Quasi-Cyclic Low-Density Parity-Check Codes From Circulant Permutation Matrices

Marc P. C. Fossorier, *Senior Member, IEEE*

***Abstract*—In this correspondence, the construction of low-density parity-check (LDPC) codes from circulant permutation matrices is investigated. It is shown that such codes cannot have a Tanner graph representation with girth larger than 12, and a relatively mild necessary and sufficient condition for the code to have a girth of $6, 8, 10$, or 12 is derived. These results suggest that families of LDPC codes with such girth values are relatively easy to obtain and, consequently, additional parameters such as the minimum distance or the number of redundant check sums should be considered. To this end, a necessary condition for the codes investigated to reach their maximum possible minimum Hamming distance is proposed.**

***Index Terms*—Iterative decoding, low-density parity-check (LDPC) codes, quasi-cyclic (QC) codes.**

I. Introduction

Recently, several methods for constructing good families of low-density parity-check (LDPC) codes have been proposed. These methods can be decomposed into two main classes: random or pseudorandom constructions, and algebraic constructions. For long code lengths, random constructions [1]–[4] or pseudorandom constructions [5]–[7] of irregular LDPC codes have been shown to closely approach the theoretical limits for the additive white Gaussian noise (AWGN) channel. Generally, these codes outperform algebraically constructed LDPC codes. On the other hand, for medium-length LDPC codes (say, up to a few thousand bits long for rate $1/2$), the situation is quite different. For these lengths, irregular constructions are generally not better than regular ones, and graph-based or algebraic constructions can outperform random ones [8].

Algebraic constructions of LDPC codes can be decomposed into two main categories. The first category is based on finite geometries [9]–[12], while the second category is based on circulant permutation matrices.[1] This second approach was initially proposed by Gallager [13, Appendix C] (although in this original construction, the permutation matrices are not restricted to circulants). A special class of these codes was later analyzed in [14] and several recent works consider structured ways to design such codes [15]–[20]. In fact, these two methods are interrelated and, for example, many of the code constructions based on finite geometries have an equivalent circulant permutation matrix representation [21, p. 286].

A (J, L)-regular LDPC code is defined as a code represented by a parity-check matrix H in which each column has weight J and each row has weight L[13]. Hence, to construct the parity-check matrix H of a (J, L)-regular LDPC code of length $N = Lp$ with the second method, J rows of L circulant permutation matrices of size $p \times p$ can be judiciously adjoined. The code obtained is quasi-cyclic (QC) and therefore, can be encoded in linear time with shift registers [22, pp. 256–261]. Furthermore, since by row and column permutations, an equivalent code with only identity matrices in the first row block and the first column block of H can be obtained, at most $(J-1)(L-1)$ integers suffice to entirely specify the code. In this correspondence, we derive a simple necessary and sufficient condition for the Tanner graph [23] of these QC LDPC codes to have a given girth. In fact, we show that these QC LDPC codes have a girth g of at most 12, which generalizes the result of [16]. For $g = 6$, the condition is very loose and, therefore, it is very easy is construct QC LDPC codes which perform quite well when iteratively decoded with the belief propagation (BP) algorithm [1]. The conditions for $g = 8, 10$, or 12 are also quite easy to satisfy. This suggests that for LDPC codes of moderate lengths, additional constraints other than the girth need to be considered.

Based on a result of [25], it directly follows that the minimum Hamming distance d_H of a (J, L)-regular QC LDPC code satisfies $d_H \leq (J+1)!$. A set of $(J+1)!$ columns in H summing to zero is explicitly determined in this correspondence. A necessary condition to have all columns in this set distinct is then proposed.

The correspondence is organized as follows. The necessary and sufficient condition for a given girth is derived in Section II. Applications of this condition to construct families of QC LDPC codes are presented in Section III. Code searches and simulation results are discussed in Section IV. In Section V, the necessary condition for a QC LDPC code to reach the upper bound on its minimum distance is developed. Finally, concluding remarks are given in Section VI.

II. Girth of QC LDPC Graph Representations

A. Preliminaries

The parity-check matrix H of a (J, L)-regular QC LDPC code of length $N = pL$ can be represented by

$$H = \begin{bmatrix} I(0) & I(0) & \cdots & I(0) \\ I(0) & I(p_{1,1}) & \cdots & I(p_{1,L-1}) \\ \vdots & & \ddots & \vdots \\ I(0) & I(p_{J-1,1}) & \cdots & I(p_{J-1,L-1}) \end{bmatrix} \tag{1}$$

where for $1 \leq j \leq J-1$, $1 \leq l \leq L-1$, $I(p_{j,l})$ represents the circulant permutation matrix with a one at column-$(r + p_{j,l}) \bmod p$ for row-r, $0 \leq r \leq p-1$, and zero elsewhere. It follows that $I(0)$ represents the $p \times p$ identity matrix. Also, since the p rows of each of the J submatrices $[I(0)I(p_{j,1}) \cdots I(p_{j,L-1})]$, $0 \leq j \leq J-1$, in (1) sum to the all-1 vector, the rank of H is at most $Jp - J + 1$.

A cycle of length $2i$ in $H = [h_{x,y}]$ is defined by $2i$ positions $h_{x,y} = 1$ such that: 1) two consecutive positions are obtained by changing alternatively of row or column only; and 2) all positions are distinct, except the first and last ones. It follows that two consecutive positions in any cycle belong to distinct circulant permutation matrices which are either in the same row, or in the same column. Hence, a cycle of length $2i$ can be associated with an ordered series of circulant permutation matrices

$$I(p_{j_0,l_0}), I(p_{j_1,l_0}), I(p_{j_1,l_1}), \ldots, I(p_{j_{i-1},l_{i-1}}), I(p_{j_0,l_{i-1}}), I(p_{j_0,l_0})$$

with for $1 \leq k \leq i$, $j_k \neq j_{k-1}$ and $l_k \neq l_{k-1}$. With the convention of going from $I(p_{j_{k-1},l_{k-1}})$ to $I(p_{j_k,l_k})$ via $I(p_{j_k,l_{k-1}})$ (i.e., of changing first of row and then of column), any cycle of length $2i$ in H can be represented by the ordered series

$$(j_0, l_0); (j_1, l_1); \cdots (j_{i-1}; l_{i-1}); (j_0, l_0) \tag{2}$$

Manuscript received August 13, 2003; revised January 22, 2004. This work was supported by the National Science Foundation under Grant CCR-0098029. The material in this correspondence was presented at the IEEE International Symposium on Information Theory, Yokohama, Japan, June/July 2003.

The author is with the Department of Electrical Engineering, University of Hawaii, Honolulu, HI 96822 USA (e-mail: marc@spectra.eng.hawaii.edu).

Communicated by S. Litsyn, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2004.831841

[1]A permutation matrix is any square matrix with constant row and colum weight of one; a circulant permutation matrix is a permutation matrix which is cyclic.

for $1 \leq k \leq i$, $j_k \neq j_{k-1}$, and $l_k \neq l_{k-1}$ We note that (2) does not necessarily define a unique cycle of length $2i$ in H, but this is not an issue for the following results. Defining

$$\Delta_{j_x,j_y}(l) = p_{j_x,l} - p_{j_y,l} \tag{3}$$

the matrix H contains a cycle of length $2i$ given by (2) if and only if

$$\sum_{k=0}^{i-1} \Delta_{j_k,j_{k+1}}(l_k) = 0 \mod p \tag{4}$$

with $j_0 = j_i$, $j_k \neq j_{k+1}$, and $l_k \neq l_{k+1}$. This simple necessary and sufficient condition can be rewritten in the following theorem.

Theorem 2.1: A necessary and sufficient condition for the Tanner graph representation of the matrix H defined in (1) to have a girth at least $2(i+1)$ is

$$\sum_{k=0}^{m-1} \Delta_{j_k,j_{k+1}}(l_k) \neq 0 \mod p \tag{5}$$

for all m, $2 \leq m \leq i$, all j_k, $0 \leq j_k \leq J-1$, all j_{k+1}, $0 \leq j_{k+1} \leq J-1$, and all $0 \leq l_k \leq L-1$, with $j_0 = j_m$, $j_k \neq j_{k+1}$, and $l_k \neq l_{k+1}$.

Note that an equivalent condition with respect to row index differences rather than column index differences as in Theorem 2.1 can also be obtained based on H^t, the transpose of H. From Theorem 2.1, the next corollary follows.

Corollary 2.1: For QC LDPC codes with $J = 2$, $g = 4i$ only is possible.

This result directly follows from the series given in (2), in which j_0 and j_1 have to alternate.

In the following two subsections, a lower bound on the minimum value of p for which $g \geq 6$ and $g \geq 8$, respectively, is determined. Unfortunately, for larger girth values, no meaningful bound was obtained.

B. Girth $g \geq 6$

A simple necessary condition for $g \geq 6$ is given by the following theorem

Theorem 2.2: A necessary condition to have $g \geq 6$ is $p_{j_1,l_1} \neq p_{j_2,l_1}$ for $j_1 \neq j_2$, and $p_{j_1,l_1} \neq p_{j_1,l_2}$ for $l_1 \neq l_2$.

Proof: The first part of the theorem directly follows from (3) and (4) with $i = 2$. For $g \geq 6$, Theorem 2.1 for rows 0 and j_1 and columns l_1 and l_2 in H becomes

$$\Delta_{0,j1}(l_1) + \Delta_{j1,0}(l_2) \neq 0 \mod p \tag{6}$$

with $\Delta_{0,j_1}(l_1) + \Delta_{j_1,0}(l_2) = -p_{j_1,l_1} + p_{j_1,l_2}$, which completes the proof.

A lower bound on the minimum value of p for which $g \geq 6$ is given by the following.

Corollary 2.2: A necessary condition to have $g \geq 6$ in the Tanner graph representation of a (J,L)-regular QC LDPC code is $p \geq L$, or $N \geq L^2$.

Theorem 2.2 and its corollary suggest that finding a (J,L)-regular QC LDPC code with $g \geq 6$ should not be necessarily difficult. Corollary 2.2 can be refined depending on whether L is odd or even as follows.

Theorem 2.3: A necessary condition to have $g \geq 6$ in the Tanner graph representation of a (J,L)-regular QC LDPC code is $p \geq L$, or $N \geq L^2$ if L is odd, and $p \geq L+1$, or $N \geq L(L+1)$ if L is even.

Proof: Assume $p = L$ and $g \geq 6$. Without loss of generality, we can choose $p_{0,l} = 0$ and $p_{1,l} = l$ in (1) for $0 \leq l \leq L-1$ based on Corollary 2.2. For $l > 0$, define e and o as the number of even and odd values $p_{1,l}$, respectively. If $L = p$ is even, then $e = p/2 - 1$ and $o = p/2$, so that $o - e = 1$.

We can choose $p_{2,0} = 0$ and, from Theorem 2.2, $p_{2,l_1} \neq p_{2,l_2}$ for $l_1 \neq l_2$. For $l > 0$, define o_1 and o_2 as the numbers of odd values $p_{1,l}$ corresponding to odd and even values $p_{2,l}$, respectively, so that $o_1 + o_2 = o$. Similarly, for $l > 0$, define e_1 and e_2 as the numbers of even values $p_{1,l}$ corresponding to odd and even values $p_{2,l}$, respectively, so that $e_1 + e_2 = e$. We also have $o_1 + e_1 = o$ and $o_2 + e_2 = e$, which implies $e_1 = o_2$ and $o_1 = e_2$.

If o_1 is odd, then e_2 is also odd. If e is even, then e_1 and, hence, o_2 are odd too, and o is even; else if e is odd, then e_1 and, hence, o_2 are even, and o is odd. Similarly, if o_1 is even, then e_2 is also even. If e is even, then e_1 and hence o_2 are even too, and so is o; else if e is odd, then e_1 and, hence, o_2 are odd, and so is o. As a result, in each case, e and o are either both odd or both even, which is impossible since $o - e = 1$. It follows that for L even, $p \geq L+1$, which completes the proof.

C. Girth $g \geq 8$

The previous approach is extended to the case $g \geq 8$.

Theorem 2.4: For $J \geq 3$ and $L \geq 3$, a necessary condition to have $g \geq 8$ is $p_{j_1,l_1} \neq p_{j_2,l_2}$ for $0 < j_1 < j_2$ and $0 < l_1 < l_2$.

Proof: Assume $p_{j_1,l_1} = p_{j_2,l_2}$, with $0 < j_1 < j_2$ and $0 < l_1 < l_2$, which requires $J \geq 3$ and $L \geq 3$, respectively. Then

$$\Delta_{j_1,j_2}(0) + \Delta_{j_2,0}(l_2) + \Delta_{0,j_1}(l_1) = 0 + p_{j_2,l_2} - p_{j_1,l_1} = 0.$$

Based on Theorem 2.1, this indexing defines a cycle of length 6 with respect to rows 0, j_1, and j_2 and columns 0, l_1, and l_2 of H, which contradicts $g \geq 8$.

A lower bound on the minimum value of p for which $g \geq 8$ is given by the following.

Corollary 2.3: A necessary condition to have $g \geq 8$ in the Tanner graph representation of a (J,L)-regular QC LDPC code is $p > (J-1)(L-1)$ or $N > (J-1)(L-1)L$.

D. Girth $g \geq 10$

The next theorem shows that a (J,L)-regular QC LDPC code necessarily has $g \leq 12$.

Theorem 2.5: For any (J,L)-regular QC LDPC code, we have $g \leq 12$.

Proof: For $J \geq 3$, this result directly follows from Theorem 2.1 with $j_1 = j_4$, $j_2 = j_5$, and $j_3 = j_6$, as well as $i_1 = i_3 = i_5$ and $i_2 = i_4 = i_6$. For $J = 2$, the result follows in a straightforward way from the equivalent expression of Theorem 2.1 with respect to H^t and row index differences, which completes the proof.

Theorem 2.5 generalizes the result of [16] to any (J,L)-regular QC LDPC code. Based on the distance bounds presented in [23], it importantly indicates that for a given code rate, the only way of increasing the guaranteed minimum Hamming distance of a QC LDPC code is to increase both J and L.

We finally note that Theorem 2.1 can be viewed as a simplified formulation of [15, Theorem 2] in the case of circulant permutation matrices. A formulation of some results derived in this section with the notations of [15] has been given in [24].

III. Families of QC LDPC Codes

A. Random Constructions

For given values of the code length N, the code dimension K, and the desired girth g, the most straightforward approach is to determine corresponding values of J, L, and p, and then randomly generate $(J-1)(L-1)$ integers until Theorem 2.1 is satisfied. For given values of J and L, the smallest value of p for which a (J,L)-regular QC LDPC

TABLE I
SMALLEST VALUE OF p FOR WHICH A (J, L)-REGULAR QC LDPC CODE WITH GIRTH $g \geq 6$ WAS FOUND WITH COMPUTER SEARCH

J \ L	4	5	6	7	8	9	10	11	12
3	5	5	7	7	9	9	11	11	13
4	-	5	7	7	9	*10*	11	11	13
5	-	-	7	7	9	*10*	11	11	13

TABLE II
SMALLEST VALUE OF p FOR WHICH A (J, L)-REGULAR QC LDPC CODE WITH GIRTH $g \geq 8$ WAS FOUND WITH COMPUTER SEARCH

J \ L	4	5	6	7	8	9	10	11	12
3	9	14	18	21	26	33	39	46	54

code with girth $g = 6$ and $g = 8$ was found with computer search are recorded in Tables I and II, respectively. Note that although the search for smaller values of p failed, there is no guarantee that such codes do not exist, except for the values of p which meet the lower bound of Theorem 2.3 or of Corollary 2.3. For $g = 6$, the optimum value was found in each case, except for $L = 9$ and $J \geq 4$ (represented in italics in Table I). As suggested from Theorem 2.3, we observe that the smallest values of p remain the same as J increases in Table I. For $g = 8$, none of the values recorded in Table II corresponds to the smallest possible value $p = (J-1)(L-1)+1$ given in Corollary 2.3. It should be noted that some of these values, as well as those for $g = 6$, $J = 5$, and $L \geq 8$ were found after relatively long computer searches, which suggests to search for structured values of $p_{j,l}$ in the matrix H of (1). Several such constructions are discussed in the next section.

B. Structured Constructions

In order to speed up the code search based on Theorem 2.1, a particular structure on the $(J-1)(L-1)$ integers necessary to specify the matrix H of (1) can be imposed. As a result, each structure determines a particular family of QC LDPC codes. In the following, examples of such families are given. These families generally correspond to previous works which are therefore now proposed within the same framework and often generalized.

1) Sum $p_{j,l} = j\,q_1 + l q_2 \bmod p$: In this case, we compute

$$\Delta_{j_1,j_2}(l) = (j_1 - j_2)q_1$$

so that $\Delta_{j_1,j_2}(l_1) + \Delta_{j_2,j_1}(l_2) = 0$. It follows from Theorem 2.1 that $g \leq 4$ for this construction.

2) Product $p_{j,l} = jl \bmod p$: For this family, we compute

$$\Delta_{j_1,j_2}(l) = (j_1 - j_2)l.$$

For $g \geq 6$, Theorem 2.1 becomes $(j_1 - j_2)(l_1 - l_2) \neq 0 \bmod p$ for all $j_1 \neq j_2$ and all $l_1 \neq l_2$. This condition is always satisfied for p prime, but depending on J and L, other values of p are also valid. For example, for $(J, L) = (3, 6)$ and $p \leq 15$, $p \in \{7, 9, 11, 12, 13, 14, 15\}$ is a valid choice, while for $J \geq 4, L = 6$, and $p \leq 15, p \in \{7, 11, 13, 14\}$ works. It is finally interesting to point out that this form defines array codes [15] and that for p prime and $J = L = p$, the $p^2 \times p^2$ matrix H of (1) defines the Euclidean geometry plane EG$(p, 2)$. For example, for $p = J = L = 5$, we obtain a 25×25 matrix H of rank 21 corresponding to EG$(5, 2)$.

For $g \geq 8$, Theorem 2.1 becomes

$$(j_1 - j_2)(l_1 - l_3) + (j_2 - j_3)(l_2 - l_3) \neq 0 \mod p.$$

This is impossible for $l_1 = j_3, l_2 = j_1$, and $l_3 = j_2$. It follows that $g \leq 6$ only with this construction.

3) Power $p_{j,l} = q_1^j q_2^l \bmod p$: It should first be noted that while the form $p_{j,l} = q_1^j q_2^l \bmod p$ is that used in [16], an equivalent representation which satisfies the form (1) is $p_{j,l} = (q_1^j - 1)(q_2^l - 1) \bmod p$. For this family, we compute

$$\Delta_{j_1,j_2}(l) = (q_1^{j_1} - q_1^{j_2})q_2^l$$

and after a little elementary algebra, (5) can be rewritten as

$$\sum_{k=0}^{m-2} (q_1^{j_k} - q_1^{j_{k+1}})(q_2^{l_k} - q_2^{l_{m-1}}) \neq 0 \mod p. \tag{7}$$

This equation can be satisfied for $g \leq 12$. In fact, this construction is a generalization of [16] in which p was chosen as a prime and q_1 and q_2 as two nonzero distinct elements of GF(p) with order $o_1 = J$ and $o_2 = L$, respectively. However, for p prime, only $o_1 \geq J$ and $o_2 \geq L$ is necessary to have $g \geq 6$. For example, for $p = 7$, $J = 3$, and $L = 5$, we can choose $q_1 \in \{2, 3, 4, 5\}$ and $q_2 \in \{3, 5\}$, not necessarily distinct. Note also that for this construction, we have $J \leq L \leq p - 1$. Finally, for $q_1 = q_2$, $g > 6$ is impossible as (7) is not satisfied for $l_0 = j_2, l_1 = j_0$, and $l_2 = j_1$.

Theorem 2.3 can be refined for this construction as follows.

Theorem 3.1: For $p_{j,l} = q_1^j q_2^l \bmod p$, a necessary condition to have $g \geq 6$ in the Tanner graph representation of a (J, L)-regular QC LDPC code is $p \geq L + 1$, and p prime.

Proof: For $l_1 \neq l_2$, $p_{j,l_1} \neq p_{j,l_2}$ is equivalent to

$$q_2^{l_1} \neq q_2^{l_2} \mod p. \tag{8}$$

For p prime, it follows $o_2 \geq L$ and since $o_2 \leq p-1$, we have $p \geq L+1$.

For this construction and given values of J and L, the smallest value of p for which a (J, L)-regular QC LDPC code with girth $g = 6$ and $g = 8$ was found with computer search are recorded in Tables III and IV, respectively. We observe that, in general, the values found are larger than those given in Tables I and II. By structuring the search, not only can much larger values of J and L be considered, but most importantly, the optimum values of p for this construction can be determined. For $g = 6$ (note that $g \geq 8$ for $L = 2$ based on Corollary 2.1), we observe that the optimum value of p given in Table III corresponds to that of Theorem 3.1. On the other hand, as already noted in [16], an analytical derivation of the optimum value of p for $g \geq 8$ seems quite difficult. This is further confirmed by the fact that the same value of p can be found for the same value of J and different values of L. We also notice that the optimum value of p does not have to be prime.

A (J, L)-regular LDPC code obtained by this construction can be extended to either a $(J+1, L)$-regular LDPC code, or a $(J, L+1)$-regular LDPC code by appending to H a row of L $I(0)$'s, or a column of J $I(0)$'s. Similarly, a $(J+1, L+1)$-regular LDPC code can be obtained by appending to H both a row of L $I(0)$'s and a column of J $I(0)$'s. Since $q_1^j q_2^l \neq 0$, and for p prime, $o_1 \geq J$ and $o_2 \geq L$, these extensions preserve $g = 6$ and can be applied to any code given in Table III.

In the preceding sections, the main motivation was to find the smallest value of p for which a (J, L)-regular QC LDPC code exists. However, the search can be conducted with additional constraints such as a large number of dependent check sums in the matrix H of (1).

IV. SEARCH AND SIMULATION RESULTS

Comparative error performance studies of LDPC codes constructed with various methods have been conducted for given values of N and K. For example, two QC LDPC codes with $N = 1053$, $K = 812$, $J = 3$, $L = 13$, $p = 81$, and $g = 6$ and 8, respectively, and one QC LDPC code with $N = 1062$, $K = 819$, $J = 4$, $L = 18$, $p = 59$, and $g = 6$ have been generated randomly based on Section III-A for $g = 6$ and $g = 8$, respectively, and compared in Fig. 1 to other LDPC codes with similar parameters. We notice that these codes slightly outperform their LDPC counterparts constructed from [1] with $J = 3$ and $L = 12$ or 13, and $J = 4$ and $L = 17$ or 18 [8]. They are easier to design,

TABLE III
SMALLEST VALUE OF p FOR WHICH A (J, L)-REGULAR QC LDPC CODE WITH GIRTH $g \geq 6$ WAS FOUND WITH COMPUTER SEARCH FOR THE CONSTRUCTION $p_{j,l} = q_1^j q_2^l \bmod p$

J \ L	3	4	5	6	7	8	9	10	11	12	13
2	5	5	7	7	11	11	11	11	13	13	17
3	5	5	7	7	11	11	11	11	13	13	17
4	-	5	7	7	11	11	11	11	13	13	17
5	-	-	7	7	11	11	11	11	13	13	17
6	-	-	-	7	11	11	11	11	13	13	17

TABLE IV
SMALLEST VALUE OF p FOR WHICH A (J, L)-REGULAR QC LDPC CODE WITH GIRTH $g \geq 8$ WAS FOUND WITH COMPUTER SEARCH FOR THE CONSTRUCTION $p_{j,l} = q_1^j q_2^l \bmod p$

J \ L	3	4	5	6	7	8	9	10	11	12	13
2	5	5	7	7	11	11	11	11	13	13	17
3	7	13	17	19	29	31	37	49	61	65	73
4	-	25	29	37	53	53	73	89	89	109	131
5	-	-	59	67	67	97	109	131	161	169	209

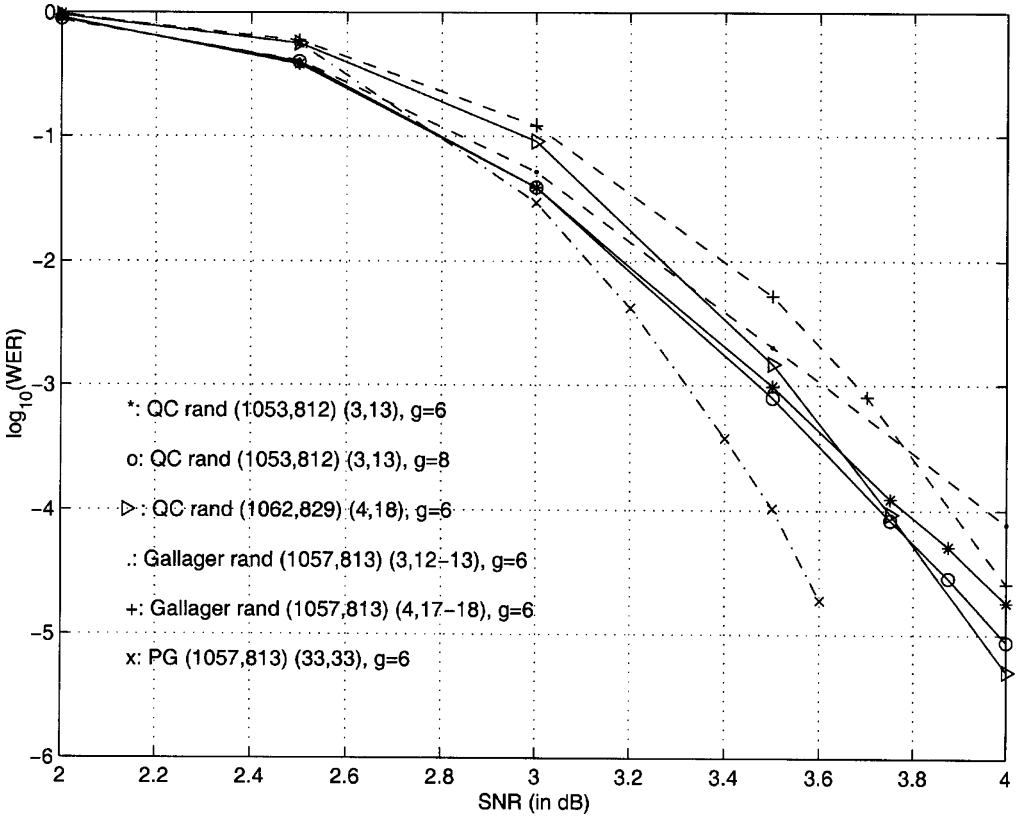

Fig. 1. BP decoding of different LDPC codes of about rate 0.77 and length 1050 (maximum of 200 iterations).

represent, and encode than random Gallager codes. We also notice that increasing g from 6 to 8 had little effect on the error performance. On the other hand, the QC LDPC codes do not perform as well as the $(1057, 813)$ projective geometry (PG) code for which $J = L = 33$ and the matrix H used for decoding has size 1057×1057. However, they have a much lower decoding complexity than the PG code. Note also that, in general, QC LDPC codes can be constructed in a more flexible manner than PG codes for given values of N and K. However, while the PG code has a minimum distance of 34, that guaranteed from the bounds of [23] for the three QC LDPC codes are much smaller.

In Fig. 2, a similar comparison has been represented for longer codes of lower rate. Based on Section III-A, two QC LDPC codes with $N = 4104$, $K = 2283$, $J = 4$, $L = 9$, $p = 456$, and $g = 6$ and 8, respectively, and one QC LDPC code with $N = 4104$, $K = 2287$, $J = 8$, $L = 18$, $p = 228$, and $g = 6$ have been generated randomly. A random $(4, 9)$-regular LDPC code with $N = 4104$ and $N = 2281$ and the $(4096, 2238)$ with $J = L = 16$ and $g = 8$ constructed in [12] (referred to as finite-geometry (FG) code in the figure) are also considered. For these longer codes, compared with that of the previous example, we observe that the three LDPC codes with $J = 4$, $L = 9$ have similar error performance. Hence, at the word error rates represented, increasing the girth has no great influence. These codes also outperform that of [12] constructed from finite geometry. We finally notice that the QC LDPC code with $J = 8$ performs quite poorly.

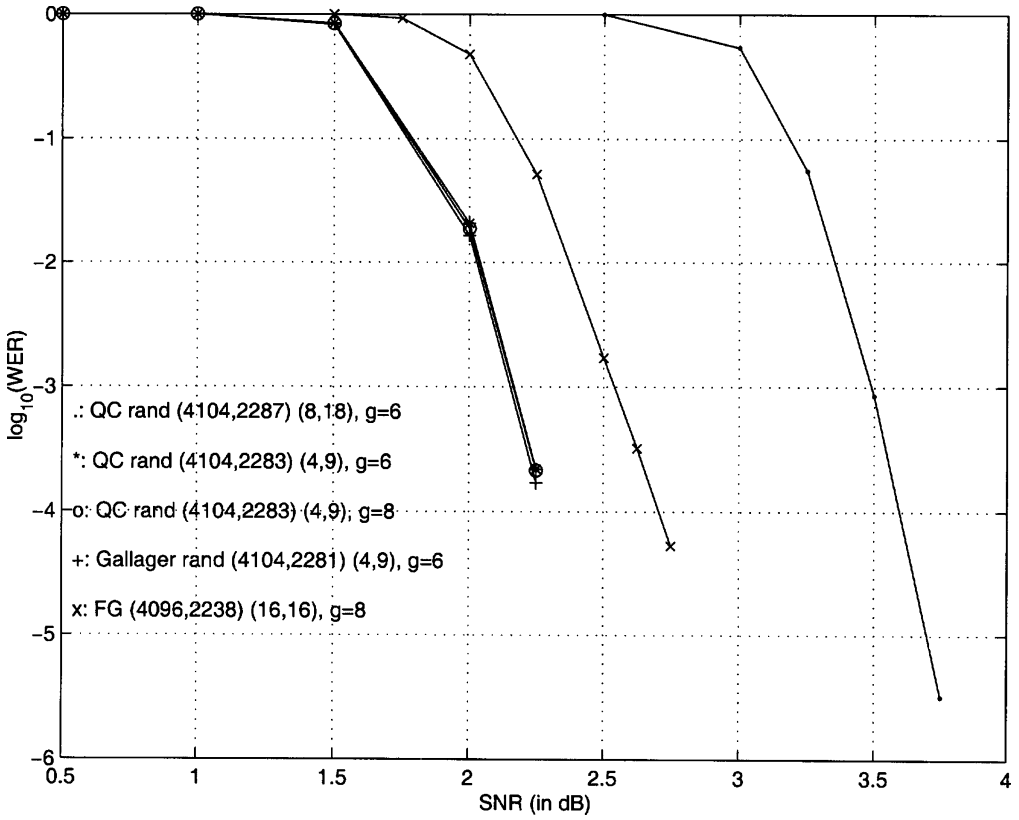

Fig. 2. BP decoding of different LDPC codes of about rate 0.55 and length 4100 (maximum of 200 iterations).

V. Minimum Distance of QC LDPC Codes

A result of [25] implies that the minimum Hamming distance d_H of a (J, L)-regular QC LDPC code is upper-bounded by $d_H \leq (J+1)!$. Consequently, for a (J, L)-regular QC LDPC code, d_H cannot grow with N, which suggests that QC LDPC codes compare favorably to random LDPC codes only for short to medium code lengths. Observations along the same lines were made in [16]. In the following, we derive for $(3, L)$-regular QC LDPC codes a necessary condition for $d_H = 24$. Extensions to larger values of J are then discussed.

A. $(3, L)$-Regular QC LDPC Codes

Let us consider four columns of the matrix H given in (1). With respect to Theorem 2.1, the indexes $p_{j,l}$ can be normalized $(\mathrm{mod}\ p)$ as

$$[H_0 H_1 H_2 H_3] = \begin{bmatrix} I(0) & I(0) & I(0) & I(0) \\ I(0) & I(i_1) & I(i_2) & I(i_3) \\ I(0) & I(j_1) & I(j_2) & I(j_3) \end{bmatrix}. \qquad (9)$$

In each $3p \times p$ submatrix H_k, $k = 0, \ldots, 3$, define l as the position of the lth column of H_k for $l = 0, \ldots, p-1$, and define S_k as a subset of column positions in H_k. Then it is readily seen that the following 24 columns sum to zero:

$$\begin{aligned} S_0 &= \{-i_2 - j_3, -i_1 - j_2, -i_3 - j_1, -i_3 - j_2, \\ &\qquad -i_1 - j_3, -i_2 - j_1\} \\ S_1 &= \{-i_2 - j_3, -j_2, -i_3, -i_3 - j_2, -j_3, -i_2\} \\ S_2 &= \{-i_1 - j_3, -j_1, -i_3, -i_3 - j_1, -j_3, -i_1\} \\ S_3 &= \{-i_2, -i_1 - j_2, -j_1, -j_2, -i_2 - j_1, -i_1\} \end{aligned}$$

where each value in each subset S_k is taken modulo-p. Note that for $k = 0, \ldots, 3$, S_k is composed of the negative sums of all pairs of elements (i_x, j_y) of (9) indexed by $x \neq y$, $x \neq k$, and $y \neq k$. A necessary condition for $d_H = 24$ is, therefore, that all six columns in each set S_i are distinct.

Considering the matrix H given in (1), this can be jointly achieved for all L columns of submatrices by the following procedure.

1. Construct the $L \times L$ table with the L columns and the L rows labeled by the indexes of the second row and of the third row of H in (1), respectively.
2. For all nondiagonal elements of the table, insert the modulo-p sum of the corresponding row and column labels.
3. For any three distinct values x, y, and z in $\{0, \ldots, L-1\}$, check that no two of the six nondiagonal elements in the xth, yth, and zth rows and columns of the table are the same.

Note that any pair of similar indexes found at step-(3) decreases the designed distance by two.

Example: Consider a $(3, 5)$-regular code of length 155 and dimension 64 obtained with $p = 31$ and represented by the matrix

$$H = \begin{bmatrix} I(0) & I(0) & I(0) & I(0) & I(0) \\ I(0) & I(4) & I(24) & I(1) & I(5) \\ I(0) & I(12) & I(10) & I(3) & I(15) \end{bmatrix}. \qquad (10)$$

The corresponding table is depicted in Table V. Since 15 appears twice when considering the zeroth, second, and fourth rows and columns, and 8 appears twice when considering the seond, third, and fouth rows and columns, we obtain $d_H \leq 20$. We also notice that 5 appears twice in Table V, but not in the same three row and column positions.

TABLE V
THE (3,5)-REGULAR (155,64) QC LDPC CODE REPRESENTED BY (10)

	0	4	24	1	5
0	-	4	24	1	5
12	12	-	5	13	17
10	10	14	-	11	15
3	3	7	27	-	8
15	15	19	8	16	-

If we consider now the $(3, 5)$-regular code of the same length and dimension constructed in [16] as described in Section III-B3 for $q_1 = 5$, $q_2 = 2$, and $p = 31$, its matrix H is given by

$$H = \begin{bmatrix} I(0) & I(0) & I(0) & I(0) & I(0) \\ I(0) & I(4) & I(12) & I(28) & I(29) \\ I(0) & I(24) & I(10) & I(13) & I(19) \end{bmatrix}. \quad (11)$$

Although $d_H = 20$ for this code [16], no two elements are the same in the table obtained by the proposed procedure. This confirms that this method only represents a necessary condition for $d_H = 24$.

We finally mention that Theorem 2.3 can be further refined in order to have $d_H = 24$. For example, it is readily verified by contradiction that all nonzero values in (9) have to be distinct, which implies $p \geq 2(L-1)+1$ for $(3, L)$-regular QC LDPC codes with $d_H = 24$. Further consideration of this interesting problem is beyond the scope of this correspondence.

B. (J, L)-Regular QC LDPC Codes

The results derived in Section V-A can be extended to any (J, L)-regular QC LDPC code but the procedure becomes quite tedious as $(J+1)!$ columns have to be identified. However, this can be achieved by considering $J+1$ submatrices H_k of size $Jp \times p$ in (9). Each of the $J+1$ corresponding sets S_k is then composed of all $J!$ possible negative sums indexed on $\{0, \ldots, J\} \backslash \{k\}$.

VI. CONCLUSION

In this correspondence, a simple necessary and sufficient condition to determine QC LDPC codes with a given girth has been derived. This condition implies that such codes cannot have a girth larger than 12. Consequently, for a given code rate, their minimum distance cannot be increased by increasing the code length and thus, the girth as for random constructions. In fact, an upper bound on the minimum Hamming distance of QC LDPC codes was derived in [25], and a necessary condition to reach this bound has been proposed.

These simple results suggest that when constructing families of LDPC codes, either relatively large girth (i.e., $g > 12$), or additional constraints such as large minimum distance, a large number of redundant check sums, or appropriate coset weight distribution (see [26]) have to be considered.

ACKNOWLEDGMENT

The author wishes to thank the two reviewers for their constructive comments which greatly improve the presentation of these results, and Norifumi Kamiya for interesting discussions.

REFERENCES

[1] D. J. C. MacKay, "Good error-correcting codes based on very sparse matrices," *IEEE Trans. Inform. Theory*, vol. 45, pp. 399–431, Mar. 1999.
[2] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, "Design of capacity-approaching irregular low-density parity check codes," *IEEE Trans. Inform. Theory*, vol. 47, pp. 619–637, Feb. 2001.
[3] M. G. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, "Improved low-density parity check codes using irregular graphs," *IEEE Trans. Inform. Theory*, vol. 47, pp. 585–598, Feb. 2001.
[4] S. Y. Chung, G. D. Forney, T. J. Richardson, and R. L. Urbanke, "On the design of low-density parity check codes within 0.0045 dB of the Shannon limit," *IEEE Commun. Lett.*, vol. 5, pp. 58–60, Feb. 2001.
[5] X.-Y. Hu, "Low-delay low-complexity error correcting codes on sparse graphs," Doctoral dissertation, Swiss Federal Institute of Technology Lausanne (EPFL), Lausanne, Switzerland, 2002.
[6] X.-Y. Hu, E. Eleftheriou, and D.-M. Arnold, "Irregular progressive-edge growth (PEG) Tanner graphs," in *Proc. IEEE Int. Symp. Information Theory*, Lausanne, Switzerland, July 2002, p. 480.
[7] P. O. Vontobel and H. A. Loeliger, "Irregular codes from regular graphs," in *Proc. IEEE Int. Symp. Information Theory*, Lausanne, Switzerland, July 2002, p. 284.
[8] R. Lucas, M. Fossorier, Y. Kou, and S. Lin, "Iterative decoding of one-step majority logic decodable codes based on belief propagation," *IEEE Trans. Commun.*, vol. 48, pp. 931–937, June 2000.
[9] Y. Kou, S. Lin, and M. Fossorier, "Low-density parity-check codes based on finite geometries: A Rediscovery and new results," *IEEE Trans. Inform. Theory*, vol. 47, pp. 2711–2736, Nov. 2001.
[10] P. O. Vontobel and R. M. Tanner, "Construction of codes based on finite generalized quadrangles for iterative decoding," in *Proc. IEEE Int. Symp. Information Theory*, Washington, DC, June 2001, p. 223.
[11] S. J. Johnson and S. R. Weller, "Codes for iterative decoding from partial geometries," in *Proc. IEEE Int. Symp. InformationTheory*, Lausanne, Switzerland, July 2002, p. 310.
[12] J. L. Kim, U. N. Peled, I. Perepelitsa, and V. Pless, "Explicit construction of families of LDPC codes with girth at least six," in *Proc. 40th Annu. Allerton Conf. Communication, Control and Computing*, Monticello, IL, 2002.
[13] R. G. Gallager, *Low-Density Parity-Check Codes*. Cambridge, MA: MIT. Press, 1963.
[14] R. Townsend and E. J. Weldon, "Self orthogonal quasicyclic codes," *IEEE Trans. Inform. Theory*, vol. IT-13, pp. 183–195, Mar. 1967.
[15] J. L. Fan, "Array codes as low-density parity-check codes," in *Proc. 2nd Int. Symp. Turbo Codes*, Brest, France, Sept. 2000, pp. 545–546.
[16] R. M. Tanner, D. Sridhara, and T. Fuja, "A class of group-structured LDPC codes," in *Proc. ISTA*, Ambleside, England, 2001.
[17] B. Vasic, "Combinatorial constructions of low-density parity check codes for iterative decoding," in *Proc. IEEE Int. Symp. Information Theory*, Lausanne, Switzerland, July 2002, p. 312.
[18] T. Mittleholzer, "Efficient encoding and minimum distance bounds of Reed-Solomon-type array codes," in *Proc. IEEE Int. Symp. Information Theory*, Lausanne, Switzerland, July 2002, p. 282.
[19] 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, pp. 317–319, July 2003.
[20] T. Okamura, "Designing LDPC codes using cyclic shifts," in *Proc. IEEE Int. Symp. Information Theory*, Yokohama, Japan, June/July 2003, p. 151.
[21] J. Denes and A. D. Keedwell, *Latin Squares and their Applications*. New York: Academic Press, 1974.
[22] W. W. Peterson and E. J. Weldon Jr, *Error-Correcting Codes*, 2nd ed. Cambridge, MA: MIT Press, 1972.
[23] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 533–547, Sept. 1981.
[24] N. Kamiya, "Recent results on the girth of a block matrix consisting of permutations," Mitsubishi , Kanagawa, Japan, Tech. Rep., 2003.
[25] D. J. C. MacKay and M. Davey, "Evaluation of Gallager codes for short block length and high rate applications," in *Proc. IMA Workshop Codes, Systems and Graphical Models*, 1999.
[26] D. J. C. MacKay and M. S. Postol, "Weaknesses of Margulis and Ramanujan-Margulis low-density parity-check codes," *Electron. Notes in Theor. Comput. Sci.*, vol. 74, 2003.