

Turbo Codes Based on Time-Variant Memory-1 Convolutional Codes over \mathbb{F}_q

Gianluigi Liva, Enrico Paolini, Sandro Scalise and Marco Chiani

Abstract—Two classes of turbo codes over high-order finite fields are introduced. The codes are derived from a particular protograph sub-ensemble of the $(d_v = 2, d_c = 3)$ low-density parity-check code ensemble. A first construction is derived as a parallel concatenation of two non-binary, time-variant accumulators. The second construction is based on the serial concatenation of a non-binary, time-variant differentiator and of a non-binary, time-variant accumulator, and provides a highly-structured flexible encoding scheme for $(d_v = 2, d_c = 4)$ ensemble codes. A cycle graph representation is provided. The proposed codes can be decoded efficiently either as low-density parity-check codes (via belief propagation decoding over the codes bipartite graph) or as turbo codes (via the forward-backward algorithm applied to the component codes trellis). The forward-backward algorithm for symbol maximum a posteriori decoding of the component codes is illustrated and simplified by means of the fast Fourier transform. The proposed codes provide remarkable gains (~ 1 dB) over binary low-density parity-check and turbo codes in the moderate-short block regimes.

I. INTRODUCTION

Low-density parity-check (LDPC) codes [1] constructed on high-order finite fields [2]–[4] show remarkable coding gains with respect to (w.r.t.) binary LDPC/turbo codes [5]–[8]. The gain is especially visible in the moderate-to-short block length ($k \leq 1000$ bits) regime [3], [4], where binary iteratively-decodable codes tend to exhibit either high error floors or non-negligible coding gain losses [9] w.r.t. available benchmarks (e.g., 1 dB with respect to the random coding bound (RCB) [10]).¹ Ultra-sparse non-binary LDPC codes based on fields of order $q \geq 64$ for short block lengths allow approaching the average performance of random codes by ~ 0.2 dB down to medium-low codeword error rates (CERs).

In this paper, we provide a novel turbo code construction, which leads to *non-binary* turbo codes based on convolutional codes on a finite field \mathbb{F}_q of order $q = 2^m > 2$. The proposed construction bridges rate-1/3 non-binary turbo codes and regular $(d_v = 2, d_c = 3)$ non-binary LDPC codes, where d_c and d_v are the check node (CN) and variable node (VN) degrees, respectively. More specifically, the turbo code construction

follows from a specific expansion of a $(d_v = 2, d_c = 3)$ protograph.² The so-obtained turbo codes have performance close to that of their non-binary LDPC counterparts, with the advantage of an efficient encoding structure. Even more important, the proposed construction allows building families of rate-compatible turbo codes with flexible block size, by adopting combinatorial (on-the-fly) interleaver constructions.

Convolutional turbo(-like) codes over non-binary finite fields/rings have been investigated previously, e.g. in [14]–[20]. With respect to the past works, the main novelties of our construction are listed next. Most of the previous contributions devote attention to fields of low order, whereas we focus on high order fields, e.g. of order $q = 2^m = 256$. Moreover, our construction is based on codes with memory 1 (in symbols), whereas in [17], [19] codes with larger memories are considered. The convolutional codes adopted by the proposed construction are time-variant, while in [15], [17]–[19] the feed-forward / feedback polynomials are fixed. To our knowledge, the only non-binary iterative schemes adopting time-variant convolutional codes are the irregular repeat accumulate (IRA) codes of [20]. However, in [20] a turbo code structure is not considered explicitly. We further propose an alternative serial turbo code interpretation of the $(d_v = 2, d_c = 3)$ regular protograph ensemble which allows to efficiently encode rate-1/2 $(d_v = 2, d_c = 4)$ regular LDPC codes as a serial concatenation of a non-binary time-variant differentiator, and interleaver, and a non-binary time variant accumulator. The proposed construction features a nice graph interpretation which provides useful insights for the interleaver design. High rates can be obtained by suitably puncturing the code symbols, whereas low rates can be easily obtained by using the multiplicative repetition approach of [21]. A discussion on how decoding can be performed either in a turbo-like fashion (i.e., by iterating a BCJR decoder on the q -states trellises of the component codes) or via the classical belief propagation (BP) algorithm for LDPC codes is provided. In both cases, the decoder complexity growth w.r.t. the field order q can be limited to $\mathcal{O}(q \log_2 q)$ by adopting fast Fourier transforms.

The contribution is structured as follows. Section II describes the code structure. In Section III the iterative decoding algorithm is discussed. Numerical results and conclusions follow in Sections IV and V respectively.

Gianluigi Liva and Sandro Scalise are with the Institute of Communications and Navigation, German Aerospace Center (DLR), Oberpfaffenhofen, 82234 Weßling, Germany. Email:{Gianluigi.Liva,Sandro.Scalise}@dlr.de.

Enrico Paolini and Marco Chiani are with DEIS/WiLAB, University of Bologna, via Venezia 52, 47521 Cesena (FC), Italy. Email:{e.paolini,marco.chiani}@unibo.it.

¹Although the RCB provides an upper bound to the block error probability achievable by a (n, k) code, for moderate-long block it provides a tight estimation of the performance of the best codes. In the short-length regime, properly-designed codes can surpass the RCB even remarkably. However, it will be kept as a reference through the paper together with the sphere packing bound (SPB) of [11].

²Similarly, in [12], [13] a bridge between LDPC and turbo code constructions was provided in the binary context. However, in [12], [13] protograph ensembles have not been considered.

II. CODE STRUCTURE

Regular ($d_v = 2, d_c$) non-binary LDPC codes are characterized by excellent iterative decoding thresholds [3]. In this paper, we shall focus on the ($d_v = 2, d_c = 3$) rate-1/3 case. The iterative decoding threshold over the binary-input additive white Gaussian noise (AWGN) channel for the ($d_v = 2, d_c = 3$) unstructured ensembles with random choice of the non-zero coefficients in the parity-check matrix is $(E_b/N_0)^* \simeq -0.25$ dB,³ only 0.25 dB away from the Shannon limit. The turbo codes described in this paper are constructed on a specific protograph sub-ensemble of the ($d_v = 2, d_c = 3$) regular ensemble, depicted in Fig. 1(a). A protograph [22], [23] is a Tanner graph [24] with a relatively small number of nodes. A protograph $\mathcal{G} = (\mathcal{V}, \mathcal{C}, \mathcal{E})$ consists of a set of N variable nodes \mathcal{V} , a set of M check nodes \mathcal{C} , and a set of edges \mathcal{E} . Each edge $e_{i,j} \in \mathcal{E}$ connects a VN $V_j \in \mathcal{V}$ to a CN $C_i \in \mathcal{C}$. A larger *derived* graph can be obtained by a copy-and-permute procedure: the protograph is copied K times, and the edges of the individual replicas are permuted among the K replicas. A protograph can be described by a *base matrix* \mathbf{B} of size $M \times N$. The element $b_{i,j}$ of \mathbf{B} represents the number of edges connecting the VN V_j to the CN C_i . The base matrix associated with the protograph in Fig. 1(a) is given by

$$\mathbf{B} = \begin{bmatrix} 1 & 2 & 0 \\ 1 & 0 & 2 \end{bmatrix}.$$

We proceed by expanding the protograph into the derived graph as follows. We first replace the upper-left ‘1’ in \mathbf{B} with a $K \times K$ identity matrix, \mathbf{I} . The lower-left ‘1’ is replaced by a $K \times K$ permutation matrix $\mathbf{\Pi}$. Each of the ‘2’ entries of \mathbf{B} is replaced by a $K \times K$ cyclic matrix

$$\mathbf{P} = \begin{bmatrix} 1 & 0 & \dots & 0 & 1 \\ 1 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & \dots & 1 & 1 \end{bmatrix}.$$

The $(2K) \times (3K)$ derived graph adjacency matrix has the form

$$\mathbf{\Gamma} = \begin{bmatrix} \mathbf{I} & \mathbf{P} & \mathbf{0} \\ \mathbf{\Pi} & \mathbf{0} & \mathbf{P} \end{bmatrix}.$$

We then construct a parity-check matrix on \mathbb{F}_q by replacing each ‘1’ in $\mathbf{\Gamma}$ with a suitable element of $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. The $2K \times 3K$ full-rank non-binary parity-check matrix is given by

$$\mathbf{H} = \begin{bmatrix} \tilde{\mathbf{I}} & \tilde{\mathbf{P}}^{(1)} & \mathbf{0} \\ \tilde{\mathbf{\Pi}} & \mathbf{0} & \tilde{\mathbf{P}}^{(2)} \end{bmatrix} \quad (1)$$

where

- $\tilde{\mathbf{I}}$ is a $K \times K$ matrix with non-zero entries only on the main diagonal (*pseudo-identity matrix*). More specifically, $\tilde{i}_{j,l} = g_j^{(1)}$ for $j = l$, otherwise $\tilde{i}_{j,l} = 0$.
- $\tilde{\mathbf{\Pi}}$ is a $K \times K$ matrix with non-0 entries only for $\tilde{\pi}_{\pi(j),j}, \forall j \in (1, K)$. In particular, $\tilde{\pi}_{j,\pi(j)} = g_j^{(2)}, \forall j \in (1, K)$. Thus, $\tilde{\mathbf{\Pi}}$ can be described as the product between

³Throughout the paper, E_b will denote the energy per information bit and N_0 the one-sided noise power spectral density.

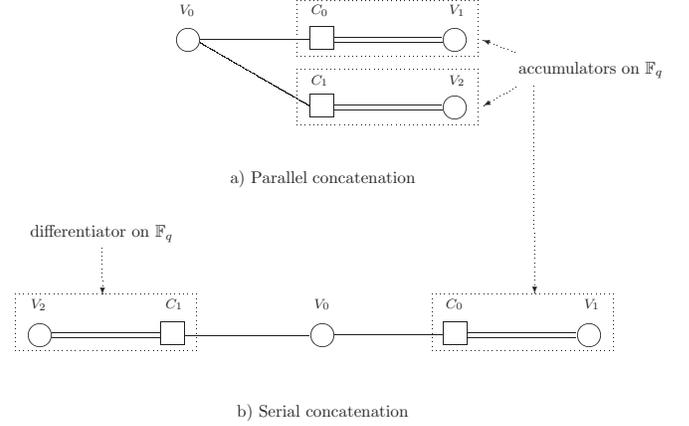


Fig. 1. Rate-1/3 protograph as parallel (a) and serial (b) concatenation.

a permutation matrix $\mathbf{\Pi}$ and a pseudo-identity matrix with diagonal coefficients $g_0^{(2)}, g_1^{(2)}, \dots, g_{K-1}^{(2)}$, with $\pi(j)$ being the permutation function.

- Both $\tilde{\mathbf{P}}^{(1)}, \tilde{\mathbf{P}}^{(2)}$ are double diagonal matrices with form

$$\tilde{\mathbf{P}}^{(z)} = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & f_0^{(z)} \\ f_1^{(z)} & 1 & 0 & \dots & 0 & 0 \\ 0 & f_2^{(z)} & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & f_{K-1}^{(z)} & 1 \end{bmatrix}, \quad z = 1, 2.$$

A. Parallel Concatenation

The parity-check matrix (1) may be interpreted as the parity-check matrix of the parallel concatenated convolutional code (PCCC). The information word \mathbf{u} of $K = k/m$ symbols in \mathbb{F}_q , $q = 2^m$, is input to a rate-1, memory-1 time-variant recursive systematic convolutional (RSC) tail-biting encoder (*non-binary accumulator*). The first set of parity symbols $\mathbf{p}^{(1)}$ is obtained as

$$p_i^{(1)} = g_i^{(1)} u_i + f_i^{(1)} p_{i-1}^{(1)} \quad \forall i \in [0, K-1] \quad (2)$$

and with $p_{-1}^{(1)} = p_{K-1}^{(1)}$ properly initialized.⁴ Here, $p_i^{(1)}, g_i^{(1)}, f_i^{(1)} \in \mathbb{F}_q$, and all operations are in \mathbb{F}_q . The second set of parity symbols are obtained by first permuting the symbols of \mathbf{u} according to the interleaving rule $i \rightarrow \pi(i)$. The permuted information word \mathbf{u}' (with $u'_i = u_{\pi(i)}$) is then fed in a second rate-1, memory-1 time-variant RSC tail-biting encoder. The second set of parity symbols $\mathbf{p}^{(2)}$ is obtained as

$$p_i^{(2)} = g_i^{(2)} u'_i + f_i^{(2)} p_{i-1}^{(2)} \quad \forall i \in [0, K-1] \quad (3)$$

and with $p_{-1}^{(2)} = p_{K-1}^{(2)}$. The systematic codeword is given by $\mathbf{c} = [\mathbf{u} | \mathbf{p}^{(1)} | \mathbf{p}^{(2)}]$ and has length $3K$ symbols. The code length is $n = 3Km$ bits and the code dimension is $k = Km$. The code rate for the proposed construction is $r = k/n = 1/3$.

⁴The initialization of $p_{-1}^{(1)}$ (and consequently of $p_{-1}^{(2)}$) can be obtained as indicated in [25, Lemma 4].

B. Serial Concatenation

By stretching the protograph of Fig. 1(a) onto the one of Fig. 1(b), it is possible to devise an alternative encoder which is based on the serial concatenation of a memory-1 non-recursive encoder (*non-binary differentiator*), and interleaver, and a rate-1 RSC encoder (*non-binary accumulator*). The information vector \mathbf{u} is first multiplied by the transpose of $\tilde{\mathbf{P}}^{(2)}$, resulting in the intermediate vector \mathbf{v} , with $v_i = u_i + f_i^{(2)}u_{i-1}$ and $v_0 = u_0 + f_0^{(2)}u_{K-1}$. The vector \mathbf{v} is then point-wise multiplied by the coefficient vector $\mathbf{g}^{(2)}$ and permuted according to $\mathbf{\Pi}$, obtaining a second intermediate vector \mathbf{v}' , which is then input to a rate-1, memory-1 time-variant RSC tail-biting encoder leading to a parity vector \mathbf{p} .

$$p_i = g_i^{(1)}v'_i + f_i^{(1)}p_{i-1} \quad \forall i \in [0, K-1] \quad (4)$$

and with $p_{-1} = p_{K-1}$. The final codeword is hence given by $\mathbf{c} = [\mathbf{u}|\mathbf{p}]$, and the code has length $2K$ symbols. The proposed construction brings gives a turbo code with code rate $r = k/n = 1/2$. We will refer to this construction as differentiate accumulate (DA) code. A lower rate $r = 1/3$ can be obtained by providing at the output of the encoder the intermediate vector \mathbf{v} as well, i.e. by setting $\mathbf{c} = [\mathbf{u}|\mathbf{p}|\mathbf{v}]$. Note that, while for the rate 1/3 code the parity-check matrix is still given by (1) (with proper columns permutation), for the rate 1/2 code (1) represents an extended parity-check matrix, where the first K columns are associated with punctured symbols. The parity-check matrix for the rate 1/2 DA code can be obtained by noting that $\mathbf{v}^T = \tilde{\mathbf{P}}^{(2)}\mathbf{u}^T$ and

$$\mathbf{v}' = \mathbf{v}\tilde{\mathbf{\Pi}} = \mathbf{u} \left[\left(\tilde{\mathbf{P}}^{(2)} \right)^T \tilde{\mathbf{\Pi}} \right].$$

The parity-check matrix is hence given by the parity-check matrix of a non-binary IRA code [20], [26]

$$\mathbf{H} = \left[\tilde{\mathbf{\Pi}}^T \tilde{\mathbf{P}}^{(2)} \mid \tilde{\mathbf{P}}^{(1)} \right]. \quad (5)$$

This parity-check matrix form is a particular case of the construction of [27], with left and right sub-matrices characterized by a single cycle involving all their associated variable nodes.

C. Cycle Graph Representation and Interleaver Design

The codes specified by the parity-check matrices of (1) and (5) can be conveniently described as cycle (circuit) codes [25], [27], [28], as the corresponding Tanner graphs have a regular VN degree $d_v = 2$. A graph representation for cycle codes can be obtained by associating a vertex with each parity-check equation and an edge with each codeword symbol. Considering the parity-check matrix (1), the graph is hence given by $3K$ edges connecting $2K$ vertices.

An example is provided in Fig. 2. The graph of a rate 1/3, $K = 5$ code (Fig. 2(a)) is obtained by connecting two length-5 cycles according to the interleaver generated by the relative prime rule $\pi(j) = (a + p \cdot j) \bmod K$ with $a = 1$ and $p = 2$. The graph of Fig. 2(a) turns to be the Petersen graph [28], [29], and hence is a (3, 5)-cage [29], [30], i.e. a graph with minimal

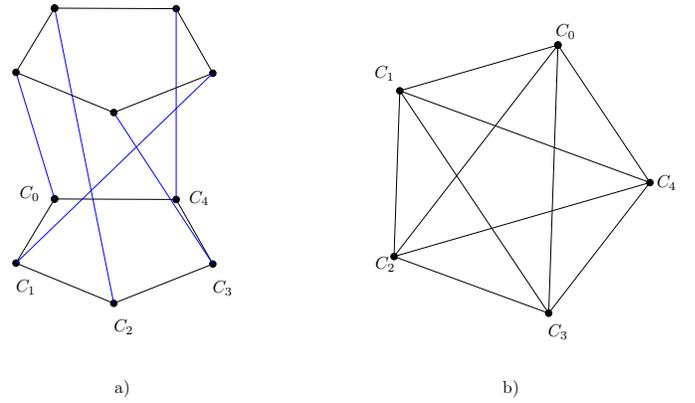


Fig. 2. Example of graphs for the cycle codes: (a) associated with the parity-check matrix of (1) for a rate 1/3, $K = 5$ PCCC, and (b) associated with the parity-check matrix of (5) a the rate 1/2, $K = 5$ DA code.

number of vertexes with degree 3 having girth 5.⁵ The graph associate with the parity-check matrix of (5) can be directly obtained by pruning the graph of Fig. 2(a) as follows: Each edge connecting a vertex of the lower pentagon to a vertex of the upper pentagon is eliminated, and the corresponding upper and lower vertexes are merged together. The obtained graph is shown in Fig. 2(b).⁶

In general, the connections between the upper and the lower cycles in the rate 1/3 graph define the interleaver, which may be selected according to rules for increasing the interleaver spread (*turbo code perspective*), or may be generated by filling the sub-matrix $\tilde{\mathbf{\Pi}}$ of \mathbf{H} according to girth optimization techniques (*LDPC code perspective*). The first approach has the inherent advantage of allowing code constructions for various block sizes on-the-fly by adopting efficient high-spread interleaver construction algorithms [31], [32].⁷

III. MAP DECODING OF THE COMPONENT CODES

As for the code construction, both the LDPC and the turbo code perspectives can be used to perform iterative decoding. For the former case we refer to the vast literature on fast Fourier transform (FFT)-based BP decoders for non-binary LDPC codes (see for instance [33]), giving decoding algorithms with complexity that scales as $\mathcal{O}(q \log_2 q)$. For the latter, the conventional turbo decoding algorithm based on the BCJR algorithm [34] applied on the trellis of the component codes can be simplified by FFTs as well, resulting in a complexity growth $\mathcal{O}(q \log_2 q)$ as for the LDPC BP decoder case [15]. We shall focus next on the symbol maximum a-posteriori (MAP) decoding for the component convolutional codes. We discuss the case of a time-variant memory-1 RSC code, the non-recursive convolutional code case derivation being similar. Each of the two RSC encoders of the proposed

⁵Note that the girth of the Tanner graph associated with a cycle code is twice the girth of the cycle code graph, i.e. for the code based on the Petersen graph the Tanner graph girth is $g = 2 \cdot 5 = 10$.

⁶It is worth to note that by construction the graph of the cycle DA code is always given by two nested Hamiltonian cycles associated with the right and the left sub-matrices of the parity-check matrix (5).

⁷ Additionally, the coefficients of $\mathbf{g}^{(1)}$, $\mathbf{f}^{(1)}$, $\mathbf{g}^{(2)}$, $\mathbf{f}^{(2)}$ may be optimized according to the technique introduced in [3].

PCCC scheme is in fact a time-variant memory-1 encoder (i.e., the current output symbol depends only on the current input symbol and on the past output symbol). The time variant nature of the component codes is due to the multiplications by the coefficients g_i, f_i (we omitted the superscript indicating the branch index). The RSC encoder is fully specified by the relations $S_i = g_i u_i + f_i S_{i-1}$ and $p_i = S_i$, where the state of the encoder is defined by the value stored at the input of the delay unit. The number of states in the code trellis corresponds to the field order q .

We first consider the case where the component RSC codes are terminated. The a posteriori probability mass function (p.m.f.) vector for the symbol u_i given the channel output \mathbf{y} is denoted by $\mathbf{L}_i^u = [L_i^u(0), L_i^u(1), L_i^u(\alpha), \dots, L_i^u(\alpha^{q-2})]$ with $L_i^u[\omega] = \Pr\{u_i = \omega | \mathbf{y}\}$, $\omega \in \mathbb{F}_q$. The channel observation \mathbf{y} is given by $\mathbf{y} = (\mathbf{y}_0, \mathbf{y}_1, \dots, \mathbf{y}_K)$ where each element can be further split as $\mathbf{y}_i = (y_i^u, y_i^p)$, $y_i^u (y_i^p)$ being the channel output corresponding to $u_i (p_i)$.⁸ We further introduce the notation $\mathbf{y}[i:j] = (\mathbf{y}_i, \mathbf{y}_{i+1}, \dots, \mathbf{y}_j)$ ($0 \leq i < j \leq K$).

The computation of the a posteriori probability for the symbol u_i can be accomplished by evaluating

$$L_i^u(\omega) = \Pr\{u_i = \omega | \mathbf{y}\} = \sum_{T_i^u(s, s') = \omega} \varphi_{i-1}(s) \gamma_i(s, s') \beta_i(s').$$

The operator $T_i^u(s, s')$ returns the label associated with u_i for the trellis edge connecting the state s at time $i-1$ to the state s' at time i , $\varphi_{i-1}(s)$ denotes the forward metric for the state s at time $i-1$, $\beta_i(s')$ is the backward metric for the state s' at time i , and $\gamma_i(s, s')$ is the transition metric between states s, s' at time i . We normalize the metrics such that

$$\begin{aligned} \varphi_i(s) &= \Pr\{S_i = s | \mathbf{y}_{[0:i]}\}, & \varphi_0(0) &= 1, \\ \beta_i(s) &= \Pr\{S_i = s | \mathbf{y}_{[i+1:K]}\}, & \beta_K(0) &= 1, \\ \gamma_i(s, s') &= \Pr\{S_{i-1} = s, S_i = s' | \mathbf{y}_i\} \\ &= \Pr\{u_i = \omega, p_i = \nu | y_i^u, y_i^p\}, \end{aligned} \quad (6)$$

with $\omega = T_i^u(s, s')$, $\nu = s'$. Assuming independent outputs y_i^u, y_i^p , (6) can be factored into

$$\gamma_i(s, s') = \underbrace{\Pr\{u_i = \omega | y_i^u\}}_{\gamma_i^u(s, s')} \underbrace{\Pr\{p_i = \nu | y_i^p\}}_{\gamma_i^p(s')}, \quad (7)$$

where $\gamma_i^p(s')$ depends on s' only since $p_i = S_i$. The forward/backward metrics can be computed recursively as

$$\begin{aligned} \varphi_i(s) &\propto \sum_{s'} \varphi_{i-1}(s') \gamma_i(s', s) = \sum_{s'} \varphi_{i-1}(s') \gamma_i^u(s', s) \gamma_i^p(s) \\ &= \gamma_i^p(s) \sum_{s'} \varphi_{i-1}(s') \gamma_i^u(s', s) \end{aligned} \quad (8)$$

$$\begin{aligned} \beta_i(s) &\propto \sum_{s'} \beta_{i+1}(s') \gamma_{i+1}(s, s') \\ &= \sum_{s'} \beta_{i+1}(s') \gamma_{i+1}^u(s, s') \gamma_{i+1}^p(s') \\ &= \sum_{s'} [\beta_{i+1}(s') \gamma_{i+1}^p(s')] \gamma_{i+1}^u(s, s'). \end{aligned} \quad (9)$$

⁸The vector $\mathbf{y} = (\mathbf{y}_0, \mathbf{y}_1, \dots, \mathbf{y}_K)$ is composed by $K+1$ elements to account for the additional input/output symbol required by the termination.

Note that (8) involves a convolution since s', s are related by $s = g_i u_i + f_i s'$. Similarly, for (9) s, s' are related by $s' = g_{i+1} u_{i+1} + f_{i+1} s$. We introduce the p.m.f. vectors

$$\begin{aligned} \varphi_i &= [\varphi_i(0), \varphi_i(1), \varphi_i(\alpha), \dots, \varphi_i(\alpha^{q-2})], \\ \beta_i &= [\beta_i(0), \beta_i(1), \beta_i(\alpha), \dots, \beta_i(\alpha^{q-2})], \\ \gamma_i^p &= [\gamma_i^p(0), \gamma_i^p(1), \gamma_i^p(\alpha), \dots, \gamma_i^p(\alpha^{q-2})], \\ \gamma_i^u &= [\gamma_i^u(0), \gamma_i^u(1), \gamma_i^u(\alpha), \dots, \gamma_i^u(\alpha^{q-2})], \end{aligned}$$

where in the last expression (with a slight abuse of the notation) we re-defined $\gamma_i^u(\omega) = \Pr\{u_i = \omega | y_i^u\}$. In vector form, we can re-arrange (8), (9) into

$$\begin{aligned} \varphi_i &= \gamma_i^p \cdot [\pi_{f_i}(\varphi_{i-1}) \otimes \pi_{g_i}(\gamma_i^u)] \\ \beta_i &= \pi_{f_{i+1}}^{-1} \{ [\beta_{i+1} \cdot \gamma_{i+1}^p] \otimes \pi_{g_{i+1}}(\gamma_{i+1}^u) \}. \end{aligned} \quad (10)$$

In (10), $\pi_a(\mathbf{Q})$ denotes the permutation, induced by the multiplication by a scalar a of a random variable with p.m.f. vector \mathbf{Q} , on \mathbf{Q} , while $\pi_a^{-1}(\mathbf{Q})$ denotes the inverse permutation (or equivalently the permutation induced by the multiplication by a^{-1}). Furthermore, $'\cdot'$ denotes the (point-wise) multiplication of two vectors, and $'\otimes'$ denotes the convolution of the two vectors. The a posteriori p.m.f. vector of u_i given the channel output \mathbf{y} is finally given (up to a normalization factor) by

$$\mathbf{L}_i^u = \underbrace{\pi_{g_i}^{-1} \{ \pi_{f_i}(\varphi_{i-1}) \otimes [\beta_i \cdot \gamma_i^p] \}}_{\mu_i^u} \cdot \gamma_i^u \quad (11)$$

where μ_i^u represents the extrinsic information, $\mu_i^u(\omega) = \Pr\{u_i = \omega | \mathbf{y} \setminus y_i^u\}$. The message update can be easily followed on the normal factor graph of a section of the trellis provided in Fig. 3.⁹ The complexity is here dominated by the convolution operations, and thus scales as $\mathcal{O}(q^2)$.¹⁰ The algorithm can be simplified by applying the (fast) Fourier transform (FT) [33], [36], [37] for finite Abelian groups on the vectors involved in the convolutions. Assuming extension fields with characteristic 2, the FT reduces to the Walsh-Hadamard transform [33], i.e. given a function $x(\omega)$, $\omega \in \mathbb{F}_{2^m}$, its Fourier (Walsh-Hadamard) transform $X(\nu)$, $\nu \in \mathbb{F}_{2^m}$, is obtained as

$$X(\nu) = \sum_{\omega \in \mathbb{F}_{2^m}} x(\omega) (-1)^{\langle \underline{\omega}, \underline{\nu} \rangle}$$

$\langle \underline{\omega}, \underline{\nu} \rangle$ being the inner product over \mathbb{F}_2 between the length- m binary vector representations $\underline{\omega}, \underline{\nu}$ of ω, ν . By employing FFTs, the decoding complexity is reduced to $\mathcal{O}(q \log_2 q)$.

IV. NUMERICAL RESULTS

Simulation results on the AWGN channel for codes on \mathbb{F}_{256} are presented next. In all the simulations, we adopted the BP decoding over the Tanner graph of the codes with a maximum number of iterations set to $I_{max} = 200$. Binary antipodal modulation has been considered.

Fig. 4 shows the performance for a rate-compatible code family with input block size $k = 128$ bits. The mother code is

⁹When decoding on tail-biting trellises, the recursion for the forward metric calculation shall be circularly extended [35].

¹⁰Recall that q is the field order, and hence the length of the vectors involved in the convolutions of (10).

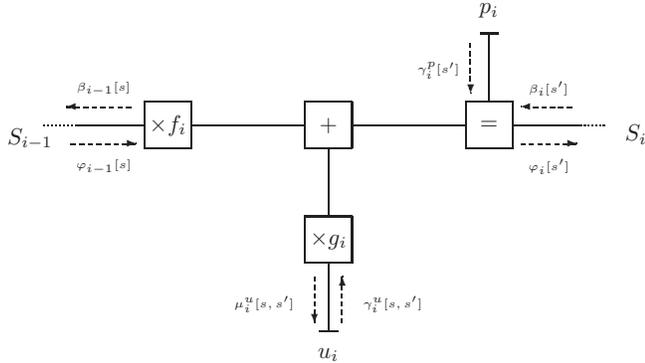


Fig. 3. Normal factor graph for a trellis section.

a (384, 128) code, whose parity-check matrix coefficients have been selected according to the method of [3]. A lower code rate 1/6 has been obtained by repeating each code symbol twice, and by multiplying the replicas by random elements in \mathbb{F}_{256}^* as for the multiplicative repeat (MR) approach of [21]. Higher code rates have been obtained in two different ways, i.e. (i) according to the parallel concatenation scheme, by periodically-puncturing parity symbols at the output of the two accumulators and (ii) by puncturing the VNs of type V_0 (thus, a rate 1/2 DA code is obtained, and further higher rates can be achieved by puncturing symbols periodically at the output of the accumulator in the DA encoder). In both cases, symbol-wise puncturing pattern (SPP) has been applied. The interleaver has been designed according to a circulant version of the progressive edge growth (PEG) algorithm [38]. The rate 1/3 mother code does not show floors down to $\text{CER} = 10^{-5}$, performing within 0.2 dB from the RCB [10]. Similar results are obtained by the lowest-rate code. For the two schemes with rate 1/2, the performance is still within 0.3 from the RCB down to $\text{CER} = 10^{-4}$, with a slight advantage for the DA construction. The advantage is more visible for the rate 2/3 case. Here, the PCCC performance suffers for a lack of steepness, which is not due to a low minimum distance (low-weight error patterns have not been detected), but to a slow decoding convergence associable with the large fraction of punctured symbols. For the DA case, the rate 1/2 code parity-check matrix of (5) has been used for the Tanner graph, and hence the higher rates have been obtained with a reduced fraction of punctured symbols. The same plot provides the performance of the (384, 128) double-binary turbo code of the DVB-RCS standard [7]. The \mathbb{F}_{256} PCCC outperforms the double-binary one by more than 0.7 dB at $\text{CER} = 10^{-4}$.

Fig. 5 depicts the minimum E_b/N_0 required to achieve $\text{CER} = 10^{-4}$ for several rate 1/3 parallel concatenated convolutional codes and rate 1/2 DA codes, with block sizes spanning from $k = 40$ bits to $k = 1024$ bits. The performances of rate 1/2 binary irregular protograph-based LDPC and accumulate repeat accumulate (ARA) codes from [5], [9] are provided too. The chart is completed by the SPB [11] for the continuous-input AWGN channel. The DA codes have been again obtained by puncturing the V_0 -type nodes of the PCCC graph. The interleavers have been generated on the fly

according to [32]. Additionally, the rate 1/3 and 1/2 $k = 40$ bits codes associated with the cycle graphs of Fig. 2 have been simulated. The rate 1/3 PCCCs perform within 0.5 dB from the SPB all over the block sizes (with the exception of $k = 40$). For the largest ($k = 1024$) block length, the gap is reduced to 0.3 dB. For the rate 1/2, the gap w.r.t. the SPB is slightly larger (0.2 dB more). The gain of the proposed non-binary turbo codes over the binary LDPC codes is remarkable (~ 1 dB or more) for the shortest block sizes. For the largest ($k = 1024$) block length, the gain is reduced to ~ 0.3 dB. The performance of two short codes from [39] are provided as well. The first is a (128, 64, 22) extended BCH code under maximum likelihood (ML) decoding, which achieves $\text{CER} = 10^{-4}$ at $E_b/N_0 = 3.03$ dB, only ~ 0.3 dB away from the SPB with a coding gain of ~ 0.4 dB over the (128, 64) DA code. We shall consider in the comparison that the DA code does not perform a complete ML decoding, and hence provides an error detection mechanism that may be required by critical application, e.g. telecommand in the up-link of space communication systems [9]. The second code is a (600, 270) terminated binary convolutional code with constraint length 30. This code performs close to the (512, 256) DA code, which however has a slightly higher code rate (0.5 vs. 0.45) and a lower block size (256 vs 270 information bits).

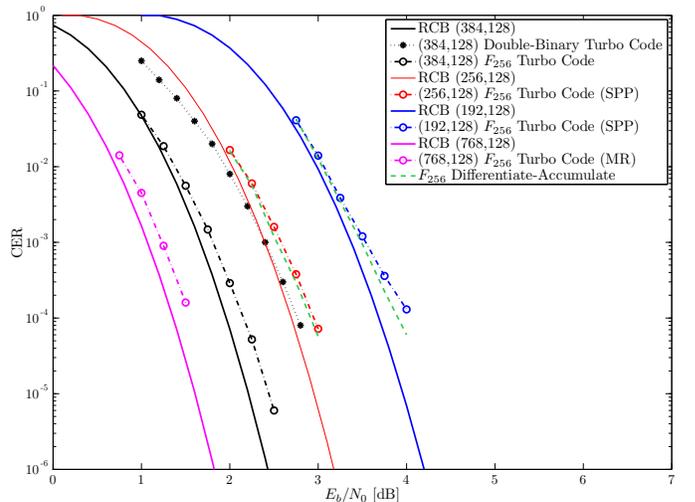


Fig. 4. Performance for a rate-compatible family of turbo codes on \mathbb{F}_{256} , $k = 128$ bits.

V. CONCLUSIONS

Two novel classes of turbo codes constructed over high-order finite fields have been presented. The codes are derived from a protograph sub-ensemble of the ($d_v = 2, d_c = 3$) regular LDPC ensemble. One of the proposed construction is based on the serial concatenation of a non-binary, time-variant differentiator and a of non-binary, time-variant accumulator, and provides a highly-structured flexible encoding scheme for ($d_v = 2, d_c = 4$) LDPC ensembles. Symbol MAP decoding of the component codes has been illustrated, together with its FFT-based simplification. The proposed codes allow efficient decoding either as LDPC or as turbo codes. Remarkable

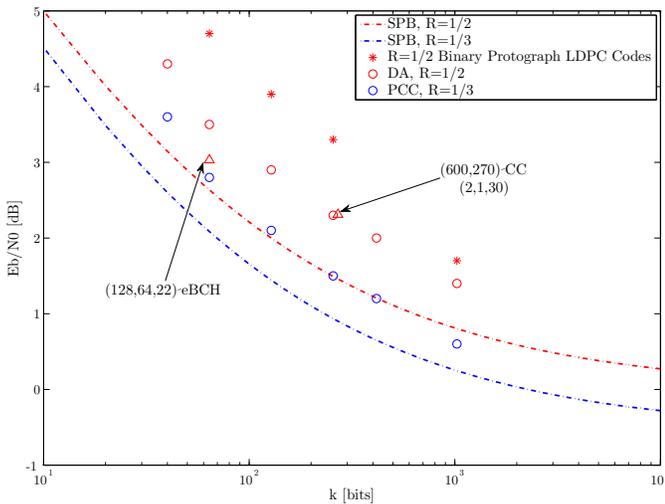


Fig. 5. Required E_b/N_0 for achieving $\text{CER} = 10^{-4}$ for various codes with rates 1/2, 1/3, compared with the corresponding SPBs.

gains (~ 1 dB) w.r.t. binary LDPC/turbo codes have been demonstrated in the moderate-short block regimes.

ACKNOWLEDGMENT

This research was supported in part by the ESA Project ANTARES and in part by the EC under Seventh FP grant agreement ICT OPTIMIX n. INFSO-ICT-214625.

REFERENCES

- [1] R. Gallager, *Low-Density Parity-Check Codes*. Cambridge, MA: MIT Press, 1963.
- [2] M. Davey and D. MacKay, "Low Density Parity Check Codes over $\text{GF}(q)$," *IEEE Commun. Lett.*, vol. 2, no. 6, pp. 165–167, Jun. 1998.
- [3] C. Poulliat, M. Fossorier, and D. Declercq, "Design of Regular $(2, d_c)$ -LDPC Codes over $\text{GF}(q)$ Using Their Binary Images," *IEEE Trans. Commun.*, vol. 56, no. 10, pp. 1626–1635, Oct. 2008.
- [4] X.-Y. Hu and E. Eleftheriou, "Cycle Tanner-Graph Codes over $\text{GF}(2^b)$," in *Proc. of IEEE Int. Symp. on Information Theory*, Yokohama, Japan, Jun./Jul. 2003, p. 87.
- [5] D. Divsalar, S. Dolinar, and C. Jones, "Low-Rate LDPC Codes with Simple Protograph Structure," in *Proc. IEEE Int. Symp. on Information Theory*, Adelaide, Sep. 2005.
- [6] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon Limit Error-Correcting Coding and Decoding: Turbo-Codes," in *Proc. IEEE Int. Conf. on Communications*, Geneva, Switzerland, May 1993.
- [7] C. Douillard and C. Berrou, "Turbo Codes with Rate- $m/(m+1)$ Constituent Convolutional Codes," *IEEE Trans. Commun.*, vol. 53, no. 10, pp. 1630–1638, 2005.
- [8] G. Liva, W. E. Ryan, and M. Chiani, "Quasi-Cyclic Generalized LDPC Codes with Low Error Floors," *IEEE Trans. Commun.*, vol. 56, no. 1, pp. 49–57, Jan. 2008.
- [9] D. Divsalar, S. Dolinar, and C. Jones, "Short Protograph-Based LDPC Codes," in *Proc. of IEEE MILCOM 2007*, Orlando, FL (USA), Oct. 2007, pp. 1–6.
- [10] R. G. Gallager, *Information Theory and Reliable Communication*. New York: Wiley, 1968.
- [11] C. Shannon, "Probability of Error for Optimal Codes in a Gaussian Channel," *Bell System Tech. J.*, vol. 38, pp. 611–656, 1959.
- [12] D. MacKay, "Turbo Codes are Low-Density Parity-Check Codes," 1998. Available: <http://www.inference.phy.cam.ac.uk/mackay/turbo-ldpc.pdf>.

- [13] G. Colavolpe, "Design and Performance of Turbo Gallager Codes," *IEEE Trans. Commun.*, vol. 52, no. 11, pp. 1901–1908, Nov. 2004.
- [14] J. Berkmann, "On Turbo Decoding of Nonbinary Codes," *IEEE Commun. Lett.*, vol. 2, no. 4, pp. 94–96, Apr. 1998.
- [15] —, "Symbol-by-Symbol MAP Decoding of Nonbinary Codes," in *Proc. ITG-Fachtagung Codierung für Quelle, Kanal und Übertragung*, Aachen, Germany, 1998.
- [16] —, *Iterative Decoding of Nonbinary Codes*. Munich, Germany: Ph.D. dissertation, Tech. Univ. München, 2000.
- [17] G. White and J. Costello, D.J., "Construction and Performance of q -ary Turbo Codes for Use with m -ary Modulation Techniques," in *Proc. of IEEE Int. Symp. on Information Theory*, 2000, p. 220.
- [18] K. Yang, "Weighted Nonbinary Repeat-Accumulate Codes," *IEEE Trans. Inf. Theory*, vol. 50, no. 3, pp. 527–531, Mar. 2004.
- [19] A. Reid, T. Gulliver, and D. Taylor, "Rate-1/2 Component Codes for Nonbinary Turbo Codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 9, pp. 1417–1422, sept. 2005.
- [20] W. Lin, B. Bai, Y. Li, and X. Ma, "Design of q -ary Irregular Repeat-Accumulate Codes," in *Proc. Int. Conf. on Advanced Information Networking and Applications*, Los Alamitos, USA, 2009, pp. 201–206.
- [21] K. Kasai, D. Declercq, C. Poulliat, and K. Sakaniwa, "Rate-Compatible Non-Binary LDPC Codes Concatenated with Multiplicative Repetition Codes," in *Proc. IEEE Int. Symp. on Information Theory*, Austin, Texas, USA, Jun. 2010.
- [22] J. Thorpe, "Low-Density Parity-Check (LDPC) Codes Constructed from Protographs," JPL INP, Tech. Rep., Aug. 2003, 42-154.
- [23] W. E. Ryan and S. Lin, *Channel Codes – Classical and Modern*. Cambridge University Press, 2009.
- [24] R. Tanner, "A recursive Approach to Low Complexity Codes," *IEEE Trans. Inf. Theory*, vol. 27, pp. 533–547, Sep. 1981.
- [25] J. Huang and J. Zhu, "Linear Time Encoding of Cycle $\text{GF}(2^p)$ Codes through Graph Analysis," *IEEE Commun. Lett.*, vol. 10, no. 5, pp. 1060–1071, May 2006.
- [26] H. Jin, A. Khandekar, and R. McEliece, "Irregular Repeat-Accumulate Codes," in *Proc. Int. Symp. on Turbo codes and Related Topics*, Sep. 2000, pp. 1–8.
- [27] J. Huang, S. Zhou, and P. Willett, "Structure, Property, and Design of Nonbinary Regular Cycle Codes," *IEEE Trans. Commun.*, vol. 58, no. 4, pp. 1060–1071, Apr. 2010.
- [28] W. W. Peterson and J. E. J. Weldon, *Error-Correcting Codes, Second Edition*. MIT Press, 1972.
- [29] D. A. Holton and J. Sheehan, *The Petersen Graph*. Cambridge University Press, 1993.
- [30] A. Venkiah, D. Declercq, and C. Poulliat, "Design of Cages with a Randomized Progressive Edge Growth Algorithm," *IEEE Commun. Lett.*, vol. 12, no. 14, pp. 301–303, April 2008.
- [31] S. Crozier and P. Guinand, "High-Performance Low-Memory Interleaver Banks for Turbo-Codes," in *Proc. IEEE Vehicular Technology Conf. (VTC)*, Atlantic City, NJ, USA, Oct. 2001, pp. 2394–2398.
- [32] S. Crozier, J. Lodge, P. Guinand, and A. Hunt, "Performance of Turbo Codes with Relative Prime and Golden Interleaving Strategies," in *Proc. 6th International Mobile Satellite Conference*, Ottawa, Ontario, Canada, Jun. 1999, pp. 268–275.
- [33] A. Goupil, M. Colas, G. Gelle, and D. Declercq, "FFT-based BP Decoding of General LDPC Codes over Abelian Groups," *IEEE Trans. Commun.*, vol. 55, pp. 644–649, Apr. 2007.
- [34] L. R. Bahl, J. Cocke, F. Jelinek, and J. Raviv, "Optimal Decoding of Linear Codes for Minimizing Symbol Error Rate," *IEEE Trans. Inf. Theory*, vol. 20, pp. 284–287, Mar. 1974.
- [35] J. B. Anderson and S. M. Hladik, "Tailbiting MAP Decoders," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 2, pp. 297–302, Feb. 1998.
- [36] G. D. Forney Jr., "Codes on Graphs: Normal Realizations," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 520–548, Feb. 2001.
- [37] J. Berkmann and C. Weiss, "On Dualizing Trellis-Based APP Decoding Algorithms," *IEEE Trans. Commun.*, vol. 50, no. 11, pp. 1743–1757, Nov. 2002.
- [38] X. Y. Hu, E. Eleftheriou, and D. M. Arnold, "Regular and Irregular Progressive Edge-Growth Tanner Graphs," *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 386–398, Jan. 2005.
- [39] "Code Imperfectness." [Online]. Available: <http://www331.jpl.nasa.gov/public/imperfectness.html>