Double-Hamming based QC LDPC codes with large minimum distance

Bocharova, Irina; Hug, Florian; Johannesson, Rolf; Kudryashov, Boris

Published in:
[Host publication title missing]

DOI:
10.1109/ISIT.2011.6034273

2011

Last Update: May 30, 2011

Double-Hamming Based QC LDPC Codes with Large Minimum Distance

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

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

***Abstract*—A new method using Hamming codes to construct base matrices of (J, K)-regular LDPC convolutional codes with large free distance is presented. By proper labeling the corresponding base matrices and tailbiting these parent convolutional codes to given lengths, a large set of quasi-cyclic (QC) (J, K)-regular LDPC block codes with large minimum distance is obtained. The corresponding Tanner graphs have girth up to 14. This new construction is compared with two previously known constructions of QC (J, K)-regular LDPC block codes with large minimum distance exceeding $(J + 1)!$. Applying all three constructions, new QC (J, K)-regular block LDPC codes with $J = 3$ or 4, shorter codeword lengths and/or better distance properties than those of previously known codes are presented.**

I. Introduction

During the last decade low-density parity-check (LDPC) codes invented in the sixties [1] have attracted a lot of attention as being the main competitors of turbo-codes [2]. One important class of LDPC codes is the class of quasi-cyclic (QC) LDPC codes. It is well-known that such codes can be represented in the form of tailbitten convolutional codes, which supports searching for new codes with low encoding complexity.

Typically, the length of the shortest cycle in the Tanner graph of a QC LDPC code, that is, the *girth*, is considered to be one of the important code parameters, as it determines the number of independent iterations in low-complexity belief-propagation decoding. However, the minimum distance of such codes is significantly smaller compared to the best known linear codes with the same length and dimension.

Note that the error correcting capability of belief-propagation decoding does not depend directly on the minimum distance. However, as the existence of low-weight codewords can lead to the error-floor phenomenon, that is, in the high signal-to-noise (SNR) region the bit error probability decreases very slowly with growing SNR, LDPC codes with large minimum distance are of particular interest.

A (J, K)-regular QC LDPC block code is a quasi-cyclic code with exactly J ones in each column and exactly K ones in each row of its parity-check matrix. It can be determined by an $M(c-b)\times Mc$ binary parity-check matrix or, in polynomial form, by a $(c - b) \times c$ parity-check matrix of its parent rate $R = b/c$ convolutional code, where M is the corresponding tailbiting length.

Let $H(D)$ denote a $(c - b) \times c$ polynomial parity-check matrix of a parent convolutional code, then the integer matrix B is called the corresponding *base matrix* if it satisfies $B = H(D)\big|_{D=1}$. Thus it is possible to interpret the construction of QC LDPC codes as labeling base matrices with proper polynomials. Such polynomials can belong to different classes. The most commonly used structure of a parent convolutional code implies that each entry of $H(D)$ is monomial, that is, $D^{w_{ij}}$, where w_{ij} is a nonnegative integer, or zero. The base matrix in this case consists of only zeros and ones. As a straight-forward generalization binomial and trinomial entries are considered in [3], [4]. The corresponding base matrices contain symbols from $\{0, 1, 2\}$ and $\{0, 1, 2, 3\}$, respectively. Base matrices constructed from Steiner Triple Systems were considered in [5].

Among a large number of papers studying QC LDPC codes only a small fraction focuses on their minimum distance. The upper-bound $(J + 1)!$ on the minimum distance of QC LDPC codes constructed from all-ones base matrices is presented in [6], [7]. In particular $d_{\text{min}} \leq 24$ for $J = 3$. A lower bound on the minimum distance of such LDPC codes was derived in [8] and improved for some special cases in [9]. Some short codes with $J = 3$ achieving the upper bound $(J + 1)! = 24$ were found in [10] by computer search. In [11] the minimum distance of the well known $(155, 64, 20)$ $(J = 3, K = 5)$-regular code is computed. Moreover, in [12], [3], [4] a generalized approach of [6] is used to derive upper bounds on the minimum distance of QC LDPC codes with base matrices containing zeros and ones and of QC LDPC codes constructed from base matrices labeled by binomials and trinomials. Finally, in [13], [14] it is shown that the minimum distance of $(J = 3, K)$-regular QC LDPC codes constructed from Steiner Triple Systems STS(m) of order m, where $m = 1, 3 \mod 6$ except $m = 7$ and 13, is lower-bounded by 6.

It is well-known that by labeling the all-ones base matrix, $(J = 3, K)$-regular QC LDPC codes with girth up to 12 and minimum distance up to 24 can be obtained. In order to increase both the minimum distance and the girth of the code, base matrices with zero and nonzero entries together with monomial, binomial, and trinomial labelings have to be used. For example, in [5] the class of $(J = 3, K)$-regular

QC LDPC codes constructed from Steiner Triple Systems with monomial labelings and girth up to 18 is presented. The disadvantage of these codes is their high computational complexity for both searching and encoding. Generalizing this construction to $(J \geq 3, K)$-regular QC LDPC codes requires very large base matrices which further increases the computational complexities.

In [4], $(J = 3, K)$-regular QC LDPC codes determined by polynomial parity-check matrices constructed from binomial and trinomial labelings of $J \times K$ base matrices with girth less than or equal to 10 were analyzed. In particular, it was shown that by using trinomial labelings, only codes with girth 6 can be obtained. However, a generalization of this construction to $J \geq 3$ is not straight-forward.

The above mentioned shortcomings of the existing code constructions motivated the introduction and study of a class of $(J \geq 3, K)$-regular QC LDPC codes constructed from $(2J \times 2K)$ base matrices with zeros and ones obtained by using two parity-check matrices of the Hamming $(2^J - 1, J)$ linear block code together with monomial labelings. In the following, we will call these codes *double-Hamming based* QC LDPC codes. It is shown that codes of this class can achieve girth up to 14. Upper bounds on the minimum distances for such a construction are obtained for given labelings by calculating the free distance of the corresponding parent convolutional code. Applying this approach to QC LDPC codes with $J \geq 3$ is straight-forward. An example of a base matrix with $J = 4$ is given.

The proposed construction is compared with constructions of $(J=3, K)$-regular QC LDPC codes considered in [4] and [5] and new codes for all three constructions are presented. Thereby, we focus mostly on finding the minimum distance of QC LDPC codes under restrictions on their girth, using either monomial or binomial labelings. In particular, new codes with girth 8 and 10 obtained from the double-Hamming based construction with minimum distances up to 32 are found. Moreover, we included the previously unknown minimum distance for some codes presented in [5] for comparison.

II. Tailbitten convolutional LDPC codes and their Tanner graphs

A rate $R = b/c$ parent convolutional LDPC code of memory m is determined by its polynomial parity-check matrix $H(D)$

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

where $h_{ij}(D)$ is either zero, monomial or binomial, that is, $h_{ij}(D) = a_{1,ij}D^{w_{1,ij}} + a_{2,ij}D^{w_{2,ij}}$, where $a_{1,ij}, a_{2,ij} \in \{(0,0),(1,0),(1,1)\}$ and $w_{k,ij}$, $k = 1, 2$, are nonnegative integers.

By tailbiting the parent convolutional code to length $M > m$ we obtain the parity-check matrix

$$H_{\text{TB}}^{\text{T}} = \begin{pmatrix} H_0^{\text{T}} & H_1^{\text{T}} & \dots & H_{m-1}^{\text{T}} & H_m^{\text{T}} & \mathbf{0} \\ \mathbf{0} & H_0^{\text{T}} & H_1^{\text{T}} & \dots & H_{m-1}^{\text{T}} & H_m^{\text{T}} \\ H_m^{\text{T}} & \mathbf{0} & H_0^{\text{T}} & H_1^{\text{T}} & \dots & H_{m-1}^{\text{T}} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ H_1^{\text{T}} & \dots & H_{m-1}^{\text{T}} & H_m^{\text{T}} & \mathbf{0} & H_0^{\text{T}} \end{pmatrix} \quad (2)$$

of an (Mc, Mb) QC LDPC block code, where

$$H(D) = H_0 + H_1 D + \dots + H_m D^m$$

and H_i, $i = 0, 1, \dots, m$, are binary $(c - b) \times c$ matrices.

Notice that by reordering columns and rows of (2) we can obtain a parity-check matrix of an equivalent (Mc, Mb) block code, consisting of $(c - b) \times c$ circulants of size $M \times M$. The free distance d_{free} of the parent convolutional code upper-bounds the minimum distance d_{min} of the corresponding QC LDPC block code.

As previously mentioned, the polynomial parity-check matrix $H(D)$ (1) can be interpreted as a base matrix B labeled by the corresponding polynomials, where B is a $(c - b) \times c$ matrix with positive nonzero integers on positions of nonzero entries of $H(D)$. In particular, monomial entries in $H(D)$ correspond to the integer 1 in the base matrix, while binomial entries correspond to the integer 2. Both B and H_{TB} can be considered as *biadjacency matrices* [15] of their corresponding Tanner graphs [8]. In other words, we can reduce the problem of finding new QC LDPC codes to the problem of labeling a base Tanner graph determined by the biadjacency matrix B. The length of the shortest cycle in the graph constructed from the biadjacency matrix given by the parity-check matrix H_{TB} is called the girth g and is used as a target when searching for good QC LDPC codes. Similarly, denote the girth of the graph constructed by the biadjacency matrix given by the base matrix B and by the parity-check matrix $H(D)$ of the parent convolutional code by g_{B} and g_{free}, respectively, where the girth g_{free} is an upper bound on the girth g.

In the next section three constructions with base matrices of different types are compared. Upper bounds on the minimum distance for given labelings are calculated and restrictions on the girth g for the three different constructions are discussed.

III. Three constructions of QC LDPC codes

A. Binomial QC LDPC codes

We start by considering QC LDPC block codes constructed from a $J \times K$ base matrix B with binomial labeling, that is, with both binomial and monomial labelings. Such a construction was proposed and analyzed in [3] and [4]. The parent convolutional code of such a QC LDPC block code is determined by a polynomial parity-check matrix containing only zeros, monomials, and binomials, constructed from the corresponding base matrix with integer entries $\{0, 1, 2\}$. In [4] the related upper bounds on the girth and on the minimum distance of QC LDPC block codes for this class of codes are obtained. More precisely, for codes of rate $R = 1/4$ it is shown that depending on the labeling the minimum distance is upper-bounded either by 32 with girth ≤ 8 or by 30 and 28 with girth

TABLE I
PARAMETERS FOR NEW BINOMIAL RATE $R = 1/4$
$(J = 3,\ K = 4)$-REGULAR QC LDPC CODES

(n, k, $d_{\min}$)	M	d_{free}	g	Labeling
$(96, 25, 24)$	24	30	8	$(4, 0), (13), (4)$; $(4), (3), (0, 1)$; $(10, 0), (3, 0)$
$(112, 29, 26)$	28	30	8	
$(124, 32, 28)$	31	30	8	
$(144, 37, 30)$	36	30	8	
$(108, 28, 24)$	27	28	8	$(0, 2), (13), (2)$; $(10), (3), (0, 1)$; $(13, 0), (0, 3)$
$(116, 30, 26)$	29	30	8	
$(136, 35, 28)$	34	30	8	
$(152, 39, 30)$	38	30	8	

≤ 10. For rate $R = 2/5$ the minimum distance is less than or equal to 28 with girth ≤ 8. In particular, a $(184, 47, 32)$ QC LDPC block code with girth $g = 8$ achieving the upper bound on the minimum distance is presented.

Starting from the base matrix

$$B = \begin{pmatrix} 2 & 0 & 1 & 1 \\ 1 & 1 & 2 & 0 \\ 0 & 2 & 0 & 2 \end{pmatrix} \tag{3}$$

we applied the search algorithm presented in [16] using random labelings to obtain such a labeling, that the Tanner graph determined by the biadjacencey matrix, which is given by the parity-check matrix of the corresponding tailbiting block code, has a given girth g. Using the strengthened algorithm [10], we calculated the corresponding minimum distance and found in such a way new QC LDPC block codes with minimum distance up to 30 as well as a new QC LDPC block code with the very short codeword length $n = 96$ and minimum distance $d_{\min} = 24$.

The obtained results are summarized in Table I, where n is the code length and k is the code dimension. The free distance of the parent convolutional code is given by d_{free} while the minimum distance and girth of the corresponding QC LDPC block code after tailbiting to length M are given by $d_{\min}$ and g, respectively. The obtained labeling of the base graph B is specified in the last column, where the labelings for each row are separated by semicolon. In particular, a tuple (a, b) corresponds to a binomial entry $(D^a + D^b)$ while a single value (a) specifies a monomial entry (D^a). Finally, note that positions with zero entries in the base matrix B are omitted, that is, the jth labeling in the kth row (block) corresponds to the jth nonzero entry in the kth row of the base matrix B. According to [4], the minimum distance and girth of any QC LDPC block code obtained from the base matrix (3) is upper-bounded by $d_{\min} \leq 32$ and $g \leq 8$.

In [4] a special type of monomial labeling for $2J \times 2K$ base matrices with zeros and ones, obtained from shorter base matrices with binomial labeling, was studied. The minimum distance of this construction is upper-bounded by 64 and a $(J = 3, K = 4)$-regular QC LDPC block code of length $n = 368$ whose corresponding Tanner graph has girth $g = 8$ is presented. We calculated the minimum distance of this code to be $d_{\min} = 32$, reaching the upper-bound determined by the free distance of the corresponding parent convolutional code with $d_{\text{free}} = 32$. Furthermore, it is easy to verify that the girth of this construction is limited by a maximum girth of 8 since there always exists a submatrix within the parity-check matrix which can be normalized to

$$\begin{pmatrix} 1 & D^a & 1 & D^b \\ D^a & 1 & D^b & 1 \end{pmatrix} \tag{4}$$

where a and b are nonnegative integers, that is, it corresponds to a cycle of length 8 in the corresponding Tanner with labeling $-0 + b - 0 + 0 - a + 0 - b + a = 0$.

B. Double-Hamming based QC LDPC codes

Next we consider a new class of rate $R = b/c$ QC LDPC block codes constructed from $(2J \times 2K)$ base matrices of zeros and ones with monomial labeling. In this case the base matrix B is constructed using the parity-check matrix of the Hamming code, that is,

$$B = \begin{pmatrix} I_J & P & \mathbf{1} & \mathbf{0} & W_1 \\ P_{\text{p}} & I_J & \mathbf{0} & \mathbf{1} & W_2 \end{pmatrix} \tag{5}$$

where I_J is the identity matrix of size $J \times J$, the submatrix $(P\ \ \mathbf{1})$ corresponds to the parity part of the parity-check matrix of the Hamming $(2^J - 1$,$J)$-code, $\mathbf{0}$, $\mathbf{1}$ are the all-zero and all-one column vectors, respectively, and P_{p} is a permutation of P.

Depending on the desired rate of the QC LDPC block code, the dimensions of the matrices W_1 and W_2 are adjusted correspondingly to $J \times (c - 2^J)$. Note that the columns of W_1 and W_2 can be chosen arbitrarily with the restriction that the number of nonzero elements in each column and in each row of the base matrix B have to be equal to J and K, respectively, and that there are no identical columns in B.

For example, the base matrix B for an $R = 2/8$ $(J = 3, K = 4)$-regular QC LDPC code can be chosen as

$$B = \left(\begin{array}{ccc|ccc|c|c} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ \hline 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \end{array}\right) \tag{6}$$

where the matrices W_1 and W_2 are not present.

It is easy to verify that there exist always some columns in the base matrix B that coincide in two positions, and thus the girth of the corresponding Tanner graph follows as $g_{\text{B}} = 4$. According to Theorem 2 [10] the achievable girth of a Tanner graph constructed from the biadjacency matrix obtained by labeling the nonzero positions in B, is $g_{\text{free}} \geq 3g_{\text{B}} \geq 12$. However, as the second generalized Hamming distance d_2 of the $R = 10/24$ convolutional code whose parity-check matrix coincides with the incidence matrix of the Tanner graph specified by the base matrix (6) is equal to 7, it follows from the same theorem that a code with $g \geq 2d_2 = 14$ exists. The $(2112, 528)$ QC LDPC block code with $g = 14$

TABLE II
PARAMETERS OF NEW DOUBLE-HAMMING BASED RATE $R = 1/4$ $(J = 3, K = 4)$-REGULAR, $R = 2/5$ $(J = 3, K = 5)$-REGULAR AND $R = 1/2$ $(J = 3, K = 6)$-REGULAR QC LDPC CODES

$(n, k, d_{\min})$	$d_{\text{free}}(\widehat{d}_{\text{free}})$	g	Labeling
Rate $R = 1/4$			
$(168, 42, 30)$	$54\ (\le 66)$	8	$7, 3, 0, 5$ **;** $1, 0, 4, 10$ **;** $0, 4, 7, 9$ **;** $7, 6, 0, 3$ **;** $0, 0, 7, 6$ **;** $7, 7, 0, 10$
$(160, 40, 32)$	$76\ (\le 102)$	10	$0, 6, 15, 11$ **;** $6, 9, 0, 0$ **;** $6, 0, 2, 14$ **;** $19, 0, 12, 4$ **;** $13, 4, 0, 4$ **;** $12, 0, 5, 0$
Rate $R = 2/5$			
$(380, 144, 26)$	$\ge 40\ (\le 72)$	8	$0, 5, 0, 19, 9$ **;** $3, 0, 0, 11, 0$ **;** $3, 12, 9, 0, 4$ **;** $0, 0, 12, 9, 14$ **;** $6, 5, 13, 0, 2$ **;** $5, 0, 5, 0, 0$
$(370, 148, \ge 30)$ $(d_{\min} \le 36)$	$\ge 38\ (\le 86)$	10	$0, 22, 28, 6, 24$ **;** $0, 7, 0, 0, 11$ **;** $0, 8, 25, 0, 0$ **;** $19, 6, 0, 15, 0$ **;** $14, 8, 0, 31, 21$ **;** $0, 11, 5, 27, 6$
Rate $R = 1/2$			
$(1080, 540, \ge 28)$	(≤ 90)	10	$40, 47, 17, 77, 36, 10$ **;** $19, 74, 43,$ $24, 86, 31$ **;** $86, 56, 3, 83, 52, 56$ **;** $26, 38, 0, 22, 81, 25$ **;** $77, 47, 13,$ $6, 6, 70$ **;** $76, 0, 56, 11, 20, 57$

was found by labeling the rows in (6) as follows, $(0, 0, 0, 0)$, $(0, 13, 0, 181)$, $(0, 87, 66, 101)$, $(7, 260, 245, 0)$, $(0, 124, 33, 6)$, $(107, 0, 130, 55)$, where the ith entry within the jth 4-tuple corresponds to the monomial degree of the ith nonzero entry in the jth row of the base matrix. Notice that so far, the shortest published QC LDPC code of rate $R = 1/4$ with $g = 14$ has length 2208 [5].

Moreover, this construction can be generalized in a straight forward manner to $J \ge 3$. Consider, for example, the rate $R = 8/16$ base matrix with $J = 4$ given by

$$B = \begin{pmatrix} I_4 & P_1 & P_2 & \mathbf{1} & \mathbf{0} & W_1 \\ P_{2\text{p}} & P_{1\text{p}} & I_4 & \mathbf{0} & \mathbf{1} & W_2 \end{pmatrix} \tag{7}$$

where the parity part P of the Hamming code in (5) has been split into two submatrices P_1 and P_2 for notational convenience. In particular, the submatrices of the parity part of the corresponding Hamming code are given by $P_2 = P_{2\text{p}} = I_4^{\text{c}}$, that is, the complement of the identity matrix I_4,

$$P_1 = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 \end{pmatrix} \tag{8}$$

and

$$P_{1\text{p}} = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{9}$$

TABLE III
PARAMETERS OF NEW RATE $R = 1/4$ $(J = 3, K = 4)$-REGULAR QC LDPC CODES CONSTRUCTED FROM STEINER TRIPLE SYSTEMS

$(n, k, d_{\min})$	$d_{\text{free}}(\widehat{d}_{\text{free}})$	g	Labeling
Rate $R = 1/4$ (STS(9))			
$(168, 42, 30)$	$38\ (\le 84)$	8	$1, 0, 1, 0$ **;** $0, 2, 4, 3$ **;** $0, 2, 0, 1$ **;** $0, 5, 2, 0$ **;** $1, 1, 0, 2$ **;** $4, 3, 4, 4$ **;** $2, 7, 0, 0$ **;** $0, 0, 4, 4$ **;** $0, 0, 3, 3$
$(216, 54, 34)$	$\ge 62\ (\le 172)$	10	$0, 1, 3, 0$ **;** $14, 11, 0, 0$ **;** $7, 12, 0, 3$ **;** $4, 0, 5, 13$ **;** $0, 9, 3, 0$ **;** $10, 0, 3, 11$ **;** $0, 2, 3, 4$ **;** $0, 0, 4, 12$ **;** $1, 8, 0, 12$
$(144, 36, 28)$	$46\ (\le 98)$	10	as specified in [5]

Using the base matrix (7) and tailbiting to length $M = 1168$, a $(18688, 9344)$ QC $(J{=}4, K{=}8)$-regular LDPC block code with girth $g = 10$ was found. The corresponding labeling is omitted due to space restrictions, but is available at [17].

Parameters of new QC LDPC block codes found by labeling the base matrix (6) with monomials are presented in Table II, where n is the code length and k the code dimension. The free distance of the parent convolutional code is, if possible, given by d_{free} together with the corresponding upper bound $\widehat{d}_{\text{free}}$, computed by applying the approach of [4], [12], that is,

$$\widehat{d}_{\text{free}} = \min_{J} \sum_{i=1}^{c-b+1} W(\Delta_{J,i}) \tag{10}$$

where J is a subset of $c - b$ columns of the parity-check matrix $H(D)$, and $W(\Delta_{J,i})$, $i = 1, 2, \ldots, c - b + 1$, denotes the weight of the corresponding polynomial determinant.

The minimum distance and girth of the corresponding QC LDPC block code after tailbiting to length M are given by $d_{\min}$ and g, respectively, while the obtained labeling of the base graph B is specified in the last column, separating the labelings for each row by a semicolon. As positions with zero entries with the base matrix B are omitted, the jth labeling in the kth block corresponds to the jth nonzero entry in the kth row of the base matrix B. So far, the shortest published $R = 2/5$ $(J{=}3, K{=}5)$-regular QC LDPC code with $g = 10$ has length $n = 550$ [5].

Finally, consider the base matrix B as a matrix of weights of polynomials. Applying the same approach as before, we obtain an upper bound on the free distance, equal to 110, for the presented construction independently of the chosen labeling.

C. Steiner Triple System based QC LDPC codes

A third class of QC LDPC codes was previously considered in [5]. Codes from this class are obtained by labeling base matrices constructed from Steiner Triple Systems and integer lattices. It is proven [5] that the girth of the base Tanner graphs from this class is at least $g_{\text{B}} = 6$, that is, the achievable girth of the labeled Tanner graph is lower-bounded by 18. Examples of QC LDPC codes of this type with girth of their Tanner graphs equal to 14, 16, and 18 are presented in [5].

In Table III, examples of QC LDPC codes from the third class with computed minimum distances and girths are given. One of the codes was found in [5] but we calculated its minimum distance and by applying the BEAST algorithm

[18] the free distance of its parent convolutional code. The other codes are new, found by applying our labeling algorithm [16], [19] using base matrices from [5], and they have better minimum distances.

IV. Conclusion

Advantages of our new double-Hamming based construction of QC LDPC codes compared to the constructions using binomial and trinomial labelings are a higher achievable girth and a straight-forward generalization to larger J values. The Steiner Triple System based construction can achieve a larger girth, but is limited to QC (J, K)-regular LDPC block codes with $J = 3$. Moreover, due to the large sizes of their base matrices the LDPC block codes constructed by this method are much longer than those obtained by using the newly presented construction based on Hamming codes.

Acknowledgements

This research was supported in part by the Swedish Research Council under Grant 2010-5847.

References

[1] R. G. Gallager, "Low-density parity-check codes," *IRE Trans. Inform. Theory*, vol. IT-8, no. 1, pp. 21–28, Jan. 1962.

[2] A. G. C. Berrou and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo codes," in *Proc. IEEE International Conference on Communications (ICC'93)*, vol. 2, Geneva, Switzerland, May 23–26, 1983, pp. 1064–1070.

[3] R. Smarandache and P. O. Vontobel, "On Regular Quasi-Cyclic LDPC Codes from Binomials," in *Proc. IEEE International Symposium on Information Theory (ISIT'04)*, Chicago, USA, Jun. 27 – Jul. 2, 2004, p. 274.

[4] ——, "Quasi-cyclic LDPC codes: Influence of Proto- and Tanner-Graph Structure on Minimum Hamming Distance Upper Bounds," *IEEE Trans. Inf. Theory*, arXic:0901.4129v1 [cs.IT] 26 Jan 2009, submitted for publication.

[5] M. Esmaeili and M. Gholami, "Structured quasi-cyclic LDPC codes with girth 18 and column-weight $J \geq 3$," *Int. Journal of Electron. and Commun. (AEU)*, vol. 64, no. 3, pp. 202–217, 2010.

[6] 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.

[7] 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, Aug. 2004.

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

[9] O. Milenkovic, N. Kashyap, and D. Leyba, "Shortened Array Codes of Large Girth," *IEEE Trans. Inf. Theory*, vol. 52, no. 8, pp. 3707–3722, Aug. 2006.

[10] I. E. Bocharova, F. Hug, R. Johannesson, B. D. Kudryashov, and R. V. Satyukov, "New Low-Density Parity-Check Codes with Large Girth Based on Hypergraphs," in *Proc. IEEE International Symposium on Information Theory (ISIT'10)*, Austin, Texas, Jun. 13 – 18, 2010, pp. 819–823.

[11] R. M. Tanner, D. Sridhara, and T. Fuja, "A Class of Group-Structured LDPC Codes," in *Proc. ISTA*, Ambleside, England, 2001.

[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'10)*, Austin, Texas, Jun. 13 – 18, 2010, pp. 551–555.

[13] S. J. Johnson and S. R. Weller, "Regular low-density parity-check codes from combinatorial designs," in *Proc. IEEE Inform. Theory Workshop (ITW'01)*, Cairns, Australia, pp. 90–92.

[14] ——, "Construction of Low-density Parity-check Codes from Kirkman Triple Systems," in *Proc. IEEE Global Telecommunications Conference (GLOBECOM'01)*, vol. 2, San Antonio, USA, Nov. 25–29, 2001, pp. 970–974.

[15] A. S. Asratian, T. M. J. Denley, and R. Haggkvist, *Bipartite Graphs and Their Applications*. Cambridge University Press, 1998.

[16] I. E. Bocharova, F. Hug, R. Johannesson, B. D. Kudryashov, and R. V. Satyukov, "Some voltage graph-based LDPC tailbiting codes with large girth," in *Proc. IEEE International Symposium on Information Theory (ISIT'11)*, St. Petersburg, Russia, Jul. 31 – Aug. 5, 2011.

[17] Labelings for QC LDPC codes. [Online]. Available: http://www.eit.lth.se/goto/QC_LDPC_Codes

[18] I. E. Bocharova, M. Handlery, R. Johannesson, and B. D. Kudryashov, "A BEAST for prowling in trees," *IEEE Trans. Inf. Theory*, vol. 50, no. 6, pp. 1295–1302, Jun. 2004.

[19] I. E. Bocharova, F. Hug, R. Johannesson, B. D. Kudryashov, and R. V. Satyukov, "Searching for Voltage Graph-Based LDPC Tailbiting Codes with Large Girth," submitted.