On the Girth of (3,L) Quasi-Cyclic LDPC Codes based on Complete Protographs

Sudarsan V. S. Ranganathan*, Dariush Divsalar† and Richard D. Wesel*
*Department of Electrical Engineering, University of California, Los Angeles, Los Angeles, California 90095
†Jet Propulsion Laboratory, California Institute of Technology, Pasadena, California 91109
Email: sudarsanvsr@ucla.edu, Dariush.Divsalar@jpl.nasa.gov, wesel@ee.ucla.edu

***Abstract*—We consider the problem of constructing $(3, L)$ quasi-cyclic low-density parity-check (LDPC) codes from complete protographs. A complete protograph is a small bipartite graph with two disjoint vertex sets such that every vertex in the variable-node set is connected to every vertex in the check-node set by a unique edge. This paper analyzes the required lifting factor for achieving girths of six or eight in the resulting quasi-cyclic codes with constraints on lifting. The required lifting factors provide lower bounds on the block-length of such codes.**

I. Introduction and Background

Protograph-based quasi-cyclic LDPC codes (protograph QC-LDPC) [1], [2] are LDPC codes [3] with encoders and decoders amenable to implementation for practical purposes. Generally, a code constructed from a protograph need not be quasi-cyclic. A QC code is built from a protograph by restricting the permutation matrices used in the lifting process to be circulants. A protograph QC-LDPC code can be described by specifying the permutation shift indices of the circulant permutation matrices associated with the lifting process [2].

A protograph [1] defines the family of codes that can be obtained from it by lifting and many properties of the codes in the family depend on the graphical structure of the chosen protograph. In this paper, we consider the case where the protograph is a *simple* (has no loops or multiple links between two vertices) and *complete* (every vertex in the variable-node set is connected to every vertex in the check-node set) bipartite graph. QC-LDPC codes obtained from simple and complete protographs are called *conventional* QC-LDPC codes in [4], which considers simple QC-LDPC codes in general, including the subset which are conventional.

The performance of LDPC codes is dictated, to a certain extent, by the girth of the codes. Also, in the regime of short-to-moderate block-lengths, the minimum distance of an LDPC code affects its performance in the error-floor region if the variable-node degrees are small [5]. In this regard, the minimum distance of a protograph QC-LDPC code and its girth are interrelated as suggested by the work in [6]. The works in [2], [4] derive lower bounds on the required lifting factors (and thus block-lengths) for obtaining various girths for QC codes constructed from protographs and provide the foundations for this paper. Works including [2], [4], [7]–[9] have focused on obtaining these bounds because they are of practical importance and have demonstrated code construction techniques to obtain codes with as high a girth as possible.

We focus on the case of $(3, L)$ protograph QC-LDPC codes. These are regular codes that perform well over many rates. The paper is organized as follows: Section II introduces notation. Section III completely characterizes the lifting requirements to construct a $(3, L)$ code with girth 6 when the lifting factor is equal to L and gives an explicit construction that achieves a girth of 6 for any possible value of L. Section IV derives a bound (under a constrained setting) on the lifting factor required to obtain a girth of at least 8. This bound improves on the bounds in [2], [4]. Section V concludes the paper.

II. Definitions and Notation

A *protograph* [1] is a small bipartite Tanner graph [10] and a *protomatrix* is a biadjacency matrix of the protograph. A graph's *girth* is the length of its shortest cycle(s). The protomatrices considered in this paper have the form

$$H_{\text{protomatrix}} = \begin{bmatrix} 1 & 1 & 1 & \cdots \\ 1 & 1 & 1 & \cdots \\ 1 & 1 & 1 & \cdots \end{bmatrix}_{3\times L}. \tag{1}$$

At places, the terms protograph and protomatrix are used interchangeably. Associated with any protomatrix, the process of *lifting* to obtain a QC code is the replacement of every non-zero entry z in the protomatrix by a sum of z circulant permutation matrices (CPMs) of size $N \times N$ with distinct support and every 0 in the protomatrix by an $N \times N$ matrix of all zeros. If the protomatrix is of size $J \times L$ then lifting yields a parity-check matrix H of size $JN \times LN$. Because our protomatrices are simple and complete, lifting replaces every entry in the protomatrix with an $N \times N$ CPM.

Definition 1 (Permutation-shift matrix [4]): The permutation-shift matrix P of a QC-LDPC code constructed from a $J \times L$ protomatrix with entries at most equal to 1 is the $J \times L$ matrix of permutation shift indices that are chosen for the non-zero entries of the protomatrix during the process of lifting. With the lifting factor being N, an element $0 \leq x \leq N-1$ in P corresponds to a CPM in the

This material is based upon work supported by the Broadcom Foundation and the National Science Foundation under Grant Numbers 1162501 and 1161822. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation. This research was carried out in part at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with NASA and JPL-NSF Task Plan 82-17473.

parity-check matrix H obtained via x circular shifts of the rows of the identity matrix of size $N \times N$. The orientation (left or right) of the permutation shifts is unspecified in this paper without loss of generality (WLOG).

The cyclic group of integers modulo N, $\{0, 1, \ldots, N-1\}$, is denoted $\mathbb{Z}/N$. This is the set of first N non-negative integers with addition modulo-N as the associated binary operation, represented by $x_i + x_j$. Similarly, $x_i - x_j = x_i + (-x_j)$ represents adding the inverse of x_j to x_i. The *order* of a group is its cardinality. A *permutation* π is a bijective map of a finite set of elements onto itself.

Definition 2: A permutation π of $\mathbb{Z}/N$ is said to have a *fixed point* if $\pi(i) = i$ for any $i = 0, 1, \ldots, N-1$.

III. On the Minimum Lifting Factor for Girth Greater Than or Equal To 6

We consider the special case of this problem with the constraint that the lifting factor N satisfies $N = L$. This is the least value of N for which one can possibly obtain a girth of $g > 4$ [2], [4]. By looking at this special case we arrive at a combinatorial interpretation to the problem of obtaining codes with girth at least 6 from complete protomatrices of size $J \times L$. Since $N = L$, we may use N and L interchangeably.

Works including [2] have constructed codes via computer searches to show empirically the existence of codes with girth $g \geq 6$ for some odd values of $N = L$ (including analytical constructions for all primes; see [11] also). We show analytically that for all odd values of $N = L$, there exist $(3, L)$ codes with girth $g \geq 6$. [9] has established this result and our contribution is a proof via combinatorial structures called *complete mappings* [12]. We provide an algebraic construction that produces codes with girth $g = 6$ for any odd $N = L$. This construction includes, as a special case, the array-code based proof of [9] for the $(3, L)$ case.

Lemma 3 ([2]): With the lifting factor being N, in any QC-LDPC code with a protomatrix with no entry larger than 1, a cycle of length ℓ (ℓ even) in the Tanner graph of the code can be equivalently described by a sequence of edges $(e_1, e_2, \ldots, e_\ell)$ in the protograph whose corresponding permutation shifts in P that are given as $x_1, x_2, \ldots, x_\ell$ satisfy

$$\sum_{i=1}^{\ell} (-1)^{i+1} x_i = 0 \mod N, \tag{2}$$

where $e_i \neq e_{i+1}$ for all $i \in \{1, 2, \ldots, \ell - 1\}$ and $e_1 \neq e_\ell$. Consecutive pairs of consecutive edges $\{e_i, e_{i+1}\}$ for all $i \in \{1, 2, \ldots, \ell-1\}$ and $\{e_\ell, e_1\}$ alternatingly lie in the same row or same column of the protomatrix.

The elements of P are assumed to be in $\mathbb{Z}/N$ and thus "mod N" may not be mentioned at most places that involve operations with elements from P.

Lemma 4 (Extension of [2], Theorem 2.2): With a lifting factor of $N = L$, any permutation-shift matrix P that could lead to $g > 4$ for a $(3, L)$ code with a complete protomatrix may be written WLOG as

$$P = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 2 & \cdots & N-1 \\ \pi(0) = 0 & \pi(1) & \pi(2) & \cdots & \pi(N-1) \end{bmatrix}, \tag{3}$$

where π has only one fixed point at $\pi(0) = 0$.

Proof: Irrespective of the $3L$ indices that are chosen for P, one can always apply circular shifts to the row blocks and the column blocks of H (after lifting) to obtain an isomorphic graph for which the first row and column have all-zero indices in P, as observed in [2]. For girth $g > 4$, [2] shows that no non-zero element can repeat in the same row or the same column. Thus the non-zero entries in each of rows 2 and 3 are all unique within the respective rows and the ordering of row 2 in (3) can be obtained WLOG by rearranging the columns once we have 0's in row 1 and column 1. To ensure that no column repeats a nonzero value, the permutation cannot have any fixed point except $\pi(0) = 0$. ∎

The preceding lemma implies that, WLOG, only $L-1$ non-zero permutation shifts need to be specified and these belong to the third row. As an example where repetition in the same column prevents $g > 4$, the case of $L = 2$ leads to $g = 4$ as there is only one non-zero element in $\mathbb{Z}/2$. The probability that a permutation of a finite number of elements $(N-1)$ has no fixed points asymptotically, as $N \to \infty$, equals $\frac{1}{e}$ [13]. If we search randomly for permutations of $N-1$ non-zero elements to achieve a girth of $g > 4$, then the number of permutations to be considered when constructing a code for large values of $N-1$ is very high but only approximately 36.8% of them will pass the preliminary test of not having a fixed point.

Definition 5 (Complete mapping [12], [14]): A complete mapping of the cyclic group $(\mathbb{Z}/N, +)$ is a permutation π which satisfies $\pi(0) = 0$ and that $(0, \pi(1) - 1, \pi(2) - 2, \ldots, \pi(N-1) - (N-1))$ is also a valid permutation.

Theorem 6: With a lifting factor of $N = L$, the parity-check matrix H of a code with a complete protomatrix of size $3 \times L$ has a girth $g > 4$ if and only if the permutation π of $\mathbb{Z}/N$ that specifies the third row of P in (3) is a complete mapping.

Proof: Consider any two columns of the shift matrix of (3) and form a 2×2 sub-matrix of rows 2 and 3 out of the chosen columns as

$$\begin{bmatrix} x_i & x_j \\ x_k & x_\ell \end{bmatrix}, x_k = \pi(x_i), x_\ell = \pi(x_j).$$

From the general condition of (2) in Lemma 3, x_i, x_j, x_k, x_ℓ lead to cycle(s) of length four if and only if (iff)

$$x_i - x_k + x_\ell - x_j = 0. \tag{4}$$

Rewriting the above, the girth is greater than 4 iff

$$(x_\ell - x_j) - (x_k - x_i) \neq 0, \tag{5}$$

which means that $x_\ell - x_j \neq x_k - x_i$ should be satisfied for any x_i, x_j, x_k, x_ℓ as considered above. This is possible iff

$$(\pi(\text{row } 2) - \text{row } 2) \tag{6}$$

describes a permutation (i.e. the sequence contains each distinct element in the group exactly once), which occurs iff row 3 is a complete mapping. ∎

Theorem 7: There exists a $(3, L)$ quasi-cyclic LDPC code with a complete protograph lifted by a factor $N = L$ satisfying girth $g > 4$ iff L is odd.

Proof: From [12], there exists a complete mapping of a finite abelian group of order N iff the group does not possess exactly one element of order 2. When N is even, this condition is violated as one can verify that $\frac{N}{2}$ is the only order-2 element in the finite abelian group $\mathbb{Z}/N$. On the contrary, in finite groups $\mathbb{Z}/N$ of odd orders there exists no element of order 2, according to Lagrange's theorem on the order of elements in a finite group. This argument in conjunction with Theorem 6 completes this proof. ∎

The number of complete mappings of $\mathbb{Z}/N$ is documented in [14]. The first few terms of this sequence as a function of N, from $N = 1, 3, 5, \ldots$, are 1, 1, 3, 19, 225, 3441, 79259, 2424195, 94471089, 4613520889. For odd $N = L$ all the complete mappings that yield codes with girth $g \geq 6$ lead to $g = 6$ since girth $g \geq 8$ requires a higher lifting factor (see Section IV). For odd $N = L$, random search might identify a complete mapping and hence a $g = 6$ code, but the probability of any randomly selected mapping being complete decreases quickly with increasing L. For instance, when $L = 15$ corresponding to a design rate $R = \frac{L-3}{L} = 0.8$ this probability is $\frac{2424195}{14!} = 0.000028$ and when $L = 17$ and $R = 0.8235$ this probability is 0.000004 and so on. In the following we present a family of complete mappings and thus a family of codes for any odd $N = L, L \geq 3$ that have $g = 6$.

Corollary 8 (Product construction): Consider the following mapping for row 3 in (3) with $h \in \{2, 3, \ldots, N-1\}$:

$$\pi_p(i) = hi \mod N, 0 \leq i \leq N-1, \tag{7}$$

where $hi \mod N$ is multiplication modulo-N of integers h and i. For $N = L$ odd and $N \geq 3$, if h and $h-1$ are each coprime with N, then π_p is a complete mapping of $\mathbb{Z}/N$ and thus leads to a $(3, L)$ code with girth 6.

Proof: Note that since h is chosen to be coprime with respect to N, $(hi \mod N : 0 \leq i \leq N-1)$ is a valid permutation of $\mathbb{Z}/N$. This is because $hi - hj = h(i-j) \neq 0 \mod N, \forall i \neq j$ as h is not a factor of N. We need to further show that (4) from Theorem 6 has no solution. Writing (5), which is obtained from (4), for this permutation:

$$\begin{aligned} &(x_\ell - x_j) - (x_k - x_i) \neq 0 \\ \iff &h(x_j - x_i) - (x_j - x_i) \neq 0, \text{ as } x_k = hx_i, x_\ell = hx_j \\ \iff &(h-1)(x_j - x_i) \neq 0, \end{aligned}$$

which is satisfied for this permutation for all $x_j \neq x_i$ since $h - 1 \geq 1$ is chosen to be coprime with respect to N. ∎

There exists such an h for every odd $N \geq 3$. An example is $h = N - 1$ for which

$$P = \begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 2 & \cdots & N-2 & N-1 \\ 0 & N-1 & N-2 & \cdots & 2 & 1 \end{bmatrix}. \tag{8}$$

Also, $(3, L)$ array codes [2], [11], for any odd $L \geq 3$ (not necessarily prime), are a special case of the preceding construction with $h = 2$ and thus have $g = 6$ [9].

Corollary 9: If $N = L$ is even then there exists a $(3, L)$ complete-protomatrix-based code with girth equal to 4 whose Tanner graph has exactly N cycles of length four.

Proof: This follows from [12], which proves that in case the order of a finite abelian group is even then there exists an "almost complete" mapping π of the group such that the sequence $(0, \pi(1) - 1, \pi(2) - 2, \ldots, \pi(N-1) - (N-1))$ has exactly $N - 1$ distinct elements. Thus, one element appears twice. This implies that there exists a mapping for the third row such that only one 2×2 block from the second and the third rows leads to N length-4 cycles. ∎

As shown in [9], it can also be observed that if L is even then there exists a $(3, L)$ complete-protomatrix-based code with a girth of 6 if the lifting factor is $N = L + 1$.

One can generalize the discussion so far to see that for the (J, L) case there could be a code with $g > 4$ when the lifting factor is $N = L$ only if there exist $J - 2$ distinct complete mappings of $\mathbb{Z}/N$. This condition is necessary but not sufficient because the rows produced by the $J-2$ complete mappings also have to satisfy the following condition: Every pair of the $\binom{J-2}{2}$ rows indexed by $\{\{i, j\} : 3 \leq i < j \leq J\}$ are such that row j is a complete mapping of row i.

Consider the computer-search based Table I of [2] (reproduced below). When $N = L = 9$, the computer search could not find a $(J, 9)$ code with girth $g = 6$ when $J \geq 4$. Using the previous paragraph, we can confirm that such a code does not exist. There are 225 complete mappings of $\mathbb{Z}/9$. We can corroborate the result in this table since not even one pair out of $\binom{225}{2}$ pairs of complete mappings can satisfy the requirement that one row in the pair is a complete mapping of the other.

TABLE I
SMALLEST VALUE OF N FOR WHICH A (J, L) CODE WITH GIRTH $g \geq 6$ WAS FOUND IN [2] USING 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

IV. TOWARDS A TIGHTER BOUND ON THE REQUIRED LIFTING FACTOR FOR GIRTH ≥ 8 WHILE $L \geq 4$

Assuming $L \geq 4$, it is known that the lifting factor N has to satisfy $N > 2(L-1)$ to obtain a girth of $g \geq 8$ for our $(3, L)$ codes [2]. In this section, we derive an improved bound on this required lifting factor under a constraint by using an additive combinatorics formulation of the problem. It is conjectured, for future investigation, that the bound holds without this imposed constraint.

The following lemma states the necessary and sufficient conditions of [2] for the permutation-shift matrix P of a complete-protomatrix-based $(3, L)$ code to achieve $g \geq 8$.

Lemma 10: For $L \geq 4$, let $L' = L-1$ and the lifting factor be N. The permutation-shift matrix

$$P = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 \\ 0 & x_1 & x_2 & \dots & x_{L'} \\ 0 & x_{L'+1} & x_{L'+2} & \dots & x_{2L'} \end{bmatrix} \tag{9}$$

leads to a girth of $g \geq 8$ iff all the following conditions hold: With $i, j \in \{1, 2, \dots, 2L'\}$,

1) $x_i \neq x_j$ for all $i \neq j$ and $x_i \neq 0$ for all i.

Fixing $i \geq L'+1$ and $j = i - L'$ (so that x_i and x_j are in the same column of P, with x_i in the third row):

2) $x_i - x_j \neq -x_k$, where $k \in \{1, 2, \dots, L'\} \setminus \{j\}$,
3) $x_i - x_j \neq x_k$, where $k \in \{L'+1, L'+2, \dots, 2L'\} \setminus \{i\}$,
4) $x_i - x_j \neq x_k - x_\ell$, where $k \in \{L'+1, L'+2, \dots, 2L'\} \setminus \{i\}, \ell \in \{1, 2, \dots, L'\} \setminus \{j\}, k \neq \ell + L'$,
5) $x_i - x_j \neq x_k - x_\ell$, where $k \in \{L'+1, L'+2, \dots, 2L'\} \setminus \{i\}, k = \ell + L'$.

Proof: Condition 1 is Theorem 2.4 of [2], which yields the necessary condition $N > 2(L-1) = 2L'$ for achieving $g \geq 8$. Conditions 2 and 3 apply (2) to the first column and any other two columns of the shift matrix in (9). Condition 4 similarly considers any three columns apart from the first (all-zeros) column. Condition 5 avoids length-4 cycles from rows 2 and 3 of P. ∎

Definition 11 (Girth-8 table): A *girth-8 table* (G_8 table) of a $(3, L)$ complete-protomatrix-based QC-LDPC code whose permutation-shift matrix is P, using the notation of Lemma 10, is a table of $L' \times L'$ differences:

+\-	x_1	x_2	…	$x_{L'}$
$x_{L'+1}$	$d_1 = x_{L'+1} - x_1$	$x_{L'+1} - x_2$	…	$x_{L'+1} - x_{L'}$
$x_{L'+2}$	$x_{L'+2} - x_1$	d_2	…	$x_{L'+2} - x_{L'}$
⋮	⋮	⋮	⋱	⋮
$x_{2L'}$	$x_{2L'} - x_1$	$x_{2L'} - x_2$	…	$d_{L'}$

A *valid* G_8 table is one which leads to a girth of $g \geq 8$.

Lemma 12: A G_8 table is valid iff

1) The set of row and column headers together has $2L'$ distinct non-zero elements,
2) The diagonal elements $d_1, d_2, \dots, d_{L'}$ are all different from the inverses of the column headers,
3) The diagonal elements are all different from the row headers,
4) None of the diagonal elements is equal to any of the off-diagonal elements of the table,
5) The diagonal elements are all distinct.

Proof: These conditions are the equivalent conditions of Lemma 10 in the same order. Note that a valid G_8 table has no 0 anywhere in it. Conditions 4 and 5, which are mathematically the same albeit for the choice of elements involved but stated separately for clarity, according to Lemma 10, justify uniquely identifying the diagonal elements as $d_1, d_2, \dots, d_{L'}$. ∎

Theorem 13: Let the L' rows of any valid G_8 table be considered as sets of L' elements each and denoted $A_1, A_2, \dots, A_{L'}$. If there exist two rows $i \neq j$ such that $|A_i \cap A_j| = 0$ or $|A_i \cap A_j| = L' - 1$ then such a valid G_8 table corresponds to a lifting factor of $N \geq 3L' - 1$.

Proof: In general, $|A_i \cap A_j| \leq L' - 1, i \neq j$ since every row has a diagonal element that is distinct from the elements in the rest of the table. The proof, which is given in the rest of this section, applies conditions 1, 4 and 5 from Lemma 10.

The case where $\exists\ i \neq j : |A_i \cap A_j| = 0$ is considered first. If so, then $|A_i| + |A_j| = 2L'$ and the rest of the $L' - 2$ rows contribute at least one distinct element each as their diagonal elements have to be distinct and thus the number of distinct non-zero elements is at least $3L' - 2$ and $N \geq 3L' - 1$.

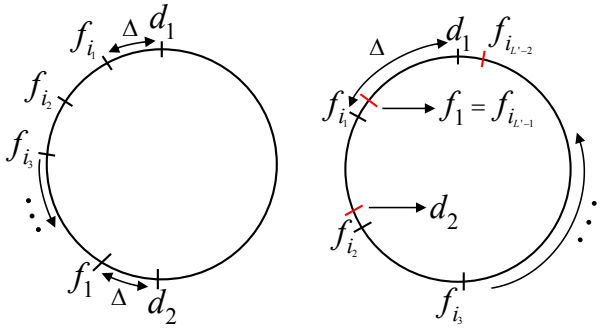
For the second case, assume WLOG that the rows i, j are the first two rows of the G_8 table, corresponding to A_1 and A_2, or the table can be rearranged accordingly (this corresponds to permuting the columns of P). Denote the L' distinct elements of A_1 (in order from left to right) as

$$d_1 = x_{L'+1} - x_1, f_1, f_2, \dots, f_{L'-1}.$$

Any $A_i, i \neq 1$ can be derived from A_1 through an offset. For example, A_2 can be obtained from A_1 by adding $\Delta = x_{L'+2} - x_{L'+1}$ to $d_1, f_1, f_2, \dots, f_{L'-1}$ in that order.

The supposition $|A_1 \cap A_2| = L' - 1$ implies that A_1, A_2 differ in only $d_1 \neq d_2$. Since d_1 does not repeat or "lead to" a new element (or else $|A_1 \cap A_2| < L' - 1$), while adding $\Delta \neq 0$ to it and since the only new element that is formed in this second row is $d_2 = f_1 + \Delta$, this means that $d_1 + \Delta = f_i$ for some $i \in \{1, 2, \dots, L' - 1\}$. Also $\forall k \in \{2, 3, \dots, L' - 1\}$ there exists a unique $\ell_k \in \{1, 2, \dots, L' - 1\} \setminus \{k\}$ such that $f_k + \Delta = f_{\ell_k}, f_k + \Delta \neq d_1, f_k + \Delta \neq d_2$.

Definition 14 (Circular representation): We choose to represent the elements of $\mathbb{Z}/N$ as unique points on a circle in order from 0 through $N - 1$ in the anticlockwise direction such that $N - 1$ appears on the circle before crossing 0 when counting from 0 (as integers). With this representation, addition corresponds to moving along the anticlockwise direction.



(a) Without wrap around (b) With wrap around

Fig. 1. One possible arrangement of elements of row 1 for Theorem 13

A. Case 1

Fig. 1 shows one of the two possible cases for the structure of the elements in $A_1 \cup \{d_2\}$ with respect to the circular representation. In this case, the $L'+1$ elements $d_1, \dots, f_1, d_2$ form a single chain from d_1 to d_2, through L' intervals of

$\Delta = x_{L'+2} - x_{L'+1}$ points each, as shown in Fig. 1. WLOG the chain begins at d_1 and progresses anticlockwise or else the two rows can be exchanged to yield this. Fig. 1(b) considers any possible wrap around.

Lemma 15: For a valid G_8 table that falls in the case illustrated by Fig. 1, there exists a third row whose L' elements are all different from the $L'+1$ elements in the chain $(d_1, f_{i_1}, f_{i_2}, \ldots, f_{i_{L'-2}}, f_1, d_2)$, where $\{i_1, i_2, \ldots, i_{L'-2}\} = \{2, 3, \ldots, L'-1\}$.

Proof: Any row beyond the first two rows of the G_8 table relates to A_1 by an offset $\Delta' \neq \Delta$. If d_1 or d_2 repeat in such a row then the G_8 table is not valid. With $\{i_1, i_2, \ldots, i_{L'-1}\} = \{1, 2, \ldots, L'-1\}$ and with $i_{L'-1} = 1$, we need to show that for a valid G_8 table that falls in Case 1, for any $k \neq \ell \in \{1, 2, \ldots, L'-1\}$, $f_{i_k} + \Delta' \neq f_{i_\ell}$ and $d_1 + \Delta' \neq f_{i_\ell}$.

Assume for a contradiction that $\exists\ k \neq \ell : f_{i_k} + \Delta' = f_{i_\ell}$. Define $n\Delta = \underbrace{\Delta + \Delta + \cdots + \Delta}_{n \text{ times}}$, where n is any non-negative integer. If n is negative, define $n\Delta = \underbrace{-\Delta - \Delta - \cdots - \Delta}_{-n \text{ times}}$. If $\ell > k$, then $f_{i_\ell} = f_{i_k} + (\ell - k)\Delta$ and hence $\Delta' = (\ell - k)\Delta$. Since $1 \leq \ell - k < L' - 1$ we can also obtain that $d_2 = f_{i_{L'-(\ell-k)}} + (\ell - k)\Delta$. This shows that d_2 would be an element of the new row, yielding a contradiction. The same argument in the opposite direction will show that d_1 will repeat as $d_1 = f_{i_{k-\ell}} + \Delta'$ if $\ell < k$. Similarly, one can show that, if $d_1 + \Delta' = f_{i_\ell}$ then d_2 will repeat. ∎

To summarize, there exist at least $(L'+1) + L' + (L'-3) = 3L' - 2$ distinct non-zero elements in a G_8 table that is valid and falls in Case 1, which means $N \geq 3L' - 1$: $L'+1$ elements from $A_1 \cup \{d_2\}$, L' elements in a third row and the term $L'-3$ appears from counting at least one distinct non-zero entry (on the diagonal) from each of the remaining rows.

B. Case 2

The situation where a single chain is not present within the set $A_1 \cup \{d_2\}$ is considered now. This is because, introducing only one new element when creating the second row from the first row, i.e. d_2, can also arise from the situation shown by the example in Fig. 2 (refer to the following description).

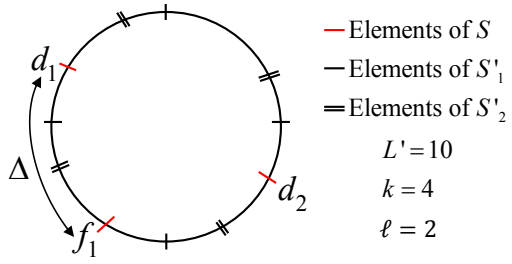


Fig. 2. Alternative arrangement of elements of row 1 for Theorem 13

The elements of $A_1 \cup \{d_2\}$ could be in $\ell + 1$ disjoint sets:

1) Set S with elements $\{d_1, \underbrace{f_{i_1}, \ldots, f_{i_{L'-2-k\ell}}, f_1}_{L'-1-k\ell \text{ elements}}, d_2\}$.
2) ℓ other sets denoted $S'_j, 1 \leq j \leq \ell$ each comprising k elements such that within each set adding $n\Delta, n \in \mathbb{Z}$ to any element yields another element within the set itself.

While this case is introduced here, the proof that the theorem holds for it is given in the Appendix. This concludes the proof of Theorem 13. ∎

Although Theorem 13 only applies under specific constraints on the girth-8 table, we conjecture that the bound $N \geq 3L' - 1$ applies without these imposed constraints that $\exists\ i \neq j \in \{1, 2, \ldots, L'\}$ such that $|A_i \cap A_j|$ equals 0 or $L' - 1$.

V. Conclusion

This paper considers the problem of constructing $(3, L)$ quasi-cyclic low-density parity-check (LDPC) codes from complete protographs. An application of complete mappings from finite group theory provides explicit constructions of $(3, L)$ QC-LDPC codes that achieve girth $g = 6$ with the minimum possible lifting factor of L when L is odd. Identifying the minimum lifting factor required to obtain a girth of $g \geq 8$ is posed as a problem in additive combinatorics using the construct of a girth-8 table (G_8 table). An improved bound on the lifting factor is obtained under certain constraints on the cardinality of girth-8-table row-set intersections. We conjecture that this improved bound applies in general.

References

[1] J. Thorpe, "Low-Density Parity-Check (LDPC) Codes Constructed from Protographs," JPL, IPN-PR 42-154, Aug. 2003.

[2] M. 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.

[3] R. G. Gallager, "Low-Density Parity-Check Codes," 1963.

[4] M. Karimi and A. Banihashemi, "On the Girth of Quasi-Cyclic Protograph LDPC Codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 7, pp. 4542–4552, Jul. 2013.

[5] S. Ranganathan, D. Divsalar, K. Vakilinia, and R. Wesel, "Design of High-Rate Irregular Non-binary LDPC Codes Using Algorithmic Stopping-Set Cancellation," in *Proc. IEEE Int. Symp. Inform. Theory*, Jun. 2014, pp. 711–715.

[6] R. Smarandache and P. Vontobel, "Quasi-Cyclic LDPC Codes: Influence of Proto- and Tanner-Graph Structure on Minimum Hamming Distance Upper Bounds," *IEEE Trans. Inf. Theory*, vol. 58, no. 2, pp. 585–607, Feb. 2012.

[7] K.-J. Kim, J.-H. Chung, and K. Yang, "Bounds on the Size of Parity-Check Matrices for Quasi-Cyclic Low-Density Parity-Check Codes," *IEEE Trans. Inf. Theory*, vol. 59, no. 11, pp. 7288–7298, Nov. 2013.

[8] Y. Wang, J. Yedidia, and S. Draper, "Construction of High-Girth QC-LDPC Codes," in *Proc. 5th Int. Symp. Turbo Codes & Related Topics*, Sep. 2008, pp. 180–185.

[9] M. Hagiwara, K. Nuida, T. Kitagawa, M. Fossorier, and H. Imai, "On the Minimal Length of Quasi Cyclic LDPC Codes with Girth greater than or equal to 6," in *Proc. IEEE Int. Symp. Inform. Theory Applicat.*, Oct. 2006, CD-ROM.

[10] R. Tanner, "A Recursive Approach to Low Complexity Codes," *IEEE Trans. Inf. Theory*, vol. 27, no. 5, pp. 533–547, Sep. 1981.

[11] J. L. Fan, "Array Codes as Low-Density Parity-Check Codes," in *Proc. 2nd Int. Symp. Turbo Codes & Related Topics*, Brest, Sep. 2000, pp. 543–546.

[12] L. J. Paige, "A Note on Finite Abelian Groups," *Bulletin of the American Mathematical Society*, vol. 53, no. 6, pp. 590–593, Jun. 1947.

[13] J. Matousek and J. Nesetril, *Invitation to Discrete Mathematics*. OUP Oxford, 2008.

[14] N. Sloane, "The On-Line Encyclopedia of Integer Sequences," http://oeis.org/A003111, Number of Complete Mappings of The Cyclic Group Z_{2n+1}.

APPENDIX
PROOF OF CASE 2

We prove here that Theorem 13 holds for Case 2 which was introduced in Section IV-B. The ℓ sets being referred to in Case 2 (from Fig. 2) have the same number of elements, denoted k here, or else adding Δ will create a new element for the second row, apart from d_2 which is already being created from $f_1 \in S$. To show that the theorem holds for this case, we focus on the $k\ell$ elements from the ℓ sets. For this case, a "linear" relationship within the elements of the $\ell+1$ sets holds as follows. For the elements in S,

$$\begin{aligned} d_1 + \Delta &= f_{i_1}, \\ f_{i_1} + \Delta &= f_{i_2}, \\ &\vdots \\ f_{i_{L'-2-k\ell}} + \Delta &= f_1, \\ f_1 + \Delta &= d_2. \end{aligned}$$

For the elements in the ℓ sets S'_j,

$$\forall x \in S'_j, 1 \le j \le \ell, x + n\Delta \in S'_j, \forall n \in \mathbb{Z}. \tag{10}$$

Observe that if the elements from the group $\mathbb{Z}/N$ are chosen for A_1 according to Case 2, then the following holds:

$$\forall x \in \mathbb{Z}/N, x + k\Delta = x. \tag{11}$$

Each column of the G_8 table has a diagonal element that appears only once in the table. By adding offsets to the $k\ell$ elements in $(A_1 \cup \{d_2\}) \setminus S$ to obtain the $k\ell$ corresponding diagonal elements (and their respective rows), we have the following crucial observation.

Lemma 16: For each column corresponding to an element in $(A_1 \cup \{d_2\}) \setminus S$, when obtaining a new diagonal element, at least k new non-zero elements are obtained in the corresponding row. Considering all $k\ell$ such rows, a total of $k^2\ell$ distinct elements, that are different from the elements in $A_1 \cup \{d_2\}$, is guaranteed for any valid G_8 table that falls under Case 2.

Proof: Consider $x_1 \in (A_1 \cup \{d_2\}) \setminus S$ and assume that $x_1 \in S'_{i_1}$ for some $1 \le i_1 \le \ell$. There is an offset $\Delta_1 \neq \Delta$ such that $x_1 + \Delta_1 = d_{x_1}$, where d_{x_1} is the diagonal element in the column containing x_1. Note that the row containing d_{x_1} also contains every element in $S'_{i_1} + \Delta_1 = \{s + \Delta_1 : s \in S'_{i_1}\}$. No element in $S'_{i_1} + \Delta_1$ appears in $A_1 \cup \{d_2\}$ as this would force either $S'_{i_1} + \Delta_1 = S'_j, j \neq i_1$ so that $d_{x_1} \in A_1 \cup \{d_2\}$ or $S \subseteq S'_{i_1} + \Delta_1$ so that d_1 and d_2 appear in the row containing d_{x_1} due to (10). Either of these results would lead to a G_8 table that is not valid.

Now consider a second element $x_2 \in (A_1 \cup \{d_2\}) \setminus S$, $x_2 \neq x_1$ and $x_2 \in S'_{i_2}$, where $1 \le i_2 \le \ell$ is not necessarily different from i_1. There is an offset $\Delta_2 \notin \{\Delta, \Delta_1\}$ such that $x_2 + \Delta_2 = d_{x_2}$, where d_{x_2} is the diagonal element in the column containing x_2. Note that the row containing d_{x_2} also contains every element in $S'_{i_2} + \Delta_2$. Following the same reasoning as with x_1, no element in $S'_{i_2} + \Delta_2$ appears in $A_1 \cup \{d_2\}$. Also, $\left(S'_{i_1} + \Delta_1\right) \cap \left(S'_{i_2} + \Delta_2\right) = \emptyset$ or else $S'_{i_1} + \Delta_1 = S'_{i_2} + \Delta_2$ due to (10) and in particular $d_{x_2} \in S'_{i_1} + \Delta_1$ which would lead to a G_8 table that is not valid.

Continuing by induction yields $k^2\ell$ distinct elements that are not in the first row and are different from d_2. ∎

Thus we have for any valid G_8 table in Case 2 that

$$N \ge L' + 2 + k^2\ell, \tag{12}$$

where $L'+2$ arises from counting the elements in $A_1 \cup \{d_2, 0\}$.

Lemma 17: In the context of Case 2, where $|S| = L' - k\ell + 1$,

$$L' - k\ell + 1 \le k. \tag{13}$$

Proof: Due to (11). ∎

Case 2 is only possible when $L' \ge 5$, $k \ge 3$ and $\ell \ge 1$. We consider two ranges for k as follows: If $k \ge \sqrt{2L'-3}$, then

$$\begin{aligned} N &\ge L' + 2 + k^2\ell \\ &\ge L' + 2 + k^2 \\ &\ge L' + 2 + 2L' - 3 = 3L' - 1. \end{aligned} \tag{14}$$

If $k < \sqrt{2L'-3}$, we first use (13) in (12) to get

$$\begin{aligned} N &\ge L' + 2 + k^2\ell \\ &\ge L' + 2 + k(L' - k + 1) \\ &= L' + 2 + kL' - k^2 + k, \end{aligned} \tag{15}$$

which yields a quadratic expression in k for every L'. This is concave in k and it can be verified that the maximum of the right-hand side is obtained at $k_{\max} = \frac{L'+1}{2}$. Under the supposition that $k < \sqrt{2L'-3}$, we can also trivially verify that $k < \sqrt{2L'-3} < k_{\max}$ for $L' \ge 5$ and thus (by concavity) to minimize the right-hand side, we have to set k to the smallest feasible value, which is $k = 3$. This yields

$$\begin{aligned} N &\ge L' + 2 + 3L' - 9 + 3 \\ &= 4L' - 4 > 3L' - 1, \forall L' \ge 5, \end{aligned} \tag{16}$$

which completes the proof for Case 2 and thus of Theorem 13.