parity check (LDPC) codes. In this method, we design a connection graph with three kinds of special paths to ensure that the Tanner graph of the parity check matrix mapped from the connection graph is without short cycles. The new construction method results in a class of (3, ρ)-regular quasi-cyclic LDPC codes with a girth of 12. Based on the structure of the parity check matrix, the lower bound on the minimum distance of the codes is found. The simulation studies of several proposed LDPC codes demonstrate powerful bit-error-rate performance with iterative decoding in additive white Gaussian noise channels.

Keywords: LDPC codes, Tanner graph, girth, linear congruence.

I. Introduction

Low-density parity check (LDPC) codes, discovered by Gallager in the early 1960s [1], were rediscovered in late 1990s and were shown to form a class of Shannon-limit-approaching codes. An LDPC code can be described by a bipartite graph called a Tanner graph [2]. The length of the shortest cycle in a Tanner graph is referred to as its girth. Since short cycles prevent the iterative decoding from converging and degrade the performance of the LDPC decoders, they must be avoided in code construction; for this reason, many methods for constructing LDPC codes without short cycles have been proposed in [3]-[15]. Fossorier [6] constructed a family of quasi-cyclic (QC)-LDPC codes from circulant permutation matrices, and derived necessary and sufficient conditions for such codes to have girths of eight, ten, and twelve, respectively. A high-girth code can be obtained from an array code by deleting certain columns of their parity check matrices [7]. Tanner and others [9] gave an explicit construction of high-girth QC-LDPC codes using an underlying structure of multiplicative groups in the set of integers modulo m.

The parity check matrix of a (λ, ρ)-regular LDPC code is sparse, with λ 1-entries in each column and ρ 1-entries in each row. Although the irregular LDPC codes outperform regular LDPC codes, the regular structure of the latter can be exploited to simplify the decoder. It is shown that the best performance of regular LDPC codes under iterative decoding can be achieved with $\lambda = 3$ [16]; therefore, we restrict regular LDPC codes with $\lambda = 3$.

In general, the structured LDPC codes have encoding advantages over the random LDPC codes, especially QC-LDPC codes. The QC-LDPC codes can be encoded in linear time with shift registers [17], and some classes of QC-LDPC

Manuscript received Sept. 05, 2006; revised Jan. 04, 2007.

Long-Jiang Jing (phone: +86 28 83202204, email: jlj200@sohu.com), Jing-Li Lin (email: linjingli77@163.com), and Wei-Le Zhu (email: wlzhu@uestc.edu.cn) are with the College of Electronic Engineering, University of Electronic Science and Technology of China, Chengdu, China.

codes based on circulant permutation matrices can be encoded by division circuits as cyclic codes [18]. In addition, the QC-LDPC codes achieve better memory efficiency in comparison with conventional LDPC codes.

This paper presents a graph-theoretic method to construct QC-LDPC codes with large girth. Unlike other construction methods based on circulant permutation matrices, to the best of our knowledge, for the first time, we have designed a special connection graph with three kinds of special paths to ensure that the Tanner graph of the parity check matrix mapped from the connection graph is without short cycles. These vertices of the special connection graph and two kinds of special paths are mapped from the 1-entries and rows (columns) of the parity check matrix of an array code, respectively. The third kind of special path is obtained by connecting the corresponding vertices in this graph based on linear congruence. In the next step, we map the vertices and the three kinds of special paths of this connection graph to the columns and rows of parity check matrix $\boldsymbol{H}$. The length of the shortest cycles of the Tanner graph defined by parity check matrix $\boldsymbol{H}$ is 12 using this construction method. Hence, a class of QC-LDPC code with a girth of 12 is obtained.

II. Construction of Codes

1. Graph Structure

Let $\boldsymbol{G}=(\boldsymbol{V}, \boldsymbol{E})$ be an undirected connection graph with vertex set $\boldsymbol{V}$ of size n and edge set $\boldsymbol{E}$. A path in $\boldsymbol{G}$ is a finite alternating sequence of distinct vertices and edges, beginning and ending with a vertex. A path of length β contains $\beta+1$ vertices. Let $\boldsymbol{L}$ be a set of m paths of length $\rho-1$, which satisfies the constraint that any two paths in $\boldsymbol{L}$ are either disjointed (have no vertex in common) or singularly crossing (have exactly one vertex in common). Any two paths in $\boldsymbol{L}$ have no edges in common; furthermore, each vertex in $\boldsymbol{V}$ just lies on 3 paths in $\boldsymbol{L}$. A *p-cycle* of length γ in $\boldsymbol{G}$ is a closed path which begins and ends at the same vertex, and the p-cycle passes through γ paths in set $\boldsymbol{L}$ or some vertices and edges of each path. That is to say, a p-cycle of length γ is a cycle enclosed by γ paths in set $\boldsymbol{L}$. For example, in Fig. 1(b), $\boldsymbol{L}=\{L_1, L_2, \cdots, L_7\}$, the length of each path is 2, and a p-cycle of length 3 passing through some vertices and edges of L_3, L_4, and L_6 is indicated by dash lines.

Let $\boldsymbol{H}=[h_{i,j}]$ be the binary matrix whose n columns correspond to n vertices that lie on the paths in $\boldsymbol{L}$ and whose m rows correspond to the m paths in $\boldsymbol{L}$, where $h_{i,j}=1$ if, and only if, the j-th vertex is on the i-th path. Since the length of each path in $\boldsymbol{L}$ is $\rho-1$ and each vertex lies on 3 paths in $\boldsymbol{L}$, each row of $\boldsymbol{H}$ has weight ρ, and each column of $\boldsymbol{H}$ has weight 3. If ρ is very small compared to the number n, $\boldsymbol{H}$ is a sparse matrix. Therefore, the null space of $\boldsymbol{H}$ over GF(2) gives a $(3, \rho)$-regular LDPC code of length n. We call the graph corresponding to matrix $\boldsymbol{H}$ structure graph $\boldsymbol{G}_s$. Since there is a one-to-one correspondence between p-cycles in $\boldsymbol{G}_s$ and cycles in $\boldsymbol{H}$ and the p-cycles are half the length of the corresponding cycles, it is easy to identify the cycles in $\boldsymbol{H}$. For example, Fig. 1 shows a cycle of length 6 in $\boldsymbol{H}$ and the corresponding p-cycle of length 3 in its structure graph. Therefore, a new class of LDPC codes with large girth can be easily obtained by designing the structure graph without short p-cycles.

Consider path subsets $\boldsymbol{L}_1 \subseteq \boldsymbol{L}$, $\boldsymbol{L}_2 \subseteq \boldsymbol{L}$, and $\boldsymbol{L}_1 \cap \boldsymbol{L}_2 = \emptyset$. We define $\boldsymbol{L}_1(V_i)$ and $\boldsymbol{L}_2(V_i)$ as the number of paths in $\boldsymbol{L}_1$ and $\boldsymbol{L}_2$ passing vertex V_i, respectively. The vertex set $\boldsymbol{V}_1 = \{V_i : \boldsymbol{L}_1(V_i) \bmod 2=1,\ V_i \in \boldsymbol{V}\}$, $\boldsymbol{V}_2 = \{V_i : \boldsymbol{L}_2(V_i) \bmod 2=1,\ V_i \in \boldsymbol{V}\}$. If $\boldsymbol{V}_1=\boldsymbol{V}_2$, there is a redundant row in $\boldsymbol{H}$, and we call $\boldsymbol{L}_1$ and $\boldsymbol{L}_2$ cor-path subsets. As seen in Fig. 1, rows l_2, l_3, l_4, and l_5 in $\boldsymbol{H}$ are correlative, as $\boldsymbol{L}_1=\{L_3, L_4\}$, $\boldsymbol{L}_2=\{L_2, L_5\}$, and $\mathbf{V}_1=\mathbf{V}_2=\{V_4, V_5, V_6, V_7\}$ in $\boldsymbol{G}_s$.

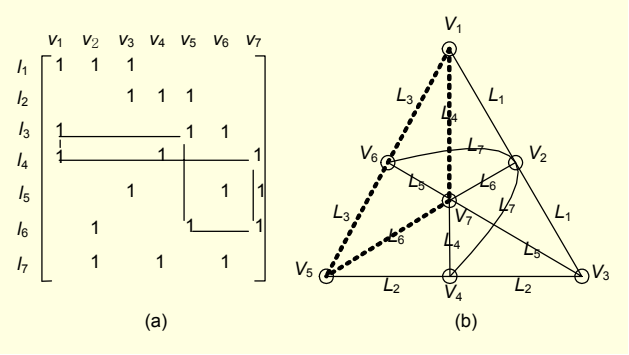


Fig. 1. (a) A cycle with a length of 6 in parity check matrix $\boldsymbol{H}$ and (b) the corresponding p-cycle with a length of 3 (indicated by dashed lines) in its structure graph.

2. Design Procedure

Consider the Galois field GF(p) where p is a prime. The addition and multiplication of GF(p) are modulo-p addition $\oplus$ and modulo-p multiplication $\otimes$. Let $\boldsymbol{T}$ be the set of p^2 p-tuples over GF(p):

$$\boldsymbol{T} = \{T_{i,j} = (f(0), \cdots, f(p-1)) : f(X) = (i \otimes X) \oplus j, i, j \in GF(p)\}. \quad (1)$$

Theorem 1. Any two p-tuples in $\boldsymbol{T}$ have no more than one component in all p positions in common.

Proof. For $0 \le k, i, i', j, j' < p$, the k-th component $T_{i,j}^{\ k}$ of $T_{i,j}$ and the k-th component $T_{i',j'}^{\ k}$ of $T_{i',j'}$ are $(i \otimes k) \oplus j$ and $(i' \otimes k) \oplus j'$, respectively. Therefore, a linear congruence for variable k can be obtained as follows:

$$(i - i') \cdot k + (j - j') \equiv 0 (\bmod\ p). \quad (2)$$

The number of roots of (2) exactly equals the number of the same components in all p positions between $T_{i,j}$ and $T_{i',j'}$. It is clear that (2) has no solution for $i = i'$ and $j \neq j'$, whereas (2) has a unique solution for $i \neq i'$ because $\mathbf{GCD}(i - i', p) = 1$ for $i \neq i'$. Thus, $T_{i,j}$ and $T_{i',j'}$ have no more than one component in all p positions in common. □

Let $\boldsymbol{S}_0, \boldsymbol{S}_1, \cdots, \boldsymbol{S}_{p-1}$ and $\boldsymbol{Z}_0, \boldsymbol{Z}_1, \cdots, \boldsymbol{Z}_{p-1}$ be $2p$ sets of p^2 p-tuple over GF(p). For $0 \le i, j, k < p$, the p-tuple $S_{i,j,k}$ in $\boldsymbol{S}_i$ is defined as $S_{i,j,k} = (f(0), f(1), \cdots, f(p-1))$, where $f(X) = (i \oplus k) \otimes X \oplus j$, and the p-tuple $Z_{k,i,j}$ in the set $\boldsymbol{Z}_k$ is defined as $Z_{k,i,j} = (f(0), f(1), \cdots, f(p-1))$, where $f(X) = (i \oplus k) \otimes X \oplus i \otimes k \oplus j$. Thus, from theorem 1, no two p-tuples in the same set $\boldsymbol{S}_i$ (or $\boldsymbol{Z}_k$) have more than one component in all p positions in common.

For each element $j \in \mathrm{GF}(p)$, its location vector is a p-tuple over GF(2), $M(j) = (M_j^0, M_j^1, \cdots, M_j^{p-1})$, where $M_j^j = 1$ and all other components equal zero [8]. For $0 \le i, j, k < p$, matrix $\boldsymbol{B}$ is constructed with the components of $T_{i,j}$ as follows:

$$\boldsymbol{B} = \begin{bmatrix} T_{0,0} \\ \vdots \\ T_{0,p-1} \\ \vdots \\ T_{p-1,0} \\ \vdots \\ T_{p-1,p-1} \end{bmatrix} = \begin{bmatrix} T_{0,0}{}^0 & T_{0,0}{}^1 & \cdots & T_{0,0}{}^{p-1} \\ \vdots & \vdots & \ddots & \vdots \\ T_{0,p-1}{}^0 & T_{0,p-1}{}^1 & \cdots & T_{0,p-1}{}^{p-1} \\ \vdots & \vdots & \ddots & \vdots \\ T_{p-1,0}{}^0 & T_{p-1,0}{}^1 & \cdots & T_{p-1,0}{}^{p-1} \\ \vdots & \vdots & \ddots & \vdots \\ T_{p-1,p-1}{}^0 & T_{p-1,p-1}{}^1 & \cdots & T_{p-1,p-1}{}^{p-1} \end{bmatrix}, \quad (3)$$

and each entry of matrix $\boldsymbol{B}$ is replaced by its location vector; thus, we obtain assistant matrix $\boldsymbol{A}$ with a $p \times p$ array of submatrices:

$$\boldsymbol{A} = \begin{bmatrix} \boldsymbol{A}_{0,0} & \boldsymbol{A}_{0,1} & \cdots & \boldsymbol{A}_{0,p-1} \\ \boldsymbol{A}_{1,0} & \boldsymbol{A}_{1,1} & \cdots & \boldsymbol{A}_{1,p-1} \\ \vdots & \vdots & \vdots & \vdots \\ \boldsymbol{A}_{p-1,0} & \boldsymbol{A}_{p-1,1} & \cdots & \boldsymbol{A}_{p-1,p-1} \end{bmatrix}. \quad (4)$$

For $0 \le i, k < p$, each submatrix $\boldsymbol{A}_{i,k}$ is

$$\boldsymbol{A}_{i,k} = \begin{bmatrix} M(T_{i,0}{}^k) \\ M(T_{i,1}{}^k) \\ \vdots \\ M(T_{i,p-1}{}^k) \end{bmatrix}.$$

It is a $p \times p$ identity matrix with rows cyclically shifted to the right by $i \otimes k$ positions. Hence, $\boldsymbol{A}$ is a $p^2 \times p^2$ matrix with constant column weight p and constant row weight p over GF(2). It has the same form as the parity check matrix of an array-type LDPC code [10]. Based on theorem 1, no two rows in $\boldsymbol{A}$ have more than one 1-entry in common, in other words, assistant matrix $\boldsymbol{A}$ satisfies the row-column (RC)-constraint.

Based on assistant matrix $\boldsymbol{A}$, a structure graph $\boldsymbol{G}_s$ with p isomorphic subgraphs, $\boldsymbol{G}_s{}^0, \boldsymbol{G}_s{}^1, \cdots, \boldsymbol{G}_s{}^{p-1}$, can be designed. Each subgraph has p^3 vertices (corresponding to p^3 1-entries of $\boldsymbol{A}$), p^2 paths of length p–1 called the *r-path* (corresponding to p^2 rows of $\boldsymbol{A}$), and p^2 paths of length p–1 called the *c-path* (corresponding to p^2 columns of $\boldsymbol{A}$). Since the assistant matrix $\boldsymbol{A}$ satisfies the RC-constraint, the length of the minimal p-cycles of these subgraphs is 6. For $0 \le i, j, k, l < p$, we label the vertex in $\boldsymbol{G}_s{}^l$ corresponding to the 1-entry of the j-th row of $\boldsymbol{A}_{i,k}$ of $\boldsymbol{A}$ as $V_{l,i,k,j}$. Starting from $V_{0,i,k,j}$, if we connect p vertices $\{V_{l,i,k,j'} : j' = (i \oplus k) \otimes l \oplus j, 0 \le l < p\}$, then a path of length p–1 called the *t-path* $L^T{}_{i,k,j}$ can be obtained. Thus, there are p^4 vertices, p^3 r-paths, p^3 c-paths, and p^3 t-paths together. For the different value of i, these p^3 t-paths can be partitioned into p path subsets $\boldsymbol{L}_0^T, \boldsymbol{L}_1^T, \cdots, \boldsymbol{L}_{p-1}^T$, which correspond to p p-tuple sets $\boldsymbol{S}_0, \boldsymbol{S}_1, \cdots, \boldsymbol{S}_{p-1}$, respectively. Similarly, since the column position of the 1-entry of the j'-th $(j' = (i \oplus k) \otimes l \oplus j)$ row of $\boldsymbol{A}_{i,k}$ of $\boldsymbol{A}$ is $(i \otimes k) \oplus (i \oplus k) \otimes l \oplus j$, for the different value of k, these p^3 t-paths can be partitioned into p subsets $\boldsymbol{L}_0^{T'}, \boldsymbol{L}_1^{T'}, \cdots, \boldsymbol{L}_{p-1}^{T'}$ corresponding to p p-tuple sets $\boldsymbol{Z}_0, \boldsymbol{Z}_1, \cdots, \boldsymbol{Z}_{p-1}$, respectively. Therefore, any two paths in the p^3 t-paths are disjointed, and the length of the minimal p-cycles enclosed by the p^3 t-paths and the p^3 r-paths (or p^3 c-paths) is 6. For the p-cycles enclosed by the three kinds of paths together, since any p-cycle is composed of at least two r-paths, two c-paths, and two t-paths, the length of the p-cycle is no less than 6. As a result, the length of the

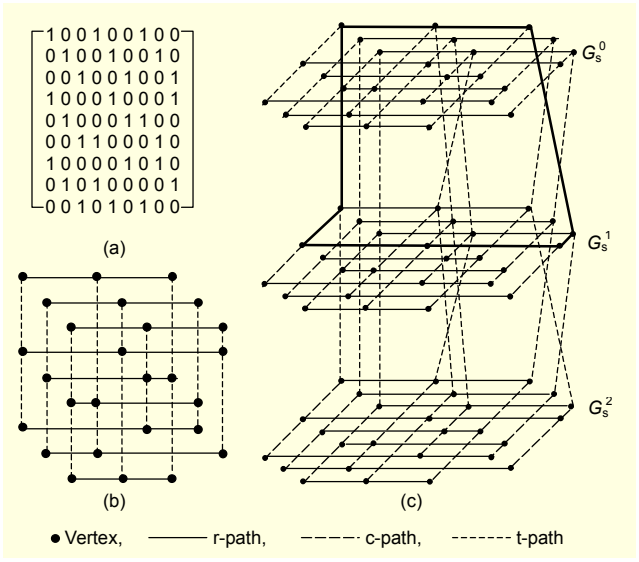


Fig. 2. Construction of the code with p=3: (a) assistant matrix $\boldsymbol{A}$, (b) subgraph $\boldsymbol{G}_s{}^0$, and (c) structure graph $\boldsymbol{G}_s$. The bold lines illustrate a p-cycle with length 6 (Only part of the t-paths is illustrated).

minimal p-cycles of $\boldsymbol{G}_s$ is 6. An example is shown in Fig. 2, where p=3.

Map the $3p^3$ paths and the p^4 vertices in $\boldsymbol{G}_s$ to the rows and the columns in parity check matrix $\boldsymbol{H}$ as follows:

- For $0 \le i, j, k, l < p$, if two paths of $\boldsymbol{G}_s^{\,l}$ intersect at the vertex $V_{l,i,k,j}$, then $h_{r1,co}=h_{r2,co}=1$ in matrix $\boldsymbol{H}$, where $co = l \cdot p^3 + l \cdot p^2 + k \cdot p + (i \otimes k \oplus j)$, $r1 = l \cdot p^2 + i \cdot p + j$, and $r2 = p^3 + l \cdot p^2 + k \cdot p + (i \otimes k \oplus j)$.
- Similarly, if the vertex $V_{l,i,k,j'}$ lies on the t-path $L^T_{\,i,k,j}$, then $h_{r3,co}=1$, where $j'=(i \oplus k) \otimes l \oplus j$, $r3=2 \cdot p^3 + i \cdot p^2 + k \cdot p + j$, and $co = l \cdot p^3 + i \cdot p^2 + k \cdot p + j'$.

Then, a $3p^3 \times p^4$ parity check matrix $\boldsymbol{H}$ can be obtained. The structure of parity check matrix $\boldsymbol{H}$ is illustrated in Fig. 3. Since the length of each path in these $3p^3$ paths is p–1 and each vertex lies on 3 paths (one r-path, one c-path, and one t-path), each row of $\boldsymbol{H}$ has weight p, each column of $\boldsymbol{H}$ has weight 3, and the null space of $\boldsymbol{H}$ gives a (3, p)-regular LDPC code with length p^4. Moreover, the length of the minimal p-cycles of $\boldsymbol{G}_s$ is 6, thus the girth of the new LDPC code is 12. Because $\boldsymbol{G}_s$ has some cor-path subsets, $\boldsymbol{H}$ has some redundant rows; as a result, the code rate is slightly higher than (p-3)/p.

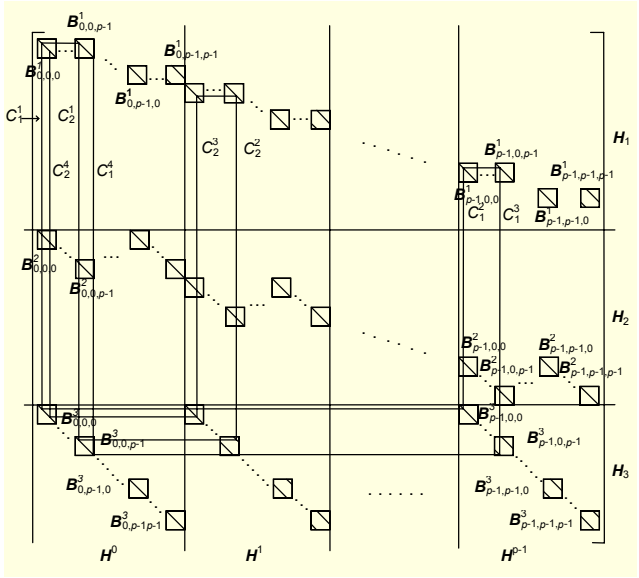


Fig. 3. Structure of parity check matrix $\boldsymbol{H}$.

3. Extension of the Construction Method

To achieve more flexible block lengths and code rates, one possible modification to the above construction method is proposed.

Masking assistant matrix $\boldsymbol{A}$ by an $r \times r$ ($r \le p$) matrix $\boldsymbol{W}_m=[w_{i,j}]$ over GF(2) with column and row weights q ($q \le r$), we obtain a new assistant matrix $\boldsymbol{A}_m$. The masking operation [11] can be modeled mathematically as $\boldsymbol{A}_m = \boldsymbol{W}_m * \boldsymbol{A} = [w_{i,j}\boldsymbol{A}_{i,j}]$, where $w_{i,j}\boldsymbol{A}_{i,j} = \boldsymbol{A}_{i,j}$ for $w_{i,j}$=1 and $w_{i,j}\boldsymbol{A}_{i,j}$=0 (zero matrix) for $w_{i,j}$=0. From the results presented in [13], we can get the following results: If there is a cycle $w_{i_1,j_1} \to w_{i_1,j_2} \to w_{i_2,j_2} \to w_{i_2,j_3} \to w_{i_3,j_3} \to w_{i_3,j_1} \to w_{i_1,j_1}$ of length 6 in $\boldsymbol{W}_m$, and

$$\sum_{a=1}^{3}[(i_a \otimes j_{(a+1) \bmod 3}) - (i_a \otimes j_a)] \bmod p \equiv 0, \qquad (5)$$

the nodes of the 6 submatrices $\boldsymbol{A}_{i_1,j_1}$, $\boldsymbol{A}_{i_1,j_2}$, ⋯, $\boldsymbol{A}_{i_3,j_3}$, $\boldsymbol{A}_{i_3,j_1}$ form p cycles of length 6. Thus, there are p corresponding p-cycles of length 6 in each subgraph $\boldsymbol{G}_s^{\,k}$ ($0 \le k < p$). In this way, we can effectively reduce the number of short p-cycles in structure graph $\boldsymbol{G}_s$ by selecting the proper matrix $\boldsymbol{W}_m$. Consequently, the number of cycles of length 12 in the Tanner graph defined by the parity check matrix can be efficiently reduced. If we randomly select q subgraphs and all $p \cdot r \cdot q$ t-paths from structure graph $\boldsymbol{G}_s$ which are constructed based on the new assistant matrix $\boldsymbol{A}_m$, a new structure graph $\tilde{\boldsymbol{G}}_s$ can be obtained. It gives rise to a $3p \cdot r \cdot q \times p \cdot r \cdot q^2$ new parity check matrix $\tilde{\boldsymbol{H}}$ with a column weight of 3 and a row weight of q. Moreover, $\tilde{\boldsymbol{H}}$ retains the quasi-cyclic structure of parity check matrix $\boldsymbol{H}$. As a result, the null space of $\tilde{\boldsymbol{H}}$ gives a new (3, q)-regular QC-LDPC code with more flexible block length $p \cdot r \cdot q^2$, compared with block length p^4.

Similarly, if we select an $r_1 \times r_2$ ($r_1, r_2 \le p$) matrix $\tilde{\boldsymbol{W}}_m$ with column weight q_1 ($q_1 \le r_1$) and row weight q_2 ($q_2 \le r_2$) to mask assistant matrix $\boldsymbol{A}$, and select q_3 ($q_3 \le p$) subgraphs from structure graph $\boldsymbol{G}_s$, a new $p \cdot (q_3 \cdot (r_1 + r_2) + q_2 \cdot r_1) \times p \cdot r_1 \cdot q_2 \cdot q_3$ parity check matrix $\tilde{\boldsymbol{H}}'$ with a constant column weight of 3 and row weights q_1, q_2, and q_3 can be obtained. It gives rise to a new QC-LDPC code with an even more flexible block length of $p \cdot r_1 \cdot q_2 \cdot q_3$ and code rate $1-(q_3 \cdot (r_1 + r_2) + q_2 \cdot r_1)/(r_1 \cdot q_2 \cdot q_3)$. Meanwhile, the girth of the new QC-LDPC code is at least 12.

III. Properties of Constructed Codes

This section describes several properties of the new LDPC codes constructed in section II.

1. Girth

The sum-product decoding algorithm converges to the maximum *a posteriori* (MAP) solution for graphs that are trees (have no cycles); for graphs with cycles, there is no such optimality. If the girth of the Tanner graph is g, then the iterative decoding algorithm is optimal for $\lceil (g-4)/4 \rceil$

iterations. Thus, large girth leads to reduced dependence in message passing and more efficient iterative decoding when the sum-product algorithm is used. An upper bound on the girth of a Tanner graph can be obtained from the well-known tree bound [1]. From the construction of the structure graph $\boldsymbol{G}_s$ described in section II, the length of the minimal p-cycles of $\boldsymbol{G}_s$ is 6; the corresponding LDPC codes have girth 12. Moreover, with the masking operation, we reduce the density of 1-entries of the assistant matrix; hence, the new structure graph, $\tilde{\boldsymbol{G}}_s$, has either larger p-cycles or a smaller number of short p-cycles than the original structure graph, $\boldsymbol{G}_s$. Consequently, the lower bound on the girth of the Tanner graph of the new LDPC codes is 12.

2. Quasi-Cyclic Structure

Figure 3 shows the structure of parity check matrix $\boldsymbol{H} = [\boldsymbol{H}_1{}^{\mathrm{T}}, \boldsymbol{H}_2{}^{\mathrm{T}}, \boldsymbol{H}_3{}^{\mathrm{T}}]^{\mathrm{T}}$. For $1 \le f \le 3$, $\boldsymbol{H}_f$ can be partitioned to a $p^2 \times p^3$ array of $p \times p$ submatrices. The p^3 nonzero submatrices (indicated by squares) in $\boldsymbol{H}_f$ are $\{\boldsymbol{B}^f{}_{l,i,k} : 0 \le i,k,l < p\}$. From the mapping method described in section II, $\boldsymbol{B}^1{}_{l,i,k}$ has the location vectors of $i \otimes k \oplus 0$, $i \otimes k \oplus 1, \cdots, i \otimes k \oplus (p-1)$ as the rows:

$$\boldsymbol{B}^1{}_{l,i,k} = \begin{bmatrix} M(i \otimes k \oplus 0) \\ M(i \otimes k \oplus 1) \\ \vdots \\ M(i \otimes k \oplus (p-1)) \end{bmatrix}. \tag{6}$$

Under modulo-p addition and multiplication, the location vector $M(i \otimes k \oplus (j+1))$ of the field element $i \otimes k \oplus (j+1)$ is the cyclic-shift of the location vector $M(i \otimes k \oplus j)$ of the field element $i \otimes k \oplus j$ for $0 \le j < p$. Therefore, $\boldsymbol{B}^1{}_{l,i,k}$ is a circulant permutation matrix. Moreover, for $0 \le i,k < p$, $\boldsymbol{B}^1{}_{0,i,k} = \boldsymbol{B}^1{}_{1,i,k} = \cdots = \boldsymbol{B}^1{}_{p\text{-}1,i,k}$. $\boldsymbol{B}^3{}_{l,i,k}$ has the location vectors of $(i \oplus k) \otimes l \oplus 0$, $(i \oplus k) \otimes l \oplus 1, \cdots, (i \oplus k) \otimes l \oplus (p-1)$ as the rows. Similarly, it is also a circulant permutation matrix. In the case of $\boldsymbol{B}^2{}_{l,i,k}$, since the 1-entry in the $(i \otimes k \oplus j)$th row of $\boldsymbol{B}^2{}_{l,i,k}$ is located at the $(i \otimes k \oplus j)$th column of $\boldsymbol{B}^2{}_{l,i,k}$, submatrix $\boldsymbol{B}^2{}_{l,i,k}$ is a $p \times p$ identity matrix. Consequently, the entire parity check matrix $\boldsymbol{H}$ can be partitioned into a $3p^2 \times p^3$ array of $p \times p$ submatrices; each submatrix is either a zero matrix or a circulant permutation matrix. Therefore, the null space of $\boldsymbol{H}$ gives a QC-LDPC code.

It is known that the decoders of general LDPC codes need a significant amount of memory to store their parity-check matrices. The QC-LDPC code, however, can solve the memory problem, since their parity-check matrices consist of circulant permutation matrices or zero matrices. In fact, in the case of general QC-LDPC codes, the memory required to store them can be reduced by a factor $1/p$ when $p \times p$ circulant permutation matrices are employed. Since there are $r \cdot q^2$ identity matrices and $\boldsymbol{B}^1{}_{0,i,k} = \boldsymbol{B}^1{}_{1,i,k} = \cdots = \boldsymbol{B}^1{}_{q\text{-}1,i,k}$ ($0 \le i < r, 0 \le k < q$), the memory required for the new QC-LDPC codes can be further reduced by a factor ω:

$$\omega = \frac{q^2 \cdot r + q \cdot r}{3q^2 \cdot r \cdot p} = \frac{q+1}{3q \cdot p} \approx \frac{1}{3p}. \tag{7}$$

3. Minimum Distance

At high signal-to-noise ratios (SNRs), the maximum-likelihood decoding performance of an error-correcting code is dominated by the code's minimum Hamming distance d_m. A lower bound on d_m for regular LDPC codes was derived in [2]:

$$d_m \ge \begin{cases} 2\dfrac{(\lambda-1)^{(g-2)/4}-1}{\lambda-2} + \dfrac{2}{\lambda}(\lambda-1)^{(g-2)/4}, & \text{when } g/2 \text{ is odd,} \\ 2\dfrac{(\lambda-1)^{g/4}-1}{\lambda-2}, & \text{when } g/2 \text{ is even,} \end{cases} \tag{8}$$

where g is the girth of the code, and λ is the column weight of the parity check matrix. For λ=3 and g=12, $d_m \ge 14$. However, this lower bound is loose for the new codes. Therefore, a new lower bound on d_m is given below in the form of a theorem.

Theorem 2: The minimum distance of the new codes is lower-bounded by 24.

Proof. The structure of the binary parity check matrix $\boldsymbol{H}$ is $\boldsymbol{H} = [\boldsymbol{H}_1^T, \boldsymbol{H}_2^T, \boldsymbol{H}_3^T]^T$ or $\boldsymbol{H} = [\boldsymbol{H}^0, \boldsymbol{H}^1, \cdots, \boldsymbol{H}^{p-1}]$ as depicted in Fig. 3. We define an inc idence vector, $D_i = (r_{i,1}, r_{i,2}, r_{i,3})$, of the i-th column in $\boldsymbol{H}$; for $1 \le i \le n$ and $1 \le j \le 3$, $r_{i,j}$ denotes the row number at which the 1-entry is located. From the structure of $\boldsymbol{H}$, if the column set $\boldsymbol{\Psi}$ satisfies the following constraints:

$$\sum_{C \in \Psi} r_{C,1} = 0 \,(\mathrm{mod}\, 2) \quad \text{and} \quad \sum_{C \in \Psi} r_{C,2} = 0 \,(\mathrm{mod}\, 2), \tag{9}$$

then $|\boldsymbol{\Psi}| \ge 6$. Moreover, these columns must belong to any one of the submatrices: $\boldsymbol{H}^0, \cdots, \boldsymbol{H}^{p-1}$. Randomly select 6 such columns, $C_1^1, \cdots, C_6^1$, for $0 \le l_1, i_1, i_2, i_3, j_1, j_1', j_1'' \le p-1$, $r_{C_1^1,1} = r_{C_2^1,1} = l_1 \cdot p^2 + i_1 \cdot p + j_1$, $r_{C_3^1,1} = r_{C_4^1,1} = l_1 \cdot p^2 + i_2 \cdot p + j_1'$, and $r_{C_5^1,1} = r_{C_6^1,1} = l_1 \cdot p^2 + i_3 \cdot p + j_1''$. It is clear that $i_1 \ne i_2 \ne i_3$. Then, the incidence vectors of C_1^1 and C_2^1 are

$$D_{C_1^1} = (r_{C_1^1,1}, r_{C_1^1,2}, 2p^3 + i_1 \cdot p^2 + k_1 \cdot p + [j_1 - (i_1 + k_1) \cdot l_1] (\mathrm{mod}\, p)), \quad \text{for } 0 \le k_1 < p,$$

$$D_{C_2^1} = (r_{C_2^1,1}, r_{C_2^1,2}, 2p^3 + i_1 \cdot p^2 + k_2 \cdot p + [j_1 - (i_1 + k_2) \cdot l_1] (\mathrm{mod}\, p)), \quad \text{for } 0 \le k_2 < p.$$

Since $k_1 \ne k_2$, $r_{C_1^1,3} \ne r_{C_2^1,3}$. Randomly select two

columns C_1^2 and C_2^2, such that $r_{C_1^2,3} = r_{C_1^1,3}$ and $r_{C_2^2,3} = r_{C_2^1,3}$, respectively. Then, their incidence vectors are

$$D_{C_1^2}=(l_2 \cdot p^2+i_1 \cdot p+j_2, r_{C_1^2,2}, r_{C_1^1,3}),$$
$$j_2=[j_1+(i_1+k_1)(l_2-l_1)](\text{mod } p), \quad \text{for } 0 \le l_2 \le p-1,$$

$$D_{C_2^2}=(l_3 \cdot p^2+i_1 \cdot p+j_3, r_{C_2^2,2}, r_{C_2^1,3}),$$
$$j_3=[j_1+(i_1+k_2)(l_3-l_1)](\text{mod } p), \quad \text{for } 0 \le l_3 \le p-1.$$

Similarly, there are C_1^3 and C_2^3, which satisfy the equations $r_{C_1^3,1} = r_{C_1^2,1}$ and $r_{C_2^3,1} = r_{C_2^2,1}$, respectively, and the incidence vector of C_2^3 is

$$D_{C_2^3}=(r_{C_2^2,1}, r_{C_2^3,2}, 2p^3+i_1 \cdot p^2+k_1 \cdot p+[j_3-(i_1+k_1) \cdot l_3](\text{mod } p)).$$

Since $(k_2-k_1) \cdot (l_3-l_1) \neq 0 (\text{mod } p)$ as $0 \le k_2, k_1, l_3, l_1 < p$, $k_1 \neq k_2$ and $l_3 \neq l_1$, then $r_{C_2^3,3} \neq r_{C_1^2,3}$. Similarly, $r_{C_1^3,3} \neq r_{C_2^2,3}$. If $r_{C_1^3,3} \neq r_{C_2^3,3}$, then two other columns, C_1^4 and C_2^4 need to be selected, such that $r_{C_1^4,3} = r_{C_1^3,3}$, $r_{C_2^4,3} = r_{C_2^3,3}$. If $r_{C_1^3,3} = r_{C_2^3,3}$, then two other columns C_1^4 and C_2^4 need to be selected, such that $r_{C_1^4,2} = r_{C_1^3,2}$, $r_{C_2^4,2} = r_{C_2^3,2}$. Therefore, we need to select at least 6 other columns $\{C_i^j \mid 1 \le i \le 2, 2 \le j \le 4\}$, such that C_1^1, C_2^1 and these columns satisfy above constraints. In the case of C_3^1, C_4^1 (and C_5^1, C_6^1), we can draw the same conclusions. Since $i_1 \neq i_2 \neq i_3$, the other 18 columns $\{C_i^j \mid 1 \le i \le 6, 2 \le j \le 4\}$, are distinct. Thus, if column set $\boldsymbol{\Phi}$ satisfies the following constraint:

$$\sum_{C \in \boldsymbol{\Phi}} r_{C,j} = 0 (\text{mod } 2), \quad 1 \le j \le 3, \tag{10}$$

then $|\boldsymbol{\Phi}| \ge 24$. Therefore, the minimal linearly dependent set of parity check matrix $\boldsymbol{H}$ has at least 24 elements. This conclusion can be readily extended to other LDPC codes with this construction method. Consequently, the minimum Hamming distance of the new LDPC codes is no less than 24. □

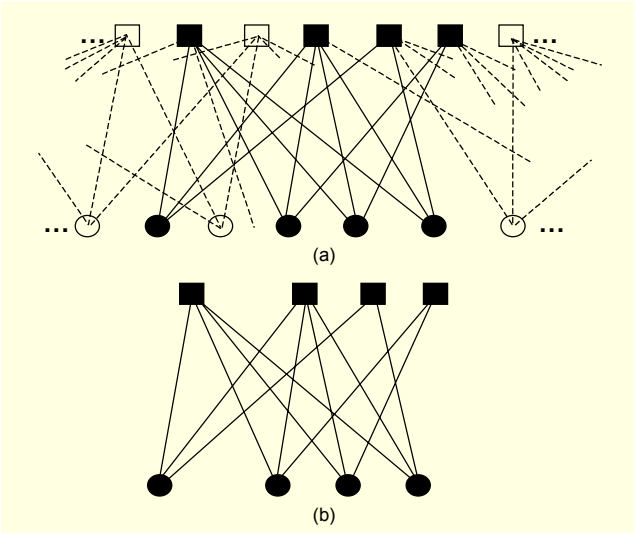


Fig. 4. (a) Tanner graph of parity check matrix H and (b) Tanner graph after removing all inactive elements. Active (inactive) bits, checks, and edges are denoted by solid (open) circles, squares, and lines, respectively.

The Tanner graph of parity check matrix $\boldsymbol{H}$ is depicted in Fig. 4(a), where check nodes are represented by squares and bit nodes by circles. We say that a bit node v_i is active for a codeword $\boldsymbol{c} = (c_0, c_1, \cdots, c_{n-1})$ if $c_i = 1$; an edge is active if it connects to an active bit node; a check node is active if it is connected to at least one active bit node. In Fig. 4, active bits, edges, and checks are indicated by solid circles, lines, and squares, respectively. Removing all inactive elements, as in Fig. 4(b), we obtain a new bipartite graph with check node set $\boldsymbol{V}_c$ and bit node set $\boldsymbol{V}_b$. As a bipartite graph, there exists the following relationship between the sum of the degrees of the check nodes in $\boldsymbol{V}_c$ and the sum of the degrees of the bit nodes in $\boldsymbol{V}_b$:

$$\sum_{v \in \boldsymbol{V}_c} d(v) = \sum_{u \in \boldsymbol{V}_b} d(u). \tag{11}$$

Since any LDPC codeword satisfies all check equations of its parity check matrix, then

$$\sum_{v \in \boldsymbol{V}_c} d(v) = 0 (\text{mod } 2). \tag{12}$$

If $d(u) \equiv 1 (\text{mod } 2)$ for $u \in \boldsymbol{V}_b$, then $|\boldsymbol{V}_b|$ is even and the codeword weight is even. In [19], the same results are also presented using the state transition diagram. For the (3, ρ)-regular QC-LDPC codes, since $d(v_i)=3$, for $0 \le i < n$, the new codes also have even Hamming weight.

IV. Error Performance of Selected LDPC Codes

In this section, we present several new QC-LDPC codes, constructed as described in section II, and their error performance with iterative decoding using the sum-product algorithm (SPA). The SPA decoder is implemented in the log domain, and the extrinsic information (log likelihood) is clipped to 10 in magnitude. It stops when either a valid codeword is found or the maximum number of decoding iterations is reached. For performance computation, we assume BPSK transmission over an AWGN channel with SNR E_b/N_0.

Figure 5 shows the bit error performance of three new (3, 6)-regular QC-LDPC codes, whose specific design parameters are shown in Table 1. At a bit error rate (BER) of 10^{-5}, the (4356, 2205) code performs only 1.48 dB from the Shannon limit, which is quite good considering that the code length is only 4356. In the case of (7956, 4009) code, it performs 1.34 dB from the Shannon limit. Moreover, both of them have no error floor down to the BER of 10^{-7}. For comparison, the error performance of a (3, 6)-regular (4906, 2453) code [15]

Table 1. Design parameters of the new regular QC-LDPC codes.

(λ, ρ)	(3, 6)			(3, 5)			(3, 4)		
Block length	4356	7956	19836	875	2200	11500	784	1936	5776
(p, r, q)	(11, 11, 6)	(17, 13, 6)	(29, 19, 6)	(7, 5, 5)	(11, 8, 5)	(23, 20, 5)	(7, 7, 4)	(11, 11, 4)	(19, 19, 4)
Vertex number	4356	7956	19836	875	2200	11500	784	1936	5776
Path number	2178	3978	9918	525	1320	6900	588	1452	4332
Design rate	0.5			0.4			0.25		
Actual rate	0.506	0.504	0.502	0.416	0.409	0.404	0.272	0.263	0.257
Girth	12								

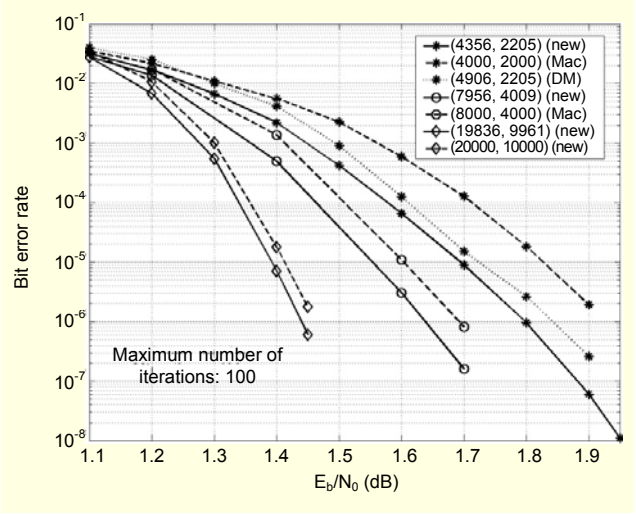


Fig. 5. Performance of the (3, 6)-regular LDPC codes.

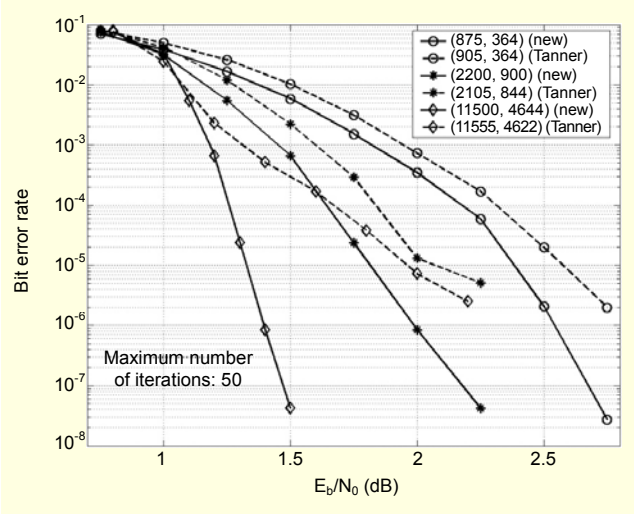


Fig. 6. Performance of the (3, 5)-regular LDPC codes.

(girth 12) and three MacKay's codes [20] (4000, 2000), (8000, 4000), and (20000, 10000) (column weight 3 and girth 6) are also included in this figure. It can be seen that the new codes outperform MacKay's codes. Both the (4906, 2453) code, constructed with the dilation matrices (DM), and the new (4356, 2205) code have a girth of 12. However, the new code slightly outperforms its counterpart. At a BER of 10^{-5}, the new (4356, 2205) code has an extra coding gain of about 0.1 dB with respect to MacKay's code (4000, 2000). As the block length increases, the improvement obtained is reduced. The advantage of the new QC-LDPC code, however, is its simple encoding which can be implemented with a simple shift register adder accumulator. Hence, the encoder complexity is linearly proportional to the number of parity check bits of the code. Moreover, the structure of the QC-LDPC code also reduces the decoder storage and hardware complexity. In the case of the new (7956, 4009) code, the memory required to store its parity check matrix can be reduced by a factor 7/306.

Figure 6 shows the bit error performance of three new (3, 5)-regular QC-LDPC codes, whose specific design parameters are also given in Table 1. It should be noted that the girth of the new (3, 5)-regular LDPC code with a length of 875 can be up to its upper bound of 12. For comparison, the performance of three (3, 5)-regular QC block LDPC codes [9] with similar block lengths and rates, constructed by Tanner and others, are also given in Fig. 6. Both the (3, 5)-regular QC block LDPC codes and the new LDPC codes have a girth of 12 and a minimum Hamming distance of 24. However, the new codes significantly outperform the QC block LDPC codes. For instance, the new codes (875, 364), (2200, 900), and (11500, 4644) achieve about 0.2, 0.25, and 0.65 dB coding gains at a BER of 10^{-5}, respectively, with respect to the QC block LDPC codes (905, 364), (2105, 844), and (11555, 4622). Moreover, we do not see any evidence of the error floor problems observed in the QC block LDPC codes. A possible reason is that the new codes have a better weight distribution of codewords than the QC block LDPC codes.

Figure 7 shows the bit error performance of three new (3, 4)-regular QC-LDPC codes, whose specific design parameters are given in Table 1. For comparison, the performance of three randomly generated (3, 4)-regular LDPC codes of the same

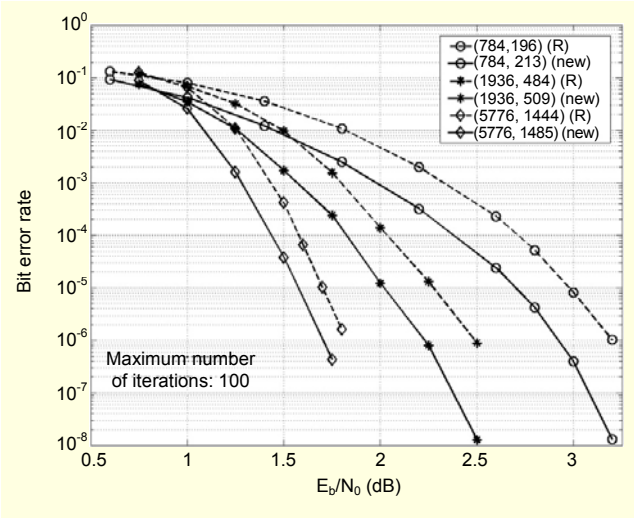


Fig. 7. Performance of the (3, 4)-regular LDPC codes.

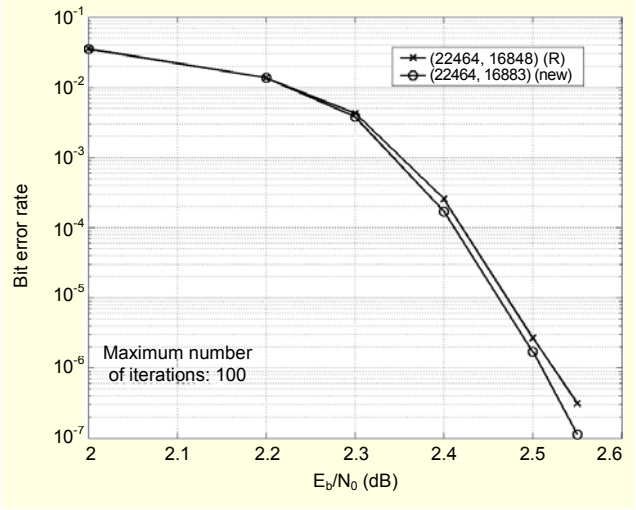


Fig. 8. Performance of the (3, 12)-regular LDPC codes.

block lengths and a girth of 6 are also given in Fig. 7. Again, the new codes outperform their random counterparts.

Let p=13, q=r=12, a new (3, 12)-regular (22464, 16883) QC-LDPC code with a girth of 12 and a rate of 0.7516 can be obtained. The error performance of this code and a random (22464, 16848) code with a girth of 6 and a rate of 0.75 are shown in Fig. 8. In the low SNR region, the new code achieves a performance similar to that of the random code. However, the new code outperforms the latter with increasing SNR.

Figure 9 shows the BER performance of two new (2904, 995) QC-LDPC codes with a girth of 12 and a rate of 0.3426. The parity check matrices of these two new codes have a constant column weight of 3 and a row weight of 4 (1452 rows) and a row weight of 6 (484 rows). Both of them have p=11, r_1=r_2=11, q_1=q_2=4, and q_3=6. The assistant matrix of the new-1 code is masked by a randomly selecting matrix $\boldsymbol{W}_m$, as a

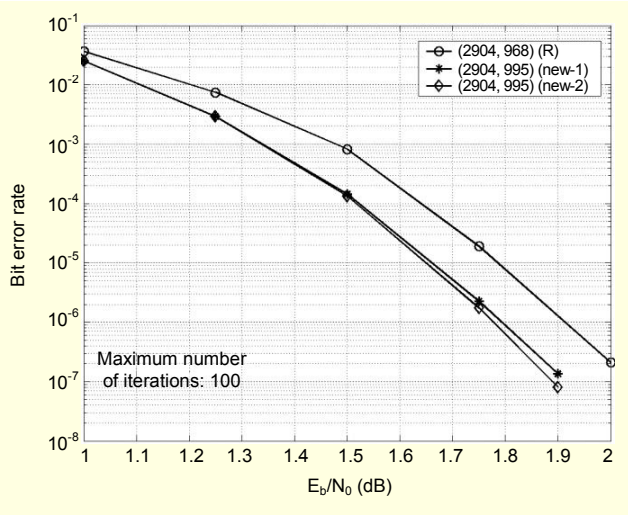


Fig. 9. Performance of the new (2904, 995) LDPC codes.

result, there are 275 p-cycles with a length of 6 in each subgraph $\boldsymbol{G}_s^k (0 \le k < q_3)$. By comparison, the assistant matrix of the new-2 code is masked by a more proper matrix $\boldsymbol{W}_m$. Then, there are only 33 p-cycles with a length of 6 in each subgraph. Hence, there are fewer cycles with a length of 12 in the Tanner graph defined by the parity check matrix of the new-2 code than that of the new-1 code. It can be seen that the new-2 code outperforms the new-1 code in the high SNR region. For comparison, the performance of a randomly generated (2904, 968) LDPC code with a girth of 6 is also given in Fig. 9. At a BER of 10^{-5}, the new-2 code outperforms the random LDPC code by 0.1 dB.

V. Conclusion

A graph-theoretic method for constructing LDPC codes was proposed in this paper, in which a connection graph with three kinds of special paths was designed to guarantee that the Tanner graph of the parity check matrix mapped from the connection graph is without short cycles. The construction method is capable of generating a class of QC-LDPC codes with a girth of 12 and a minimum Hamming distance of no less than 24. The simulation results show that the proposed LDPC codes outperformed random codes and the QC block LDPC code with similar block lengths and rates.

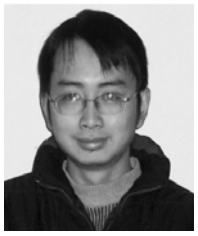
References

[1] R.G. Gallager, *Low Density Parity Check Codes*, Cambridge, MA: MIT Press, 1963.

[2] R.M. Tanner, "A Recursive Approach to Low Complexity Codes," *IEEE Trans. on Inf. Theory,* vol. 27, Sep. 1981, pp. 533-

547.
[3] Y.J. Ko and J.H. Kim, "Girth Conditioning for Construction of Short Block Length Irregular LDPC Codes," *Electron. Letter,* vol. 40, Feb. 2004, pp. 187-188.
[4] Y.Y. Mao and A.H. Banihashemi, " A Heuristic Search for Good Low-Density Parity-Check Codes at Short Block Lengths," *Proc. IEEE Int. Conf. Communications*, 2001, pp. 11-14.
[5] Y. Kou, S. Lin, and M. Fossorier, "Low-Density Parity-Check Codes Based on Finite Geometries: A Rediscovery and New Results," *IEEE Trans. on Inf. Theory*, vol. 47, Feb. 2001, pp. 619-637.
[6] M.P.C. Fossorier, "Quasi-Cyclic Low-Density Parity-Check Codes from Circulant Permutation Matrices," *IEEE Trans. on Inf. Theory*, vol. 50, Aug. 2004, pp. 1788-1793.
[7] O. Milenkovic, N. Kashyap, and D. Leyba, "Shortened Array Codes of Large Girth," *IEEE Trans. on Inf. Theory*, vol. 52, Aug. 2006, pp. 3707-3722.
[8] J. Xu, L. Chen, L.Q. Zeng, L. Lan, and S. Lin, "Construction of Low-Density Parity-Check Codes by Superposition," *IEEE Trans. on Comm*., vol. 53, Feb. 2005, pp. 243-251.
[9] R.M. Tanner, D. Sridhara, A. Sridharan, T.E. Fuja, and D.J. Costello, "LDPC Block and Convolutional Codes Based on Circulant Matrices," *IEEE Trans. on Inf. Theory*, vol. 50, Dec. 2004, pp. 2966-2984.
[10] J.L. Fan, "Array Codes as Low-Density Parity Check Codes," *Proc. 2nd Int. Symp. Turbo Codes*, Brest, France, Sep. 2000, pp. 545-546.
[11] L. Chen, I. Djurdjevic, J. Xu, S. Lin, and K. Abdel-Ghaffar, "Construction of Quasi-Cyclic LDPC Codes Based on the Minimum Weight Codewords of Reed-Solomon Codes," *Proc. ISIT*, June 2004, Chicago, USA, p. 239.
[12] V. Kumar, O. Milenkovic, and B. Vasic, "Structured LDPC Codes over GF (2) and Companion Matrix Based Decoding," *Proc. ISIT*, June 2004, Chicago, USA, p. 273.
[13] K.S. Kim, S.H. Lee, Y.H. Kim, and J.Y. Ahn, "Design of Binary LDPC Code Using Cyclic Shift Matrices," *Electron. Letters,* vol. 40, Mar. 2004, pp. 325-326.
[14] J.L Kim, U.N. Peled, I. Perepelitsa, V. Pless, and S. Friedland "Explicit Construction of Families of LDPC Codes with No 4-Cycles," *IEEE Trans. on Inf. Theory*, vol. 50, Oct. 2004, pp. 2378-2388.
[15] M. Greferath, M.E. O'Sullivan, and R. Smarandache, "Construction of Good LDPC Codes using Dilation Matrices," *Proc. ISIT*, June 2004, Chicago, USA, p. 235.
[16] T. Richardson and R. Urbanke, "Capacity of Low-Density Parity-Check Codes under Message Passing Decoding," *IEEE Trans. on Inf. Theory*, vol. 47, Feb. 2001, pp. 599-618.
[17] Z.W. Li, L. Chen, L.Q. Zeng, S. Lin, and W.H. Fong, "Efficient Encoding of Quasi-Cyclic Low-Density Parity-Check Codes," *IEEE Trans. on Comm*., vol. 54, Jan. 2006, pp. 71-81.
[18] H. Fujita and K. Sakaniwa, "Some Classes of Quasi-Cyclic LDPC Codes: Properties and Efficient Encoding Method," *IEICE Trans. Fundamentals*, vol. E88-A, Dec. 2005, pp. 3627-3635.
[19] L. Wei, "Several Properties of Short LDPC Codes," *IEEE Trans. on Comm*., vol. 52, May 2004, pp. 721-727.
[20] D.J.C. MacKay, Encyclopedia of Sparse Graph Codes. http://www.inference.phy.cam.ac.uk/mackay/codes/data.html.

Long-Jiang Jing received the MS degree in computer science and technology from Southwest Petroleum University, Nanchong, China, in 2002. Currently, he is pursuing the PhD degree in signal processing at University of Electronic Science and Technology of China (UESTC), Chengdu, China. His research interests are channel coding, modulation, and communication systems.



Jing-Li Lin received the BS degree from Sichuan Institue of Techology, Chengdu, Sichuan, China, in 1999, and the MS degree from UESTC, Chengdu, Sichuan, China, in 2003, both in electrical engineering. He is currently working toward the PhD degree in signal processing at UESTC. His research interests are channel coding, modulation, and communication systems.

Wei-Le Zhu graduated from the Chengdu Institute of Radio Engineering in 1961. From 1980 to 1982, he was a visiting research professor with the University of Illinois at Urbana-Champaign and Purdue University. Now he is a full professor of E.E. UESTC and the director of the Image Transmission and Processing Research Group. His research interests are digital communication systems, digital video, and HDTV systems.