Construction of Quasi-Cyclic LDPC Codes Using a Class of Balanced Incomplete Block Designs with Irregular Block Sizes

Hosung Park
Chonnam National University, Gwangju 61186, Korea
Email: hpark1@jnu.ac.kr

Abstract —Low-Density Parity-Check (LDPC) codes are widely used in many applications including high-speed communications such as 802.11n and 802.16e and data memory/storage systems such as NAND flash memory. For practical use, most of them take Quasi-Cyclic (QC) structure and good QC LDPC codes with various parameters are still necessary to be constructed. In this paper, we proposed a construction method of QC LDPC codes whose parity-check matrix consists of a single row of circulant matrices by using a class of balanced incomplete block design, called Perfect Difference Family (PDF). We alter the structure of PDFs with irregular block sizes and then use them to construct the proposed QC LDPC codes to support various lengths, code rates, and degree distributions. We construct two QC LDPC codes based on PDFs and compare them with the random-like LDPC codes constructed from the progressive edge-growth (PEG) algorithm via the additive white Gaussian noise channel simulation. The results show that the proposed QC LDPC codes have a very similar error-correcting performance to the PEG LDPC codes while supporting the QC structure for easy hardware implementation.

Index Terms—Balanced Incomplete Block Design (BIBD), circulant matrix, low-density parity-check (LDPC) codes, Perfect Difference Family (PDF), Quasi-Cyclic (QC) LDPC codes

I. INTRODUCTION

Low-Density Parity-Check (LDPC) codes have been being adopted in many standards of communications systems such as 802.11n, 802.16e, and 10GBase-T owing to their capacity-approaching error-correcting performance and linearly growing computational complexity with respect to code length. In particular, they are very suitable for parallel decoding and thus are scheduled to be used in enhanced mobile broadband service of 5G systems [1]. In addition, LDPC codes are adopted in memory and storage systems such as NAND flash as well as communications systems.

For a practical use, the codes need to take the form of Quasi-Cyclic (QC) structure to be efficiently implemented in terms of hardware. There have been a lot of researches on the construction of QC LDPC codes [2]-[14]. Nonetheless, more good QC LDPC codes need to be constructed to cover as many parameters as possible to give a set of abundant choices for system designers. In particular, the construction of high-rate QC LDPC codes with short lengths is still not much known compared to other parameters.

The QC structure whose parity-check matrix has a form of a single row of circulant matrices is adequate for the construction of the high-rate LDPC codes with short lengths. Regarding this type of codes, regular QC LDPC codes were constructed from cyclic difference family (CDF) in [5]-[9] and irregular QC LDPC codes were constructed by modifying CDFs [10]. To provide an abundant set of code parameters, an algorithm-based construction method for this QC structure was proposed in [13] and [14].

In this paper, we propose a construction method for irregular QC LDPC codes whose parity-check matrix consists of a single row of circulant matrices by using a class of perfect difference families with multiple block sizes. The proposed QC LDPC codes enable a flexible code design by providing various degree distributions, code rates, and code lengths unlike the existing construction methods [5]-[10], [13], [14]. In addition, the proposed construction method can result in high-rate QC LDPC codes with a quite short length, which is hardly attained by random construction methods such as the Progressive Edge-Growth (PEG) algorithm [15]. It is noted that the proposed construction provides more abundant choice of degree distribution than the construction in [10]. To verify the error-correcting performance of the proposed QC LDPC codes, we compare the proposed codes with the random-like LDPC codes constructed from the PEG algorithm via simulation and it shows that the proposed QC LDPC codes have the identical or quite similar error-correcting performance to the PEG LDPC codes.

This paper is organized as follows. In Section II, we introduce the basic concept of QC LDPC codes and the structure of a single row of circulant matrices and we provide the previous works related to our proposed

Manuscript received November 20, 2018; revised June 5, 2019.
This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2018R1D1A1B07051108).
Corresponding author email: hpark1@jnu.ac.kr.
doi:10.12720/jcm.14.7.553-559

construction. In Section III, we propose the construction method of QC LDPC codes based on perfect difference families. In Section IV, we provide simulation results to verify the proposed QC LDPC codes. Finally, we conclude this paper in Section V.

II. Preliminaries

A. LDPC Codes

A linear code can be described with either a generator matrix or a parity-check matrix **H** which satisfies $\mathbf{Hc}^T=\mathbf{0}^T$ for all codewords **c**. An LDPC code is a linear block code defined by a sparse parity-check matrix **H** which contains mostly 0's and a few 1's. An LDPC code is called regular when all columns in **H** have the same weight and all rows also have the same weight. Otherwise, the LDPC code is called irregular. A (w_c,w_r) regular LDPC code has the column weight w_c and the row weight w_r. The rate of (w_c,w_r) regular LDPC code becomes $R=1-w_c/w_r$ when the parity-check matrix has full rank. Such R is called design rate of the LDPC code regardless of whether the parity-check matrix has full rank or not. It is known that regular LDPC codes are good for applications requiring low error floors [16] and they include memory/storage system applications. On the other hand, irregular LDPC codes have a good waterfall error-correcting performance and they are mainly used in communications systems such as LTE and 5G.

When we construct LDPC codes of finite lengths, cycle structure in the parity-check matrix should be considered to have good error-correcting performance through iterative message-passing decoding. To define cycle of LDPC codes, the Tanner graph representation needs to be introduced first. The Tanner graph of a linear code is a bipartite graph whose incidence matrix is the parity-check matrix of the code. In the Tanner graph of (n,k) linear code, there are n variable nodes corresponding to codeword symbols and n-k check nodes corresponding to parity check equations. In the Tanner graph of regular LDPC codes, all variable nodes have the same degree and all check nodes also have the same degree. In the Tanner graph, a cycle is defined as the path starting from a node and coming back to itself. It is known that quite short cycles result in bad effect to message-passing decoder because they break the independency of the messages passed between variable nodes and check nodes. The girth of a Tanner graph is defined as the length of the shortest cycles. Girth at least 6 should be guaranteed for a good error-correcting performance of LDPC codes under the iterative message-passing decoding.

B. QC LDPC Codes

The codewords of QC LDPC codes are split into several subblocks of the same length and cyclically rotating bits in a subblock of every codeword still results in another codeword. The parity-check matrix of QC LDPC codes becomes an array of circulant matrices and/or zero matrices, where a circulant matrix is defined as a matrix whose each column is a downward cyclic shift of the column on its leftside. Definitely, a circulant matrix becomes a square matrix and the size of a circulant matrix is defined as the number of element in a column (row).

The weight of a circulant matrix is defined as the number of nonzero elements in the first column. A circulant matrix of weight 1 is called circulant permutation matrix. A multi-weight circulant matrix is defined as a circulant matrix of weight larger than 1. A circulant matrix is entirely described by the positions of nonzero elements in the first column. The shift value(s) of a circulant matrix is (are) defined as the index (indices) of the nonzero element(s) in the first column. Each circulant matrix has the set of shift values. A shift value is an integer which takes a value from 0 to the size of the circulant matrix minus 1.

In this paper, we focus on the QC LDPC codes whose parity-check matrix consists of a single row of circulant matrices as follows.

$$\mathbf{H} = [\ \mathbf{H}_0\ \mathbf{H}_1\ \ldots\ \mathbf{H}_{L-1}\ ]$$

Here, $\mathbf{H}_i$ represents a z x z circulant matrix. Let w_i denote the weight of circulant matrix $\mathbf{H}_i$ and $S_i=\{s_{i,0},s_{i,1},\ldots,s_{i,wi-1}\}$ denote the set of shift values of $\mathbf{H}_i$. Then, the above parity-check matrix is perfectly described with only S_i and the size of the circulant matrix z.

The protograph [17] of a QC LDPC code is a bipartite graph whose incidence matrix is $\mathbf{P}=[p_i]$, where p_i means the weight of the circulant $\mathbf{H}_i$. There are two kinds of nodes in the protograph, where horizontal (check) nodes correspond to rows in **P** and vertical (variable) nodes correspond to columns in **P**. The Tanner graph of the QC LDPC code is constructed by copying the protograph z times and cyclically permuting the z edges of the same kind. Such copy-and-permute operation is called lifting. If $p_i \geqq 2$, which is the case which this paper is mainly considering, there are multiple edges between the only horizontal node and the vertical node with index i. A shift value is assigned to each edge in the protograph so that an edge is lifted by using the cyclic permutation with the assigned shift value to generate the Tanner graph of the QC LDPC code.

Cycles in the Tanner graph of a QC LDPC code are closely related to tailless non-reversing closed (TNC) walks in its protograph [18]. A walk is an alternating sequence of vertices and edges, denoted by $v_{i0}\ e_{i0}\ v_{i1}\ \ldots\ v_{in\text{-}1}\ e_{in\text{-}1}\ v_{in}$, where the vertices v_{ij} and v_{ij+1} are the endpoints of the edge e_{ij}. A walk is closed if $v_{in}=v_{i0}$ and a walk is non-reversing if $e_{ij}\neq e_{ij+1}$ for $j=0,1,\ldots,n-2$. A closed walk is said to be tailless if $e_{in\text{-}1}\neq e_{i0}$. The shift sum of a walk W in a protograph, denoted by $s(W)$, is defined as the alternating sum of shift values assigned to the edges in W. The following lemma states the necessary and sufficient condition for a cycle of a certain length in the Tanner graph of QC LDPC codes to be generated from the protographs. The proof is directly derived from the results in [19] and [20] and thus it is omitted in this paper.

Lemma [18]: Let **W** denote the set of all TNC walks of length n in a protograph. Suppose that a QC LDPC code is lifted from the protograph with lift size z. Then, the Tanner graph of this QC LDPC code has a cycle of length n if and only if there exists a walk $W \in \mathbf{W}$ such that $s(W)=0$ mod z and W does not contain any shorter TND walks with the zero shift sum.

C. Related Works

There have been many research works to construct QC LDPC codes whose parity-check matrix consists of a single row of circulant matrices using combinatorial designs such as CDFs or a variant of CDFs. In [5], the class-I circulant Euclidean geometry (EG)-LDPC codes were proposed and the authors used EG to determine the shift values in the parity-check matrices to avoid cycles of length 4. They also provide a lower bound of minimum Hamming distance of the codes. In [6], the regular QC LDPC codes were constructed by using the trace function to determine the shift values. The authors actually mentioned that the structure can support irregular code construction but they did not provide any systematic construction method of irregular QC LDPC codes. They used a viewpoint of duals of one-generator QC codes as LDPC codes. The works [5] and [6] did not use CDF directly but they can be viewed as the first trials to construct the QC LDPC codes whose parity-check matrix consists of a single row of circulant matrices by using mathematical structures.

In [7], the QC LDPC codes were proposed by using difference families in general and the authors concretely provided the construction method using CDFs. The authors devoted a lot to analyze the proposed LDPC codes and they also provided a few construction methods of CDFs. In [8], the class-I BIBD-LDPC codes were proposed and they were constructed by using class-I Bose-BIBD which actually are equivalent to CDF. The authors first provided the construction method of the mathematical structure and also proposed the method of splitting the circulant rows of the parity-check matrix so that the resulting codes can have multiple rows of circulant matrices. In [9], the authors extended the the class of LDPC codes that can be systematically generated by presenting a construction method for regular LDPC codes based on combinatorial designs known as Kirkman triple systems. They did not mentioned that the work is related to the construction using CDFs but Kirkman triple systems are actually equivalent to CDFs and we can say that the proposed codes have the same structure with what we are interested in and are constructed from CDFs. The works [7], [8], and [9] can be viewed as the first papers which proposed the QC LDPC codes whose parity-check matrix consists of a single row of circulant matrices based on CDFs. It is also noted that all the codes in [5]-[9] are regular and the supported code lengths are very limited. The goal of this paper is clearly different from them.

In [10], the authors proposed the construction of irregular QC LDPC codes by using CDFs and splitting a block of CDF into several blocks. The resulting codes also have the parity-check matrix which consists of a single row of circulant matrices. The disadvantage of the work is that we need to start from a high-weight CDF to construct irregular QC LDPC codes which includes high-degree variable nodes but such CDFs rarely exist. Moreover, the resulting codes do not support various lengths, which means that the work is still practically limited. In [13] and [14], the authors proposed the algorithms to construct the regular QC LDPC codes which can support various code lengths. The proposed construction can be practically meaningful but they are not based on mathematical structures and are hardly constructed for a very short code length from such a reason.

III. Construction of the Proposed QC LDPC Codes

A. Perfect Difference Family

In this subsection, the definitions of mathematical structures related to the proposed QC LDPC codes are given based on [21]. A cyclic difference family is first defined as follows.

Definition 1: Let Z_v denote the set of integers from 0 to v-1. Then t k-element subsets of Z_v, $B_i=\{b_{i0}, b_{i1},\ldots,b_{i(k-1)}\}$, $i=0,1,\ldots,t-1$, form a (v,k,λ) cyclic difference family (CDF) if every nonzero element in Z_v occurs λ times among the differences $(b_{il}-b_{im})$ mod v, $0 \leqq i \leqq t-1$ and $0 \leqq l \neq m \leqq k-1$. It is noted that B_i is called block.

In this paper, a special class of CDFs, called perfect difference family, will be used to construct QC LDPC codes to avoid cycle 4 by properly assigning the shift values. Before giving the definition, we first introduce the positive and negative differences over a finite set of integers as follows.

Definition 2: Consider t k-element subsets of Z_v $B_i=\{b_{i0}, b_{i1},\ldots,b_{i(k-1)}\}$, $i=0,1,\ldots,t-1$, $b_{i0} < b_{i1} < \ldots < b_{ik-1}$. Among the $tk(k-1)$\$ differences $(b_{il}-b_{im})$ mod v, $0 \leqq i \leqq t-1$ and $0 \leqq l \neq m \leqq k-1$, the half of them $\Delta_+(B)=\{b_{il} - b_{im} \mid i=0,1,\ldots,t-1$\$, $0 \leqq m < l \leqq k-1\}$, are called the multiset of positive differences of B_i's over Z_v and the other half of differences $\Delta_-(B)$ are called the multiset of negative differences of B_i's over Z_v.

For the efficient notation of multiset, we use the expression $\{m_0^{(f0)},\ldots,m_{c-1}^{(fc-1)}\}$ when the multiset contains elements $m_0, \ldots, m_{c-1}$ and their frequencies are $f_0, \ldots, f_{c-1}$. When the frequency of an element is not known nor clear, the superscript can be omitted. It is noted that CDF can have various block sizes and the multiset of block sizes will be denoted by K.

Definition 3: Consider a (v,K,λ) CDF, $B_i=\{b_{i0}, b_{i1},\ldots,b_{i(k-1)}\}$, $i=0,1,\ldots,t-1$, $b_{i0} < b_{i1} < \ldots < b_{ik-1}$. Then the CDF is called a (v,K,λ) perfect difference family (PDF) if the union of all $\Delta_+(B_i)$ becomes the multiset $\{1^{(\lambda)},2^{(\lambda)},\ldots,(v-1)/2^{(\lambda)}\}$.

The necessary and sufficient conditions on the existence of $(v,\{3,k^{(1)}\},1)$ PDF for k=4,5,6,7 are given as follows.

- $(v,\{3,4^{(1)}\},1)$ exists if and only if f $v\equiv 1$ (mod 6), $v\geqq 19$
- $(v,\{3,5^{(1)}\},1)$ exists if and only if $v\equiv 9,15$ (mod 24), $v\geqq 33$
- $(v,\{3,6^{(1)}\},1)$ exists if and only if $v\equiv 1$ (mod 6), $v\geqq 43$
- $(v,\{3,7^{(1)}\},1)$ exists if and only if $v\equiv 1,7$ (mod 24), $v\geqq 73$

B. Proposed Code Construction

In this paper, we propose a construction method of QC LDPC codes whose parity-check matrix consists of a single row of circulant matrices by using $(v,\{3,k^{(1)}\},1)$ PDFs for k=4,5,6,7. It is noted that the construction of such PDFs are given in [21].

Let $B=\{B_0,B_1,\ldots,B_{n-1}\}$ denote a $(v,\{3,k^{(1)}\},1)$ PDF and $S_i=\{s_{i,0},s_{i,1},\ldots,s_{i,wi-1}\}$, $i=0,1,\ldots,L-1$, denote the set of shift values of $\mathbf{H}_i$ in the proposed parity-check matrix consisting of a single row of circulant matrices. Without loss of generality, we assume that the first block B_0 has size k. The procedure of the proposed construction is described as follows.

Construction:

1) Choose z and L to satisfy $z\geqq v$ and $L\leqq 3n-2$
2) Set S_0 equal to B_0
3) Among the subsets of B_i for $1\leqq i\leqq n-1$, the three subsets of size 2 are denoted by $B_{i,0}$, $B_{i,1}$, and $B_{i,2}$ and the union of B_i, $B_{i,0}$, $B_{i,1}$, and $B_{i,2}$ for all $1\leqq i\leqq n-1$ is denoted by B'. Then, select the sets of shift values $S_1, S_2, \ldots, S_{L-1}$ such that $\{B_i,B_{i,j}\}\subset\{S_1,S_2,\ldots,S_{L-1}\}$ is not satisfied and $\{S_1,S_2,\ldots,S_{L-1}\}\subset B'$ is satisfied for $1\leqq i\leqq n-1$ and $0\leqq j\leqq 2$.

The proposed QC LDPC codes have length zL and the design rate $(L-1)/L$. In many practical cases, the parity-check matrix of irregular LDPC codes which show a good error-correcting performance have a few large-weight columns and the other columns of weight 2 and 3. The proposed construction enable the parity-check matrix to have weight 2, 3, and k (k=4,5,6,7) so that it is effective in terms of good weight distribution. Hence, the proposed construction supports various code lengths, code rates, and even weight distributions. It is noted that the proposed construction gives much more flexible degree distributions than the construction in [10] because we start from the PDFs with irregular block sizes while the construction in [10] is based on only the typical PDFs with the regular block size. The proposed QC LDPC codes do not include cycle 4 as shown in the following theorem.

Theorem: The girth of the proposed QC LDPC codes is 6.

Proof: It is known that every parity-check matrix including a circulant matrix of weight larger than or equal to 3 has cycle 6 [22]. The necessary condition on the shift values for a parity-check matrix not to have cycles of length 4 is that the union of the multisets of the positive differences of S_i does not have any element of frequency larger than or equal to 2. The proposed QC LDPC codes satisfy the above condition by definition and this means that the girth of the proposed QC LDPC codes is larger than or equal to 6. Therefore, the girth of the proposed codes is 6.

To help understand the proposed construction, we provide an example as follows.

Example: Based on the aforementioned conditions on the existence of $(v,\{3,k^{(1)}\},1)$ PDF, we choose v=31 and k=4 and then a $(31,\{3,4^{(1)}\},1)$ PDF is constructed based on [21] as follows.

$$B=\{\{0,4,9,15\},\{0,1,8\},\{0,2,14\},\{0,3,13\}\}$$

The parameter n becomes 4. We choose the code parameters to be z=31 and L=5 so that they satisfy the conditions in the first step of the proposed construction. Then, B' defined in the third step of the proposed construction has the following elements.

$$B'=\{\{0,4,9,15\},\{0,1,8\},\{0,2,14\},\{0,3,13\},\{0,1\},\{0,8\},\{1,8\},\{0,2\},\{0,14\},\{2,14\},\{0,3\},\{0,13\},\{3,13\}\}$$

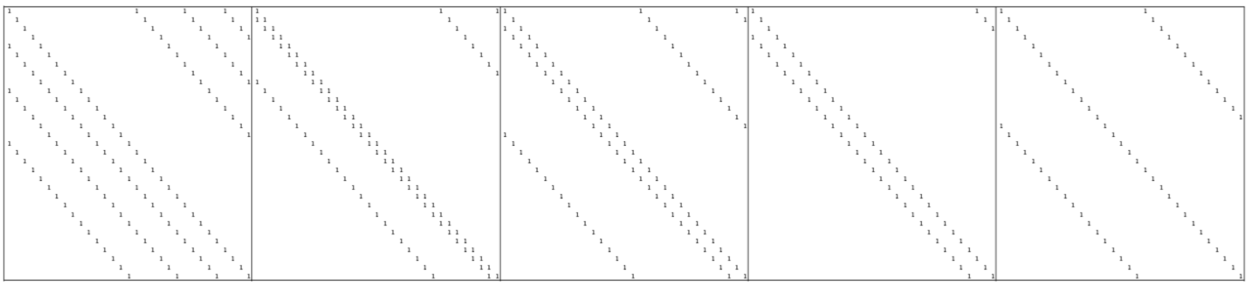

Figure 1. Parity-check matrix of the proposed QC LDPC code with n=155 and R=4/5.

We select {0,4,9,15}, {0,1,8}, {0,2,14}, {0,3}, {0,13} to form the set of shift values such that the selected blocks satisfy the condition in the third step of the proposed construction. The final resulting QC LDPC code has code length 155, code rate 4/5, and weight distribution (4,3,3,2,2). The corresponding parity-check matrix is shown in Fig. 1. The blanks in the parity-check matrix actually should be filled with 0's but they are omitted for clear representation.

IV. Verification of the Proposed QC LDPC Codes

We verify the error-correcting performance of the proposed QC LDPC codes via the additive white Gaussian noise (AWGN) channel simulation by comparing with the progressive edge-growth (PEG) LDPC codes. We construct two proposed QC LDPC codes to simulate. For the first code, the $(v,\{3,k^{(1)}\},1)$ PDF shown in the aforementioned example is again used to construct the proposed QC LDPC code of length 200 and rate 4/5 by setting z=40. Actually, the proposed construction supports very short length from 155 but the PEG algorithm cannot generate such a short LDPC code. We notice that the PEG algorithm succeeds in generating LDPC codes of length at least 190 without 4 cycles. This is why we set the code length 200 to compare the proposed construction with the PEG algorithm. For the comparison, we used the set of shift values in the example and set z=40 and L=5 so that the proposed construction results in the QC LDPC code with n=200 and R=4/5. The LDPC code constructed from the PEG algorithm has the same parameters and the resulting girth is 6.

For the second code to simulate, we used a $(25, \{3,4^{(1)}\},1)$ PDF B={{0,1,3,10},{0,4,12},{0,5,11}} to construct the proposed QC LDPC code. We build B'={{0,1,3,10},{0,4,12},{0,5},{0,11}}. We set z=32 and L=4 so that the resulting code has code length 128 and rate 3/4. The parity-check matrix of the constructed code is shown in Fig. 2. The PEG LDPC code with the same parameters is also constructed to compare. It is noted that the PEG code to compare cannot be constructed without cycles of length 4 for code length around 100 while the proposed code of length 100 can be constructed from the PDF.

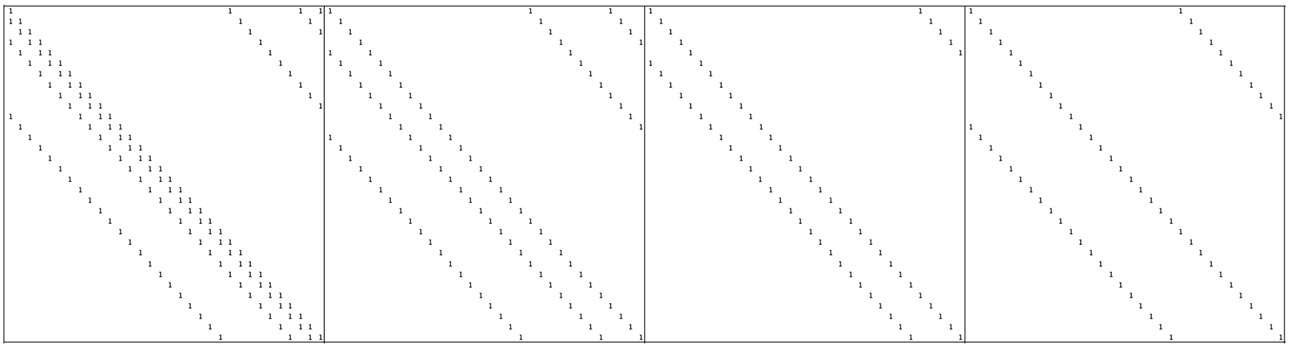

Figure 2. Parity-check matrix of the proposed QC LDPC code with n=128 and R=3/4.

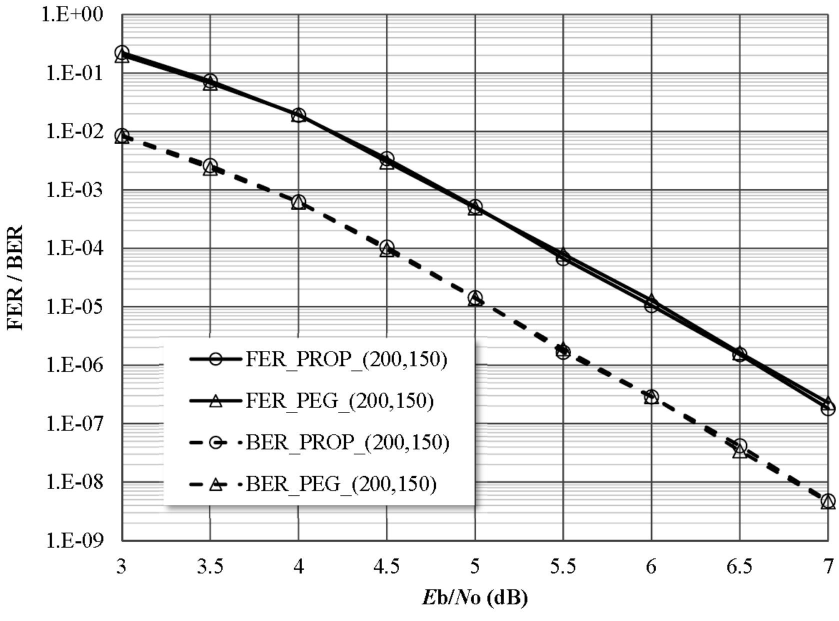

Figure 3. FER and BER of the proposed QC LDPC code and the PEG LDPC code for n=200 and R=4/5.

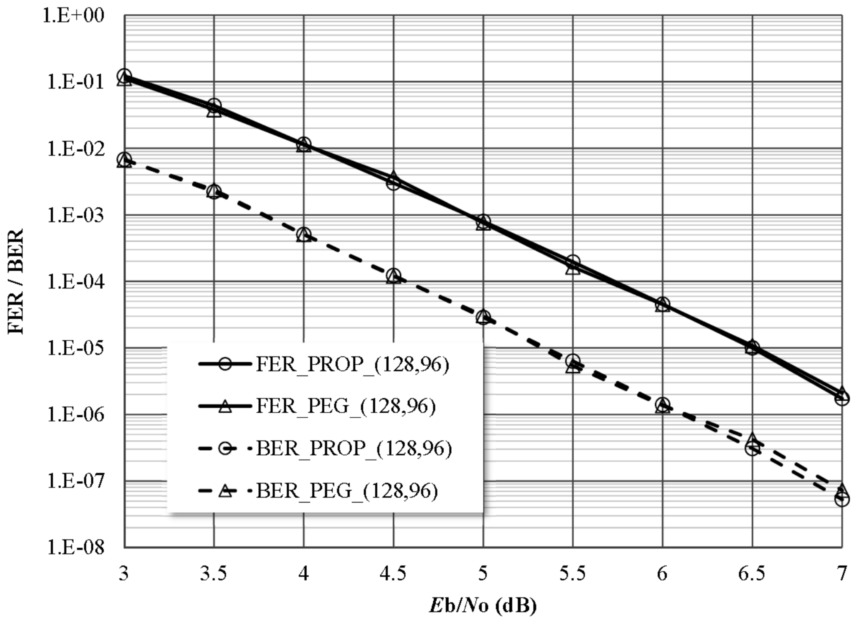

Figure 4. FER and BER of the proposed QC LDPC code and the PEG LDPC code for n=200 and R=4/5.

The Frame Error Rate (FER) and Bit Error Rate (BER) of the constructed codes are shown in Figs. 3 and 4. PROP and PEG in the legend represent the proposed QC LDPC code and the PEG LDPC code, respectively. The simulation is performed with the binary phase shift keying (BPSK) modulation and the maximum number of iteration in the LDPC decoding is set to 50.

We easily see in Figs. 3 and 4 that the proposed QC LDPC codes show a very similar error-correcting performance to the PEG LDPC codes under the same parameters. Since the PEG LDPC codes are known to have as good performance as random LDPC codes, it is said that the proposed QC LDPC codes have good error-correcting performance enough while keeping the QC structure which is crucial for ease of hardware implementation.

V. Conclusions and Future Works

In this paper, we proposed a construction method of QC LDPC codes whose parity-check matrix consists of a single row of circulant matrices by using perfect difference family. We alter the structure of PDFs with irregular block sizes and then use them to construct the proposed QC LDPC codes to support various lengths, code rates, and degree distributions. We construct two QC LDPC codes based on PDFs and compare them with the random-like LDPC codes constructed from the progressive edge-growth algorithm via AWGN simulation. The results show that the proposed QC LDPC codes have a very similar error-correcting performance to the PEG LDPC codes while supporting the QC structure for easy hardware implementation.

It would be better to extend this construction approach to construct parity-check matrices consisting of an arbitrarily sized array of circulant permutation matrices while this work considered only a single row of multi-weight circulant matrices. To maintain the girth property of the parity-check matrices, a careful decomposition of circulant matrices constructed from PDFs would be a key factor of the future research.

References

[1] 3GPP TS 38.212.3rd generation partnership project; Technical specification group radio access network; NR; Multiplexing and channel coding (Release 15). *3GPP*, [Online]. Available: http://www.3gpp.org

[2] Y. Kou, S. Lin, and M. P. C. Fossorier, "Low-density parity-check codes based on finite geometries: a rediscovery and new results," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2711–2736, Nov. 2001.

[3] I. Djurdjevic, J. Xu, K. Abdel-Ghaffar, and S. Lin, "A class of low-density parity-check codes constructed based on Reed-Solomon codes with two information symbols," *IEEE Commun. Lett.*, vol. 7, no. 7, pp. 317–319, Jul. 2003.

[4] S. J. Johnson and S. R. Weller, "Codes for iterative decoding from partial geometries," *IEEE Trans. Commun.*, vol. 52, no. 2, pp. 236–243, Feb. 2004.

[5] H. Tang, J. Xu, Y. Kou, S. Lin, and K. Abdel-Ghaffar, "On algebraic construction of Gallager and circulant low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1269–1279, Jun. 2004.

[6] N. Kamiya, "High-rate quasi-cyclic low-density parity-check codes derived from finite affine planes," *IEEE Trans. Inf. Theory*, vol. 53, no. 4, pp. 1444–1459, Apr. 2007.

[7] B. Vasic and O. Milenkovic, "Combinatorial constructions of low-density parity-check codes for iterative decoding," *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1156–1176, Jun. 2004.

[8] B. Ammar, B. Honary, Y. Kou, J. Xu, and S. Lin, "Construction of low-density parity-check codes based on balanced incomplete block designs," *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1257–1268, Jun. 2004.

[9] S. J. Johnson and S. R. Weller, "Regular low-density parity-check codes from combinatorial designs," in *Proc. IEEE Inf. Theory Workshop*, pp. 90–92.

[10] S. J. Johnson and S. R. Weller, "A family of irregular LDPC codes with low encoding complexity," *IEEE Commun. Lett.*, vol. 7, no. 2, pp. 79–81, Feb. 2003.

[11] S. J. Johnson and S. R. Weller, "Resolvable 2-designs for regular low-density parity-check codes," *IEEE Trans. Commun.*, vol. 51, no. 9, pp. 1413–1419, Sep. 2003.

[12] M. Fujisawa and S. Sakata, "A construction of high rate quasi-cyclic regular LDPC codes from cyclic difference families with girth 8," *IEICE Trans. Fundamentals*, vol. E90-A, no. 5, pp. 1055–1061, May 2007.

[13] T. Xia and B. Xia, "Quasi-cyclic codes from extended difference families," in *Proc. IEEE Wireless Commun. and Networking Conf.*, vol. 2, New Orleans, USA, Mar. 2005, pp. 1036–1040.

[14] M. Baldi and F. Chiaraluce, "New quasi cyclic low density parity check codes based on difference families," in *Proc. Int. Symp. Commun. Theory and Appl.*, Ambleside, UK, Jul. 2005, pp. 244–249.

[15] 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.

[16] T. J. Richardson, "Error floors of LDPC codes," in *Proc. Allerton Conf. Commun., Control, Comput.*, UIUC, IL, Oct. 2003, pp. 1426-1435.

[17] J. Thorpe, Low-density Parity-check (LDPC) Codes Constructed from Protograph Jet Propulsion Laboratory, Pasadena, CA, USA, 2003, *IPN Progr. Rep*. 42-154.

[18] H. Park, S. Hong, J. S. No, and D. J. Shin, "Design of multiple-edge protographs for QC LDPC codes avoiding short inevitable cycles," *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4598–4614, Jul. 2013.

[19] 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.

[20] C. A. Kelley and J. L. Walker, "LDPC codes from voltage graphs," in *Proc. IEEE Int. Symp. Inf. Theory*, Toronto, Canada, Jul. 2008, pp. 792-796.

[21] C. J. Colbourn and J. H. Dinitz, *The CRC Handbook of Combinatorial Designs*, CRC, 1996.

[22] R. M. Tanner, "Spectral graphs for quasi-cyclic LDPC codes," in *Proc. IEEE Symp. Inf. Theory*, 2001, p. 226.

Hosung Park received the B.S., M.S., and Ph.D. degrees in electrical engineering and computer science from Seoul National University, Seoul, Korea, in 2007, 2009, and 2013, respectively. He was a postdoctoral researcher at Institute of New Media and Communications, Seoul National University, Seoul, Korea, from March 2013 to August 2013, and at Qualcomm Institute, California Institute for Telecommunications and Information Technology, University of California, San Diego, CA, USA, from September 2013 to January 2015. He is now an assistant professor at School of Electronics and Computer Engineering, Chonnam National University, Gwangju, Korea, from March 2015. His research interests include low-density parity-check codes, coding theory, coding for memory/storage systems, coding for distributed storage/computation, communications systems and signal processing, compressed sensing, network information theory, and network coding.