

Woven convolutional graph codes with large free distances

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

Published in:

Problems of Information Transmission

DOI:

10.1134/S0032946011010017

2011

Link to publication

Citation for published version (APA):

Bocharova, I., Hug, F., Johannesson, R., & Kudryashov, B. (2011). Woven convolutional graph codes with large free distances. *Problems of Information Transmission*, *47*(1), 1-14. https://doi.org/10.1134/S0032946011010017

Total number of authors:

General rights

Unless other specific re-use rights are stated the following general rights apply:

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.

 • You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

Read more about Creative commons licenses: https://creativecommons.org/licenses/

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

1

Woven Convolutional Graph Codes with Large Free Distances

I. E. Bocharova¹, F. Hug², R. Johannesson², and B. D. Kudryashov¹

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

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

Abstract

Constructions of woven graph codes based on constituent convolutional codes are studied and examples of woven convolutional graph codes are presented. The existence of codes, satisfying the Costello lower bound on the free distance, within the random ensemble of woven graph codes based on s-partite, s-uniform hypergraphs, where s depends only on the code rate, is shown. Simulation results for Viterbi decoding of woven graph codes are presented and discussed.

Index Terms

Convolutional codes, girth, graphs, graph codes, hypergraphs, LDPC codes, tailbiting codes, woven codes.

I. INTRODUCTION

Woven graph codes are concatenated graph-based codes with constituent block or convolutional codes [1], [2]. The distinguishing feature of these codes is that the length of the constituent code is a multiple of the underlying graph degree c, that is, their length is equal to lc, where l is an integer. In particular, when l tends to infinity we obtain woven graph codes with constituent convolutional codes. While for example serial concatenated convolutional codes are obtained by combining generator matrices, woven graph codes are obtained by combining the corresponding parity-check matrices.

In [2], the existence of codes, satisfying the Varshamov-Gilbert (VG) bound, within the random ensemble of woven codes based on *s-partite*, *s-uniform hypergraphs*, where *s* depends only on the code rate, and constituent block codes, was proven. Due to the simple structure of woven graph codes, such codes can be analyzed with low computational complexity while their minimum distances are rather close to the minimum distances of the best known linear codes of same lengths and dimensions. Moreover, there exist linear-time encoding algorithms for this class of codes.

In this paper, we will generalize the VG bound [2] to the corresponding bound for woven graph codes with constituent convolutional codes, namely the Costello bound. Therefore, we consider woven graph codes with constituent convolutional codes, based on s-partite, s-uniform hypergraphs, in the following referred to as woven convolutional graph codes. Let the overall constraint length of woven convolutional graph codes tend towards infinity. Then, within the random ensemble of such convolutional codes with $s \ge 2$, codes satisfying the Costello lower bound on the free distance exist for any rate. Examples of woven convolutional graph codes with surprisingly large free distances are presented. Additionally, their bit error probabilities for Viterbi decoding are compared with the best known convolutional codes of the same overall constraint length.

In Section II, properties of s-partite, s-uniform, c-regular hypergraphs are introduced. A compact representation of hypergraphs as well as their relationship to Tanner graphs are discussed. Hypergraph-based block codes are defined

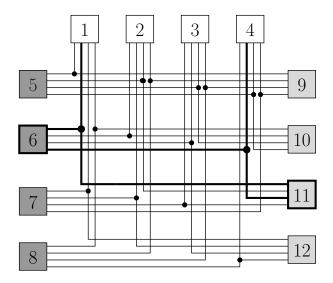


Fig. 1. A 3-partite, 3-uniform, 4-regular hypergraph with its shortest cycle being highlighted.

in Section III. Section IV is devoted to generalizations of such codes to woven graph codes with constituent block and convolutional codes. The Costello lower bound on the free distance of the random ensemble of woven convolutional graph codes is derived in Section V, and examples of promising woven convolutional graph codes are presented in Section VI. The paper is concluded by a discussion of simulation results of Viterbi decoding of woven convolutional graph codes in Section VII.

II. GRAPHS AND HYPERGRAPHS

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.

Hereinafter, we will consider only s-partite, s-uniform, c-regular hypergraphs. Such hypergraphs consist of a union of s disjoint subsets of vertices \mathcal{V}_k , $k=1,2,\ldots,s$, where each vertex is connected to s-1 vertices, one in each of the other subsets and has no connection within its own subset.

In Fig. 1, a 3-partite, 3-uniform, 4-regular hypergraph is illustrated with its three disjoint vertex subsets being represented by vertices with different shades of gray. Every hyperedge connects three vertices, one from each of the three different vertex subsets.

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. Such a simple cycle is also known as a Berge cycle [3]. Finally, the girth of a hypergraph is the length of its shortest simple cycle. The shortest cycle of the previously mentioned 3-partite, 3-uniform, 4-regular hypergraph is highlighted in bold in Fig. 1. It consists of the vertices 6, 11, and 6 and thereby has girth equal to 2.

Consider the hypergraph as illustrated in Fig. 1. The corresponding incidence matrix follows as

and can be interpreted as 12×16 parity-check matrix H_{hg} of a hypergraph code \mathcal{C}_{hg} . Each column corresponds to a hyperedge and each row represents a vertex of the hypergraph, with the three disjoint sets of vertices being separated by dashed horizontal lines. The first column represents the hyperedge connecting the vertices 1, 5 and 9, the second column the hyperedge connecting the vertices 1, 8 and 10, and so on.

By reordering the rows of (1), an equivalent parity-check matrix $H'_{\rm hg}$ (2) is obtained. Using the concept of duality, the equivalent parity-check matrix $H'_{\rm hg}$ of this hypergraph code is equal to the generator matrix $G^{\perp}_{\rm hg}$ of the corresponding dual hypergraph code $\mathcal{C}^{\perp}_{\rm hg}$,

Clearly, the generator matrix G_{hg}^{\perp} of the rate R=(sn)/(cn) dual hypergraph code $\mathcal{C}_{\mathrm{hg}}^{\perp}$ can be interpreted as a tail-bitten convolutional code, obtained by tailbiting a parent convolutional code $\mathcal{C}_{\mathrm{hg}}^{\perp\mathrm{p}}$ to length n, with its corresponding generator matrix $G_{\mathrm{hg}}^{\perp\mathrm{p}}(Z)$ being specified by

$$\begin{split} G_{\text{hg}}^{\perp \text{p}}(Z) &= \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} Z + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} Z^2 + \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} Z^3 \\ &= \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & Z & Z^2 & Z^3 \\ 1 & Z^3 & Z & Z^2 \end{pmatrix} \end{split}$$
(3)

with free distance $d_{\text{free}} = 4$. Interpreting (3) as a convolutional parity-check matrix, we obtain the corresponding convolutional code C_{hg}^{p} with free distance $d_{\text{free}} = 8$. We use Z as the delay operator for the parent convolutional codes in order to distinguish it from the delay operator D of the constituent convolutional codes introduced later.

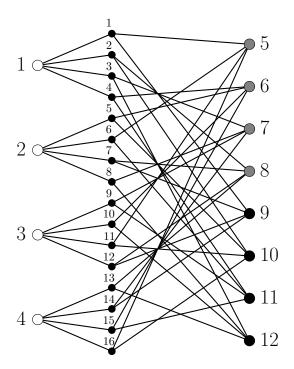


Fig. 2. A Tanner graph representation of the 3-partite, 3-uniform, 4-regular hypergraph illustrated in Fig. 1.

By tailbiting the generator matrix (3) of a rate R = s/c, memory m, parent convolutional code $\mathcal{C}_{hg}^{\perp p}$ to length n, where n is any integer such that n > m, a set of generator matrices of dual hypergraph codes \mathcal{C}_{hg}^{\perp} with different rates R = (sn)/(cn) can be obtained.

Interpreting these generator matrices as incidence matrices and parity-check matrices of hypergraphs, we can construct a set of woven graph codes with different rates, having some common properties [4] and being related to the same underlying graph. Moreover, this set of woven graph codes can be compactly represented by the generator matrix $G_{\rm hg}^{\perp \rm p}(Z)$ of the parent convolutional code.

Note that in general not every hypergraph can be represented in such a compact form by the generator matrix of its parent convolutional code. Although such a representation is not necessary for the following proofs and theorems, all examples of hypergraphs within this paper will be given using the generator matrix of their parent convolutional code.

Tanner graphs

By replacing every hyperedge of an *s*-partite, *s*-uniform, *c*-regular hypergraph with a vertex and *s* outgoing edges, we obtain an alternative representation of a hypergraph, a so-called *Tanner graph* [5]. The Tanner graph for the hypergraph shown in Fig. 1 is illustrated in Fig. 2. The three disjoint sets of vertices are represented by white, gray, and black, vertices, respectively.

The newly introduced set of $cn=4\times 4=16$ vertices are denoted *variable* or *symbol nodes*, while the $sn=3\times 4=12$ vertices on the left- and right-hand side are denoted *constraint nodes*. Interpreting the incidence matrix of a hypergraph as the parity-check matrix of a corresponding hypergraph-based code, every symbol node corresponds to one of cn codeword symbols, while every constraint node corresponds to one of sn parity-checks.

III. HYPERGRAPH-BASED BLOCK CODES

A hypergraph-based block code, based on an s-partite, s-uniform, c-regular hypergraph and a rate $R^c = b/c$ constituent block code, is determined by its parity-check matrix

$$H_{\text{hgb}} = \begin{pmatrix} H_1 \\ H_2 \\ \vdots \\ H_s \end{pmatrix} \tag{4}$$

where each of the s parity-check submatrices H_i of size $n(c-b) \times nc$, $i=1,2,\ldots,s$, corresponds to one of the s disjoint sets of vertices. By reordering rows and columns, it is possible, without loss of generality, to represent the first party-check submatrix H_1 by

$$H_1 = \left(egin{array}{cccc} H^{
m c} & \mathbf{0} & \cdots & \mathbf{0} \ \mathbf{0} & H^{
m c} & \cdots & \mathbf{0} \ dots & dots & \ddots & dots \ \mathbf{0} & \mathbf{0} & \cdots & H^{
m c} \end{array}
ight)$$

where H^c is the $(c-b) \times c$ parity-check matrix of the constituent block code and the remaining s-1 parity-check matrices H_i of size $n(c-b) \times nc$, $i=2,3,\ldots,s$, are column permutations of H_1 , determined by the underlying hypergraph.

By choosing b < c and assigning constituent block codes of different rates $R^c = b/c$ to the same hypergraph, we obtain hypergraph-based block codes of different rates. Since the total number of parity-checks of such a block code, based on an s-partite, s-uniform, c-regular hypergraph is at most sn(c-b), the code rate $R_{\rm wg}$ of a hypergraph-based block code follows as

$$R_{\text{hgb}} \ge \frac{nc - sn(c - b)}{nc} = s(R^{c} - 1) + 1$$
 (5)

with equality if and only if all parity-checks are linearly independent.

Consider the previous parity-check matrix (1). The corresponding hypergraph can be interpreted as a hypergraph-based block code whose constituent block codes are single-parity-check codes with parity-check matrix

$$H^{c} = (1 \ 1 \ 1 \ 1).$$

However, as the rows in (1) are linear dependent, two parity-checks can be removed and we obtain a (16,6) linear block code. Clearly, the rate of this hypergraph-based block code $R_{hgb} = 6/16$ satisfies the inequality (5) as $R_{hgb} \ge 3(3/4-1)+1=1/4$.

By interpreting a hypergraph as a hypergraph-based block code we impose some restrictions on the hypergraph structure. In particular, each vertex corresponds to a constituent code and each codeword has to satisfy the parity checks determined by H^c . Thus, only those cycles of the hypergraph where all participating vertices are incident with the number of hyperedges equal to the Hamming weight of a codeword of the constituent code correspond to codewords of a hypergraph-based block code.

Definition 1: A $(\geq d)$ -cycle in the hypergraph is a cycle whose vertices are incident with at least d hyperedges. Definition 2: The length (number of hyperedges) of the shortest $(\geq d)$ -cycle of an s-partite hypergraph is its (s,d)-girth $g_{s,d}$.

Consider the previously illustrated (16,6) linear block code, determined by the hypergraph-based block code based on the hypergraph (1) and a single parity-check matrix as a constituent block code. With the minimum distance of the constituent block code being $d_{\min}^c = 2$, the minimum distance of the (16,6) linear block code follows as $d_{\min} = g_{3,2}$, where $g_{3,2}$ is the (3,2)-girth.

The shortest (≥ 2) -cycle of the corresponding 3-partite, 3-uniform, 4-regular hypergraph, that is, the (3,2)-girth $g_{3,2}$, has length 4 and is illustrated in Fig. 3. It consists of the hyperedges (2,5,11), (2,6,10), (4,5,10), and (4,6,11).

The corresponding columns participating in this (≥ 2) -cycle are marked in bold in (1) and (2) and form one of the smallest sets of four linearly dependent columns. Thus, it is easy to verify that the minimum distance of the previously mentioned (16,6) linear block code is $d_{\min} = g_{3,2} = 4$.

Notice that the parent convolutional code determined by parity-check matrix (3) has free distance 8 and thus the corresponding "free" (3, 2)-girth is equal to 8 (see the first entry of Table I).

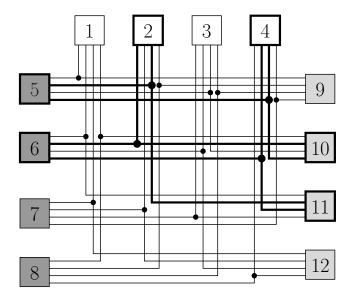


Fig. 3. A shortest (≥ 2) -cycle of the 3-partite, 3-uniform, 4-regular hypergraph illustrated in Fig. 1.

IV. WOVEN GRAPH CODES

Woven graph codes are generalizations of hypergraph-based codes with either constituent block or convolutional codes. Consider a binary (lc, lb) linear block code, determined by the parity-check matrix

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

where $H_{ij}^c \in \mathcal{B}_{l \times l}$, $i = 1, 2, \ldots, (c - b)$, $j = 1, 2, \ldots, c$, are size $l \times l$ submatrices and $\mathcal{B}_{l \times l}$ is the set of all possible binary matrices of size $l \times l$. Then, the corresponding hypergraph-based code of length nlc with a constituent block code, determined by its $l(c - b) \times lc$ parity-check matrix H^c , is called a woven graph code with constituent block codes. While in the case of hypergraph-based codes a codeword of length c is assigned to each vertex, we generalize those codes to woven graph codes by assigning a length c subblock, which is a time-cut of a length c codeword, to each vertex. Such codes were analyzed and discussed in [2].

Woven graph codes with constituent convolutional codes, hereinafter referred to as *woven convolutional graph codes*, can be considered as a straightforward generalization of woven graph codes with constituent block codes.

Let $H^{c}(D)$ denote the minimal-basic $(b-c) \times c$ parity-check matrix [6] of a rate R = b/c convolutional code

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

$$(6)$$

where $h^{\rm c}_{ij}(D)=h^{{\rm c}(0)}_{ij}+h^{{\rm c}(1)}_{ij}D+h^{{\rm c}(2)}_{ij}D^2+\cdots$, $i=1,2,\ldots,(c-b),\ j=1,2,\ldots,c$, are binary polynomials. Denote by $\mathbb{F}_2((D))$ the field of binary Laurent series and regard a rate $R^{\rm c}=b/c$ convolutional code as a rate $R^{\rm c}=b/c$ block code over the field of binary Laurent series. Then, the corresponding codewords are elements of $\mathbb{F}_2^c((D))$, which is a c-dimensional vector space over the field of binary Laurent series [6].

Representing a convolutional code as a block code over the field of binary Laurent series $\mathbb{F}_2((D))$, we obtain woven convolutional graph codes as a generalization of woven graph codes with constituent block codes.

For example, the parity-check matrix $H_{wg}(D)$ of a woven convolutional graph code, based on the hypergraph

with parity-check matrix (1), is given by

where $H^c(D) = \begin{pmatrix} h_1^c(D) & h_2^c(D) & h_3^c(D) & h_4^c(D) \end{pmatrix}$ is the parity-check matrix of the rate $R^c = 3/4$ constituent convolutional code, and $\begin{pmatrix} t_1^c(D), t_2^c(D), t_3^c(D), t_4^c(D) \end{pmatrix}$ and $\begin{pmatrix} l_1^c(D), l_2^c(D), l_3^c(D), l_4^c(D) \end{pmatrix}$ are two out of 24 possible permutations of $\begin{pmatrix} h_1^c(D), h_2^c(D), h_3^c(D), h_4^c(D) \end{pmatrix}$.

Exploiting the above definitions in connection with the Tanner graph representation in Fig. 2, we can regard the n left constituent convolutional codes as a warp with nc threads. Each of the n right constituent convolutional codes are tacked on c of the threads in the warp such that each thread of the warp is tacked on exactly once. Thus, our construction is a special case of a woven code [7].

V. ASYMPTOTIC BOUND ON THE FREE DISTANCE OF WOVEN GRAPH CODES

Consider a woven graph code with a constituent block code, obtained by tailbiting (TB) a rate $R^{\rm c}=b/c$ convolutional code with memory $m^{\rm c}$ and let the length of a codeword of the TB block code in nc-tuples be equal to l. Denote the minimum distance of the woven graph code by $d_{\rm min}^{\rm wg}$, while its rate is given by $R_{\rm wg}=s(R^{\rm c}-1)+1$ according to (5). Considering TB codes (instead of zero-tail or other termination techniques) simplifies the analysis since for TB codes the code rate coincides with the rate of the parent convolutional code. Moreover, if l tends towards infinity, the minimum distance of a TB code coincides with the free distance of its parent convolutional code. Additionally, the minimum distance of the woven graph code is then replaced by the corresponding free distance, which is denoted by $d_{\rm free}^{\rm wg}$.

Finally, following directly from (4) and (6), the memory $m_{\rm wg}$ (as well as the overall constraint length) of such a woven graph code is at most ns times larger than that of its constituent code, that is, $m_{\rm wg} \leq nsm^c$. Now we can prove the following:

Theorem 1: (Costello lower bound) For any $\epsilon > 0$, some $m_0 > 0$, and for all $m_{\rm wg} > m_0$ within the random ensemble of rate $R_{\rm wg} = s(R^{\rm c}-1)+1$ woven graph codes over s-partite, s-uniform, c-regular hypergraphs with constituent rate $R^{\rm c} = b/c$ convolutional codes with memory $m^{\rm c}$, there exists a code such that its relative free distance $\delta_{\rm free}^{\rm wg} = d_{\rm free}^{\rm wg}/cm_{\rm wg}$ satisfies the Costello lower bound [6],

$$\delta_{\text{free}}^{\text{wg}} \ge -\frac{R_{\text{wg}}}{\log_2\left(2^{1-R_{\text{wg}}}-1\right)} - \epsilon \tag{7}$$

if

$$s \ge \begin{cases} 2, & \text{if } R_{\text{wg}} \le 0.402\\ 3, & \text{if } R_{\text{wg}} > 0.402. \end{cases}$$
 (8)

Proof: Analogously to the derivations within the proof of Theorem 1 in [2], let w be the Hamming weight of the codeword v of the random binary woven graph code determined by the time-varying random parity-check matrix

$$H_{ ext{wg}} = \left(egin{array}{c} \widetilde{H}_1 \ \widetilde{H}_2 \ dots \ \widetilde{H}_s \end{array}
ight) = \left(egin{array}{c} \pi_1(H_1) \ \pi_2(H_2) \ dots \ \pi_s(H_s) \end{array}
ight)$$

where $\pi_i(H_i)$ denotes a random permutation of the columns of H_i . Each of the s submatrices $\tilde{H}_i = \pi_i(H_i)$, $i = 1, 2, \dots, s$, is an $n \times n$ block matrix (or in other words a binary matrix of size $n(c-b)l \times ncl$), where n denotes the number of constituent block codes within each subset of nodes, and

$$H_i = \left(egin{array}{cccc} H_i^{\mathrm{c}(1)} & \mathbf{0} & \cdots & \mathbf{0} \ \mathbf{0} & H_i^{\mathrm{c}(2)} & \cdots & \mathbf{0} \ dots & dots & \ddots & dots \ \mathbf{0} & \mathbf{0} & \cdots & H_i^{\mathrm{c}(n)} \end{array}
ight).$$

Within H_i , each of the n blocks denotes a random parity-check matrix $H_i^{c(t)}$, $t=1,2,\ldots,n,\ i=1,2,\ldots,s,$ given by

$$H_{i}^{c(t)} = \begin{pmatrix} H_{00}^{c} & H_{01}^{c} & \cdots & H_{0m^{c}}^{c} \\ & H_{10}^{c} & H_{11}^{c} & \cdots & H_{1m^{c}}^{c} \\ & & \ddots & \ddots & \ddots & \ddots \\ & & & H_{loc}^{c(t)} & H_{loc}^{c} & \cdots & H_{loc}^{c} \\ & & & & \ddots & \ddots & \ddots & \ddots \\ & & & & H_{(l-m^{c}-1)0}^{c} & H_{(l-m^{c}-1)1}^{c} & \cdots & H_{(l-m^{c}-1)m^{c}}^{c} \\ & & & & H_{(l-m^{c})0}^{c} & H_{(l-m^{c})1}^{c} & \cdots & H_{(l-2)1}^{c} \\ & & & & & & \ddots & \ddots \\ & & & & & & & H_{(l-1)m^{c}}^{c} & & & & H_{(l-1)m^{c}}^{c} \end{pmatrix}$$

$$(9)$$

which can be interpreted as a parity-check matrix of a rate $R = lb \times lc$ block code, whose dual generator matrix is tailbitten to length l. All matrices H_{ij}^c , $i = 0, 1, \ldots, l-1, j = 0, 1, \ldots, m^c$, in (9) are of size $(c-b) \times c$ and can be obtained separately for each block matrix $H_i^{c(t)}$ by randomly choosing 0s and 1s equiprobably and independently. In the following, we are going to find the parameter d, such that the probability $P\left(vH_{wg}^T = \mathbf{0} \mid w\right)$ tends to zero for all w < d, where w denotes the Hamming weight of the codeword v, when l tends to infinity. In this case the constituent block code becomes a constituent convolutional code. Clearly, we can rewrite $P\left(vH_{wg}^T = \mathbf{0} \mid w\right)$ as

$$P\left(\boldsymbol{v}H_{\text{wg}}^{\text{T}} = \boldsymbol{0} \mid w\right) = \sum_{h} P\left(\boldsymbol{v}H_{\text{wg}}^{\text{T}} = \boldsymbol{0} \mid w, h\right) P\left(h \mid w\right) \le \max_{h} \left\{P\left(\boldsymbol{v}H_{\text{wg}}^{\text{T}} = \boldsymbol{0} \mid h, w\right)\right\}$$
(10)

where $h \leq l$ denotes the number of nonzero subblocks of length nc in a codeword v of length ncl. The conditional probability in the last inequality can be expressed as

$$P\left(\boldsymbol{v}H_{\text{wg}}^{\text{T}} = \boldsymbol{0} \mid h, w\right) = \sum_{\boldsymbol{j}} P\left(\boldsymbol{v}H_{\text{wg}}^{\text{T}} = \boldsymbol{0} \mid h, w, \boldsymbol{j}\right) P\left(\boldsymbol{j} \mid h, w\right)$$
(11)

where $j = (j_1, j_2, \dots, j_s)$, with j_i denoting the number of nonzero constituent codewords within the *i*th subset of check nodes corresponding to the codeword of weight w, $i = 1, 2, \dots, s$.

The events that a random codeword v and a random matrix H_i satisfy the ith subset of parity checks, i.e., $vH_i^{\rm T}=\mathbf{0}$, for different i are stochastically dependent in the product space of random equiprobable sequences v and random parity-check matrices, because the same fragments of v participate in different sets of parity checks. However, for all v satisfying the conditions v, v, and v, the probabilities of v.

thus the events are *conditionally* independent for given v, w, h, and j. Taking into account that there exist not more than $\binom{nch}{w}$ sequences of v satisfying the mentioned conditions, we obtain the upper bounds

$$P\left(\boldsymbol{v}H_{\text{wg}}^{\text{T}} = \boldsymbol{0} \mid h < l, w, \boldsymbol{j}\right) \leq l^{2ls/m^{c}} \binom{nch}{w} \left(\prod_{i=1}^{s} 2^{j_{i}b(h-m^{c})} 2^{-j_{i}ch}\right)$$
(12)

and

$$P\left(\boldsymbol{v}H_{\text{wg}}^{\text{T}} = \boldsymbol{0} \mid h = l, w, \boldsymbol{j}\right) \leq {ncl \choose w} \left(\prod_{i=1}^{s} 2^{j_i b l} 2^{-j_i c l}\right).$$
(13)

Note that in the derivation of (12), codewords containing h nontrivial c-subblocks are generated by not more than $(h-m^c)$ nontrivial binary information b-tuples. Additionally, the number of possible locations of these h nontrivial subblocks among l subblocks can be upper-bounded by l^{2l/m^c} . This bound follows directly by taking into account that every codeword contains one or more (cyclic) bursts of at least m^c nontrivial subblocks. Thus, the number of bursts cannot be larger than l/m^c . Additionally, as there are at most l possible starting positions for each burst and less than l possible ending positions within each of the s subsets, the maximum total number of possible configurations for h nontrivial subblocks follows as $\left((l^2)^{(l/m^c)}\right)^s$.

On the other hand, if all l blocks of a codeword are nontrivial, in other words, if h = l, these considerations do not have to be taken into account and the corresponding probability can be upper-bounded by the tighter expression (13).

In order to estimate the probability $P(j \mid h, w)$ for a woven graph code with constituent block codes, consider the following lemma which was proved in [2].

Lemma 1: For the random ensemble of binary woven graph codes with constituent block codes the probability $P(j \mid h, w)$ that a codeword of length ch and weight w contains $j = (j_1, j_2, \dots, j_s)$ nonzero constituent codewords in the s parity-check subsets can be upper-bounded by

$$P\left(\boldsymbol{j} \mid h, w\right) \leq \prod_{i=1}^{s} \frac{\binom{n}{j_i} \binom{ch}{w/j_i}^{j_i} \binom{w-1}{j_i-1}}{\binom{nch}{w}}.$$

By combining (11), (12), and Lemma 1 we obtain

$$P\left(\boldsymbol{v}H_{\text{wg}}^{\text{T}} = \boldsymbol{0} \mid h < l, w\right) \leq l^{2l/m^{c}} \sum_{\boldsymbol{j}} \binom{nch}{w}^{1-s} \prod_{i=1}^{s} 2^{j_{i}b(h-m^{c})-j_{i}ch} \binom{n}{j_{i}} \binom{ch}{w/j_{i}}^{j_{i}} \binom{w-1}{j_{i}-1}$$

$$\leq l^{2l/m^{c}} \binom{nch}{w}^{1-s} (n+1)^{s} \max_{(j_{1}, \dots, j_{s})} \prod_{i=1}^{s} 2^{j_{i}b(h-m^{c})-j_{i}ch} \binom{n}{j_{i}} \binom{ch}{w/j_{i}}^{j_{i}} \binom{w-1}{j_{i}-1}$$

$$\leq l^{2l/m^{c}} (n+1)^{s} \binom{nch}{w}^{1-s} \max_{\boldsymbol{j} \leq n} \left\{ \left(2^{jb(h-m^{c})-jch} \binom{n}{j} \binom{ch}{w/j}^{j} \binom{w-1}{j-1} \right)^{s} \right\}. (14)$$

As mentioned previously, in case all l blocks of a codeword are nontrivial, we have to replace (12) by (13), and it thereby follows from (11), (13), and Lemma 1 in a similar fashion that

$$P\left(\boldsymbol{v}H_{\text{wg}}^{\text{T}} = \boldsymbol{0} \mid h = l, w\right) \leq (n+1)^{s} \binom{ncl}{w}^{1-s} \max_{j \leq n} \left\{ \left(2^{jl(b-c)} \binom{n}{j} \binom{cl}{w/j}^{j} \binom{w-1}{j-1}\right)^{s} \right\}. \tag{15}$$

Finally, we define the corresponding exponents of (14) and (15) and lower-bound their values by

$$F_{l < h}(\delta) = \lim_{m^{c} \to \infty} \frac{-\log_{2} P\left(\boldsymbol{v}H_{\text{wg}}^{T} = \boldsymbol{0} \mid h < l, w\right)}{ncm^{c}s}$$

$$\geq \min_{\gamma \in (0,1], \ \mu \geq 1} \left\{ \left(1 - \frac{1}{s}\right) \mu h\left(\frac{\delta s}{\mu}\right) + \gamma\left(1 + \frac{\mu - 1}{s}(1 - R_{\text{wg}})\right) - \gamma\mu h\left(\frac{\delta s}{\gamma\mu}\right) \right\}$$

$$F_{l = h}(\delta) = \lim_{m^{c} \to \infty} \frac{-\log_{2} P\left(\boldsymbol{v}H_{\text{wg}}^{T} = \boldsymbol{0} \mid h = l, w\right)}{ncm^{c}s}$$

$$\geq \max_{\theta > 1} \min_{\gamma \in (0,1]} \left\{ \left(1 - \frac{1}{s}\right) \theta h\left(\frac{\delta s}{\theta}\right) + \gamma\theta\frac{1 - R_{\text{wg}}}{s} - \gamma\theta h\left(\frac{\delta s}{\gamma\theta}\right) \right\}$$

$$(17)$$

using the fact that

$$\log_2 \binom{b}{a} \simeq bh \left(\frac{a}{b}\right)$$

where $h(x) = -x \log_2 x - (1-x) \log_2 (1-x)$ is the binary entropy function together with the following abbreviations

$$\delta = \frac{w}{ncm^{c}s}, \quad \mu = \frac{h}{m^{c}}, \quad \theta = \frac{l}{m^{c}}, \quad \text{and} \quad \gamma = \frac{j}{n}.$$

Similarly, the exponent of (10) can be lower-bounded with (16) and (17) by

$$F(\delta) = \lim_{m^c \to \infty} \frac{-\log_2 P\left(\boldsymbol{v}H_{\text{wg}}^{\text{T}} = \boldsymbol{0} \mid w\right)}{ncm^c s} = \min\left\{F_{l < h}(\delta), F_{l = h}(\delta)\right\}.$$

Consider the truncation length l tending towards infinity, that is, $\theta \to \infty$. Then it is straightforward to verify that $F_{l=h} \to \infty$ and only $F_{l< h}$ determines the probability exponent $F(\delta)$. To find the minimum of $F_{l< h}(\delta)$ in (16) over μ and γ , we use the fact that the function

$$f(x) = \beta x - xh(\alpha/x)$$

is convex if $x > \alpha > 0$ and achieves its minimum

$$f(x_0) = \alpha \log_2(2^{\beta} - 1)$$

at the point

$$x_0 = \frac{\alpha}{1 - 2^{-\beta}}.$$

Minimizing (16) in the same way over $0 < \gamma \le 1$, leads to

$$\gamma_{\text{opt}} = \min\left\{1, \frac{\delta s}{\mu(1 - 2^{-\beta})}\right\} \tag{18}$$

with

$$\beta = \frac{s + (\mu - 1)(1 - R_{\text{wg}})}{s\mu}.$$
(19)

Obviously, if s is chosen large enough, γ_{opt} follows from (18) as $\gamma_{\text{opt}} = 1$ and (16) can be expressed by

$$F_{l < h}(\delta) \ge \min_{\mu \ge 1} \left\{ -\frac{\mu}{s} h\left(\frac{\delta s}{\mu}\right) + \frac{\mu}{s} (1 - R_{\text{wg}}) \right\} + 1 - \frac{1 - R_{\text{wg}}}{s}. \tag{20}$$

By finally minimizing (20) over μ , we obtain

$$\mu_{\text{opt}} = \frac{\delta s}{1 - 2R_{\text{wg}} - 1} \tag{21}$$

which leads to

$$F_{l < h}(\delta) \ge \delta \log_2 \left(2^{1 - R_{\text{wg}}} - 1 \right) + 1 - \frac{1 - R_{\text{wg}}}{s}.$$
 (22)

Clearly, for the Costello bound (7) to hold, $F(\delta)$ needs to be strictly positive, so that the probability of codewords of relative weight below the Costello bound tends to zero if s is large enough. To complete the proof we find the minimal value of s for which this holds. The lower limit on s within our derivation was imposed by the assumption that $\gamma_{\rm opt}=1$, which holds as long as

$$\frac{\delta s}{\mu(1-2^{-\beta})} \ge 1\tag{23}$$

where β was defined by (19). By combining (7), (18), and (21), it can be shown that (23) is fulfilled if s is selected according to (8), which completes the proof.

Graph	ТВ	Constituent	Permutation	ν	$d_{ m free}$	Spectrum
	code	code			- Irec	
Rate $R_{ m wg}=1/4$						
Hyper, $g = 2$, $g_{3,2} = 8$ $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & Z & Z^2 & Z^3 \\ 1 & Z^3 & Z & Z^2 \end{pmatrix}$	(16, 4)	$h_1^{c}(D) = 1 + D + D^2 + D^4$ $h_2^{c}(D) = 1 + D + D^2 + D^3 + D^4$ $h_3^{c}(D) = 1 + D + D^3 + D^5$ $h_4^{c}(D) = 1 + D^2 + D^5$ $d_{\text{free}}^{c} = 5$	(1,4,2,3) $(3,4,1,2)$	51	64	1,
	(20, 5)			67	120	1,
Rate $R_{ m wg}=1/3$						
Utility, $g = 4$, $g_{2,2} = 4$ $\begin{pmatrix} 1 & 1 & 1 \\ 1 & Z & Z^2 \end{pmatrix}$	(9,3)	$h_1^{c}(D) = 1 + D + D^4$ $h_2^{c}(D) = 1 + D + D^3 + D^4 + D^5$ $h_3^{c}(D) = 1 + D^2 + D^3 + D^4 + D^5$	(3, 1, 2)	26	30	4,0,0,0,0,0,3,0,6,0,
Heawood, $g = 6$, $g_{2,2} = 6$ $\begin{pmatrix} 1 & 1 & 1 \\ 1 & Z & Z^3 \end{pmatrix}$	(21,7)	$d_{ m free}^{ m c}=6$	(1,3,2)	64	32	7,0,0,0,0,0,7,0,7,0,
Rate $R_{ m wg}=1/2$						
Bipartite, $g = 4$, $g_{2,2} = 4$ $\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & Z & Z^2 & Z^3 \end{pmatrix}$	(16,8)	$h_1^{c}(D) = 1 + D + D^2 + D^4$ $h_2^{c}(D) = 1 + D + D^2 + D^3 + D^4$ $h_3^{c}(D) = 1 + D + D^3 + D^5$ $h_4^{c}(D) = 1 + D^2 + D^5$ $d_{\text{free}}^{c} = 5$	(3, 4, 2, 1)	39	31	12,

 $\begin{tabular}{l} TABLE\ I\\ EXAMPLES\ OF\ PROMISING\ WOVEN\ CONVOLUTIONAL\ GRAPH\ CODES \end{tabular}$

VI. EXAMPLES

Parameters for some promising examples of woven convolutional graph codes are presented in Table I for rates $R_{\rm wg}=1/4$, $R_{\rm wg}=1/3$, and $R_{\rm wg}=1/2$ with free distances up to $d_{\rm free}=120$. For each entry in Table I, the parameters of the underlying graph or hypergraph are given in compact form by

For each entry in Table I, the parameters of the underlying graph or hypergraph are given in compact form by the generator matrix $G_{\text{hg}}^{\perp p}(Z)$ of its parent convolutional code in the first column, as well as the corresponding girth and (s,d)-girth. By tailbiting we obtain the generator matrix G_{hg}^{\perp} of the dual hypergraph-based block code \mathcal{C}_{hg} , which is equal to the parity-check matrix H_{hg} of the hypergraph-based block code \mathcal{C}_{hg} which we will utilize hereinafter.

Consider the parity-check polynomials of the rate R=b/c constituent convolutional code in column three, and their permutations as specified in the fourth column. By interpreting these codes as rate R=b/c block codes over the field of binary Laurent series, we obtain our final woven convolutional graph codes.

In column four the overall constraint length ν of the corresponding minimal-basic [6] generator matrix $G_{\text{wg}}(D)$ is specified. By applying the BEAST [8], the free distance d_{free} as well as the first Viterbi spectral components have been calculated and are given in the last two columns of Table I.

Even though the girth of the underlying graph as well as the free distance $d_{\text{free}}^{\text{c}}$ of the constituent convolutional code is in general rather small, it is possible to construct woven convolutional graph codes with free distances up to at least 120 [9].

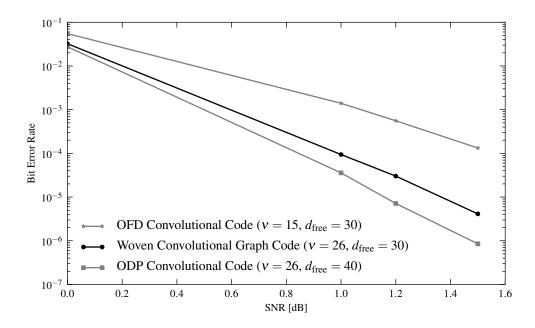


Fig. 4. Comparison of bit-error rate performances for Viterbi decoding for a rate $R_{\rm wg}=3/9$ woven convolutional graph code with $\nu=26$ and $d_{\rm free}=30$ in comparison to a rate R=1/3 ODP convolutional code with $\nu=26$ and $d_{\rm free}=40$ as well as a rate R=1/3 OFD convolutional code with $\nu=15$ and $d_{\rm free}=30$.

Consider for example the first entry in Table I, where the generator matrix of the parent convolutional code is given by

$$G_{\text{hg}}^{\perp p}(Z) = \begin{pmatrix} 1 & 1 & 1 & 1\\ 1 & Z & Z^2 & Z^3\\ 1 & Z^3 & Z & Z^2 \end{pmatrix}.$$
(24)

As specified by the second column, we want to obtain the parity-check matrix for a (16,4) hypergraph-based block code. By tailbiting (24) to length 4 we obtain the generator matrix G_{hg}^{\perp} of the rate R=12/16 dual hypergraph-based code \mathcal{C}_{hg} , which is equal to the parity-check matrix H_{hg} of the rate R=4/16 hypergraph-based code \mathcal{C}_{hg} .

Clearly, the obtained 3-partite, 3-uniform, 4-regular hypergraph has three disjoint sets of vertices \mathcal{V}_t , t=1,2,3. While we assign the parity-check polynomials from column three to the vertices within \mathcal{V}_1 in their natural order, that is, $(h_1(D),h_2(D),h_3(D),h_4(D))$, the parity-check polynomials for the second and third sets \mathcal{V}_2 and \mathcal{V}_3 are permuted according to (1,3,4,2) and (3,4,1,2), that is, $(h_1(D),h_3(D),h_4(D),h_2(D))$ for \mathcal{V}_2 and $(h_3(D),h_4(D),h_1(D),h_2(D))$ for \mathcal{V}_3 .

We thereby have constructed a rate $R_{\rm wg}=1/4$ woven convolutional graph code with free distance 64, whose minimal-basic generator matrix has an overall constraint length of 51.

VII. SIMULATION RESULTS

To demonstrate the error-correcting capabilities of woven convolutional graph codes, the bit-error rate (BER) performance for Viterbi decoding is simulated for a rate $R_{\rm wg}=3/9$ woven convolutional graph code with overall constraint length $\nu=26$ and free distance $d_{\rm free}=30$. The obtained BER performance for Viterbi decoding is illustrated in Fig. 4. For comparison, the BER performance for Viterbi decoding for the optimum distance profile (ODP) rate R=1/3 convolutional code with the same overall constraint length $\nu=26$ but with the larger free distance $d_{\rm free}=40$ as well as the optimal free distance (OFD) rate R=1/3 convolutional code with the same free distance $d_{\rm free}=30$ but with a smaller overall constraint length $\nu=15$ are included in Fig. 4.

At low signal-to-noise ratios (SNRs) (0.0-0.5 dB) the BER for the woven convolutional graph code is very close to the BER of the ODP convolutional code, despite the large difference in their free distances. However, for higher SNRs, around BER= 10^{-5} , the woven convolutional graph codes loses about 0.2 dB compared to the ODP convolutional code. The OFD convolutional code, on the other hand, has a significantly worse BER performance over the whole range of SNRs.

VIII. CONCLUSIONS

The asymptotic behavior of woven graph codes with constituent convolutional codes has been studied. It has been shown that within the random ensemble of such codes based on s-partite, s-uniform, c-regular hypergraphs we can find a value $s \ge 2$ such that for any code rate there exist codes satisfying the Costello lower bound on the free distance. Examples of rate $R_{\rm wg}=1/2$, $R_{\rm wg}=1/3$, and $R_{\rm wg}=1/4$ woven convolutional graph codes with free distances up to 120 have been presented. By simulations it has been shown that, at low signal-to-noise ratios the bit error rate performance for Viterbi decoding of a woven convolutional graph code is rather close to that of the optimum distance profile convolutional code with same overall constraint length.

ACKNOWLEDGMENT

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

REFERENCES

- [1] I. Bocharova, B. Kudryashov, R. Johannesson, and V. Zyablov, "Asymptotically good woven codes with fixed constituent convolutional codes," in *Proc. IEEE International Symposium on Information Theory (ISIT'07)*, Nice, France, Jun. 24–29, 2007, pp. 2326–2330.
- [2] I. E. Bocharova, B. D. Kudryashov, R. Johannesson, and V. V. Zyablov, "Woven graph codes: Asymptotic performances and examples," *IEEE Trans. Inf. Theory*, vol. 56, no. 1, pp. 121–129, Jan. 2010.
- [3] C. Berge, Graphs and Hypergraphs. Amsterdam: North Holland, 1976.
- [4] I. E. Bocharova, B. D. Kudryashov, and R. V. Satyukov, "Graph-based convolutional and block LDPC codes," *Problems of Information Transmission*, vol. 45, no. 4, pp. 69–90, 2009.
- [5] R. M. Tanner, "A recursive approach to low complexity codes," IEEE Trans. Inf. Theory, vol. 27, no. 5, pp. 533-547, Sep. 1981.
- [6] R. Johannesson and K. S. Zigangirov, Fundamentals of Convolutional Coding. Piscataway, NJ: IEEE Press, 1999.
- [7] S. Höst, R. Johannesson, and V. V. Zyablov, "Woven convolutional codes I: Encoder properties," *IEEE Trans. Inf. Theory*, vol. 48, no. 1, pp. 149–161, Jan. 2002.
- [8] 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.
- [9] F. Hug, I. Bocharova, R. Johannesson, and B. Kudryashov, "A rate R=5/20 hypergraph-based woven convolutional code with free distance 120," *IEEE Trans. Inf. Theory*, vol. 56, no. 4, pp. 1618–1623, Apr. 2010.