Explicit Constructions for Type-1 QC-LDPC Codes With Girth 12

Guohua Zhang and Rudolf Mathar, *Senior Member, IEEE*

***Abstract*— Given any $J \times J$ ($J > 3$) square matrix over $\mathbf{Z}_P$ such that the differences of any two row vectors contain each element in $\mathbf{Z}_P$ at most once, a class of (3, L)-regular quasi-cyclic low-density parity-check codes is explicitly constructed with lengths PJL^2 and girth 12, where L is any integer satisfying $3 < L \leq J$. Simulation results show that the new codes perform very well for moderate rates and lengths.**

***Index Terms*— Low-density parity-check (LDPC) codes, quasi-cyclic (QC), circulant permutation matrix (CPM), girth.**

I. Introduction

A low-density parity-check (LDPC) code is defined as the null space of its sparse parity-check matrix (PCM). A *classical* QC-LDPC code [1] is associated with a PCM consisting of circulant permutation matrices (CPMs) of the same size P, while a *type-1* QC-LDPC code is associated with a PCM composed of both CPMs and zero matrices (ZMs) of the same size P. Compared with classical QC-LDPC codes, their type-1 counterparts usually enable a larger upper bound in terms of minimum distance [2], which in turn hopefully leads to a better decoding performance.

If a PCM has R 1's in each column and L 1's in each row, then the associated LDPC code is called (R, L)-regular. Girth is the length of the shortest cycles in the Tanner graph corresponding to a PCM. To the best of our knowledge, Tanner's method [3] and Jing's one [4] are the only existing ways to explicitly construct $(3, L)$-regular structured QC-LDPC codes with girth 12. However, Tanner's method only works for classical codes with $L = 5$ and a prime P, while Jing's one only for type-1 codes with a prime P. In this Letter, we present a novel method to construct type-1 $(3, L)$-regular QC-LDPC codes with girth exactly 12 for any P, which naturally includes Jing's method as a special case.

Our method is based on a type of $J \times J$ matrix over $\mathbf{Z}_P$ in which the differences of any two rows do not contain repetitive elements. Obviously, such matrices can be directly used to construct (J, J)-regular QC-LDPC codes free of 4-cycles (if the fact that the rate is most often zero is not considered). From such matrices, column-weight-*two* LDPC codes with girth 12 can be constructed by the approach in [5], while our method enables column-weight-*three* type-1 QC-LDPC codes with girth 12.

Manuscript received October 29, 2016; revised November 20, 2016; accepted November 22, 2016. Date of publication December 1, 2016; date of current version March 8, 2017. This work was supported by the China Scholarship Council (CSC) and the National Natural Science Foundation of China under Grant 61471294. The associate editor coordinating the review of this letter and approving it for publication was Z. Ma.

G. Zhang is with the Institute for Theoretical Information Technology, RWTH Aachen University, 52074 Aachen, Germany, and also with the China Academy of Space Technology (Xi'an), Xi'an 710100, China (e-mail: zhangghcast@163.com).

R. Mathar is with the Institute for Theoretical Information Technology, RWTH Aachen University, 52074 Aachen, Germany (e-mail: mathar@ti.rwth-aachen.de).

Digital Object Identifier 10.1109/LCOMM.2016.2634022

II. Construction

The $MP \times NP$ PCM $\mathbf{H}$ for a classical or type-1 QC-LDPC code with length NP can be determined by its corresponding $M \times N$ exponent matrix $\mathbf{E}$ and the CPM size P [6]. Precisely, when $\mathbf{H}$ is generated from $\mathbf{E}$, the element ∞ within $\mathbf{E}$ corresponds to a $P \times P$ ZM and any other element (say e) corresponds to a $P \times P$ identity matrix with rows cyclically shifted to the right by e $(mod\ P)$ positions. Denote by $g(\mathbf{E}, P)$ the girth of the Tanner graph associated with an exponent matrix $\mathbf{E}$ and the CPM/ZM size P.

A. A Class of Exponent Matrices

In this Letter, we investigate a special type of exponent matrices $\mathbf{E}$ which can be viewed as an array of matrices as follows:

$$\mathbf{E} = \left[\begin{array}{cccc} \mathbf{S} & \infty_0 & \cdots & \infty_0 \\ \infty_0 & \mathbf{S} & \cdots & \infty_0 \\ \vdots & \vdots & \ddots & \vdots \\ \infty_0 & \infty_0 & \cdots & \mathbf{S} \\ \hline \mathbf{W} & \infty_0 & \cdots & \infty_0 \\ \infty_0 & \mathbf{W} & \cdots & \infty_0 \\ \vdots & \vdots & \ddots & \vdots \\ \infty_0 & \infty_0 & \cdots & \mathbf{W} \\ \hline \mathbf{C}_0 & \mathbf{C}_1 & \cdots & \mathbf{C}_{J-1} \end{array}\right], \tag{1}$$

where $\mathbf{S}$, $\mathbf{W}$ and ∞_0 are all $J \times J^2$ matrices, and $\mathbf{C}_u$ $(0 \leq u \leq J-1)$ is a $J^2 \times J^2$ matrix. Therefore, $\mathbf{E}$ is a $3J^2 \times J^3$ matrix. To be specific, (i) $\mathbf{S}$ is a $J \times J$ array defined by

$$\mathbf{S} = \begin{bmatrix} \mathbf{S}_0 & \infty_1 & \cdots & \infty_1 \\ \infty_1 & \mathbf{S}_1 & \cdots & \infty_1 \\ \vdots & \vdots & \ddots & \vdots \\ \infty_1 & \infty_1 & \cdots & \mathbf{S}_{J-1} \end{bmatrix}, \tag{2}$$

where ∞_1 is a $1 \times J$ matrix of ∞'s, and $\mathbf{S}_j$ is a $1 \times J$ matrix denoted by $[s_{j,0}\ s_{j,1}\ \cdots\ s_{j,J-1}]$, for $0 \leq j \leq J-1$; (ii) $\mathbf{W}$ is a $1 \times J$ array of $\mathbf{W}_0$'s, i.e. $\mathbf{W} = [\mathbf{W}_0, \mathbf{W}_0, \cdots, \mathbf{W}_0]$, where $\mathbf{W}_0$ is a $J \times J$ matrix with 0's on the main diagonal and ∞'s otherwise; (iii) ∞_0 is a $J \times J^2$ matrix composed of ∞'s; (iv) $\mathbf{C}_u$ $(0 \leq u \leq J-1)$ is a $J \times J$ array defined by

$$\begin{bmatrix} D(T^0(\mathbf{S}_u)) & \infty_2 & \cdots & \infty_2 \\ \infty_2 & D(T^1(\mathbf{S}_u)) & \cdots & \infty_2 \\ \vdots & \vdots & \ddots & \vdots \\ \infty_2 & \infty_2 & \cdots & D(T^{J-1}(\mathbf{S}_u)) \end{bmatrix}. \tag{3}$$

For any vector $\mathbf{x} = [x_0, x_1, \cdots, x_{J-1}]$, $T^k(\mathbf{x})$ denotes $\mathbf{x}$ with elements cyclically shifted to the *left* by k $(mod\ J)$ positions,

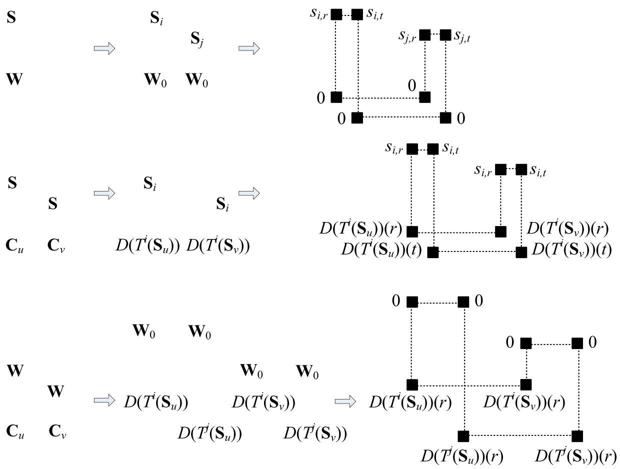

Fig. 1. All types of possible 8-cycles.

and

$$D(\mathbf{x}) \triangleq \begin{bmatrix} x_0 & \infty & \cdots & \infty \\ \infty & x_1 & \cdots & \infty \\ \vdots & \vdots & \ddots & \vdots \\ \infty & \infty & \cdots & x_{J-1} \end{bmatrix}. \quad (4)$$

Denote the r-th element in the diagonal of $D(\mathbf{x})$ by $D(\mathbf{x})(r)$, $0 \le r \le J-1$. Finally, ∞_2 is $J \times J$ matrix composed of ∞'s.

From the above construction, it is obvious that $\mathbf{E}$ can be uniquely determined on the basis of the following matrix:

$$\mathbf{B} \triangleq \begin{bmatrix} \mathbf{S}_0 \\ \mathbf{S}_1 \\ \vdots \\ \mathbf{S}_{J-1} \end{bmatrix} = \begin{bmatrix} s_{0,0} & s_{0,1} & \cdots & s_{0,J-1} \\ s_{1,0} & s_{1,1} & \cdots & s_{1,J-1} \\ \vdots & \vdots & \ddots & \vdots \\ s_{J-1,0} & s_{J-1,1} & \cdots & s_{J-1,J-1} \end{bmatrix}. \quad (5)$$

Let $\oplus$ and $\otimes$ denote modulo-J addition and modulo-J multiplication, respectively. From the above definitions, it is easily seen that $D(T^k(\mathbf{S}_u))(r) = s_{u,r\oplus k}$, $0 \le u, r, k \le J-1$.

Remark 1: The profile of $\mathbf{E}$ (Equ. (1)) is motivated by Jing's work ([4], Fig. 3); however, our method for the core matrices, $\mathbf{S}$ and $\mathbf{C}_u$ $(0 \le u \le J-1)$, is completely new. As will be seen later, one of the advantages of new method over Jing's one is that, the former allows any P, but the latter requires a prime P.

B. Girth Property

Theorem 1: If $g(\mathbf{B}, P) \ge 6$, then $g(\mathbf{E}, P) = 12$.

Proof: (1) Obviously, independent of $\mathbf{B}$, 4-cycles and 6-cycles are impossible due to the special structure (Equ.1) of $\mathbf{E}$. (2) For possible 8-cycles, there are only three patterns as shown in Fig.1. (2a): For the 8-cycle in Fig.1 (upper, $i < j; r < t$), we have $(s_{i,r} - 0) + (0 - s_{j,r}) + (s_{j,t} - 0) + (0 - s_{i,t}) = 0 \ (mod \ P)$, that is, $(s_{i,r} - s_{j,r}) + (s_{j,t} - s_{i,t}) = 0 \ (mod \ P)$. This equation suggests a 4-cycle in the Tanner graph associated to $\mathbf{B}$, which contradicts $g(\mathbf{B}, P) \ge 6$. (2b): The 8-cycle in Fig.1 (middle, $r < t; u < v$) can be expressed by $(s_{i,r} - s_{u,r\oplus i}) + (s_{v,r\oplus i} - s_{i,r}) + (s_{i,t} - s_{v,t\oplus i}) + (s_{u,t\oplus i} - s_{i,t}) = 0 \ (mod \ P)$, equivalent to $(s_{v,r\oplus i} - s_{u,r\oplus i}) + (s_{u,t\oplus i} - s_{v,t\oplus i}) = 0 \ (mod \ P)$. This equation implies a 4-cycle in the Tanner graph associated to $\mathbf{B}$, which is impossible as $g(\mathbf{B}, P) \ge 6$. (2c): The 8-cycle in Fig.1 (lower, $i < j; u < v$) can be denoted by $(0 - s_{u,r\oplus i}) + (s_{v,r\oplus i} - 0) + (0 - s_{v,r\oplus j}) + (s_{u,r\oplus j} - 0) = 0 \ (mod \ P)$. This equation is equivalent to $(s_{v,r\oplus i} - s_{u,r\oplus i}) + (s_{u,r\oplus j} - s_{v,r\oplus j}) = 0 \ (mod \ P)$, which suggests a 4-cycle in the Tanner graph associated to $\mathbf{B}$, in contradiction with $g(\mathbf{B}, P) \ge 6$. (3) For 10-cycles, there are only two possibilities as shown in Fig.2 ($i < j$; $r < t$; $u < v$); however, both cases fail to enable a closed path, which is irrelevant to $\mathbf{B}$. (4) Independent of $\mathbf{B}$, there are inevitable 12-cycles as shown in Fig.3 ($i \ne j$; $r < t$).

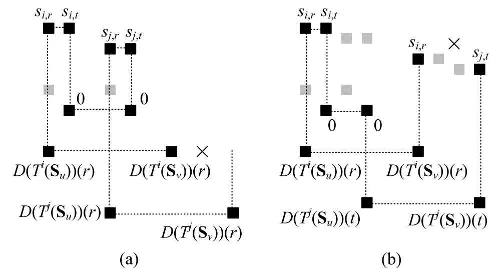

Fig. 2. Two types of possible 10-cycles.

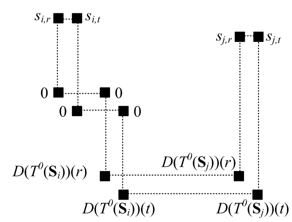

Fig. 3. A pattern of inevitable 12-cycles.

III. Some Options for Matrix B

Lemma 1: Let $d_m = max\{d_{i,j}, 0 \le i, j \le J-1, i \ne j\}$, where $d_{i,j} = max\{s_{i,k} - s_{j,k}, 0 \le k \le J-1\} + max\{s_{j,k'} - s_{i,k'}, 0 \le k' \le J-1\}$. If $g(\mathbf{B}, Q) \ge 6$ for some fixed integer Q (Q may be ∞), then $g(\mathbf{B}, P) \ge 6$ for any $P \ge d_m + 1$.

Proof: We give a proof by contradiction. Suppose there exists a cycle of length 4 within i-th and j-th rows, and r-th and t-th columns of $\mathbf{B}$ ($0 \le i \ne j \le J-1, 0 \le r \ne t \le J-1$) for a certain CPM size $P \ge d_m + 1$. Then, this cycle can be expressed as $(s_{i,r} - s_{j,r}) + (s_{j,t} - s_{i,t}) = 0 \ (mod \ P)$. As $-d_{i,j} \le (s_{i,r} - s_{j,r}) + (s_{j,t} - s_{i,t}) \le d_{i,j}$, and $(s_{i,r} - s_{j,r}) + (s_{j,t} - s_{i,t}) \ne 0$ (otherwise there exists a 4-cycle for the CPM size Q), we have $(s_{i,r} - s_{j,r}) + (s_{j,t} - s_{i,t}) \ne 0 \ (mod \ P)$ for any $P \ge d_{i,j} + 1$. Therefore, $P \ge d_m + 1$ is sufficient for avoiding all cycles within $\mathbf{B}$.

A. Method 1: Array Construction

Let J be an odd prime integer. The $J \times J$ matrix $\mathbf{B}_{arr}$ is defined by $\mathbf{B}_{arr}(i, r) = i \otimes r$ for $0 \le i, r \le J-1$.

Theorem 2: For $P = J$, $g(\mathbf{B}_{arr}, P) = 6$ [7]; and, for any $P \ge 2J-3$, $g(\mathbf{B}_{arr}, P) \ge 6$.

Proof: It is readily seen that $d_m = d_{1,J-1} = [(J-1) - 1] + [(J-1) - 1] = 2J-4$. As $g(\mathbf{B}_{arr}, P = J) = 6$ and $d_m = 2J-4$, the proof is completed due to Lemma 1.

B. Method 2: Cyclic Construction

Let J be an arbitrary integer larger than 2. The $J \times J$ matrix $\mathbf{B}_{cyc}$ is defined by $\mathbf{B}_{cyc}(i,r) = a_{r-i(mod\ J)}$ for $0 \le i, r \le J-1$, where $a_k = k(k-1)/2$ for $0 \le k \le J-1$.

Lemma 2: For any $1 \le k \le J-2$, if $0 \le i < j \le J-1-k$, then $a_{j+k} - a_j > a_{i+k} - a_i$.

Proof: By definition, if $j+k \le J-1$, then $a_{j+k} - a_j = [(j+k)(j+k-1) - j(j-1)]/2 = k(k-1)/2 + kj$. Therefore, $(a_{j+k} - a_j) - (a_{i+k} - a_i) = k(j-i) > 0$ for $j > i$.

Theorem 3: (1) For any $J > 2$ and $P \ge 3(J-1)^2/4$, $g(\mathbf{B}_{cyc}, P) \ge 6$; and (2) for any odd prime J, $g(\mathbf{B}_{cyc}, P) \ge 6$ for $P = J$.

Proof: Due to Lemma 2 and the cyclic structure of $\mathbf{B}_{cyc}$, it is easily seen that there exist no 4-cycles for $P = \infty$, i.e., $g(\mathbf{B}_{cyc}, \infty) \ge 6$. Now, we consider the lower bound, d_m.

(1a) J even. $d_{0,1} = (a_{J-1} - a_{J-2}) + (a_{J-1} - a_0)$, $d_{0,2} = (a_{J-1} - a_{J-3}) + (a_{J-1} - a_1)$, $\cdots$, $d_{0,J/2-1} = (a_{J-1} - a_{J-J/2}) + (a_{J-1} - a_{J/2-2})$, $d_{0,J/2} = (a_{J-1} - a_{J/2-1}) + (a_{J-1} - a_{J/2-1})$, $d_{0,J/2+1} = (a_{J-1} - a_{J/2-2}) + (a_{J-1} - a_{J/2})$, $\cdots$, $d_{0,J-2} = (a_{J-1} - a_1) + (a_{J-1} - a_{J-3})$, $d_{0,J-1} = (a_{J-1} - a_0) + (a_{J-1} - a_{J-2})$.

Since $d_{0,1} = d_{0,J-1} < d_{0,2} = d_{0,J-2} < \cdots < d_{0,J/2-1} = d_{0,J/2+1} < d_{0,J/2}$, we have $d_m = d_{0,J/2} = 3J(J-2)/4$.

(1b) J odd. $d_{0,1} = (a_{J-1} - a_{J-2}) + (a_{J-1} - a_0)$, $d_{0,2} = (a_{J-1} - a_{J-3}) + (a_{J-1} - a_1)$, $\cdots$, $d_{0,(J-1)/2} = (a_{J-1} - a_{(J-1)/2}) + (a_{J-1} - a_{(J-3)/2})$, $d_{0,(J+1)/2} = (a_{J-1} - a_{(J-3)/2}) + (a_{J-1} - a_{(J-1)/2})$, $\cdots$, $d_{0,J-2} = (a_{J-1} - a_1) + (a_{J-1} - a_{J-3})$, $d_{0,J-1} = (a_{J-1} - a_0) + (a_{J-1} - a_{J-2})$.

Since $d_{0,1} = d_{0,J-1} < d_{0,2} = d_{0,J-2} < \cdots < d_{0,(J-1)/2} = d_{0,(J+1)/2}$, we have $d_m = d_{0,(J-1)/2} = [3J(J-2) - 1]/4$.

(2) J prime ($P = J$): For $0 \le i, r \le J-1$, $\mathbf{B}_{cyc}(i,r) = (xJ - i + r)(xJ - i + r + 1)/2$, where $x \in \{0, 1\}$. Suppose i_1 and i_2 are two distinct row indexes ($0 \le i_1, i_2 \le J-1$), and j_1 and j_2 are two distinct column indexes ($0 \le r_1, r_2 \le J-1$). If there exists a cycle of length 4 in the two rows and two columns, then this cycle can be expressed as $(x_1 J - i_1 + r_1)(x_1 J - i_1 + r_1 - 1)/2 - (x_2 J - i_2 + r_1)(x_2 J - i_2 + r_1 - 1)/2 + (x_3 J - i_2 + r_2)(x_3 J - i_2 + r_2 - 1)/2 - (x_4 J - i_1 + r_2)(x_4 J - i_1 + r_2 - 1)/2 = 0\ (mod\ J)$, where x_1, x_2, x_3 and $x_4 \in \{0, 1\}$. Arranging terms, we have $(i_1 - i_2)(r_2 - r_1) = 0\ (mod\ J)$, which is impossible as $0 < |i_1 - i_2| \le J-1$, $0 < |r_2 - r_1| \le J-1$ and J is prime.

Remark 2: From the above analysis, it is obvious that $\mathbf{B}_{arr}$ and $\mathbf{B}_{cyc}$ are more general than original array construction (P prime) [7], in terms of J and P.

Remark 3: If J is an odd prime integer and $\mathbf{B} = \mathbf{B}_{arr}$, then $s_{i,r} = i \otimes r$ and $s_{u,r\oplus k} = u \otimes (r \oplus k)$. Therefore, in this case, the proposed construction is reduced to Jing's method [4]. However, Jing's method only works for a prime J, while our new method is applicable for any J, if a $J \times J$ matrix $\mathbf{B}$ exists such that $g(\mathbf{B}, P) \ge 6$ for some integer P.

IV. Codes With Length of PJL^2

The QC-LDPC codes directly obtained from $\mathbf{E}$ only possess a length of the form J^3P. To enable a flexible length while still maintain the regularity of row/column weight, we present a simple procedure applied to $\mathbf{E}$.

Algorithm 1 A List of Columns to be Deleted

$DS = \emptyset, num = 0$
$for\ j = 1\ to\ J$
  $for\ k = 1\ to\ J$
    $num = num + 1$
    $if\ \mathbf{M}(j,k) = 0$
      $DS = DS \cup num$
    end
  end
end
$DS_2 = \emptyset$
$for\ i = 0\ to\ L-1$
  $DS_2 = DS_2 \cup \{DS + J^2 i\}$
end
$DS_2 = DS_2 \cup \{1 + J^2L, 2 + J^2L, \cdots, J^3\}$

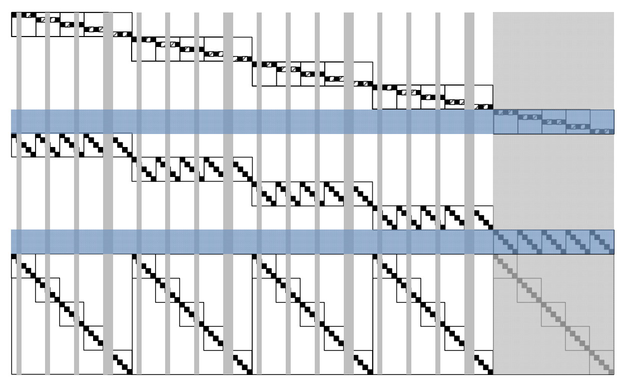

Fig. 4. Target matrix $\mathbf{E}'$ obtained by deleting the columns indexed by DS_2 and the resultant rows only including ∞'s (the grey bars are the deleted columns/rows). $\mathbf{M}(1,2) = \mathbf{M}(2,3) = \mathbf{M}(3,4) = \mathbf{M}(4,5) = \mathbf{M}(5,1) = 0$.

(Step 1): Let $\mathbf{M}$ be an arbitrary $J \times J$ matrix composed of 1's and 0's, where each row/column has L elements of 1's, $3 < L \le J$. (Step 2): Given $\mathbf{E}$ and $\mathbf{M}$, the following Algorithm 1 can be employed to obtain a list of columns to be deleted.

(Step 3): Delete all the columns (from 1 to J^3) indexed by DS_2 from $\mathbf{E}$. Denote the resultant matrix by $\mathbf{E}_1$. Then, delete each row which only includes $\infty's$. The resulting matrix is our target matrix, $\mathbf{E}'$.

From the algorithm and the illustration above (Fig.4), it is readily observed that (i) the regular (constant) row weight of the first part of $\mathbf{E}$' is ensured by the constant row weight of mask matrix $\mathbf{M}$; (ii) the constant row weight of the second part of $\mathbf{E}$' is ensured by the constant column weight of $\mathbf{M}$; and (iii) the constant row weight of the last part of $\mathbf{E}$' is guaranteed by the same deletion manner for the first L column blocks and the complete deletion of the last $J-L$ column blocks.

Therefore, the derived exponent matrix $\mathbf{E}'$ corresponds to a $(3, L)$-regular code with length PJL^2 and girth at least twelve. It should be pointed out that, the number of information bits for the proposed QC-LDPC code from $\mathbf{E}'$ is slightly larger than $PJL(L-3)$, due to some dependent rows of PCM.

V. Simulations

In this section, several examples are given to demonstrate the decoding performance of the new proposed

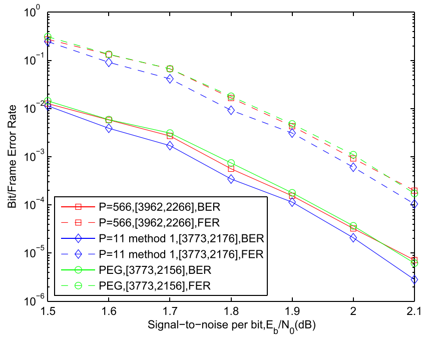

Fig. 5. Performance comparison of type-1 code ($P = 11$) from method 1, the classical code ($P = 566$) in [8] and the random PEG code [9].

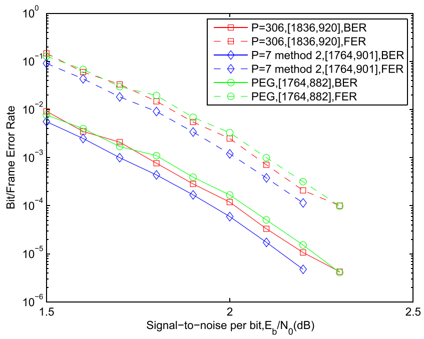

Fig. 6. Performance comparison of type-1 code ($P = 7$) from method 2 combined with mask matrix, the classical code ($P = 306$) from [8] and the random PEG code [9].

girth-12 type-1 QC-LDPC codes. For comparison purpose the state-of-the-art (the largest girth and the smallest length) classical QC-LDPC codes are chosen as long as they are available. The sum-product algorithm (SPA) decoding (with 50 iteration) of BPSK modulated signals over AWGN channel are assumed.

Example 1: On the basis of $\mathbf{B}_{arr}$ with $J = 7$ and $P = 11$, a $(3,7)$-regular type-1 QC-LDPC code is generated with girth 12. For comparison, the $(3,7)$-regular girth-12 classical QC-LDPC code with $P = 566$ in [8] is selected, and a random PEG-LDPC code [9] with column weight of three is generated.

Example 2: An exponent $\mathbf{E}$ is obtained from $\mathbf{B}_{cyc}$ with $J = 7$ and $P = 7$; by using a 7×7 mask matrix $\mathbf{M}$ with 0's in diagonal and 1's otherwise, $\mathbf{E}$' is obtained, which corresponds to a (3,6)-regular type-1 code with girth 12 and length 1764. The girth-12 classical code with $P = 306$ in [8] and a random PEG-LDPC code with column weight of three are generated for comparison.

Example 3: From $\mathbf{B}_{cyc}$ with $J = 6$ and $P = 25$, a $(3,6)$-regular type-1 QC-LDPC code is obtained with girth 12 and length 5400. The $(3,6)$-regular girth-12 classical QC-LDPC code with $P = 900$ [10] and a random PEG-LDPC code with column weight of three are chosen as counterparts.

From Figs. 5-6, we observe that, while the proposed type-1 codes possess shorter lengths, they outperform some state-of-the-art (with the shortest lengths and the largest girth 12) classical QC-LDPC codes. This can be partly explained by a larger upper bound in terms of minimum distance for type-1 codes compared with that for classical

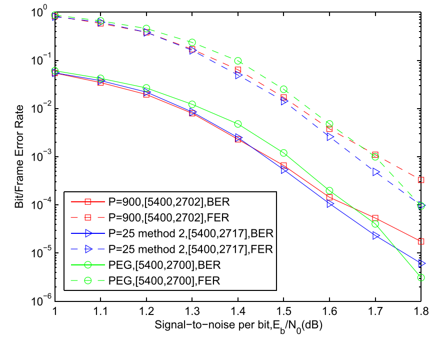

Fig. 7. Performance comparison of type-1 code ($P = 25$) from method 2, the classical code ($P = 900$) from [10] and the random PEG code [9].

codes [2]. Besides, the two type-1 codes perform slightly better than the famous PEG-LDPC codes for such lengths. From Fig. 7, we see that the type-1 code outperforms the classical QC-LDPC code with girth 12 [10] in a higher SNR region; and it has a reasonably good performance compared with its PEG counterpart, in the sense that the type-1 code is highly structured and hence enables a relatively simple decoder hardware.

VI. Conclusion

From any $J \times J$ matrix without two identical differences $(mod\ P)$ between any two rows, a novel class of $(3, L)$-regular QC-LDPC codes is proposed with girth exactly 12 and length PJL^2 for any $3 < L \leq J$. The comparison of type-1 codes from $\mathbf{B}_{arr}$ and $\mathbf{B}_{cyc}$ is a further research problem in the future.

References

[1] M. P. C. Fossorier, "Quasicyclic low-density parity-check codes from circulant permutation matrices," *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1788–1793, Aug. 2004.
[2] R. Smarandache and P. O. Vontobel, "Quasi-cyclic LDPC codes: Influence of proto- and Tanner-graph structure on minimum Hamming distance upper bounds," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 585–607, Feb. 2012.
[3] S. Kim, J.-S. No, H. Chung, and D.-J. Shin, "On the girth of Tanner (3, 5) quasi-cyclic LDPC codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1739–1744, Apr. 2006.
[4] L.-J. Jing, J.-L. Lin, and W.-L. Zhu, "Design of quasi-cyclic low-density parity check codes with large girth," *ETRI J.*, vol. 29, no. 3, pp. 381–389, Jun. 2007.
[5] X. Tao, L. Zheng, W. Liu, and D. Liu, "Recursive design of high girth $(2, k)$ LDPC codes from (k, k) LDPC codes," *IEEE Commun. Lett.*, vol. 15, no. 1, pp. 70–72, Jan. 2011.
[6] S. Myung and K. Yang, "A combining method of quasi-cyclic LDPC codes by the Chinese remainder theorem," *IEEE Commun. Lett.*, vol. 9, no. 9, pp. 823–825, Sep. 2005.
[7] K. Yang and T. Helleseth, "On the minimum distance of array codes as LDPC codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 12, pp. 3268–3271, Dec. 2003.
[8] I. E. Bocharova, R. Johannesson, F. Hug, B. D. Kudryashov, and R. V. Satyukov, "Searching for voltage graph-based LDPC tailbiting codes with large girth," *IEEE Trans. Inf. Theory*, vol. 58, no. 4, pp. 2265–2279, Apr. 2012.
[9] X.-Y. Hu, E. Eleftheriou, and D. M. Arnold, "Regular and irregular progressive edge-growth Tanner graphs," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 386–398, Jan. 2005.
[10] G. Zhang and X. Wang. (Jan. 2010). "Girth-12 quasi-cyclic LDPC codes with consecutive lengths." [Online]. Available: https://arxiv.org/abs/1001.3916