New Low-Density Parity-Check Codes with Large Girth Based on Hypergraphs

Irina E. Bocharova[1], Florian Hug[2], Rolf Johannesson[2], Boris D. Kudryashov[1], and Roman V. Satyukov[1]

[1] Dept. of Information Systems
St. Petersburg Univ. of Information Technologies,
Mechanics and Optics
St. Petersburg 197101, Russia
Email: {irina, boris}@eit.lth.se
Email: satyukov@gmail.com

[2] Dept. of Electrical and Information Technology,
Lund University
P. O. Box 118, SE-22100 Lund, Sweden
Email: {florian, rolf}@eit.lth.se

***Abstract*—The relation between low-density parity-check (LDPC) codes and hypergraphs supports searching for powerful LDPC codes based on hypergraphs. On the other hand, coding theory methods can be used in searching for hypergraphs with large girth. Moreover, compact representations of hypergraphs based on convolutional codes can be found. Algorithms for iteratively constructing LDPC codes with large girth and for determining their minimum distance are introduced. New quasi-cyclic (QC) LDPC codes are presented, some having both optimal girth and optimal minimum distance.**

I. Introduction

An important consequence of the relation between low-density parity-check (LDPC) codes and hypergraphs (see, for example [1]–[3]) is the new possibilities in searching for powerful LDPC codes. Moreover, coding theory methods can be used in searching for hypergraphs better than previously known. In particular, compact representations of hypergraphs based on convolutional codes can be found.

Typically, LDPC codes have a minimum distance which is less than those for the best known linear codes, but due to their structure they are suitable for low-complexity iterative decoding. In general, however, belief propagation [4] works better if the minimum distance of an LDPC code is large.

A parity-check matrix of a quasi-cyclic (QC) LDPC code can be regarded as the incidence matrix of a regular hypergraph. Although QC LDPC codes are not asymptotically optimal, they can outperform pseudo-random (asymptotically optimal) LDPC codes of short or moderate lengths [5]. This motivated our search for good short QC LDPC codes.

The problem of finding QC LDPC codes with large girth were considered in [6]–[10]. Best known examples are a $(155, 64, 20)$ code with girth 8, a $(305, 124)$ code with girth 10, and a $(905, 364)$ code with girth 12; the latter two codes with previously unknown minimum distance. In [10], rate $R = 1/2$ codes of lengths 970 and 2534 with girth 10 and 12, respectively, were presented.

We present new examples of regular QC LDPC codes in the form of tailbiting (TB) LDPC codes with girth 8, 10, and 12; some of them having optimal girth and/or optimal minimum distance. This representation is compact and we can apply low-complexity encoding, as well as efficient searching and decoding procedures developed for convolutional and TB codes [11]. Moreover, the girth and free distance of the parent convolutional code upper-bound the girth and the minimum distance of the corresponding TB LDPC code [12].

Relations between the girth of the basic Tanner graph and the hypergraph corresponding to the parent LDPC convolutional code are derived. We introduce new algorithms for iteratively constructing LDPC codes with large girth and for determining their corresponding minimum distance. Examples of newly found QC LDPC codes and best known examples are tabulated together with their girth and minimum distance.

II. Parity-Check Matrices

A rate $R = b/c$ LDPC convolutional code $\mathcal{C}$ is determined by its parity-check matrix of memory m

$$H(D) = \begin{pmatrix} h_{11}(D) & h_{12}(D) & \dots & h_{1c}(D) \\ h_{21}(D) & h_{22}(D) & \dots & h_{2c}(D) \\ \vdots & & \ddots & \\ h_{(c-b)1}(D) & h_{(c-b)2} & \dots & h_{(c-b)c}(D) \end{pmatrix} \tag{1}$$

where the parity-check polynomials $h_{ij}(D) = D^{w_{ij}}$ are monomials of degree w_{ij}. If each column and each row contain exactly J and K nonzero elements, respectively, we call $\mathcal{C}$ a *regular* (J, K) LDPC convolutional code. Denoting the degree of 0 by $-\infty$, such a parity-check matrix can be represented by its *degree matrix*

$$W = \{w_{ij}\}$$

with $i = 1, 2, \dots, c - b$ and $j = 1, 2, \dots, c$ [13]. Expressing the $(c-b) \times c$ parity-check matrix $H(D)$ in terms of its binary matrices H_i, $i = 0, 1, \dots, m$, that is,

$$H(D) = H_0 + H_1 D + H_2 D^2 + \cdots + H_m D^m$$

we obtain the binary semi-infinite parity-check matrix H, which can be written as

$$H^T = \begin{pmatrix} H_0^T & H_1^T & \cdots & H_m^T & & & \\ & H_0^T & H_1^T & \cdots & H_m^T & & \\ & & H_0^T & H_1^T & \cdots & H_m^T & \\ & & & \ddots & \ddots & \ddots & \ddots \end{pmatrix} \tag{2}$$

where H^T denotes the transpose of H.

By TB the parent convolutional parity-check matrix (2) to length $M > m$, we obtain the following $M(c-b) \times Mc$ parity-

978-1-4244-7892-7/10/$26.00 ©2010 IEEE

check matrix H_{TB} of the corresponding tailbitten linear binary block code $\mathcal{B}$ of block-length Mc as

$$H_{\mathrm{TB}}^T = \begin{pmatrix} H_0^T & H_1^T & \cdots & H_{m-1}^T & H_m^T & \mathbf{0} \\ \mathbf{0} & H_0^T & H_1^T & \cdots & H_{m-1}^T & H_m^T \\ H_m^T & \mathbf{0} & H_0^T & H_1^T & \cdots & H_{m-1}^T \\ \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\ H_1^T & \cdots & H_{m-1}^T & H_m^T & \mathbf{0} & H_0^T \end{pmatrix}.$$

Note that H_{TB} is (J, K) regular, that is, there are exactly J ones in every column and exactly K ones in every row. With J and K being much smaller than M, H_{TB} is considered to be sparse. Furthermore, the first c columns of H_{TB} are repeated in a cyclicly shifted manner throughout the whole matrix.

III. Graphs and Hypergraphs

Every parity-check matrix of an LDPC code can be interpreted as an incidence matrix of a *graph* $\mathcal{G}$ or *hypergraph* $\mathcal{HG}$. A hypergraph is a generalization of a graph and is determined by a set of *vertices* $\mathcal{V} = \{v_i\}$ and a set of *hyperedges* $\mathcal{E} = \{e_i\}$, where each hyperedge is a subset of vertices and may connect (contain) any number of vertices. If each hyperedge connects not more than two vertices it is called an *edge* and we obtain an ordinary graph.

A hypergraph is called *s-uniform* if every hyperedge has cardinality s, that is, it connects s vertices. For $s = 2$, a hypergraph is a simple graph. The *degree of a vertex* in a hypergraph is the number of hyperedges that are connected to (contain) it. If all vertices have the same degree c, then the hypergraph is *c-regular*, that is, c is the *degree of the hypergraph*.

Let the set of vertices $\mathcal{V}$ of an s-uniform hypergraph be partitioned into t disjoint subsets $\mathcal{V}_k$, $k = 1, 2, \ldots, t$. If no hyperedge connects (contains) two vertices from the same set $\mathcal{V}_k$, $k = 1, 2, \ldots, t$, the hypergraph is said to be *t-partite*.

A *path* of length L in a hypergraph is an alternating sequence of $L + 1$ vertices v_i, $i = 1, 2, \ldots, L + 1$, and L hyperedges e_i, $i = 1, 2, \ldots, L$, with $e_i \neq e_{i+1}$. If the first and the final vertex coincide, that is, $v_1 = v_{L+1}$, we obtain a *cycle*. A cycle is called *simple* if all its vertices and edges are distinct, except the first and final vertex which coincide. A simple cycle is also known as a *Berge cycle* [14]. Finally, the *girth* of a hypergraph is the length of its shortest simple cycle. For graphs it has been shown in [15] that their girth coincides with the minimum distance of the corresponding block code.

Example 1: Consider the rate $R = 1/4$ convolutional code $\mathcal{C}$ with parity-check matrix

$$H(D) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & D & D \\ 1 & D & 1 & D \end{pmatrix} \tag{3}$$

and degree matrix

$$W = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

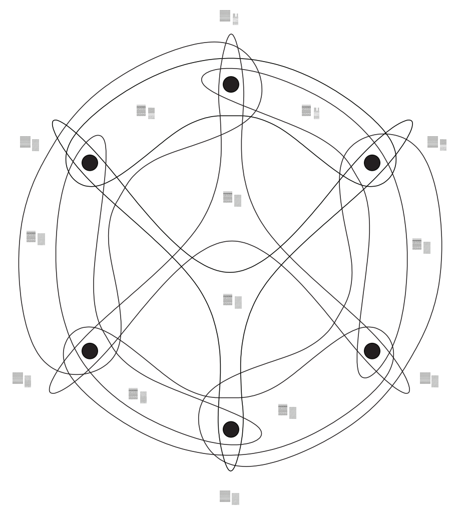

Fig. 1. A 3-partite, 3-uniform, 4-regular hypergraph $\mathcal{HG}$ with vertices v_i, $i = 1, 2, \ldots, 6$, and hyperedges e_j, $j = 1, 2, \ldots, 8$.

Tailbiting (3) via its dual generator matrix [11] to length $M = 2$, we obtain the tailbitten 6×8 parity-check matrix

$$H_{\mathrm{TB}} = \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{array}\right). \tag{4}$$

Interpreting (4) as an incidence matrix, we obtain the 3-partite, 3-uniform, 4-regular hypergraph $\mathcal{HG}$ as illustrated in Fig. 1 with 6 vertices and 8 hyperedges. Every row of the incidence matrix corresponds to a vertex of the hypergraph, while the columns are represented by hyperedges (subsets of vertices).

It is easy to see that the girth of this hypergraph is $g = 2$.

IV. Tanner, Voltage, and Basic Graphs

In order to construct hypergraphs with large girth we need to introduce some auxiliary graph representations. The Tanner graph $\mathcal{G}_{\mathrm{T}}$ [16] of a regular (J, K) convolutional parity-check matrix $H(D)$ (1) is determined by the $(2c - b) \times Jc$ incidence matrix

$$H_{\mathrm{T}} = \begin{pmatrix} C_1 & C_2 & \ldots & C_c \\ J_1 & J_2 & \ldots & J_c \end{pmatrix} \tag{5}$$

where each column of the $(c - b) \times J$ submatrix C_i contains not more than one of the J nonzero elements of column i of $H(D)$, $i = 1, 2, \ldots, c$. The elements of the $c \times J$ matrix J_i are all zero except for the elements of the ith row, which are equal to one. In other words, every hyperedge is replaced by an additional vertex and J new edges between the newly introduced vertex and each of the original vertices connected to the hyperedge.

In order to represent the monomials in the incidence matrix of the Tanner graph (5), every edge is labeled by an *edge voltage*, that is, the degree difference of the corresponding monomials. Note, the sign of the edge voltage depends on

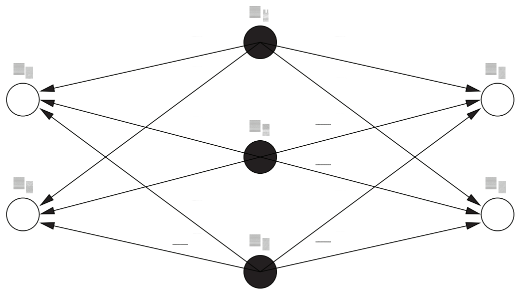

Fig. 2. A bi-partite Tanner graph $\mathcal{G}_{\mathrm{T}}$ with 7 vertices v_i, $i = 1, 2, \ldots, 7$, and 12 edges. Since the edges are labeled according to (6), this is equal to a voltage Tanner graph $\mathcal{G}_{\mathrm{VT}}$

the passing direction. The edge voltage μ_{uv} from vertex u to vertex v; $u, v \in \{1, 2, \ldots, (2c-b); u < v\}$ is given by

$$\begin{aligned} \mu_{uv} &= w_{vk} - w_{uk} \qquad (6)\\ \mu_{vu} &= -\mu_{uv} \end{aligned}$$

where w_{ij} is the degree of the ith row and jth column entry of the degree matrix W corresponding to the incidence matrix H_{T} (5) with entries h_{ij} and k is chosen such that both h_{vk} and $h_{uk} \neq 0$. (Note, that in general k is not necessarily unique.) Hereinafter we will refer to a Tanner graph with its edges labeled according to (6) as a *voltage Tanner graph* $\mathcal{G}_{\mathrm{VT}}$ [17]. The *voltage* of a path is the sum of all edge voltages involved.

If we neglect all monomials in the incidence matrix of the Tanner graph (5), we obtain an unlabeled graph, which we call *basic Tanner graph* $\mathcal{G}_{\mathrm{BT}}$.

While the girth of a basic Tanner graph g_{BT} follows directly as the length of the smallest simple cycle, the girth of a voltage Tanner graph g_{VT} corresponds to its smallest simple cycle with voltage zero. It can be easily seen that $g_{\mathrm{VT}} \geq g_{\mathrm{BT}}$. Moreover, if we denote the girth of the corresponding parent convolutional code, determined by its parity-check matrix $H(D)$ (1), *free girth* g_{free} [12], we obtain the relation $g_{\mathrm{VT}} = 2g_{\mathrm{free}}$.

The binary parity-check matrix H of a block code $\mathcal{B}$, whose hypergraph has girth g, can be represented as a Tanner graph in a similar way. If all monomials are replaced by 1s, there is no difference between the voltage and basic Tanner graphs, and we refer to either of them as the Tanner graph for block codes with girth $g_{\mathrm{T}} = 2g$.

Example 1 (continued): The Tanner graph $\mathcal{G}_{\mathrm{T}}$ for the $(4, 3)$ regular convolutional parity-check matrix $H(D)$ (3) is determined by the 7×12 incidence matrix

$$H_{\mathrm{T}} = \left(\begin{array}{ccc|ccc|ccc|ccc} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0\\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & D & 0 & 0 & D & 0\\ 0 & 0 & 1 & 0 & 0 & D & 0 & 0 & 1 & 0 & 0 & D\\ \hline 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{array}\right)$$

which is illustrated in Fig. 2 with 7 vertices and 12 edges. Since its edges are labeled according to (6), Fig. 2 corresponds to a voltage Tanner graph $\mathcal{G}_{\mathrm{VT}}$ with girth $g_{\mathrm{VT}} = 4$ (for example, $v_1 \to v_4 \to v_2 \to v_5 \to v_1$). The edge from, for example, vertex 2 to vertex 6 is labeled according to

$$\mu_{26} = -\mu_{62} = w_{68} - w_{28} = -1.$$

We conclude that the girth of the corresponding parent convolutional code $\mathcal{C}$, determined by its parity-check matrix $H(D)$ (3), follows as $g_{\mathrm{free}} = 0.5g_{\mathrm{VT}} = 2$. However, if we neglect all labels, we would obtain the corresponding basic Tanner graph $\mathcal{G}_{\mathrm{BT}}$ with girth $g_{\mathrm{BT}} \leq g_{\mathrm{VT}}$.

V. Bounds on Girth and Minimum Distance

Theorem 1: The minimum distance $d_{\min}$ and the girth g of an $(n, k, d_{\min})$ QC LDPC block code $\mathcal{B}$ obtained from a rate $R = b/c$ convolutional code $\mathcal{C}$ with free distance d_{free} and girth g_{free} by TB to length M are upper-bounded by the inequalities

$$\begin{aligned} d_{\min} &\leq d_{\mathrm{free}}\\ g &\leq g_{\mathrm{free}}. \end{aligned}$$

In [13] a lower bound on the girth of a voltage Tanner graph g_{VT} was found via the girth of corresponding basic Tanner graph g_{BT} for ordinary graphs. It is straightforward to generalize this bound:

Theorem 2: Consider a basic Tanner graph of a regular $(J \geq 3, K)$ QC LDPC convolutional code with girth g_{BT} and let d_s denote the sth generalized minimum Hamming distance, that is, the number of nontrivial (not identically zero) positions of an s-dimensional linear subcode. Then there exist a TB length M and a set of edge labels, such that the girth g_{T} of the Tanner graph for the corresponding TB block code of length $N = Mc$ satisfies the inequality

$$g_{\mathrm{T}} \geq 2\max\{g_{\mathrm{BT}} + \lfloor g_{\mathrm{BT}}/2 \rfloor, d_2\}$$

where d_2 is the second generalized minimum Hamming distance of the linear $(JMc, M((J-2)c+b))$ block code determined by the Tanner graph.

Finally, we want to recall the following upper bounds on the achievable girth and minimum distance.

Theorem 3 ([5], [12], [18]): Let $H(D)$ be the parity-check matrix of a rate $R = b/c$ convolutional code with all its entries being nonzero monomials and free distance d_{free}. By TB to length M we obtain a QC LDPC block code of block length Mc and minimum distance $d_{\min}$, together with its hypergraph representation with girth g, which satisfies the following inequalities:

$$\begin{aligned} g &\leq 12 && (7)\\ d_{\min} \leq d_{\mathrm{free}} &\leq (c-b+1)!. && (8) \end{aligned}$$

VI. Search for codes with large girth

Every QC LDPC rate $R = Mb/Mc$ block code $\mathcal{B}$ can be obtained from a rate $R = b/c$ parent convolutional code $\mathcal{C}$ using a TB length M. Limiting the parity-check matrix $H(D)$ of the parent convolutional code $\mathcal{C}$ to only nonzero monomial entries, we can represent it by its basic Tanner graph $\mathcal{G}_{\mathrm{BT}}$. Then we can use the algorithm, as presented in [13], to find

	R	W	M	g	$d_{\min}$
#1 [6]	2/5	$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 12 & 28 & 29 \\ 0 & 24 & 10 & 13 & 19 \end{pmatrix}$	31 $N=155$	8	20
#2 [7]	2/5	$\begin{pmatrix} 13 & 7 & 25 & 25 & 0 \\ 0 & 18 & 8 & 0 & 25 \\ 8 & 0 & 0 & 21 & 2 \end{pmatrix}$	61 $N=305$	10	24*
#3 [7]	2/5	$\begin{pmatrix} 6 & 54 & 13 & 8 & 53 \\ 0 & 31 & 0 & 53 & 0 \\ 54 & 0 & 19 & 0 & 0 \end{pmatrix}$	181 $N=905$	12*	24*
#4 [12]	2/5	$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 3 & 10 & 14 \\ 15 & 10 & 1 & 3 & 0 \end{pmatrix}$	45 $N=225$	8	24*
#5	2/5	$\begin{pmatrix} 0 & 0 & 47 & 0 & 119 \\ 9 & 19 & 30 & 42 & 11 \\ 55 & 1 & 3 & 7 & 37 \end{pmatrix}$	138 $N=690$	10	24*
#6	2/5	$\begin{pmatrix} 11 & 1 & 53 & 0 & 73 \\ 0 & 0 & 0 & 12 & 42 \\ 55 & 73 & 11 & 17 & 0 \end{pmatrix}$	196 $N=980$	12*	24*
#7	3/6	$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 \\ 5 & 8 & 1 & 11 & 0 & 16 \\ 7 & 1 & 6 & 0 & 11 & 0 \end{pmatrix}$	24 $N=144$	8	12
#8	3/6	$\begin{pmatrix} 0 & 0 & 47 & 0 & 0 & 18 \\ 5 & 8 & 1 & 31 & 0 & 27 \\ 39 & 1 & 6 & 0 & 11 & 0 \end{pmatrix}$	72 $N=432$	8	24*

TABLE I

DEGREE MATRICES W FOR VARIOUS CONVOLUTIONAL CODES WITH RATE R. THE BLOCK CODES, AFTER TB TO LENGTH M, HAVE OPTIMUM $(*)$ OR ALMOST OPTIMUM GIRTH g AND MINIMUM DISTANCE $d_{\min}$.

a voltage labeling together with a TB length M, such that the girth of the tailbitten QC LDPC block code is g.

For the sake of completeness, this algorithm is given below.

1) Choose a desired girth g, the rate of the parent convolutional code $R = b/c$, and a TB length M.
2) Construct a list of n equations describing all cycles of lengths less than $2g$ in the basic Tanner graph $\mathcal{G}_{\mathrm{BT}}$ corresponding to the chosen convolutional code rate.
3) Represent these n cycles by an $n \times Jc$ matrix, where each row $\boldsymbol{a} = (a_1, a_2, \ldots, a_{Jc})$ corresponds to one cycle with the value a_i denoting the difference between the number of passes of the ith edge in forward and backward directions.
4) Search randomly for a vector $\boldsymbol{\mu} = (\mu_1, \mu_2, \ldots, \mu_{Jc})$ such that
$$\boldsymbol{\mu} A^T \neq \mathbf{0} \bmod M.$$
5) Label the edges of the basic Tanner graph according to $\boldsymbol{\mu}$ to obtain a voltage Tanner graph. Tailbite the parity-check matrix of the corresponding parent convolutional code via its dual generator matrix to length M; this yields the parity-check matrix of a block code of block length $N = Mc$ corresponding to a hypergraph with girth not less than g.

Note, that using voltage Tanner graphs instead of circulant permutation matrices as in [5] gives the freedom to choose voltage labels and TB length M independently. Moreover, it allows us to generalize this construction to parity-check matrices of convolutional codes with zero entries.

VII. MINIMUM DISTANCE

Clearly, every codeword $\boldsymbol{v}$ of a tailbitten linear block code $\mathcal{B}$ of block-length $N = Mc$ with an $M(c-b) \times Mc$ parity-check matrix H_{TB} fulfills
$$\boldsymbol{v} H_{\mathrm{TB}}^T = \mathbf{0}.$$
The minimum distance for a linear block code is equal to the minimal number of columns of H_{TB} that sum up to zero.

Starting with each of the first c columns as a root, c separate trees can be constructed, where each node ξ at depth ℓ is associated with a state column-vector $\boldsymbol{\sigma}(\xi)$.

Initially assign column $\boldsymbol{h}_i$ to the state of the root node $\boldsymbol{\sigma}(\xi_{\mathrm{root},i})$ of the ith tree, $i = 1, 2, \ldots, c$. Then build up a tree in such a way, that every branch between any two nodes ξ and ξ' is labeled by a column $\boldsymbol{h}_j$, $j = 1, 2, \ldots, Mc$, $j \neq i$, such that $\boldsymbol{\sigma}(\xi') = \boldsymbol{\sigma}(\xi) + \boldsymbol{h}_j$, where every branch label on the path $\xi_{\mathrm{root},i} \to \xi'$ does not occur more than once.

Consider now a certain node ξ with nonzero state $\boldsymbol{\sigma}(\xi)$. Assuming that the kth position of $\boldsymbol{\sigma}(\xi)$ is nonzero, there are at most $L-1$ columns which can cancel this nonzero position in $\boldsymbol{\sigma}(\xi)$ and have not been considered previously. Therefore, every node ξ has at most $L-1$ children nodes per nonzero position.

However, such a tree would grow until all possible linear combinations have been found. Therefore, we limit ourselves to linear combinations of at most t columns; that is, the maximum depth of the tree is $t-1$. Moreover, a node ξ at depth ℓ will not be extended, if the number of nonzero positions of its state $\boldsymbol{\sigma}(\xi)$ is larger than $J(t-\ell-1)$, since at most J ones can be canceled by each branch.

Remark: Initially reordering the rows of the tailbitten parity-check matrix H_{TB} such that each block of M rows contains not more than a single one per column, strengthens the stopping criterion as follows: A node ξ at depth ℓ will not be extended, if the number of nonzero positions in each block of M rows in its state $\boldsymbol{\sigma}(\xi)$ is larger than $(t-\ell-1)$, as at most one 1 in each block can be canceled by each branch.

VIII. RESULTS

Using the algorithms presented in Sections VI and VII, we have obtained new regular QC LDPC codes. In Table I, a few best-known rate $R = 2/5$ QC LDPC codes [6]–[8] are listed together with our newly found codes of rate $R = 2/5$ and $R = 3/6$ having almost optimum or optimum girth 8, 10 and 12 and optimum minimum distance 24 (except code #7 with minimum distance 8).

For each code, the degree matrix W of the parent convolutional code is given together with the TB length M needed to construct the corresponding (Mc, Mb) block code of block length $N = Mc$ with girth g and minimum distance $d_{\min}$. Table I also includes the minimum distance for the best-known examples of rate $R = 2/5$ QC LDPC codes, which, for the two longer ones (codes #2 and #3), were previously unknown.

Note, all codes in Table I achieving either the upper bound on the minimum distance $d_{\min} = 24$ or on the girth $g = 12$ according to (8) and (7), respectively, are marked by $*$.

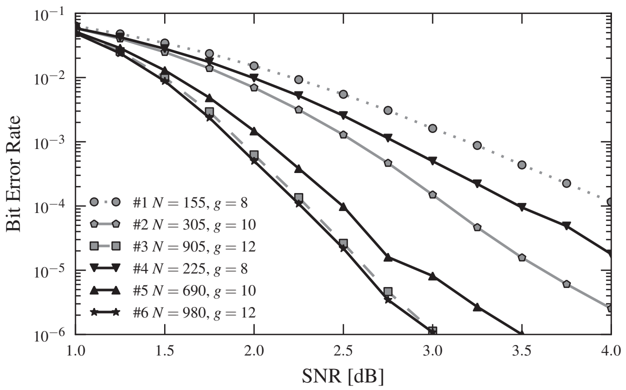

Fig. 3. Bit error rate performance for the best known rate $R = 2/5$ and the newly found rate $R = 2/5$ regular QC block codes of various lengths N using belief propagation with 60 iterations.

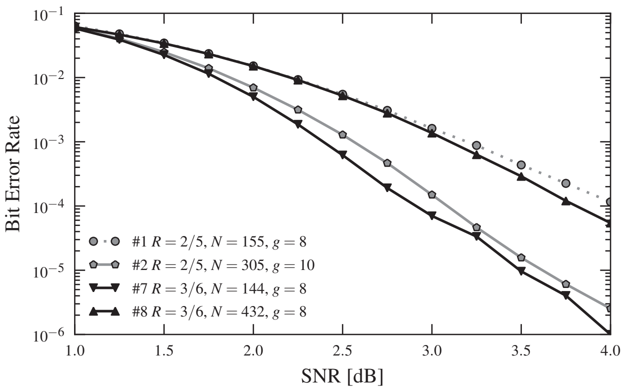

Fig. 4. Bit error rate performance for the best known rate $R = 2/5$ and the newly found rate $R = 3/6$ regular QC block codes of pair-wise approximately same lengths N using belief propagation with 60 iterations.

IX. Bit Error Performance

Using belief propagation decoding [4] with 60 iterations, the bit error rate performance of all regular QC LDPC codes from Table I is simulated and shown in Figs. 3 and 4. The best previously known rate $R = 2/5$ QC LDPC codes are compared with our newly found ones of the same rate in Fig. 3 and with our newly found codes of rate $R = 3/6$ in Fig. 4.

As expected, larger girth leads in general to better bit error rate performance. However, by comparing codes $\#1$ and $\#4$ or codes $\#2$ and $\#5$ in Fig. 3, we can also conclude that a larger tailbiting length M, and thereby a larger resulting block length N, yields better performance.

However, comparing codes $\#1$ and $\#7$ in Fig. 4, both of approximately the same block length N and girth $g = 8$ but of rates $R = 2/5$ and $R = 3/6$, respectively, as well as minimum distance $d_{\min} = 20$ and $d_{\min} = 8$, respectively, we conclude that the chosen monomials, and thereby the underlying edge voltages μ_{uv}, seem to play the most important role in achieving good bit error rate performance. Comparing codes $\#2$ and $\#8$ supports this assumption, even though their corresponding block length differ slightly more.

X. Conclusion

Using the relation between hypergraphs and LDPC codes, new searching techniques have been presented. Starting from a hypergraph, any number of LDPC codes of different rates can be obtained by tailbiting the corresponding parent convolutional code via its dual generator matrix to different lengths.

By representing hypergraphs in different ways, lower and upper bounds on the girth as well as on the minimum distance of the corresponding tailbiting block code have been obtained.

Algorithms for finding hypergraphs with optimum or almost optimum girth and for determining their minimum distance have been presented. Their bit error rate performance has been compared using belief propagation decoding, verifying that a larger girth result in an overall better code performance.

Acknowledgements

This research was supported in part by the Swedish Research Council under Grant 621-2007-6281.

References

[1] G. Schmidt, V. V. Zyablov, and M. Bossert, “On expander codes based on hypergraphs,” in *Proc. IEEE International Symposium on Information Theory (ISIT’03)*, Yokohama, Japan, Jun. 29 – Jul. 4, 2003, p. 88.

[2] A. Barg and G. Zemor, “Distance properties of expander codes,” *IEEE Trans. Inf. Theory*, vol. 52, no. 1, pp. 78–90, Jan. 2006.

[3] I. E. Bocharova, R. Johannesson, B. D. Kudryashov, and V. V. Zyablov, “Woven graph codes: Asymptotic performances and examples,” *IEEE Trans. Inf. Theory*, vol. 56, no. 1, pp. 121–129, Jan. 2010.

[4] A. Shokrollahi, “LDPC codes: An introduction,” in *Coding, cryptography, and combinatorics*, ser. Progress in Computer Science and Applied Logic (PCS), K. Feng, H. Niederreiter, and C. Xing, Eds. Basel, Switzerland: Birkhäuser Verlag, 2004, vol. 23, pp. 85–110.

[5] M. P. C. Fossorier, “Quasi-cyclic low-density parity-check codes from circulant permutation matrices,” *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1788–1793, Dec. 2004.

[6] R. M. Tanner, “A $[155, 64, 20]$ sparse graph (LDPC) code,” presented at the Recent Results Session at IEEE International Symposium on Information Theory (ISIT’00), Sorrento, Italy, Jun. 25–30, 2000.

[7] R. Tanner, D. Sridhara, and T. Fuja, “A class of group-structured LDPC codes,” in *Proc. ISTA*, Ambleside, England, 2001.

[8] R. M. Tanner, D. Sridhara, A. Sridharan, T. E. Fuja, and D. J. Costello Jr., “LDPC block and convolutional codes based on circulant matrices,” *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 2966–2984, Dec. 2004.

[9] S. Kim, J.-S. No, H. Chung, and D.-J. Shin, “Quasi-cyclic low-density parity-check codes with girth larger than 12,” *IEEE Trans. Inf. Theory*, vol. 53, no. 8, pp. 2885–2891, Aug. 2007.

[10] M. O’Sullivan, “Algebraic construction of sparse matrices with large girth,” *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 718–727, Feb. 2006.

[11] R. Johannesson and K. S. Zigangirov, *Fundamentals of Convolutional Coding*. Piscataway, NJ: IEEE Press, 1999.

[12] I. E. Bocharova, B. D. Kudryashov, R. V. Satyukov, and S. Stiglmayr, “Short quasi-cyclic LDPC codes from convolutional codes,” in *Proc. IEEE International Symposium on Information Theory (ISIT’09)*, Seoul, South-Korea, Jun. 28 –Jul. 3, 2009, pp. 551–555.

[13] I. E. Bocharova, B. D. Kudryashov, and R. Satyukov, “Graph-based convolutional and block LDPC codes (in Russian),” *Problems of Information Transmission*, vol. 45, no. 4, pp. 69–90, 2009.

[14] C. Berge, *Graphs and Hypergraphs*. Amsterdam: North Holland, 1976.

[15] X.-Y. Hu, M. Fossorier, and E. Eleftheriou, “On the computation of the minimum distance of low-density parity-check codes,” in *Proc. IEEE International Conference on Communications (ICC’04)*, vol. 2, Paris, France, Jun. 20–24, 2004, pp. 767–771.

[16] R. M. Tanner, “A recursive approach to low complexity codes,” *IEEE Trans. Inf. Theory*, vol. IT-27, no. 5, pp. 533–547, Sep. 1981.

[17] J. L. Gross, “Voltage graphs,” *Discrete Mathematics*, vol. 9, no. 3, pp. 239–246, 1974.

[18] D. J. MacKay and M. C. Davey, “Evaluation of Gallager codes for short block length and high rate applications,” in *Codes, Systems and Graphical Models*. Springer-Verlag, 1999, pp. 113–130.