Construction of High-Rate Regular Quasi-Cyclic LDPC Codes Based on Cyclic Difference Families

Hosung Park, Seokbeom Hong, Jong-Seon No, *Fellow, IEEE,* and Dong-Joon Shin, *Senior Member, IEEE*

***Abstract*—For a high-rate case, it is difficult to randomly construct good low-density parity-check (LDPC) codes of short and moderate lengths because their Tanner graphs are prone to have short cycles. Also, the existing high-rate quasi-cyclic (QC) LDPC codes can be constructed only for very restricted code parameters. In this paper, based on special classes of cyclic difference families, we propose a new construction method of high-rate regular QC LDPC codes having parity-check matrices consisting of a single row of circulants with column-weight 3 or 4. The proposed QC LDPC codes can be constructed for various code rates and lengths including the minimum achievable length for given column-weight and design rate under girth 6. It is observed that the parity-check matrices of the proposed QC LDPC codes have full rank for column-weight 3 and just one redundant row for column-weight 4. It is shown that the error correcting performance of the proposed QC LDPC codes of short and moderate lengths is almost the same as that of the existing ones through numerical analysis.**

***Index Terms*—Code length, code rate, cyclic difference families (CDFs), girth, quasi-cyclic (QC) low-density parity-check (LDPC) codes.**

I. Introduction

LOW-density parity-check (LDPC) codes [1] have been one of dominant error-correcting codes for high-speed communication systems or data storage systems because they asymptotically have capacity-approaching performance under iterative decoding with moderate complexity. Among them, quasi-cyclic (QC) LDPC codes are well suited for hardware implementation using simple shift registers due to the regularity in their parity-check matrices so that they have been adopted in many practical applications.

For a high-rate case, it is difficult to randomly construct good LDPC codes of short and moderate lengths because their parity-check matrices are so dense compared to a low-rate case for the given code length and degree distribution. This makes them prone to have short cycles. Among well-known structured LDPC codes, finite geometry LDPC codes [2]–[6] and LDPC codes constructed from combinatorial designs [7]–[12] are adequate for high-rate LDPC codes. The error correcting performance of these LDPC codes is verified under proper decoding algorithms but they have severe restrictions on flexibly choosing the code rate and length. Also, since finite geometry LDPC codes usually have much redundancy and large weights in their parity-check matrices, they are not suitable for a strictly power-constrained system with iterative message-passing decoding.

It is known that the parity-check matrix structure consisting of a single row of circulants [5]–[10], [13], [14] is adequate for generating high-rate QC LDPC codes of short and moderate lengths. The class-I circulant EG-LDPC codes in [5] and the duals of one-generator QC codes in [6] are constructed from the affine geometry and they have very restricted rates and lengths and much redundancy. In [7]–[10], QC LDPC codes constructed from cyclic difference families (CDFs) [15] are proposed, which also have restricted lengths. Computer search algorithms are proposed in [13] and [14] for various-length QC LDPC codes of the single-row circulant structure, but they cannot generate QC LDPC codes as short as the QC LDPC codes constructed from CDFs for most of code rates.

In this paper, new high-rate regular QC LDPC codes having parity-check matrices consisting of a single row of circulants with column-weight 3 or 4 are proposed based on special classes of CDFs. In designing the proposed QC LDPC codes, we can flexibly choose the code rate and length including the minimum achievable code length for the given column-weight and design rate under girth 6. The parity-check matrices of the proposed QC LDPC codes have full rank when the column-weight is 3, and they have almost full rank when the column-weight is 4 because there is just one redundant row. Numerical analysis shows that the error correcting performance of the proposed QC LDPC codes of short and moderate lengths is almost the same as that of the existing high-rate QC LDPC codes.

The remainder of the paper is organized as follows. Section II introduces the definition and the existence theorems of CDFs, and provides a construction method of a class of CDFs. In Section III, high-rate regular QC LDPC codes are proposed and analyzed. In Section IV, the error correcting performance of the proposed QC LDPC codes is compared to that of the existing high-rate QC LDPC codes via numerical analysis. Finally, the conclusions are provided in Section V.

Manuscript received November 18, 2012; revised April 30 and June 23, 2013. The editor coordinating the review of this paper and approving it for publication was K. Abdel-Ghaffar.

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government(MSIP) (No. NRF-2009-0081441).

H. Park was with the Department of Electrical and Computer Engineering, Institute of New Media and Communications, Seoul National University, Seoul 151-744, Korea. He is now with the Department of Electrical and Computer Engineering, University of California, San Diego, CA 92093 USA (e-mail: hpark1@snu.ac.kr).

S. Hong was with the Department of Electrical and Computer Engineering, Institute of New Media and Communications, Seoul National University, Seoul 151-744, Korea. He is now with Samsung Electronics, Co., Ltd., Gyeonggi-do 445-701, Korea (e-mail: fousbyus@ccl.snu.ac.kr).

J.-S. No is with the Department of Electrical and Computer Engineering, Institute of New Media and Communications, Seoul National University, Seoul 151-744, Korea (e-mail: jsno@snu.ac.kr).

D.-J. Shin is with the Department of Electronic Engineering, Hanyang University, Seoul 133-791, Korea (e-mail: djshin@hanyang.ac.kr).

Digital Object Identifier 10.1109/TCOMM.2013.070213.120879

II. Cyclic Difference Families

A. Definition and Existence

A cyclic difference family is defined as follows.

Definition 1 ([15]): Consider the additive group $\mathbb{Z}_v = \{0, 1, \ldots, v-1\}$. Then t k-element subsets of $\mathbb{Z}_v$, $B_i = \{b_{i1}, b_{i2}, \ldots, b_{ik}\}$, $i = 1, 2, \ldots, t$, $b_{i1} < b_{i2} < \cdots < b_{ik}$, form a (v, k, λ) *cyclic difference family* (CDF) if every nonzero element of $\mathbb{Z}_v$ occurs λ times among the differences $b_{im} - b_{in}$, $i = 1, 2, \ldots, t$, $m \neq n$, $m, n = 1, 2, \ldots, k$.

According to [7]–[12], $(k(k-1)t+1, k, 1)$ CDFs are adequate for constructing parity-check matrices of QC LDPC codes with girth at least 6. Theorem 1 shows the existence of such CDFs.

Theorem 1: The existence of $(k(k-1)t+1, k, 1)$ CDFs is given as:

1) There exists a $(6t+1, 3, 1)$ CDF for all $t \geq 1$ [16].
2) A $(12t+1, 4, 1)$ CDF exists for all $1 \leq t \leq 1000$ [17].
3) A $(20t+1, 5, 1)$ CDF exists for $1 \leq t \leq 50$ and $t \neq 16, 25, 31, 34, 40, 45$ [18].

In this paper, a special class of CDFs, called perfect difference family (PDF), will be used to construct high-rate regular QC LDPC codes having parity-check matrices consisting of a single row of circulants so that more various code parameters can be achieved. Before introducing its definition, we will define two terms as follows. Consider t k-element subsets of $\mathbb{Z}_v$, $B_i = \{b_{i1}, b_{i2}, \ldots, b_{ik}\}$, $i = 1, 2, \ldots, t$, $b_{i1} < b_{i2} < \cdots < b_{ik}$. Among the differences $b_{im} - b_{in}$, $i = 1, 2, \ldots, t$, $m \neq n$, $m, n = 1, 2, \ldots, k$, we will call $tk(k-1)/2$ differences $b_{im} - b_{in}$, $i = 1, 2, \ldots, t$, $1 \leq m < n \leq k$, as the *forward differences over* $\mathbb{Z}_v$ of the subsets and the remaining $tk(k-1)/2$ differences as the *backward differences over* $\mathbb{Z}_v$ of the subsets.

Definition 2 ([15]): Consider a $(v, k, 1)$ CDF, $B_i = \{b_{i1}, b_{i2}, \ldots, b_{ik}\}$, $i = 1, 2, \ldots, t$, $b_{i1} < b_{i2} < \cdots < b_{ik}$, with $v = k(k-1)t + 1$. Then the CDF is called a $(v, k, 1)$ *perfect difference family* (PDF) if the $tk(k-1)/2$ backward differences cover the set $\{1, 2, \ldots, (v-1)/2\}$.

The condition on the existence of PDFs is stricter than that of CDFs. Some recent results on the existence of PDFs are summarized in the following theorem.

Theorem 2: The existence of $(k(k-1)t+1, k, 1)$ PDFs is given as:

1) A $(6t+1, 3, 1)$ PDF exists if and only if $t \equiv 0$ or $1 \mod 4$ [19].
2) A $(12t+1, 4, 1)$ PDF exists for $t = 1$, $4 \leq t \leq 1000$ [17].
3) $(20t+1, 5, 1)$ PDFs are known for $t = 6, 8, 10$ but for no other values in $1 \leq t \leq 50$ [20].
4) There is no $(k(k-1)t+1, k, 1)$ PDF for $k \geq 6$ [20].

Since there are no PDFs for $k \geq 6$ and no sufficiently many PDFs for $k = 5$ from Theorem 2, we focus on the case of $k = 3, 4$. The construction of PDFs for $k = 3$ and 4 is provided in [15] and [17], respectively.

B. Construction of $(6t+1, 3, 1)$ CDFs for $t \equiv 2$ or $3 \mod 4$

Although $(6t+1, 3, 1)$ PDFs do not exist for $t \equiv 2$ or $3 \mod 4$, a class of $(6t+1, 3, 1)$ CDFs constructed from hooked Skolem sequences for $t \equiv 2$ or $3 \mod 4$ can be used to construct parity-check matrices of QC LDPC codes for various code parameters, which consist of a single row of circulants.

Definition 3 ([15]): A *Skolem sequence* of order t is a sequence $S = (a_1, a_2, \ldots, a_{2t})$ of integers satisfying the following two conditions:

i) For every $k \in \{1, 2, \ldots, t\}$, there exist exactly two elements a_i and a_j in S such that $a_i = a_j = k$.
ii) If $a_i = a_j = k$ with $i < j$, then $j - i = k$.

Skolem sequences are also written as collections of ordered pairs $\{(u_i, v_i) : 1 \leq i \leq t, v_i - u_i = i\}$ with $\bigcup_{i=1}^{t} \{u_i, v_i\} = \{1, 2, \ldots, 2t\}$. A *hooked Skolem sequence* of order t is a sequence $S = (a_1, a_2, \ldots, a_{2t-1}, a_{2t} = 0, a_{2t+1})$ satisfying the conditions i) and ii).

A hooked Skolem sequence of order t exists if and only if $t \equiv 2$ or $3 \mod 4$, and it can be constructed by the method in [15] as follows. Note that the ordered pairs are used to represent a hooked Skolem sequence as in Definition 3.

- $t = 2$; $(1, 2), (3, 5)$
- $t = 3$; $(1, 4), (2, 3), (5, 7)$
- $t = 4s + 2$, $s \geq 1$;
$$\begin{cases} (r, 4s - r + 2), & r = 1, \ldots, 2s \\ (4s + r + 3, 8s - r + 4), & r = 1, \ldots, s-1 \\ (5s + r + 2, 7s - r + 3), & r = 1, \ldots, s-1 \\ (2s + 1, 6s + 2), (4s + 2, 6s + 3), & \\ (4s + 3, 8s + 5), (7s + 3, 7s + 4) & \end{cases}$$
- $t = 4s - 1$, $s \geq 2$;
$$\begin{cases} (4s + r, 8s - r - 2), & r = 1, \ldots, 2s-2 \\ (r, 4s - r - 1), & r = 1, \ldots, s-2 \\ (s + r + 1, 3s - r), & r = 1, \ldots, s-2 \\ (s - 1, 3s), (s, s + 1), (2s, 4s - 1), & \\ (2s + 1, 6s - 1), (4s, 8s - 1) & \end{cases}$$

From hooked Skolem sequences, $(6t+1, 3, 1)$ CDFs can be constructed for $t \equiv 2$ or $3 \mod 4$. After constructing a hooked Skolem sequence (u_i, v_i) of order t, $1 \leq i \leq t$, a $(6t+1, 3, 1)$ CDF is obtained by letting $B_i = \{0, i, v_i + t\}$. We can easily check that all differences in B_i's cover the set $\{1, 2, \ldots, 6t\}$.

III. High-Rate QC LDPC Codes Constructed From PDFs and CDFs

A. Proposed QC LDPC Codes

Consider a binary regular LDPC code whose parity-check matrix H is a $1 \times L$ array of $z \times z$ circulants given as

$$H = \begin{bmatrix} H_1 & H_2 & \cdots & H_L \end{bmatrix} \tag{1}$$

where a *circulant* H_i is defined as a square matrix whose each row is a cyclic shift of the row above it. This LDPC code is quasi-cyclic because applying circular shifts within each length-z subblock of a codeword gives another codeword.

A circulant is entirely described by the positions of nonzero elements in the first column. Let $\gamma, 0 \le \gamma \le z-1$, be the index of the $(\gamma+1)$-st element in the first column. Then, the *shift value*(s) of a circulant is (are) defined as the index (indices) of the nonzero element(s) in the first column. Note that a shift value takes the value from 0 to $z-1$. Let d_v (d_c) denote the column-weight (row-weight) of H. Then we have $d_c = d_v L$ and the design rate of this LDPC code is $R = (L-1)/L$. Let s_{ij}, $i = 1, \ldots, L$ and $j = 1, \ldots, d_v$, denote the j-th smallest shift value of H_i, that is, $s_{i1} < s_{i2} < \cdots < s_{id_v}$, which correspond to the indices of 1's in the first column of H_i.

We propose a new class of high-rate QC LDPC codes which have the parity-check matrix form in (1) constructed from PDFs or hooked Skolem sequence-based CDFs given in Subsection II-B. Under some proper constraints, a parity-check matrix with the column-weight 3 or 4 can be obtained by taking shift values of H_i from B_i in the hooked Skolem sequence-based CDF or the PDF. More concretely, QC LDPC codes can be constructed by using B_i, $i = 1, \ldots, L$, of the CDF or the PDF as follows:

1) Choose the code parameters $d_v = 3$ or 4, L, and z such that
   i) $L \ge 2$ for $d_v = 3$ and $4 \le L \le 1000$ for $d_v = 4$
   ii) $z \ge d_v(d_v-1)L+1$, where $z \ne 6L+2$ for $d_v = 3$ and $L \equiv 2$ or $3 \mod 4$.
2) If $d_v = 3$ and $L \equiv 2$ or $3 \mod 4$, construct a hooked Skolem sequence-based $(6L+1, 3, 1)$ CDF B_i, $i = 1, \ldots, L$, as in Subsection II-B. Otherwise, construct a $(d_v(d_v-1)L+1, d_v, 1)$ PDF B_i, $i = 1, \ldots, L$, as in [15] and [17].
3) Let $s_{ij} = b_{ij}$, $i = 1, 2, \ldots, L$ and $j = 1, 2, \ldots, d_v$.

For $d_v = 5$, QC LDPC codes having parity-check matrices consisting of a single row of circulants can also be constructed by the proposed procedure, but for L other than 6, 8, and 10, $(20L+1, 5, 1)$ PDFs are still unknown as in Theorem 2.

B. Girth of the Proposed QC LDPC Codes

Parity-check matrices including circulants of column-weight larger than or equal to 3 have a girth at most 6 [21] because the circulants inevitably generate cycles of length 6. In this subsection, we will show that the proposed QC LDPC codes have girth 6 through Corollaries 1 and 2 by proving that there is no cycle of length 4 in the parity-check matrices. Let $\delta_{ijk}^{(z)}$ denote the difference $s_{ij} - s_{ik} \mod z$ of shift values s_{ij} and s_{ik} in H_i. For QC LDPC codes constructed from CDFs, we define $\delta_{\max}$ as the maximum backward difference over $\mathbb{Z}_z$ of the L sets of shift values, that is, $\delta_{\max} := \max_{i,j,k} \delta_{ijk}^{(z)}$ for $1 \le i \le L$ and $1 \le k < j \le d_v$.

Theorem 3: QC LDPC codes constructed from CDFs do not have any cycle of length 4 for every $z \ge 2\delta_{\max} + 1$.

Proof: The necessary and sufficient condition for avoiding cycles of length 4 is that all $\delta_{ijk}^{(z)}$'s, $i = 1, \ldots, L$ and $1 \le j \ne k \le d_v$, are distinct. The backward differences over $\mathbb{Z}_z$ of the shift values fall into the interval $[1, \delta_{\max}]$ and thus the forward differences over $\mathbb{Z}_z$ of the shift values fall into the interval $[z - \delta_{\max}, z-1]$. For $z \ge 2\delta_{\max} + 1$, all $\delta_{ijk}^{(z)}$'s are distinct. ∎

Corollary 1: Consider a $(d_v(d_v-1)L+1, d_v, 1)$ PDF $B_i = \{b_{i1}, b_{i2}, \ldots, b_{id_v}\}$, $i = 1, 2, \ldots, L$. The proposed QC LDPC codes constructed from the PDF do not have any cycle of length 4 for every $z \ge d_v(d_v-1)L+1$.

Proof: For these QC LDPC codes, $\delta_{\max} = d_v(d_v-1)L/2$. The proof is completed by Theorem 3. ∎

Corollary 2: For $L \equiv 2$ or $3 \mod 4$, consider a $(6L+1, 3, 1)$ CDF $B_i = \{b_{i1}, b_{i2}, b_{i3}\}$, $i = 1, 2, \ldots, L$, constructed from a hooked Skolem sequence of order L. The proposed QC LDPC codes constructed from the CDF do not have any cycle of length 4 for every $z \ge 6L+1$ and $z \ne 6L+2$.

Proof: For $z = 6L+1$, all $\delta_{ijk}^{(z)}$'s, $i = 1, \ldots, L$ and $1 \le j \ne k \le d_v$, are distinct due to the definition of CDFs. The remaining proof is completed by Theorem 3 because $\delta_{\max} = 3L+1$ for these QC LDPC codes. ∎

Note that for $d_v = 3$, $L \equiv 2$ or $3 \mod 4$, and $z = 6L+2$, the set of forward differences and the set of backward differences over $\mathbb{Z}_z$ of the shift values in the proposed QC LDPC codes have $3L+1$ as a common element. Thus it seems that another construction method is needed for $z = 6L+2$. However, in fact, there does not exist any construction method which avoids cycles of length 4 as shown in the following theorem.

Theorem 4: For $d_v = 3$, $L \equiv 2$ or $3 \mod 4$, and $z = 6L+2$, which is not the case covered in Corollary 2, QC LDPC codes whose parity-check matrices have the form in (1) cannot avoid cycles of length 4 for any shift value assignment.

Proof: Assume that there exists a shift value assignment such that the parity-check matrix avoids cycles of length 4. If $\delta_{ijk}^{(z)} = 3L+1$ for some i, j, k, the difference $\delta_{ikj}^{(z)}$ is also $3L+1$. Therefore, all $6L$ differences $\delta_{ijk}^{(z)}$, $i = 1, 2, \ldots, L$ and $1 \le j \ne k \le 3$, have to cover 1 to $6L+1$ except $3L+1$.

Let Δ_B denote the sum of backward differences over $\mathbb{Z}_z$ of the shift values. Note that the addition is calculated over the integers. Then, Δ_B is odd because

$$
\begin{aligned}
\Delta_B &= \sum_{\substack{i,j,k:\ j>k,\\ \delta_{ijk}^{(z)} < 3L+1}} \delta_{ijk}^{(z)} + \sum_{\substack{i,j,k:\ j>k,\\ \delta_{ijk}^{(z)} > 3L+1}} \delta_{ijk}^{(z)} \\
&\equiv \left\{ \sum_{\substack{i,j,k:\ j>k,\\ \delta_{ijk}^{(z)} < 3L+1}} \delta_{ijk}^{(z)} - \sum_{\substack{i,j,k:\ j>k,\\ \delta_{ijk}^{(z)} > 3L+1}} \delta_{ijk}^{(z)} \right\} \mod 2 \\
&\equiv \left\{ \sum_{\substack{i,j,k:\ j>k,\\ \delta_{ijk}^{(z)} < 3L+1}} \delta_{ijk}^{(z)} + \sum_{\substack{i,j,k:\ j>k,\\ \delta_{ijk}^{(z)} > 3L+1}} (6L+2-\delta_{ijk}^{(z)}) \right\} \mod 2 \\
&\equiv \left\{ \sum_{\substack{i,j,k:\ j>k,\\ \delta_{ijk}^{(z)} < 3L+1}} \delta_{ijk}^{(z)} + \sum_{\substack{i,j,k:\ j<k,\\ \delta_{ijk}^{(z)} < 3L+1}} \delta_{ijk}^{(z)} \right\} \mod 2 \\
&\equiv \sum_{i=1}^{3L} i \mod 2 \\
&\equiv 1 \mod 2. \qquad (2)
\end{aligned}
$$

On the other hand, since Δ_B can be expressed as

$$\begin{aligned}\Delta_B &= \sum_i \sum_{j,k:\ j>k} \delta_{ijk}^{(z)} \\ &= \sum_i \sum_{j,k:\ j>k} (s_{ij} - s_{ik}) \\ &= \sum_i 2(s_{i3} - s_{i1}),\end{aligned}$$

this contradicts (2) in that the parities of Δ_B are different. Therefore, there is no shift value assignment such that the parity-check matrix in (1) avoids cycles of length 4 for $d_v = 3$, $L \equiv 2$ or $3 \mod 4$, and $z = 6L + 2$. ■

C. Advantages of the Proposed QC LDPC Codes

The proposed QC LDPC codes have advantages mainly on being able to achieve various code parameters while guaranteeing girth 6. First, the proposed QC LDPC codes have various code rates. For $d_v = 3$, L only has to be larger than or equal to 2 and for $d_v = 4$, L can be any integer from 4 to 1000, similar to the conventional QC LDPC codes constructed from CDFs [7]–[10] except for $d_v = 4$ and $L = 2, 3$. Second, for a fixed L, the proposed QC LDPC codes have various code lengths because z can be any value as long as $z \geq d_v(d_v - 1)L + 1$ except for the case of $d_v = 3$, $L \equiv 2$ or $3 \mod 4$, and $z = 6L + 2$. On the other hand, the conventional QC LDPC codes constructed from CDFs were originally proposed only for $z = d_v(d_v - 1)L + 1$ and they generally do not guarantee girth 6 for $z > d_v(d_v - 1)L + 1$ when L is given. Moreover, like the conventional QC LDPC codes from CDFs, the proposed QC LDPC codes can achieve the minimum code length, that is, the theoretical lower bound, among all possible regular LDPC codes with girth 6 for the given d_v and design rate. This property is clearly understood from the fact that the parity-check matrix of the proposed QC LDPC code with $z = d_v(d_v - 1)L + 1$ is actually an incidence matrix of a Steiner system [7], [9]. Note that QC LDPC codes in [13] and [14] cannot achieve the minimum code length. Therefore, the proposed QC LDPC codes can be very useful in designing error-correcting systems which require short packets.

To clearly show the effectiveness of the proposed QC LDPC codes, let us compare the proposed QC LDPC codes with the conventional QC LDPC codes from CDFs [7]–[10] and the array LDPC codes [22]. In the case of the conventional QC LDPC codes from CDFs, z can be any value satisfying $z \geq d_v(d_v - 1)L + 1$ and $z \equiv 1 \mod d_v(d_v - 1)$ to have girth 6 because for the given CDF B_i, $i = 1, \ldots, L$, the conventional QC LDPC codes can be constructed by using only the sets $B_{i_1}, B_{i_2}, \ldots, B_{i_{L'}}$ for $L' < L$. Moreover, since the maximum backward difference $\delta_{\max}$ can be up to $d_v(d_v - 1)L$ for general CDFs, the conventional QC LDPC codes have girth 6 for every $z \geq 2d_v(d_v - 1)L + 1$ according to Theorem 3. However, the conventional QC LDPC codes have limited flexibility to achieve small code lengths, compared to the proposed QC LDPC codes.

In the case of array LDPC codes, assume that their parity-check matrices have the form of a $d_v \times d_v L$ array of $z' \times z'$ circulant permutation matrices, which correspond to the most common form of the existing regular QC LDPC codes. Obviously, they have the same design rate and row- and column-weights of the parity-check matrices with the proposed QC LDPC codes. The necessary condition on z' to have girth larger than or equal to 6 is $z' \geq d_v L$ [23] and, for the array LDPC codes, z' is prime and $z' \geq d_v L$. The array LDPC code cannot have sufficiently various code lengths and cannot achieve the minimum code length because the minimum achievable length of array codes is $d_v^2 L^2$ which is larger than that of the proposed QC LDPC codes $d_v(d_v - 1)L^2 + L$. Tables I and II show the number of achievable code lengths of the proposed QC LDPC codes (denoted by PROP), the conventional QC LDPC codes from CDFs (denoted by CONV), and the array LDPC codes (denoted by ARR) for each code length interval. We can see that the proposed QC LDPC codes can achieve many small code lengths, compared to the conventional QC LDPC codes from CDFs and the array LDPC codes.

The error correcting performance of the proposed QC LDPC codes may not be good for z much larger than $d_v(d_v - 1)L + 1$ because, regardless of the code length, the girth of the proposed QC LDPC codes is fixed to 6 and the minimum distance of these QC LDPC codes has a value between $d_v + 1$ and $2d_v$ [7], [13]. However, these restrictions on the girth and the minimum distance are not problematic for the error correcting performance of the proposed high-rate short QC LDPC codes. Actually, for large L and small z, the error correcting performance of the proposed QC LDPC codes will be compared with that of other QC LDPC codes in Section IV. Therefore, the proposed construction is adequate for high-rate QC LDPC codes of short and moderate lengths.

It is difficult to analyze the rank of the parity-check matrices of the proposed QC LDPC codes because they do not have an algebraic structure like the codes in [2]–[6]. Instead, the rank of the proposed parity-check matrices for various parameters can be numerically computed. It is observed that the parity-check matrices of the proposed QC LDPC codes have full rank for the parameters $d_v = 3$, $4 \leq L \leq 20$, and z such that the code length is less than or equal to 3,000. It is also observed that they have almost full rank, i.e., just one redundant row, for the parameters $d_v = 4$, $4 \leq L \leq 15$, and z such that the code length is less than or equal to 3,000. Moreover, every parity-check matrix has at least one full-rank circulant for $d_v = 3$, which enables a simple encoding of the proposed QC LDPC codes, and has at least one almost full-rank circulant for $d_v = 4$. Assume that H_L in (1) is invertible. Then, a generator matrix G of systematic form is simply obtained [10] as

$$G = \begin{bmatrix} & (H_L^{-1}H_1)^T \\ I_{z(L-1)} & (H_L^{-1}H_2)^T \\ & \vdots \\ & (H_L^{-1}H_{L-1})^T \end{bmatrix}$$

where $I_{z(L-1)}$ represents the $z(L-1) \times z(L-1)$ identity matrix. This full-rank property of the parity-check matrices differentiates the proposed QC LDPC codes from the QC LDPC codes in [5] and [6], whose parity-check matrices consist of a single row of circulants and have many redundant rows.

TABLE I
THE NUMBER OF ACHIEVABLE CODE LENGTHS IN EACH CODE LENGTH INTERVAL FOR $d_v = 3$

$R = 0.9$ ($L = 10$)				$R = 0.95$ ($L = 20$)			
Code Length	PROP	CONV	ARR	Code Length	PROP	CONV	ARR
610–929	31	6	0	2420–3659	62	11	0
930–1209	28	4	2	3660–4819	58	9	5
1210–1999	79	79	5	4820–5999	59	59	3

TABLE II
THE NUMBER OF ACHIEVABLE CODE LENGTHS IN EACH CODE LENGTH INTERVAL FOR $d_v = 4$

$R = 0.9$ ($L = 10$)				$R = 0.95$ ($L = 20$)			
Code Length	PROP	CONV	ARR	Code Length	PROP	CONV	ARR
1210–1639	43	4	0	4820–6639	91	8	0
1640–2409	77	6	5	6640–9619	149	12	8
2410–2999	59	59	4	9620–11999	119	119	5

IV. SIMULATION RESULTS

In this section, the error correcting performance of the proposed QC LDPC codes is verified via numerical analysis and compared with that of some algebraic QC LDPC codes and progressive edge-growth (PEG) LDPC codes [24] with girth 6. As algebraic QC LDPC codes, affine geometry QC LDPC codes [6] and array LDPC codes [22] are used. Note that the PEG LDPC codes are not quasi-cyclic but random-like, and they are known to have the error correcting performance as good as random LDPC codes. The parameters of the algebraic QC LDPC codes are set to have as equal values with those of the proposed QC LDPC codes as possible and the parameters of the PEG LDPC codes are exactly the same as those of the proposed QC LDPC codes. All results are obtained based on PC simulation using the sum-product decoding under the additive white Gaussian noise (AWGN) channel. The maximum number of iterations is set to 100.

First, the rate-0.9167 (1020, 935) proposed QC LDPC code with $d_v = 3$, $L = 12$, and $z = 85$ is compared with the rate-0.9131 (1024, 935) affine geometry QC LDPC code and the rate-0.9167 (1020, 935) PEG LDPC code. The bit error rate (BER) performance of these LDPC codes is shown in Fig. 1 and we can see that the proposed QC LDPC code and the PEG LDPC code show a better BER performance than the affine geometry QC LDPC code in the high signal-to-noise ratio (SNR) region. Second, the rate-0.9333 (2115, 1974) proposed QC LDPC code with $d_v = 3$, $L = 15$, and $z = 141$ is compared with the rate-0.9348 (2115, 1977) array LDPC code and the rate-0.9333 (2115, 1974) PEG LDPC code. It is shown in Fig. 1 that these LDPC codes have almost the same BER performance. Finally, the rate-0.9006 (1640, 1477) proposed QC LDPC code with $d_v = 4$, $L = 10$, and $z = 164$ is compared with the rate-0.9024 (1640, 1480) array LDPC code and the rate-0.9006 (1640, 1477) PEG LDPC code. It is shown in Fig. 1 that these LDPC codes also have almost the same BER performance.

V. CONCLUSIONS

In this paper, a new class of high-rate QC LDPC codes with $d_v = 3$ or 4 is proposed, which have parity-check matrices consisting of a single row of circulants and having girth 6. The construction of these QC LDPC codes exploits the CDFs constructed from hooked Skolem sequences in the case of $d_v = 3$ and $L \equiv 2$ or $3 \mod 4$, and the PDFs in other cases. In designing the proposed QC LDPC codes, we can flexibly choose the values of L and z including the minimum achievable code length for the given d_v and design rate under girth 6. The parity-check matrices of the proposed QC LDPC codes have full rank when $d_v = 3$ and have almost full rank, i.e., just one redundant row, when $d_v = 4$. Via numerical analysis, it is verified that the error correcting performance of the proposed QC LDPC codes is better than or almost equal to that of the affine geometry QC LDPC codes, the array LDPC codes, and the PEG LDPC codes.

REFERENCES

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

[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. 2001 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.

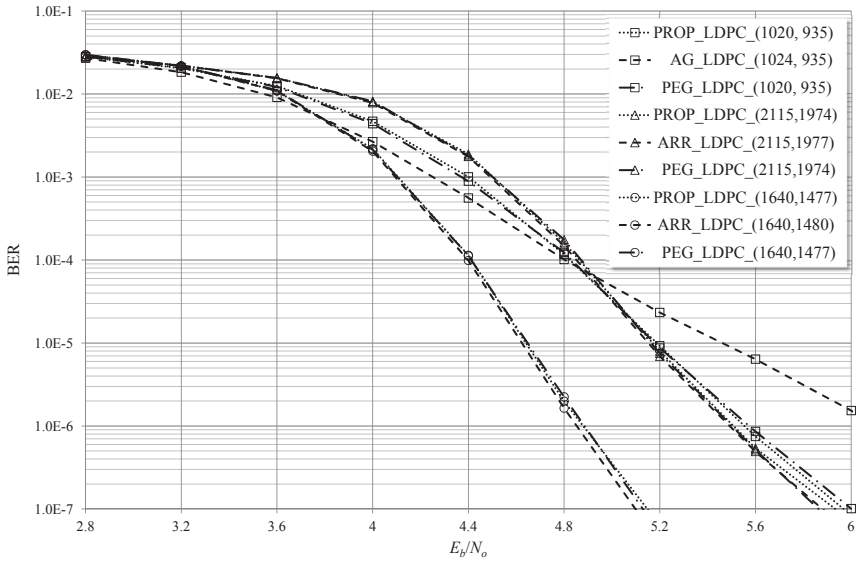

Fig. 1. BER performance comparison of the proposed QC LDPC codes (denoted by PROP_LDPC), the affine geometry QC LDPC codes (denoted by AG_LDPC), the array LDPC codes (denoted by ARR_LDPC), and the PEG LDPC codes (denoted by PEG_LDPC).

[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. 2005 IEEE Wireless Commun. Networking Conf.*, pp. 1036–1040.
[14] M. Baldi and F. Chiaraluce, "New quasi cyclic low density parity check codes based on difference families," in *Proc. 2005 Int. Symp. Commun. Theory and Appl.*, pp. 244–249.
[15] C. J. Colbourn and J. H. Dinitz, *The CRC Handbook of Combinatorial Designs*. CRC, 1996.
[16] R. Peltesohn, "Eine Losung der beiden Heffterschen Differenzenprobleme," *Compos. Math.*, vol. 6, pp. 251–257, 1938.
[17] G. Ge, Y. Miao, and X. Sun, "Perfect difference families, perfect difference matrices, and related combinatorial structures," *J. Combin. Des.*, vol. 18, no. 6, pp. 415–449, Nov. 2010.
[18] R. Julian, R. Abel, S. Costa, and N. J. Finizio, "Directed-ordered whist tournaments and $(v, 5, 1)$ difference families: Existence results and some new classes of Z-cyclic solutions," *Discrete Appl. Math.*, vol. 143, pp. 43–53, 2004.
[19] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*. Cambridge University Press, 1986.
[20] R. Mathon, "Construction for cyclic Steiner 2-designs," *Ann. Discrete Math.*, vol. 34, pp. 353–362, 1987.
[21] R. M. Tanner, "Spectral graphs for quasi-cyclic LDPC codes," in *Proc. 2001 Int. Symp. Inf. Theory*, p. 226.
[22] J. L. Fan, "Array codes as low-density parity-check codes," in *Proc. 2000 Int. Symp. Turbo Codes*, pp. 543–546.
[23] 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.
[24] 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.

Hosung Park received the B.S., M.S., and Ph.D. degrees in electrical engineering from Seoul National University, Seoul, Korea, in 2007, 2009, and 2013, respectively. He was a postdoctoral researcher working with Prof. Jong-Seon No and Prof. Young-Han Kim at Institute of New Media and Communications in Seoul National University, Seoul, Korea, from March 2013 to August 2013. Since September 2013, he has worked with Prof. Young-Han Kim as a postdoctoral scholar in Department of Electrical and Computer Engineering, University of California, San Diego, USA. His research interests include low-density parity-check codes, coding theory, coding for memory, compressed sensing, network information theory, and network coding.

Seokbeom Hong received the B.S. and Ph.D. degrees in electrical and computer engineering from Seoul National University, Seoul, Korea, in 2007 and 2013, respectively. He is currently a senior engineer at Samsung Electronics, Gyeonggi-do, Korea. His area of research interests includes compressed sensing, error-correcting codes, and communications theory.

Jong-Seon No (S'80–M'88–SM'10–F'12) received the B.S. and M.S.E.E. degrees in electronics engineering from Seoul National University, Seoul, Korea, in 1981 and 1984, respectively, and the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, in 1988. He was a Senior MTS at Hughes Network Systems from February 1988 to July 1990. He was also an Associate Professor in the Department of Electronic Engineering, Konkuk University, Seoul, from September 1990 to July 1999. He joined the Faculty of the Department of Electrical and Computer Engineering, Seoul National University, in August 1999, where he is currently a Professor. His area of research interests includes error-correcting codes, sequences, cryptography, space-time codes, LDPC codes, and wireless communication systems.

Dong-Joon Shin (S'96-M'99-SM'09) received the B.S. degree in electronics engineering from Seoul National University, Seoul, Korea, the M.S. degree in electrical engineering from Northwestern University, Evanston, USA, and the Ph.D. degree in electrical engineering from University of Southern California, Los Angeles, USA. From 1999 to 2000, he was a member of technical staff in Wireless Network Division and Satellite Network Division, Hughes Network Systems, Maryland, USA. Since September 2000, he has been a Professor in the Department of Electronic Engineering at Hanyang University, Seoul, Korea. His current research interests include error correcting codes, sequences, and wireless/mobile communication systems.