Explicit constructions of Type-II QC LDPC codes with girth at least 6

Lally, Kristine

Lally. (2007). Explicit constructions of Type-II QC LDPC codes with girth at least 6. Proceedings of the 2007 International Symposium on Information Theory, 2371–2375. https://doi.org/10.1109/ISIT.2007.4557574

Published Version: https://doi.org/10.1109/ISIT.2007.4557574

Explicit Construction of Type-II QC LDPC Codes with Girth at least 6

Kristine Lally
Department of Mathematics and Statistics
RMIT University
Melbourne, Australia
email: kristine.lally@rmit.edu.au

Abstract— **Type-II quasi-cyclic (QC) LDPC codes are constructed from combinations of weight-0, weight-1 and weight-2 circulant matrices. The structure of cycles of length $2n$ are investigated, and necessary and sufficient conditions for a type-II QC LDPC parity check matrix H to have girth at least $2(n+1)$ are given. An explicit construction of type-II codes which guarantees girth at least 6 is presented. A necessary and sufficient condition for a QC matrix with one or more rows of circulants, to be fullrank is derived.**

I. Introduction

A QC LDPC code of index L and length $N = pL$ over $\mathbb{F}_2$ can be constructed as the nullspace of a low density parity check matrix H which consist of J rows of $p \times p$ circulant submatrices. Each circulant can be specified by the polynomial corresponding to its top-row vector, and in this way the code can be viewed as an R-submodule of R^L where $R = \mathbb{F}_2[x]/I$ and $I = \langle x^p - 1 \rangle$. QC LDPC codes are known to have a very efficient encoding algorithm [1] and due to their compact representation have low storage requirements.

Type-I (where each circulant corresponds to a polynomial of weight at most 1) and type-II (where each circulant corresponds to a polynomial of weight at most 2) classes of binary QC LDPC codes are defined in [2]. The special case of (J, L)-regular type-I QC LDPC codes where H comprises of all monomial entries (that is, circulant permutation matrices) was studied in detail by Fossorier in [3]. Special cases of these codes were introduced in [4], [5], amongst others. Using circulants with higher weight has been shown in [2] to allow higher minimum distances to be achieved than one could obtain with monomial entries alone. For small to medium block lengths, type-II QC LDPC codes have been shown to compare favorably, under the sum-product iterative decoding algorithm, to randomly constructed LDPC codes, [2], [6].

Here we further study the type-II class, and note that type-I is a subclass of type-II. It is well-known (e.g. see [6]) that trinomial and higher weight circulants lead to girth at most 6 and are not considered here. We show that type-II codes can be employed to achieve a wider range of rates and minimum distances, even while maintaining (J, L)-regularity, than type-I codes. Similar to the work presented in [3], we give a comprehensive formulation of the structure of cycles of length $2n, n \geq 2$, and give necessary and sufficient conditions for a type-II QC LDPC parity check matrix to have girth at least $2(n+1)$. These necessary and sufficient conditions can be exhaustively checked to establish the girth of a given code. Equivalent conditions were given in [7] which depend on the computation of A^n, a power of the adjacency matrix. A complex sufficient condition for a more general class of codes was also given in [6, Prop. 4.1]. Here our simplified formulation for the special case of type-II QC LDPC codes depends only on the entries of H itself, and allows us to enumerate all equations governing when cycles of length 4 occur. We then provide a explicit construction of type-II codes (of any regular or irregular weight configuration that exists within a $J \times L$ array) which guarantees girth at least 6. Our construction method does not involve algorithmic checking of randomly selected values for desirable girth, as the construction techniques described in [6] and [7] involve. Here, no computer search is required, as the matrix entries are pre-specified by formulae, within any chosen weight configuration. In this way our explicit construction defines a structured class of QC LDPC codes with high girth.

In the final section we give a necessary and sufficient condition for a QC parity check matrix H with one or more rows of circulants to be fullrank. This condition can be read directly from the choice of polynomials specifying the circulants. We show that fullrank binary QC matrices with non-uniform weight configurations, can be easily constructed from a judicious choice of polynomial entries. Fullrank parity check matrices have no redundant parity check equations and thus the code achieves 'design rate' $1 - J/L$.

II. Structure of Type-II QC LDPC Codes

The parity check matrix H of a type-II QC LDPC code C of length $N = pL$ has the form (1) where $J \leq L$ and $I\left(p_{j,l}^{(i)}\right), 0 \leq j \leq J-1, 0 \leq l \leq L-1, i \in \{1,2\}$, is either the $p \times p$ zero matrix $\mathbf{0}$, or represents the circulant permutation matrix obtained by right-cyclically shifting each row of the $p \times p$ identity matrix by $p_{j,l}^{(i)} \in \{0, 1, \ldots, p-1\}$ places. If $I\left(p_{j,l}^{(i)}\right) = \mathbf{0}$ then we say that the value $p_{j,l}^{(i)}$ is undefined. When $p_{j,l}^{(i)} = 0$ the circulant $I(0)$ is the identity matrix I_p. By convention, we take $p_{j,l}^{(1)}$ to indicate the position of the left-most 1 in the top row of any non-zero circulant entry

1-4244-1429-6/07/$25.00 ©2007 IEEE

$$H = \begin{bmatrix} I\left(p_{0,0}^{(1)}\right)+I\left(p_{0,0}^{(2)}\right) & I\left(p_{0,1}^{(1)}\right)+I\left(p_{0,1}^{(2)}\right) & \cdots & I\left(p_{0,L-1}^{(1)}\right)+I\left(p_{0,L-1}^{(2)}\right) \\ I\left(p_{1,0}^{(1)}\right)+I\left(p_{1,0}^{(2)}\right) & I\left(p_{1,1}^{(1)}\right)+I\left(p_{1,1}^{(2)}\right) & \cdots & I\left(p_{1,L-1}^{(1)}\right)+I\left(p_{1,L-1}^{(2)}\right) \\ \vdots & \vdots & \ddots & \vdots \\ I\left(p_{J-1,0}^{(1)}\right)+I\left(p_{J-1,0}^{(2)}\right) & I\left(p_{J-1,1}^{(1)}\right)+I\left(p_{J-1,1}^{(2)}\right) & \cdots & I\left(p_{J-1,L-1}^{(1)}\right)+I\left(p_{J-1,L-1}^{(2)}\right) \end{bmatrix} \qquad (1)$$

of H. It follows that each entry h_{jl} of H takes one of the following forms: the weight-0 circulant $\mathbf{0}$, the weight-1 circulant $I\left(p_{j,l}^{(1)}\right)$ or the weight-2 circulant $I\left(p_{j,l}^{(1)}\right)+I\left(p_{j,l}^{(2)}\right)$, with $p_{j,l}^{(1)} < p_{j,l}^{(2)}$. In polynomial notation, each circulant entry corresponds to a polynomial $h_{jl}(x) \in \mathbb{F}_2[x]$, of degree at most $p-1$, and can have the form: the 0 polynomial, the monomial $x^{p_{j,l}^{(1)}}$ or the binomial $x^{p_{j,l}^{(1)}}+x^{p_{j,l}^{(2)}}$. Let $A_{\text{wt}} = [a_{jl}]_{J\times L}$, where $a_{jl} = wt(h_{jl}(x))$, be the (hamming) weight configuration matrix corresponding to H, as defined in [2]. We note that the matrix H does not necessarily define a regular LDPC code, as H can have any non-negative row or column weight up to $2L$ or $2J$ respectively, depending on the number and position of the zero, monomial or binomial entries in H. The code C is a $(2J, 2L)$-regular type-II QC LDPC code if and only if all entries in H are binomial, that is, weight-2 circulants. The special case of (J, L)-regular type-I QC LDPC codes where H comprises of all monomial entries was studied in [3].

A. Rate

From [3], [4] it is known that the parity check matrix of a (J, L)-regular type-I QC LDPC code with $J \geq 2$ has rank at most $pJ-(J-1)$. Similarly it can be easily seen that the parity check matrix of a $(2J, 2L)$-regular type-II QC LDPC code has rank at most $pJ-J$, since the p binary rows within each row of circulants in H sum to the all-zero row, and so the code C has rate at least $\frac{pL-(pJ-J)}{pL} = 1-\frac{J(p-1)}{Lp}$. However many type-II codes with non-uniform weight configurations (even while maintaining regularity) can facilitate a wider range of rates within a given $J \times L$ array. For example, consider the $(3,4)$-regular QC LDPC type-II code with weight configuration

$$A_{wt} = \begin{bmatrix} 2 & 0 & 1 & 1 \\ 1 & 2 & 0 & 1 \\ 0 & 1 & 2 & 1 \end{bmatrix}. \qquad (2)$$

No subset of rows in this weight configuration sum to the all-zero vector modulo 2. It is therefore possible for a parity check matrix H with this weight configuration to have fullrank pJ and thus for the code to achieve ‘design rate’ $1-J/L$.

B. Minimum Distance

A (J, L)-regular type-I QC LDPC code has minimum distance upper bounded by $d_{\min} \leq (J+1)!$, [2], [8]. As described in [2], higher minimum distances within a given $J \times L$ array can be achieved by constructing type-II codes, even while the (J, L)-regularity is maintained. In general, for a given value of J, employing weight configurations with many higher weight entries allow higher minimum distances to be obtained.

Proposition 1: A type-II QC LDPC code has minimum distance upper bounded by $d_{\min} \leq (J+1)!2^J$.

We further observe that the value of p also determines an upper bound on the minimum distance of our code. A (J, L)-regular type-I QC LDPC has $d_{\min} \leq 2p$, since the $2p$ binary columns within any 2 columns of circulants in H sum to the all-zero column. Similarly a $(2J, 2L)$-regular type-II QC LDPC code has $d_{\min} \leq p$, since the p binary columns within any single column of circulants sum to the all-zero column, as each circulant is weight-2. More generally, if t is the smallest number of columns in the weight configuration matrix A_{wt} which sum to 0 modulo 2, then C has $d_{\min} \leq tp$. It follows that we should choose the value of p to be large, not only to ensure a low density of 1s, but also to enable large minimum distances. Furthermore a non-uniform weight configuration (even when (J, L)-regularity is maintained) can often allow higher minimum distances for a given value of p.

Example 2: A $(3,4)$-regular QC LDPC type-II code with weight configuration given by (2), has no less than 3 columns which sum to 0 modulo 2. Therefore $d_{\min} \leq 3p$.

III. Analysis of Girth

Using a similar notation to that developed in [3], a cycle of length $2n, n \geq 2$, in H can be represented by an ordered sequence of non-zero circulant permutation matrices

$$I\left(p_{j_0,l_0}^{(i_0)}\right), I\left(p_{j_1,l_0}^{(i_1)}\right), I\left(p_{j_1,l_1}^{(i_2)}\right), I\left(p_{j_2,l_1}^{(i_3)}\right), \\ \ldots, I\left(p_{j_{n-1},l_{n-1}}^{(i_{2n-2})}\right), I\left(p_{j_n,l_{n-1}}^{(i_{2n-1})}\right), I\left(p_{j_n,l_n}^{(i_{2n})}\right) \qquad (3)$$

with $0 \leq k \leq n, 0 \leq j_k \leq J-1, 0 \leq l_k \leq L-1$, and $i_{2k}, i_{2k+1} \in \{1,2\}$, where $j_n = j_0, l_n = l_0, i_{2n} = i_0$. Given that the circulant entries of H can have up to two 1s in each row and column, it is possible for two consecutive positions in a cycle to belong to the same circulant, and thus, unlike the type-I scenario, we can have $j_k = j_{k+1}$ and $l_k = l_{k+1}$. However, since positions in a cycle are all distinct (except first and last), if $j_k = j_{k+1}$ in our sequence, then then we must have $i_{2k} \neq i_{2k+1}$, and similarly if $l_k = l_{k+1}$ then we must have $i_{2k+1} \neq i_{2k+2}$. In particular when completing the cycle, if $l_{n-1} = l_n = l_0$ then $i_{2n-1} \neq i_{2n} = i_0$.

Defining

$$\Delta_{j_k,j_{k+1}}^{i_{2k},i_{2k+1}}(l_k) = p_{j_k,l_k}^{(i_{2k})} - p_{j_{k+1},l_k}^{(i_{2k+1})},$$

the matrix H contains a cycle of length $2n, n \geq 2$, if and only if a sequence of non-zero circulants, given by (3), exists in H which satisfies

$$\sum_{k=0}^{n-1} \Delta_{j_k,j_{k+1}}^{i_{2k},i_{2k+1}}(l_k) = 0 \bmod p$$

where $j_n = j_0$, $i_{2k} \neq i_{2k+1}$ whenever $j_k = j_{k+1}$, and $i_{2k+1} \neq i_{2k+2}$ whenever $l_k = l_{k+1}$.

Theorem 3: A necessary and sufficient condition for the Tanner graph representation of the matrix H to have girth at least $2(n+1)$ is

$$\sum_{k=0}^{m-1} \Delta_{j_k,j_{k+1}}^{i_{2k},i_{2k+1}}(l_k) \neq 0 \bmod p$$

for all $m, 2 \leq m \leq n$, all $j_k, 0 \leq j_k \leq J-1$, all $j_{k+1}, 0 \leq j_{k+1} \leq J-1$, all $l_k, 0 \leq l_k \leq L-1$, all $i_{2k}, i_{2k+1} \in \{1,2\}$, for which $p_{j_k,l_k}^{(i_{2k})}$ and $p_{j_{k+1},l_k}^{(i_{2k+1})}$ are defined, with $j_m = j_0, l_m = l_0, i_{2m} = i_0$, $i_{2k} \neq i_{2k+1}$ whenever $j_k = j_{k+1}$, and $i_{2k+1} \neq i_{2k+2}$ whenever $l_k = l_{k+1}$.

Corollary 4: If the matrix H contains a binomial entry, that is, a $p \times p$ weight-2 circulant, then it has girth at most $2p$.

Proof: The difference $p_{j,l}^{(1)} - p_{j,l}^{(2)}$ added to itself p times specifies a $2p$-cycle. ■

Corollary 5: If the matrix H contains a 2×2 submatrix with a $p \times p$ circulant of at least weight-1 in each position, then it has girth at most $4p$.

Proof: The sum $p_{j_0,l_0}^{(1)} - p_{j_1,l_0}^{(1)} + p_{j_1,l_1}^{(1)} - p_{j_0,l_1}^{(1)}$ added to itself p times specifies a $4p$-cycle. ■

It follows that we should choose the value of p to be large enough to allow girth to be high. A QC LDPC matrix H with more than one binomial entry in a row or column has girth $g \leq 8$, since an 8-cycle exists in every weight $(2,2)$ or $(2,2)^T$ submatrix of H, [6].

IV. Girth $g \geq 6$

A 4-cycle can be represented as a sequence of non-zero circulants

$$I\left(p_{j_0,l_0}^{(i_0)}\right), I\left(p_{j_1,l_0}^{(i_1)}\right), I\left(p_{j_1,l_1}^{(i_2)}\right), I\left(p_{j_0,l_1}^{(i_3)}\right), I\left(p_{j_0,l_0}^{(i_0)}\right)$$

with $0 \leq k \leq 2, 0 \leq j_k \leq J-1, 0 \leq l_k \leq L-1, i_{2k}, i_{2k+1} \in \{1,2\}$, $j_2 = j_0, l_2 = l_0, i_4 = i_0$, $i_{2k} \neq i_{2k+1}$ whenever $j_k = j_{k+1}$, and $i_{2k+1} \neq i_{2k+2}$ whenever $l_k = l_{k+1}$, which satisfies

$$\begin{aligned} &\Delta_{j_0,j_1}^{i_0,i_1}(l_0) + \Delta_{j_1,j_0}^{i_2,i_3}(l_1) \\ &= p_{j_0,l_0}^{(i_0)} - p_{j_1,l_0}^{(i_1)} + p_{j_1,l_1}^{(i_2)} - p_{j_0,l_1}^{(i_3)} = 0 \bmod p. \end{aligned}$$

It follows that a 4-cycle can only occur in one of the following ways:

1) When $j_0 = j_1$ and $l_0 = l_1$, in a single weight-2 circulant, that is, a 1×1 submatrix of H with a binomial entry, which satisfies $p_{j_0,l_0}^{(1)} - p_{j_0,l_0}^{(2)} + p_{j_0,l_0}^{(1)} - p_{j_0,l_0}^{(2)} = 0 \bmod p$,
2) When $j_0 = j_1$ and $l_0 \neq l_1$, in a 1×2 submatrix of H with weight configuration $[2,2]$, which satisfies $p_{j_0,l_0}^{(1)} - p_{j_0,l_0}^{(2)} \pm \left(p_{j_0,l_1}^{(1)} - p_{j_0,l_1}^{(2)}\right) = 0 \bmod p$,
3) When $l_0 = l_1$ and $j_0 \neq j_1$, in a 2×1 submatrix of H with weight configuration $[2,2]^T$, which satisfies $p_{j_0,l_0}^{(1)} - p_{j_0,l_0}^{(2)} \pm \left(p_{j_1,l_0}^{(1)} - p_{j_1,l_0}^{(2)}\right) = 0 \bmod p$,
4) When $j_0 \neq j_1$ and $l_0 \neq l_1$, in a 2×2 submatrix of H with at least weight-1 entry in each position, which satisfies any one of the following 16 equalities:

$$p_{j_0,l_0}^{(i_0)} - p_{j_1,l_0}^{(i_1)} + p_{j_1,l_1}^{(i_2)} - p_{j_0,l_1}^{(i_3)} = 0 \bmod p,$$

with $i_t \in \{1,2\}, 0 \leq t \leq 3$.

Let $d_{j,l} = p_{j,l}^{(2)} - p_{j,l}^{(1)}$ when both values $p_{j,l}^{(2)}$ and $p_{j,l}^{(1)}$ are defined. We recall that $p_{j,l}^{(1)} < p_{j,l}^{(2)}$, and so $d_{j,l}$ is always a positive integer. We consider the value $d_{j,l}$ in a weight-0 or weight-1 entry to be undefined. We now give the following necessary and sufficient conditions for a type-II QC LDPC matrix H to have girth at least 6.

Theorem 6: The Tanner graph representation of the matrix H given in (1) has girth at least 6 if and only if, for all $j_0, j_1, 0 \leq j_0 \neq j_1 \leq J-1$,all $l_0, l_1, 0 \leq l_0 \neq l_1 \leq L-1$, all $i_t \in \{1,2\}, 0 \leq t \leq 3$, each of the following inequalities holds true,

(i) $d_{j_0,l_0} \neq -d_{j_0,l_0} \bmod p$
(ii) $d_{j_0,l_0} \neq \pm d_{j_0,l_1} \bmod p$
(iii) $d_{j_0,l_0} \neq \pm d_{j_1,l_0} \bmod p$
(iv) $p_{j_0,l_0}^{(i_0)} - p_{j_1,l_0}^{(i_1)} \neq p_{j_0,l_1}^{(i_2)} - p_{j_1,l_1}^{(i_3)} \bmod p$,

whenever all values in an inequality are defined.

Given any type-II QC LDPC matrix we can exhaustively check the above conditions to determine if girth is at least 6. We note that if more lower weight entries are present in H then fewer such equations are defined, and thus fewer conditions need to be satisfied.

Corollary 7: A necessary condition for a regular $(2J, 2L)$ type-II QC LDPC matrix H to have girth $g \geq 6$ is $p > 2L$.

Proof: In any row j, the set of all $d_{j,l}$ and $-d_{j,l} \bmod p, l = 0, \ldots, L-1$, must be distinct positive integers in $\mathbb{Z}_p^*$. ■

If H has girth at least 6 then we can employ well-known lower bounds on minimum distance [1]. If H (regular or irregular) has at least weight $J' \leq 2J$ in each column, and girth $g \geq 6$, then the code has $d_{\min} \geq J' + 1$. In this case, more high weight entries in each column of H ensures higher minimum distance.

A. Explicit Construction with Girth $g \geq 6$

We now present a method of constructing a parity check matrix H for a type-II QC LDPC code of length pL, with any regular or irregular weight configuration that exists in a $J \times L$ array, which guarantees girth $g \geq 6$. We start by outlining the construction for a $(2J, 2L)$-regular (that is, one with all binomial entries) type-II QC LDPC code. We then describe how this construction technique can be easily modified to obtain any regular or irregular type-II QC LDPC code, which also guarantees girth $g \geq 6$. Restrictions on the value of p apply in each case.

Suppose all entries in H are binomial circulants, that is, both $I\left(p_{j,l}^{(1)}\right)$ and $I\left(p_{j,l}^{(2)}\right)$ are non-zero and distinct circulants, for all $j, 0 \leq j \leq J-1$, and all $l, 0 \leq l \leq L-1$. In the first row, $j = 0$, we choose $d_{0,l}, l = 0, \ldots, L-1$, be to a sequence of L distinct positive integers. For each $j = 1, \ldots, J-1$, we let $d_{j,l}, l = 0, \ldots, L-1$, be a permutation of $d_{0,l}, l = 0, \ldots, L-1$, such that $d_{j_0,l} \neq d_{j_1,l}$ when $j_0 \neq j_1$. For example, this can be easily achieved by setting $d_{j,l}$ to be the $(j+1, l+1)$-element of a Latin square of size L. Let $d = \max_{0 \leq l \leq L-1} \{d_{0,l}\}$.

$$H(x)=\left[\begin{array}{cccc} x^{a_0}\left(1+x^{d_{0,0}}\right) & x^{a_1}\left(1+x^{d_{0,1}}\right) & \cdots & x^{a_{L-1}}\left(1+x^{d_{0,L-1}}\right) \\ x^{a_0}\left(1+x^{d_{1,0}}\right) & x^{a_1+\ell}\left(1+x^{d_{1,1}}\right) & \cdots & x^{a_{L-1}+(L-1)\ell}\left(1+x^{d_{1,L-1}}\right) \\ \vdots & \vdots & \ddots & \vdots \\ x^{a_0}\left(1+x^{d_{J-1,0}}\right) & x^{a_1+(J-1)\ell}\left(1+x^{d_{J-1,1}}\right) & \cdots & x^{a_{L-1}+(J-1)(L-1)\ell}\left(1+x^{d_{J-1,L-1}}\right) \end{array}\right] \qquad (4)$$

Choosing $p > 2d$ then ensures that all inequalities defined in parts (i)-(iii) of Theorem 6 hold true.

We now consider inequalities defined in part (iv). Without loss of generality, we can take $j_0 < j_1$ and $l_0 < l_1$. The 2×2 submatrix of H specified by these rows and columns has the form

$$\left[\begin{array}{cc} I\left(p_{j_0,l_0}^{(1)}\right)+I\left(p_{j_0,l_0}^{(2)}\right) & I\left(p_{j_0,l_1}^{(1)}\right)+I\left(p_{j_0,l_1}^{(2)}\right) \\ I\left(p_{j_1,l_0}^{(1)}\right)+I\left(p_{j_1,l_0}^{(2)}\right) & I\left(p_{j_1,l_1}^{(1)}\right)+I\left(p_{j_1,l_1}^{(2)}\right) \end{array}\right].$$

Let $p_{j_0,l_0}^{(1)}$ and $p_{j_0,l_1}^{(1)}$ be some non-negative integers. We will choose $p_{j_1,l_0}^{(1)}$ and $p_{j_1,l_1}^{(1)}$ in such a way that $m_{j_0,j_1}^{l_k} = p_{j_1,l_k}^{(1)} - p_{j_0,l_k}^{(1)}, k = 0,1$, are positive values, and $m_{j_0,j_1}^{l_1} > m_{j_0,j_1}^{l_0}$. The 16 inequalities in part (iv) of Theorem 6 hold true if and only if

$$\begin{aligned} m_{j_0,j_1}^{l_1} - m_{j_0,j_1}^{l_0} \notin \{0, d_{j_1,l_0}, -d_{j_0,l_0}, d_{j_1,l_0} - d_{j_0,l_0}\} \\ +\{0, -d_{j_1,l_1}, +d_{j_0,l_1}, -d_{j_1,l_1} + d_{j_0,l_1}\} \bmod p. \end{aligned} \qquad (5)$$

Since all the $d_{j,l}$ are positive integers and $p > 2d$, the elements in the above set range from $-d_{j_0,l_0} - d_{j_1,l_1} \geq -2d \bmod p$ to $d_{j_1,l_0} + d_{j_0,l_1} \leq 2d \bmod p$. If we choose $m_{j_0,j_1}^{l_1} - m_{j_0,j_1}^{l_0}$ and p large enough so that

$$2d < m_{j_0,j_1}^{l_1} - m_{j_0,j_1}^{l_0} < p - 2d \qquad (6)$$

then (5) holds true.

Choosing the entries of H satisfying (6) for all $j_0, j_1, 0 \leq j_0 < j_1 \leq J-1$, and all $l_0, l_1, 0 \leq l_0 < l_1 \leq L-1$, will ensure that no 4-cycles can occur. To this aim we set each $p_{0,l}^{(1)}, 0 \leq l \leq L-1$, in the top row, to be any non-negative integer a_l. We choose ℓ be any integer such that $\ell \geq 2d+1$, and set $m_{j,j+1}^{l} = l\ell, j = 0,1,\ldots,J-2, 0 \leq l \leq L-1$. It follows that $m_{j_0,j_1}^{l_1} - m_{j_0,j_1}^{l_0} = (j_1 - j_0)(l_1 - l_0)\ell \geq \ell > 2d$ as required. We then choose p large enough so that $p > (J-1)(L-1)\ell + 2d$ and this completes our requirements for (6). Finally, to ensure that p is greater than all values of $p_{j,l}^{(i)}$, (and thus each is already reduced $\bmod p$) we must have $p > (J-1)(L-1)\ell + d + \max_{0 \leq l \leq L-1}\{a_l\}$.

Construction: We can now define the entries of H by the following formulae:

$$\begin{aligned} p_{j,l}^{(1)} &= a_l + jl\ell, \\ p_{j,l}^{(2)} &= a_l + jl\ell + d_{j,l}, \end{aligned}$$

$0 \leq j \leq J-1, 0 \leq l \leq L-1$, where $a_l, 0 \leq l \leq L-1$, are chosen as any non-negative integers, the $d_{j,l}$ are chosen as described earlier, $d = \max_{0 \leq l \leq L-1}\{d_{0,l}\}$, $\ell \geq 2d+1$ and $p > (J-1)(L-1)\ell + \max\{2d, d + \max_{0 \leq l \leq L-1}\{a_l\}\}$. In polynomial notation H has the form given by (4). The Tanner graph of H is guaranteed to have girth at least 6. We note that the code is equivalent by row and column permutations within each circulant block (and thus has an equivalent Tanner graph) to the code generated when $a_0 = a_1 = \cdots = a_{L-1} = 0$.

Example 8: Let $J = 3, L = 4, d_{0,l} = l+1, l = 0,\ldots,3$ *and* $d_{j,l} = d_{j-1,l+1 \bmod 4}, j = 1,2$. *Then* $d = 4$. *Let* $\ell = 9 \geq 2d+1, a_l = 0, 0 \leq l \leq 3, p = 63 > \max\{6\ell + 2d, 6\ell + d + \max_{0 \leq l \leq L-1}\{a_l\}\} = 62$. *The matrix H has the form*

$$\left[\begin{array}{cccc} 1+x^1 & 1+x^2 & 1+x^3 & 1+x^4 \\ 1+x^2 & x^9+x^{12} & x^{18}+x^{22} & x^{27}+x^{28} \\ 1+x^3 & x^{18}+x^{22} & x^{36}+x^{37} & x^{54}+x^{56} \end{array}\right]$$

and defines a $[N = 252, k \geq 63]$ *linear* $(6,8)$*-regular code with girth at least* 6.

The construction described above can be easily modified to obtain a type-II QC LDPC code with girth $g \geq 6$, for any regular or irregular weight configuration that exists in a $J \times L$ array. For any choice of J and L, we use the same formulae outlined above to specify entries, but now simply omit the 2nd or both terms in a circulant entry of H where weight less than 2 is required in that position. In this case the value of a_l is first required in the formula specifying the topmost non-zero circulant in the l^{th} column, and can be chosen as before as any non-negative integer (or as 0 to obtain an equivalent standard form). Further modifications can be made to reduce the lower bounds on p and ℓ, by adjusting the values of the $d_{j,l}$ for this new weight configuration. The values of $d_{j,l}$ required to specify the weight-2 entries in each row, can be chosen as a subset of t distinct positive integers, where t is the maximum number of weight-2 entries in any row or column of the new weight configuration. As before we must ensure that for any defined values, $d_{j_0,l} \neq d_{j_1,l}$ when $j_0 \neq j_1$. Now we set d to be the maximum of all such defined values of $d_{j,l}$. The necessary lower bounds of ℓ and p have the same form as earlier, but give lower values when fewer $d_{j,l}$ are needed. With these modifications all inequalities of Theorem 6 still hold true, whenever such inequalities are defined by non-zero entries in the matrix. It follows as before that the girth is guaranteed to be at least 6.

Example 9: Let $J = 3, L = 4$. *For the weight configuration given in (2), we can choose all defined values of* $d_{j,l}$ *to be* 1, *since there is only one binomial entry in each row and column. Hence* $d = 1$. *Let* $\ell = 3$. *For any non-negative integers* $a_l, 0 \leq l \leq 3$ *and any* $p > \max\{20, 19 + \max_{0 \leq l \leq L-1}\{a_l\}\}$, *the matrix H has the form*

$$\left[\begin{array}{cccc} x^{a_0}+x^{a_0+1} & 0 & x^{a_2} & x^{a_3} \\ x^{a_0} & x^{a_1+3}+x^{a_1+4} & 0 & x^{a_3+9} \\ 0 & x^{a_1+6} & x^{a_2+12}+x^{a_2+13} & x^{a_3+18} \end{array}\right]$$

and defines a $[N = p \times 4, k \geq p]$ *linear* $(3, 4)$*-regular code with girth at least* 6*.*

Codes in the special class of (J, L)-regular type-I QC LDPC codes, (where all entries are circulant permutation matrices), with guaranteed girth $g \geq 6$, can also be obtained by our explicit construction. In this case, no values of d_{jl} are defined, and so we take $d = 0$. For any non-negative integers $a_l, 0 \leq l \leq L-1$, any $\ell \geq 1$ and $p > (J-1)(L-1)\ell$, the parity check matrix

$$H(x) = \begin{bmatrix} x^{a_0} & x^{a_1} & \cdots & x^{a_{L-1}} \\ x^{a_0} & x^{a_1+\ell} & \cdots & x^{a_{L-1}+(L-1)\ell} \\ \vdots & \vdots & \ddots & \vdots \\ x^{a_0} & x^{a_1+(J-1)\ell} & \cdots & x^{a_{L-1}+(J-1)(L-1)\ell} \end{bmatrix}$$

has girth $g \geq 6$. We note that the array codes defined in [5] are a special case of the structured class of codes defined by H above. Table I shows the smallest values $p = (J-1)(L-1)+1$ for which a (J, L)-regular type-I QC LDPC code of this form exists. Table II shows smallest values of p for which a $(2J, 2L)$-regular type-II QC LDPC code is obtained by our construction. In this case taking $d = L$ and $\ell = 2L+1$, we can choose $p = (J-1)(L-1)(2L+1)+2L+1$. The smallest values of p for which codes, with any other regular or irregular weight configuration in a $J \times L$ array, can be obtained by our construction, is upper bounded by the values in Table II.

TABLE I
Smallest value of p for which (J, L)-regular Type-I QC LDPC code with girth $g \geq 6$ are obtained by explicit construction.

L J	3	4	5	6	7	8	9	10	11	12
2	3	4	5	6	7	8	9	10	11	12
3	5	7	9	11	13	15	17	19	21	23
4		10	13	16	19	22	25	28	31	34
5			17	21	25	29	33	37	41	45

TABLE II
Smallest value of p for which $(2J, 2L)$-reg Type-II QC LDPC code with girth $g \geq 6$ are obtained by explicit construction.

L J	3	4	5	6	7	8	9	10	11	12
2	21	36	55	78	105	136	171	210	253	300
3	35	63	99	143	195	255	323	399	483	575
4		90	143	208	285	374	475	588	713	850
5			187	273	375	493	627	777	943	1125

V. Fullrank Multi-Generator QC Matrices

When $J = 1$ a QC matrix H consists of one row of circulant submatrices, and the rank can be determined directly from the polynomials specifying these circulants, using a formula given in [9]. Here we give a similar formula for ensuring fullrank for the multi-generator $(J > 1)$ case, which can be read straightforwardly from the full-size minors in the polynomial matrix $H(x)$. We note that this result applies when any weight polynomials are present in $H(x)$, and applies equally to the generator matrix of a QC code in circulant form.

Theorem 10: Let $J \leq L$. A $pJ \times pL$ QC matrix H over $\mathbb{F}$ has fullrank $k = pJ$ if and only if

$$\gcd(\Delta_1, \Delta_2, \ldots, \Delta_{\binom{L}{J}}, x^p - 1) = 1,$$

where $\Delta_i \in \mathbb{F}[x], i = 1, 2, \ldots, \binom{L}{J}$, are the determinants of the $\binom{L}{J}$ distinct $J \times J$ submatrices (that is, the fullsize minors) of the corresponding polynomial matrix $H(x) = [h_{jl}(x)]_{J \times L}$.

We note that at least one fullsize minor of $H(x)$ must be non-zero if $\gcd(\Delta_1, \Delta_2, \ldots, \Delta_{\binom{L}{J}}, x^p - 1) = 1$. When $\mathbb{F} = \mathbb{F}_2$, if we choose polynomial entries such that $\gcd(\Delta_1, \Delta_2, \ldots, \Delta_{\binom{L}{J}})$ is not divisible by $x+1$, then the value of p can be adjusted to ensure $\gcd(\Delta_1, \Delta_2, \ldots, \Delta_{\binom{L}{J}}, x^p - 1) = 1$ and thus construct a fullrank matrix.

Example 11: Let $a_0 = a_1 = a_3 = 0$ *and* $a_2 = 1$ *in example 9. Then*

$$H(x) = \begin{bmatrix} 1+x & 0 & x & 1 \\ 1 & x^3 + x^4 & 0 & x^9 \\ 0 & x^6 & x^{13} + x^{14} & x^{18} \end{bmatrix}$$

is a parity check matrix for a $(3, 4)$*-regular type-II QC LDPC code. If* $p > 20$ *then the code has girth* $g \geq 6$*. The determinants of the* 4 *distinct* 3×3 *submatrices are*

$$\begin{aligned} \Delta_1 &= x^7 + x^{16} + x^{17} + x^{18} + x^{19} \\ \Delta_2 &= x^6 + x^{15} + x^{16} + x^{21} + x^{23} \\ \Delta_3 &= x^{13} + x^{14} + x^{19} + x^{22} + x^{24} \\ \Delta_4 &= x^{18} + x^{22} + x^{23} \end{aligned}$$

and $\gcd(\Delta_1, \Delta_2, \Delta_3, \Delta_4) = x^6 + x^7 + x^8$*. If* $p = 21$ *then* $\gcd(\Delta_1, \Delta_2, \Delta_3, \Delta_4, x^{21} - 1) = x^2 + x + 1$*. Let* $p = 22$*. Then* $\gcd(\Delta_1, \Delta_2, \Delta_3, \Delta_4, x^{22} - 1) = 1$ *and the quasi-cyclic matrix* H *of order* 66×88 *has fullrank, and defines a* $[88, 22]$ *linear code with design rate* $1 - J/L = 1/4$*.*

Acknowledgment

The author would like to thank Roxana Smarandache for many interesting and helpful discussions.

References

[1] S. Lin and D.J. Costello, Jr., *Error Control Coding: Fundamentals and Applications*, (2^{nd} edition), Pearson Prentice Hall, Upper Saddle River, NJ, 2004.

[2] R. Smarandache and P.O. Vontobel, "On regular quasi-cyclic LDPC codes from binomials," in *Proc. IEEE Intern. Symp. on Inform. Theory*, (Chicago, USA), p. 274, 2004. Longer version available at http://www-rohan.sdsu.edu/~rsmarand/html/publications.html.

[3] M.P.C. Fossorier, "Quasi-cyclic low density parity check codes from circulant permutation matrices," *IEEE Trans. Inform. Theory*, 50. pp. 1788- 1793, 2004.

[4] R.M. Tanner, D.Sridhara and T. Fuja, "A class of group-structured LDPC codes," in *Proc. of ICSTA 2001*, (Ambleside, England), July, 2001.

[5] J.L. Fan, "Array codes as low-density parity-check codes," in *Proc. 2nd Intern. Conf. on Turbo Codes and Related Topics*, (Brest, France), Sept., 2000.

[6] M.E. O'Sullivan, "Algebraic construction of sparse matrices with large girth", *IEEE Trans. Inform. Theory*, 52. pp. 718- 727, 2006.

[7] X. Wu, X. You and C. Zhao, "An efficient girth-locating algorithm for quasi-cyclic LDPC codes", in *Proc. IEEE Intern. Symp. on Inform. Theory*, (Seattle, USA), p. 817-820, 2006.

[8] D.J.C. MacKay and M.C. Davey, "Evaluation of Gallager codes for short block length and high rate applications," in *Codes, Systems, and Graphical Models (Minneapolis, MN, 1999)* (B. Marcus and J. Rosenthal, eds.), vol. 123 of IMA Vol. Math. Appl., pp. 113–130, Springer Verlag, New York, Inc., 2001.

[9] H.C.A. van Tilborg, "On quasi-cyclic codes with rate $1/m$", IEEE Trans. Inform. Theory, 24, pp. 628–630, 1978.