Necessary Conditions for Quasi-Cyclic LDPC Codes to Have a Given Girth

Kyung-Joong Kim
Dept. of Electrical Engineering,
Pohang University of Science
and Technology (POSTECH),
Pohang, Gyungbuk 790-784, Korea
Email: vang@postech.ac.kr

Jin-Ho Chung
School of Electrical and Computer Engineering,
Ulsan National Institute of Science
and Technology (UNIST),
Ulsan Metropolitan City 689-798, Korea
Email: jinho@unist.ac.kr

Kyeongcheol Yang
Dept. of Electrical Engineering,
Pohang University of Science
and Technology (POSTECH),
Pohang, Gyungbuk 790-784, Korea
Email: kcyang@postech.ac.kr

***Abstract*—Short cycles in the Tanner graph of a low-density parity-check (LDPC) code may cause a severe performance degradation. In this paper, we investigate the cycle properties of quasi-cyclic LDPC (QC-LDPC) codes. We first analyze a necessary and sufficient condition for a cycle of a given length to exist, by using the sequence representation of a parity-check matrix for a QC-LDPC code. We then derive bounds which are necessary conditions for a QC-LDPC code to have a given girth in terms of its parameters. Our necessary conditions are applicable to any regular or irregular QC-LDPC codes as well as they improve the existing bounds for many classes of regular QC-LDPC codes.**

***Index Terms*—Cycle, girth, low-density parity-check (LDPC) codes, quasi-cyclic.**

I. Introduction

Low-density parity-check (LDPC) codes [1] have been extensively studied and widely applied to several communication systems due to their Shannon-limit-approaching performance [2]–[6]. It is known that short cycles in the Tanner graph [7] of an LDPC code may cause a severe performance degradation. For this reason, analysis of its cycle property has been a major issue for a long time [8]-[15].

Among several classes of LDPC codes, *quasi-cyclic* LDPC (QC-LDPC) codes have been widely studied in the literature [9]-[21]. They are based on circulant permutation matrices (CPMs) and have algebraically interesting properties. Moreover, they require a smaller amount of memory for storing their parity-check matrices (PCMs). This motivates us to take an intensive interest in constructing QC-LDPC codes without short cycles.

Several methods to construct QC-LDPC codes without short cycles based on algebraic approaches were presented in [9]-[11]. Fossorier [12] presented some necessary conditions for a QC-LDPC code to have girth 6 or 8, where the *girth* means the length of a smallest cycle in a Tanner graph. Recently, Karimi and Banihashemi [13] presented some conditions for a QC-LDPC code to have girth 6, 8, or 10. However, no meaningful bounds on the parameters of a general QC-LDPC code with an arbitrarily large girth have been given. Therefore, it is a challenging problem to develop a meaningful bound on the size of a parity-check matrix of a QC-LDPC code with an arbitrarily large girth.

In this paper we investigate the cycle properties of quasi-cyclic LDPC (QC-LDPC) codes. We analyze a necessary and sufficient condition for a cycle of a given length to exist, by using the sequence representation of a parity-check matrix for a QC-LDPC code. We then derive bounds which are necessary conditions for a QC-LDPC code to have girth $\geq 2t+2$ in terms of its parameters, where $t \geq 2$ is a positive integer. Our necessary conditions can be applied to more general cases than the previously known results, as shown in Table I.

The outline of the paper is as follows. In Section II, we describe the sequence representation of a parity-check matrix for a QC-LDPC code and analyze a necessary and sufficient condition for a cycle of a given length to exist. In Sections III, we give bounds which are necessary conditions for a QC-LDPC code to have a given girth. Finally, we give concluding remarks in Section IV.

II. Preliminaries

An LDPC code defined by a sparse parity-check matrix H of size $M \times N$ may be represented as a Tanner graph with M check nodes and N variable nodes. The code length is N and the code rate is larger than or equal to $(N-M)/N$. The edges in the Tanner graph correspond to the nonzero entries in H, i.e., an edge is connected between the i-th check node and the j-th variable node if and only if the (i,j)-th entry of H is 1. In particular, when each column of H has weight J and each row has weight K, the corresponding LDPC code is called a (J,K)-regular LDPC code.

A QC-LDPC code is an LDPC code whose parity-check matrix consists of square subblocks of size $L \times L$, where each square subblock is either the zero matrix or a CPM. For an integer a with $0 \leq a < L$, let P^a be the CPM obtained by shifting each row of the $L \times L$ identity matrix I to the right a times. For our convenience, we denote by P^∞ the $L \times L$ zero matrix. Then the parity-check matrix of a QC-LDPC code is represented as follows:

$$H' = \begin{bmatrix} P^{a_{0,0}} & P^{a_{0,1}} & \cdots & P^{a_{0,n-1}} \\ P^{a_{1,0}} & P^{a_{1,1}} & \cdots & P^{a_{1,n-1}} \\ \vdots & \vdots & \ddots & \vdots \\ P^{a_{m-1,0}} & P^{a_{m-1,1}} & \cdots & P^{a_{m-1,n-1}} \end{bmatrix}, \qquad (1)$$

for $a_{i,j} \in \mathbb{Z}_L \cup \{\infty\}$, where $\mathbb{Z}_L$ denotes the set of nonnegative residues modulo L. Each CPM is associated with L variable nodes and L check nodes, so we have $N = nL$ and $M = mL$, respectively. See [12], [20] for more details.

Another representation of a QC-LDPC code is obtained by permuting the rows of the parity-check matrix H' in a special way. More formally, the new parity-check matrix H is given by

$$H = QH', \tag{2}$$

where Q is the $mL \times mL$ permutation matrix whose (i,j)-th entry is given by

$$Q_{i,j} = \begin{cases} 1, & \text{if } i_1 = j_0 \text{ and } i_0 = j_1 \\ 0, & \text{otherwise} \end{cases} \tag{3}$$

for $i = i_1 m + i_0$ and $j = j_1 L + j_0$ with $0 \le i_1, j_0 < L$ and $0 \le i_0, j_1 < m$.

Based on the expression in (2), it is possible to simply represent H as a sequence of n integer vectors, i.e.,

$$(\mathbf{b}_0, \mathbf{b}_1, \cdots, \mathbf{b}_{n-1}) \tag{4}$$

where $\mathbf{b}_j \triangleq (b_{1,j}, b_{2,j}, \cdots, b_{d_j,j})^t$ is the j-th column vector over $\mathbb{Z}_{mL}$, $b_{l,j}$ is the row index of the l-th nonzero element in the jL-th column of H, and d_j is the (Hamming) weight of the jL-th column of H for $0 \le j < n$ and $1 \le l \le d_j$. Note that

$$b_{l_1,j} \neq b_{l_2,j} \mod m \tag{5}$$

for any $l_1 \neq l_2$, since each $L \times L$ square subblock of H' contains at most one nonzero entry in each column. The representation in (4) will be referred to as the *sequence representation* of the parity-check matrix H for a QC-LDPC code.

Conversely, the parity-check matrix H of a QC-LDPC code can be uniquely obtained from a given sequence of n vectors, $(\mathbf{b}_0, \mathbf{b}_1, \cdots, \mathbf{b}_{n-1})$, where $\mathbf{b}_j = (b_{1,j}, b_{2,j}, \cdots, b_{d_j,j})^t$ with $b_{i,j} \in \mathbb{Z}_{mL}$ satisfies $b_{l_1,j} \neq b_{l_2,j} \mod m$ for any $l_1 \neq l_2$ and $0 \le j < n$. That is,

$$H_{i,jL+k} = \begin{cases} 1, & \text{if } i \equiv b_{l,j} + km \mod mL \text{ for } 1 \le l \le d_j \\ 0, & \text{otherwise} \end{cases}$$

where $0 \le i < mL$, $0 \le j < n$, and $0 \le k < L$.

A cycle in a Tanner graph is a closed walk in which all the nodes except for the start and end nodes are pairwise distinct. The length of a cycle is simply the number of edges it contains. For short notation, a cycle of length s is denoted by an s-cycle. The cycle property of a parity-check matrix is not changed by row permutation. Therefore, it suffices to investigate the cycle property of the row-permuted parity-check matrix $H = QH'$ for a QC-LDPC code in order to analyze that of the parity-check matrix H' in (1). Throughout the paper, we will assume without loss of generality that the parity-check matrix of a QC-LDPC code is of the form in (2).

There is a 4-cycle in H if and only if there exist a pair of columns and a pair of rows such that the columns have nonzero entries at the rows and vice versa, i.e.,

$$H_{i_1,j_1} = 1, \ H_{i_1,j_2} = 1, \ H_{i_2,j_1} = 1, \ H_{i_2,j_2} = 1$$

for $0 \le i_1 \neq i_2 < mL$ and $0 \le j_1 \neq j_2 < nL$. Hence, a necessary and sufficient condition for a 4-cycle to exist in the parity-check matrix H of a QC-LDPC code may be expressed in terms of $b_{l,j}$'s in the following lemma.

Lemma 1. *A 4-cycle exists in H if and only if there are $b_{l,j}$'s such that*

$$\begin{aligned} b_{l_1,j_1} + x_1 m &\equiv b_{r_2,j_2} + x_2 m \mod mL, & (6)\\ b_{l_2,j_2} + x_2 m &\equiv b_{r_1,j_1} + x_1 m \mod mL & (7) \end{aligned}$$

for $0 \le x_k < L$, $0 \le j_k < n$, $1 \le l_k \neq r_k \le d_{j_k}$ with $j_1 \neq j_2$, where $1 \le k \le 2$.

The conditions in Lemma 1 can be more simplified by removing x_1 and x_2 in (6) and (7).

Lemma 2. *A 4-cycle exists in H if and only if there are $b_{l,j}$'s such that*

$$\begin{aligned} b_{l_1,j_1} + b_{l_2,j_2} &\equiv b_{r_1,j_1} + b_{r_2,j_2} \mod mL, & (8)\\ b_{l_1,j_1} &\equiv b_{r_2,j_2} \mod m & (9) \end{aligned}$$

for $0 \le j_k < n$, $1 \le l_k, r_k \le d_{j_k}$ with $j_1 \neq j_2$, $l_k \neq r_k$ where $1 \le k \le 2$.

By generalizing Lemma 2, it is possible to derive a necessary and sufficient condition for a $2s$-cycle to exist in H, where s is a positive integer larger than or equal to 2.

Lemma 3. *For an integer $s \ge 2$, a $2s$-cycle exists in H if and only if there are $b_{l,j}$'s such that*

$$\begin{aligned} b_{l_1,j_1} + \cdots + b_{l_s,j_s} &\equiv b_{r_1,j_1} + \cdots + b_{r_s,j_s} \mod mL, & (10)\\ b_{l_k,j_k} &\equiv b_{r_{k+1},j_{k+1}} \mod m & (11) \end{aligned}$$

for any k with $1 \le k \le s-1$, where $0 \le j_v < n$, $1 \le l_v \neq r_v \le d_{j_v}$, $j_v \neq j_{v+1}$ for $1 \le v \le s$ and $j_{s+1} = j_1$.

Myung *et al.* [20] showed that there exist some *inevitable* cycles in QC-LDPC codes, regardless of the choice of $a_{i,j}$'s in (1) under some special structures. These kinds of inevitable cycles also appear in the representation of H in (2), when the set of (l_k, j_k)'s in the LHS of (10) is equal to the set of (r_k, j_k)'s in the RHS of (10). In this case, the conditions in (10) and (11) hold regardless of the choice of $b_{l,j}$'s.

III. Necessary Conditions on the Size of the PCM of an QC-LDPC Code

In order to construct a QC-LDPC code of a given girth, it is required to carefully select n vectors $\mathbf{b}_0, \mathbf{b}_1, \cdots, \mathbf{b}_{n-1}$ over $\mathbb{Z}_{mL}$. For example, the QC-LDPC code with parity-check matrix H does not have any $2s$-cycle if no $2s$-tuples of $b_{l,j}$'s satisfy the conditions in Lemma 3.

Assume that $b_{l,j}$'s are properly selected from $\mathbb{Z}_{mL}$ for $0 \le j < n$ and $1 \le l \le d_j$ such that H has girth $g \ge 2t+2$ for an

TABLE I
NECESSARY CONDITIONS ON L FOR A (d_v, d_c)-REGULAR QC-LDPC CODE TO HAVE GIRTH $\geq 2t+2$, WHEN m IS FIXED. HERE, $-$ DENOTES 'NOT APPLICABLE'.

(d_v, d_c)	m	$t=2$	$t=3$	$t=4$	$t=5$	$t=6$	$t=7$
$(3,6)$	Proposed ($m=3$)	$L \geq 6$	$L \geq 11$	$L \geq 61$	$L \geq 111$	$-$	$-$
	Fossorier [12] ($m=3$)	$L \geq 6$	$L \geq 10$	$-$	$-$	$-$	$-$
	Karimi and Banihashemi [13] ($m=3$)	$L \geq 6$	$L \geq 11$	$L \geq 61$	$-$	$-$	$-$
	Proposed ($m=4$)	$L \geq 4$	$L \geq 9$	$L \geq 34$	$L \geq 84$	$L \geq 334$	$L \geq 834$
	Proposed ($m=5$)	$L \geq 3$	$L \geq 7$	$L \geq 27$	$L \geq 67$	$L \geq 267$	$L \geq 667$
	Proposed ($m=25$)	$L \geq 1$	$L \geq 2$	$L \geq 6$	$L \geq 14$	$L \geq 54$	$L \geq 134$
	Proposed ($m=100$)	$L \geq 1$	$L \geq 1$	$L \geq 2$	$L \geq 4$	$L \geq 14$	$L \geq 34$
$(4,8)$	Proposed ($m=4$)	$L \geq 8$	$L \geq 22$	$L \geq 169$	$L \geq 463$	$-$	$-$
	Fossorier [12] ($m=4$)	$L \geq 8$	$L \geq 21$	$-$	$-$	$-$	$-$
	Karimi and Banihashemi [13] ($m=4$)	$L \geq 8$	$L \geq 22$	$L \geq 169$	$-$	$-$	$-$
	Proposed ($m=5$)	$L \geq 6$	$L \geq 18$	$L \geq 106$	$L \geq 371$	$L \geq 2223$	$L \geq 7780$
	Proposed ($m=6$)	$L \geq 5$	$L \geq 15$	$L \geq 89$	$L \geq 309$	$L \geq 1853$	$L \geq 6483$
	Proposed ($m=25$)	$L \geq 1$	$L \geq 4$	$L \geq 22$	$L \geq 75$	$L \geq 445$	$L \geq 1556$
	Proposed ($m=100$)	$L \geq 1$	$L \geq 1$	$L \geq 6$	$L \geq 19$	$L \geq 112$	$L \geq 389$

integer $t \geq 2$, that is, no cycles of length $\leq 2t$ are generated for an integer $t \geq 2$. For $2 \leq s \leq t$ and $1 \leq u \leq d_0$, let

$$\begin{aligned}
(\mathbf{l}, \mathbf{r}, \mathbf{j})_s &\triangleq (l_1, \cdots, l_s; r_2, \cdots, r_s; j_1, \cdots, j_s), \\
\mathcal{I}_s(u) &\triangleq \{(\mathbf{l}, \mathbf{r}, \mathbf{j})_s \,|\, l_1 = u, j_1 = 0, 0 \leq j_v < n, \\
&\qquad 1 \leq l_v \neq r_v \leq d_{j_v}, j_v \neq j_{v+1} \\
&\qquad \text{for } 2 \leq v \leq s \;\text{ with } j_{s+1} = 0 \text{ and} \\
&\qquad j_2 \neq 0,\; b_{l_k, j_k} \equiv b_{r_{k+1}, j_{k+1}} \mod m \\
&\qquad \text{for } 1 \leq k \leq s-1\}, \qquad (12) \\
T_s(u) &\triangleq \{y \in \mathbb{Z}_{mL} \,|\, y \equiv b_{u,0} + b_{l_2, j_2} + \cdots + b_{l_s, j_s} \\
&\qquad - b_{r_2, j_2} - \cdots - b_{r_s, j_s} \mod mL, \\
&\qquad (\mathbf{l}, \mathbf{r}, \mathbf{j})_s \in \mathcal{I}_s(u)\}, \qquad (13)
\end{aligned}$$

and

$$R(u) \triangleq \{y \in \mathbb{Z}_{mL} \,|\, y \equiv b_{u,0} \mod m\}. \qquad (14)$$

Lemma 4. *Assume that $b_{l,j}$'s are properly selected for $0 \leq j < n$ and $1 \leq l \leq d_j$ such that no cycles of length $\leq 2t$ are generated. Let $T_s(u)$ and $R(u)$ for $2 \leq s \leq t$ and $1 \leq u \leq d_0$ be the sets defined in (13) and (14), respectively. Then*

(a) $|R(u)| = L$;
(b) $|T_s(u)| \geq (\underline{d}_c - 1)^{s-1}(\underline{d}_v - 1)^{s-1}$ *for* $2 \leq s \leq t/2+1$;
(c) $|R(u_1) \setminus \bigcup_{u_2=1}^{d_0} \bigcup_{s=2}^{t} T_s(u_2)| \geq 1$;
(d) $|R(u_1) \cap R(u_2)| = 0$ *for* $1 \leq u_1 < u_2 \leq d_0$;
(e) $|R(u) \cap T_2(u)| = 0$;
(f) $|T_{s_1}(u) \cap T_{s_2}(u)| = 0$ *for* $2 \leq s_1 < s_2 \leq t$, $s_1 + s_2 - 2 \leq t$; *and*
(g) $|T_{s_1}(u_1) \cap T_{s_2}(u_2)| = 0$ *for* $1 \leq u_1 < u_2 \leq d_0$, $2 \leq s_1 \neq s_2 \leq t$, $s_1 + s_2 - 1 \leq t$

where $\underline{d}_c$ and $\underline{d}_v$ denote the minimum row and column weights of H, respectively.

The bound on the size of the union of a finite number of sets in the following proposition is easily proved by induction.

Proposition 5. *For an integer $k \geq 2$, let $A_1, \cdots, A_k$ be arbitrary sets. Then*

$$\left| \bigcup_{i=1}^{k} A_i \right| \geq \sum_{i=1}^{k} |A_i| - \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} |A_i \cap A_j|.$$

Based on Lemma 4 and Proposition 5, it is possible to estimate the size of

$$S_{2t} \triangleq \bigcup_{u=1}^{d_0} \left(R(u) \cup \bigcup_{s=2}^{t} T_s(u) \right)$$

in the following lemma.

Lemma 6. *Assume that $b_{l,j}$'s are properly selected for $0 \leq j < n$ and $1 \leq l \leq d_j$ such that no cycles of length $\leq 2t$ are generated. Let $T_s(u)$ and $R(u)$ for $2 \leq s \leq t$ and $1 \leq u \leq d_0$ be the sets defined in (13) and (14), respectively. Then we have*

$$|S_{2t}| \geq \begin{cases} L + \underline{d}_c(\underline{d}_v - 1), & \text{if } t = 2 \\ \underline{d}_v \sum_{s=2}^{(t+1)/2} (\underline{d}_c - 1)^{s-1}(\underline{d}_v - 1)^{s-1} + \underline{d}_v, & \\ & \text{if } t \text{ is an odd integer } \geq 3 \\ \underline{d}_v \sum_{s=2}^{t/2} (\underline{d}_c - 1)^{s-1}(\underline{d}_v - 1)^{s-1} & \\ \quad + (\underline{d}_c - 1)^{t/2}(\underline{d}_v - 1)^{t/2} + \underline{d}_v, & \\ & \text{if } t \text{ is an even integer } \geq 4 \end{cases}$$

where $\underline{d}_c$ and $\underline{d}_v$ denote the minimum row and column weights of H, respectively.

Proof: Case i) $t = 2$: The size of S_4 is lower bounded by

$$\begin{aligned}|S_4| &\geq \left|\bigcup_{u=1}^{d_0} R(u) \cup T_2(1)\right| \\ &\geq \sum_{u=1}^{d_0} \left(|R(u)| - |R(u) \cap T_2(1)|\right) + |T_2(1)| \\ &\quad - \sum_{u_1=1}^{d_0-1} \sum_{u_2=u_1+1}^{d_0} |R(u_1) \cap R(u_2)|\end{aligned}$$

where the second inequality comes from Proposition 5. The statement in this case follows directly from Lemma 4, that is,

$$\begin{aligned}&|R(1)| = L; \\ &|R(1) \cap T_2(1)| = 0; \\ &|R(u)| - |R(u) \cap T_2(1)| \geq 1 \quad \text{for } 2 \leq u \leq d_0; \\ &|T_2(1)| \geq (\underline{d}_c - 1)(\underline{d}_v - 1); \text{ and} \\ &|R(u_1) \cap R(u_2)| = 0 \quad \text{for } 1 \leq u_1 < u_2 \leq d_0.\end{aligned}$$

Case ii) t is an odd integer ≥ 3: Clearly, the size of S_{2t} is lower bounded by

$$|S_{2t}| \quad \geq \quad \left|\bigcup_{u=1}^{d_0} \left(R(u) \cup \bigcup_{s=2}^{(t+1)/2} T_s(u)\right)\right|.$$

The statement comes directly from Proposition 5 and Lemma 4, as shown in Case i).

Case iii) t is an even integer ≥ 4: Clearly, the size of S_{2t} is lower bounded by

$$|S_{2t}| \quad \geq \quad \left|\bigcup_{u=1}^{d_0} \left(R(u) \cup \bigcup_{s=2}^{t/2} T_s(u)\right) \cup T_{t/2+1}(1)\right|.$$

The statement follows directly from Proposition 5 and Lemma 4, as shown in Case i). □

By Lemma 6, it is possible to derive a *necessary condition* for a QC-LDPC code to have girth $\geq 2t+2$.

Theorem 7. *Let H be an $mL \times nL$ parity-check matrix of a QC-LDPC code. Let $\underline{d}_c$ and $\underline{d}_v$ be the minimum row and column weights of H, respectively. If H has girth $g \geq 2t+2$ for an integer $t \geq 2$, then*

$$mL \geq \begin{cases} L + \underline{d}_c(\underline{d}_v - 1), & \text{if } t = 2 \\ \underline{d}_v \sum_{s=2}^{(t+1)/2} (\underline{d}_c - 1)^{s-1}(\underline{d}_v - 1)^{s-1} + \underline{d}_v, & \\ & \text{if } t \text{ is an odd integer } \geq 3 \\ \underline{d}_v \sum_{s=2}^{t/2} (\underline{d}_c - 1)^{s-1}(\underline{d}_v - 1)^{s-1} & \\ \quad + (\underline{d}_c - 1)^{t/2}(\underline{d}_v - 1)^{t/2} + \underline{d}_v, & \\ & \text{if } t \text{ is an even integer } \geq 4. \end{cases}$$

Proof: Note that $|S_{2t}| \leq mL$ since S_{2t} is a subset of $\mathbb{Z}_{mL}$. Combining this condition with Lemma 6, we complete the proof. □

In the case of a (J, K)-regular QC-LDPC code with an $mL \times nL$ parity-check matrix, the bound in Theorem 7 can be easily modified by setting $\underline{d}_v = J$ and $\underline{d}_c = K$. Note that in this case, it can also be directly translated into a bound on the code length, since $nL = mLJ/K$.

Remark: Fossorier [12], and Karimi and Banihashemi [13] gave necessary conditions for a (d_v, d_c)-regular QC-LDPC code to have a given girth, whose parity-check matrix does not have zero matrices as their subblocks so that $d_v = m$ and $d_c = n$. In this special case, our necessary conditions in Theorem 7 can also be further improved, although they are not explicitly described here. In Table I, our necessary conditions on L for a $(3, 6)$-regular or $(4, 8)$-regular QC-LDPC code are compared with the existing bounds in [12] and [13], when m is fixed. As shown in the table, our necessary conditions in Theorem 7 are applicable to any regular or irregular QC-LDPC codes as well as they improve the existing bounds in [12] and [13] for many classes of regular QC-LDPC codes.

IV. Conclusions

We derived necessary and sufficient conditions for a cycle of length $2s$ to exist in the parity-check matrix of a QC-LDPC code. By using the sequence representation, we then defined several sets associated with a QC-LDPC code with a given girth, and obtained bounds on their sizes. Based on them, necessary conditions on the size of a parity-check matrix for a QC-LDPC code with a given girth were derived in terms of its parameters.

Acknowledgment

This work was supported by the National Research Foundation (NRF) of Korea under Grant 2011-0017396 funded by the Ministry of Education, Science and Technology (MEST) of the Korea Government.

References

[1] R. G. Gallager, “Low-density parity-check codes,” *IRE Trans. Inf. Theory*, vol. IT-8, pp. 21-28, Jan. 1962.

[2] D. J. C. MacKay and R. M. Neal, “Near Shannon limit performance of low density parity check codes,” *IEE Electron. Lett.*, vol. 32, pp. 1645-1646, Aug. 1996.

[3] T. J. Richardson, A. Shokrollahi, and R. Urbanke, “Design of capacity-approaching irregular low-density parity-check codes,” *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 638-656, Feb. 2001.

[4] European Telecommunications Standards Institue (ETSI). Digital Video Broadcasting (DVB) Second generation framing structure for broadband satellite applications; EN 302 307 V.1.1.1. www.dvb.org.

[5] V. Pless, W. C. Huffman, and R. A. Brualdi, *Handbook of Coding Theory*. Elsevier Science Ltd., 2007.

[6] T. J. Richardson and R. Urbanke, *Modern Coding Theory*. Cambridge University Press, 2008.

[7] R. M. Tanner, “A recursive approach to low complexity codes,” *IEEE Trans. Inf. Theory*, vol. IT-27, no. 6, pp. 533-547, Sept. 1981.

[8] 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.

[9] J. L. Fan, “Array codes as low-density parity-check codes,” in *Proc. 2nd Int. Symp. Turbo Codes*, Brest, France, Sept. 4-7, 2000, pp. 543-546.

[10] S. J. Johnson and S. R. Weller, “Quasi-cyclic LDPC codes from difference families,” in *Proc. 3rd Austrailian Commun. Theory Workshop*, Canberra, Australia, Feb. 4-5, 2002, pp. 18-22.

[11] B. Vasic and O. Milenkovic, “Combinatorial construction of low-density parity-check codes for iterative decoding,” *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1156-1176, June 2004.

[12] M. P. C. Fossorier, “Quasi-cyclic low-density parity-check codes from circulant permutation matrices,” *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1788-1794, Aug. 2004.

[13] M. Karimi and A. H. Banihashemi, “On the girth of quasi cyclic protograph LDPC codes,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT 2012)*, Cambridge, MA, USA, July 1-6, 2012, pp. 3088-3092.

[14] Z. Li and B. V. K. V. Kumar, “A class of good quasi-cyclic low-density parity check codes based on progressive edge growth graph,” in *Proc. 38th Asilomar Conf. Signals, Syst. Comput.*, Pacific Grove, CA, USA, Nov. 7-10, 2004, pp. 1990-1994.

[15] W. Zhan, G. Zhu, L. Peng, and X. Yan, “Quasi-cyclic LDPC codes based on D and Q matrices through progressive edge growth,” in *Proc. Int. Symp. Intelligent Signal Processing and Commun. Systems*, Xiamen, China, Nov. 28 - Dec. 1, 2007, pp. 12-15.

[16] S. Myung and K. Yang, “Lifting methods for quasi-cyclic LDPC codes,” *IEEE Commun. Lett.* vol. 10, no. 6, pp. 489-491, June 2006.

[17] 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, Sept. 2005.

[18] S. Kim, J.-S. No, H. Chung, and D.-J. Shin, “Cycle analysis and construction of protographs for QC LDPC codes with girth larger than 12,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT 2007)*, Nice, France, June 24-29, 2007, pp. 2256-2260.

[19] C. A. Kelley and J. L. Walker, “LDPC codes from voltage graphs,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT 2008)*, Toronto, Canada, July 6-11, 2008, pp. 792-796.

[20] S. Myung, K. Yang, and J. Kim, “Quasi-cyclic LDPC codes for fast encoding,” *IEEE Trans. Inf. Theory*, vol. 51, no. 8, pp. 2894-2901, Aug. 2005.

[21] 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.