Non-binary protograph low-density parity-check codes for space communications

Laura Costantini[1], Balázs Matuz[2,*,†], Gianluigi Liva[2], Enrico Paolini[3] and Marco Chiani[3]

[1]*SkyTechnology s.r.l., via Gonin, 55 20147 Milano, Italy*
[2]*Institute of Communication and Navigation, Deutsches Zentrum fur Luft- und Raumfahrt (DLR), 82234 Wessling, Germany*
[3]*DEIS/WiLAB, University of Bologna, via Venezia 52, 47521 Cesena (FC), Italy*

SUMMARY

Protograph-based non-binary low-density parity-check (LDPC) codes with ultra-sparse parity-check matrices are compared with binary LDPC and turbo codes (TCs) from space communication standards. It is shown that larger coding gains are achieved, outperforming the binary competitors by more than 0.3 dB on the additive white Gaussian noise channel (AWGN). In the short block length regime, the designed codes gain more than 1 dB with respect to the binary protograph LDPC codes recently proposed for the next generation up-link standard of the Consultative Committee for Space Data Systems. Copyright © 2012 John Wiley & Sons, Ltd.

1. INTRODUCTION

Owing to their excellent error correction capability combined with the availability of low complexity encoding/decoding algorithms, low-density parity-check (LDPC) codes [1] have recently been included in several satellite communications standards. Their application ranges from deep-space communications [2, 3] to satellite broadcasting services [4] and up-links for interactive satellite systems [5]. In the past decade, LDPC code constructions were proposed that approach the Shannon limit within few tenths of decibel for large codeword lengths ($n > 10000$) [6, 7]. In the moderate codeword length regime ($1000 < n < 10000$), structured constructions with low error floors were proposed, for example, in [8–12]. These constructions achieve low codeword error rates, for example, $\sim 10^{-6}$, within 0.5 to 1 dB from the random coding bound (RCB) [13]. In order to enhance the code performance for short/moderate codeword lengths, turbo codes (TCs) constructed over high-order Galois fields (GFs) were proposed in [14], showing coding gains in the order of 1 dB over binary LDPC and TC constructions. LDPC codes over non-binary GFs were proposed in [15]. As for binary LDPC codes, decoding is based on belief propagation (BP) that is on message passing along the edges of the Tanner graph. The decoding complexity is dominated by the check node (CN) operations and scales as $\mathcal{O}(q^2)$, where q is the order of the GF. However, the probability-domain decoding algorithm can be simplified by using fast Fourier transforms (FFTs) to perform the CN elaborations, reducing the complexity to $\mathcal{O}(q log_2 q)$ [16]. Further complexity reductions for non-binary LDPC decoders were achieved in [17]. The performance of non-binary LDPC codes on high-order GFs for space communications was investigated in [18]. In this paper, we will introduce non-binary protograph-based LDPC codes with block-circulant parity-check matrices

---

*Correspondence to: Balázs Matuz, Institute of Communication and Navigation, Deutsches Zentrum für Luft- und Raumfahrt (DLR), 82234 Wessling, Germany.
†E-mail: balazs.matuz@dlr.de

for facilitating the decoder implementation. The proposed protographs are analyzed via density evolution (DE) [6], and for the derived codes, we provide a further evidence of the performance gain over both well established and recently proposed binary LDPC codes, with emphasis on codes designed for space communications. In fact, non-binary LDPC codes find their natural application to both deep-space and satellite communications. In the deep-space context, the additional coding gain w.r.t. the codes currently standardized by the Consultative Committee for Space Data Systems (CCSDS) for telemetry may reach up to 0.5 dB. Furthermore, for telecommand transmissions requiring the use of short packets, non-binary LDPC show remarkable gains (1 dB or more) over the proposals [19] within the Next Generation Uplink working group of the CCSDS. The application of non-binary LDPC codes to satellite communications could be considered for the uplink of mobile interactive satellite networks, where short packets may be required and where the link budgets are usually tight, as well as in integration with enhanced random access schemes [20–23] for satellite networks.

The work is organized as follows. Frequency-domain decoding for non-binary LDPC codes is reviewed in Section 2. Insights on the design of protograph codes are given in Section 3, before presenting simulation results in Section 4. Section 5 concludes the paper.

2. BELIEF PROPAGATION DECODING OF NON-BINARY LOW-DENSITY PARITY-CHECK CODES

In this paper, we always consider GFs of order $q = 2^p$, $p > 1$. The parity-check matrix $\mathbf{H}$ of an (n, k) LDPC code on GF(2^p) possesses $N = n/p$ columns, $M = (n - k)/p$ rows and each entry takes a value in GF(2^p). The corresponding Tanner graph is composed of a set $\{V_i\}_{i=0, \ldots, N-1}$ of N variable nodes (VNs) and a set $\{C_j\}_{j=0, \ldots, M-1}$ of M CNs. A variable node V_i is connected by an edge to a check node C_j if and only if the corresponding element of $\mathbf{H}$, namely $h_{j,i}$, is not zero. Considering a probability-domain decoder, each message is a probability mass function (PMF) and consists of a vector of q probabilities, one for each possible value of the codeword symbol associated with the message. Probability-domain BP decoding of non-binary LDPC codes on the additive white Gaussian noise (AWGN) channel was investigated in [15]. Because of a complexity scaling with $\mathcal{O}(q^2)$, only GFs of order up to $q = 16$ were considered. A more efficient approach based on the use of FFTs at the CNs was suggested in [16, 24, 25], leading to a complexity scaling with $\mathcal{O}(q log_2 q)$.

The probability-domain decoder is initialized as follows. The very first message $\mathbf{v}_{i,j}^{\text{out}}$ from VN V_i to CN C_j coincides with $\mathbf{m}_i$, a vector of q symbol probabilities given the observation from the channel. The rest of decoding algorithm is summarized in the following. Apart from the initialization, the steps described next are iterated until a valid codeword is detected, or a maximum number of iterations, I_{max}, is reached. The iterative decoding algorithm presented hereafter is very much similar to the one for binary LDPC codes. Major differences lie in the fact that each codeword symbol c_i can take $q = 2^p$ different values (with $p > 1$) so that the probabilities passed along the edges of the graph are q-dimensional vectors. Non-zero elements of the parity-check matrix may cause permutations of these vectors, once a message is passed on an edge associated with $h_{j,i}$. This is exemplified later. An overview of the decoding algorithm is given in Figure 1.

2.1. Permutation of outgoing variable node messages and check node message processing

The entries $h_{j,i}$ of the parity-check matrix are elements of GF(q). Leting c_i be the i-th codeword symbol, the j-th parity-check equation can be written as
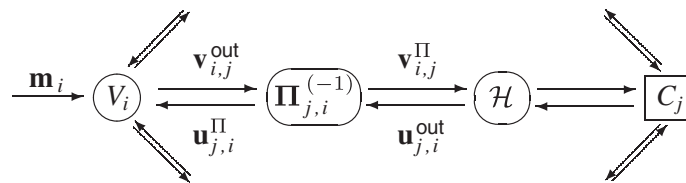

Figure 1. Overview of the message passing algorithm for non-binary low-density parity-check codes.

$$\sum_{i=0}^{N-1} h_{j,i} c_i = 0. \tag{1}$$

The multiplication of c_i by $h_{j,i}$ in (1) entails a permutation of the entries of $\mathbf{v}_{i,j}^{\text{out}}$. This is because due to the multiplication the codeword symbol c_i is mapped on the new symbol $z_i = h_{j,i} c_i$. Then, the probabilities associated with the q possible values of c_i undergo a similar mapping that turns out to be a simple permutation in GF(q). Formally, we can write $\Pr(z_i = a_w) = \Pr\left(c_i = h_{j,i}^{-1} a_w\right)$, where $h_{j,i}^{-1}$ is the multiplicative inverse of $h_{j,i}$ and $a_w \in$ GF(q). For sake of clarity, let's consider an example on GF(4) with $h_{j,i} = 2$, $h_{j,i}^{-1} = 3$ and $a_w = 1$. We are interested in the probability $\Pr(z_i = 1)$. This is equal to the probability $\Pr(c_i = 3)$. Similar considerations can be carried out for all other values of a_w. Accordingly, the permuted message from V_i to C_j is given by $\mathbf{v}_{i,j}^{\Pi} = \mathbf{v}_{i,j}^{\text{out}} \cdot \Pi_{j,i}$, where $\Pi_{j,i}$ is a $q \times q$ permutation matrix associated with $h_{j,i}$.

Modeling each $z_i = h_{j,i} c_i \in$ GF(q) as a discrete random variable, and under the independence assumption, the left-hand side in (1) is a random variable whose PMF is given by the convolution in GF(q) of the PMFs of the different z_i. For each CN C_j, define the set of indices of its neighboring VNs as $\mathcal{I}_j$ and the message outgoing towards the VN V_i as $\mathbf{u}_{j,i}^{\text{out}}$. We have

$$\mathbf{u}_{j,i}^{\text{out}} = \circledast_{l \in \mathcal{I}_j \setminus \{i\}} \mathbf{v}_{l,j}^{\Pi}$$

where $\circledast$ denotes the convolution of the PMFs. By applying the Hadamard transform (see e.g. [26, Chapter 5, p. 127]), $\mathcal{H}\{\cdot\}$, the discrete convolution turns into an element-wise multiplication. Because the Hadamard transform coincides with its inverse, this yields

$$\mathbf{u}_{j,i}^{\text{out}} = \mathcal{H}\left\{ \prod_{l \in \mathcal{I}_j \setminus \{i\}} \mathcal{H}\left\{ v_{l,j}^{\Pi} \right\} \right\}. \tag{2}$$

The right-hand side of (2) can be efficiently implemented via the fast Hadamard transform as a recursive application of sums and differences. This allows lowering the complexity of the CN elaboration to $\mathcal{O}(q \log_2 q)$.

2.2. De-permutation of outgoing check node messages and variable node message processing

The output message $\mathbf{u}_{j,i}^{\text{out}}$ has to be de-permuted before it can be passed to the VN V_i. The concept here is similar to the one mentioned previously for the VN messages. The de-permutation may be written as $\mathbf{u}_{j,i}^{\Pi} = \mathbf{u}_{j,i}^{\text{out}} \cdot \Pi_{j,i}^{-1}$. Here, $\Pi_{j,i}^{-1}$ is a $(q \times q)$ de-permutation matrix related to $h_{j,i}^{-1}$.

The generic VN V_i computes the outgoing message towards its neighboring CN C_j by multiplying (element-wise) $\mathbf{m}_i$ by the product of all incoming messages (each of which consists of a PMF) but the message emanating from C_j. For a VN V_i, we denote the set of its neighboring CNs as $\mathcal{J}_i$. Then, the message from VN V_i to CN C_j is given by

$$\mathbf{v}_{i,j}^{\text{out}} = \mathbf{m}_i \cdot \prod_{l \in \mathcal{J}_i \setminus \{j\}} \mathbf{u}_{l,i}^{\Pi}$$

where all multiplications are element-wise. Next, it is necessary to normalize the elements of $\mathbf{v}_{i,j}^{\text{out}}$ to sum up to 1.

2.3. Hard decision and stopping criterion

The algorithm stops when a given maximum number I_{max} of iterations is reached or if at the end of the current iteration a valid codeword is found. At the end of each iteration, the a posteriori probabilities of symbol c_i are obtained by multiplying element-wise all messages incoming towards the VN V_i, including $\mathbf{m}_i$:

$$\mathbf{v}_i = \mathbf{m}_i \cdot \prod_{l \in \mathcal{J}_i} \mathbf{u}_{l,i}^{\Pi}. \tag{3}$$

In (3), $\mathbf{v}_i$ is a vector of q elements (one for each possible value of c_i) and provides an estimation of the a posteriori probabilities $Pr(c_i = a_w|\mathbf{y})$, where $w \in \{0, 1, \cdots, q-1\}$ and $\mathbf{y} = (\mathbf{y}_1, \mathbf{y}_2, \ldots, \mathbf{y}_N)$ is the vector of channel observations. The decision on c_i is $\hat{c}_i = a_{\hat{w}}$ with $\hat{w} = argmax_w v_{i,w}$, where $v_{i,w}$ is the w-th element of $\mathbf{v}_i$.

3. PROTOGRAPH-BASED NON-BINARY LOW-DENSITY PARITY-CHECK CODE DESIGN

A protograph [12, 27, 28] is a Tanner graph with a relatively small number of nodes. A protograph $\mathcal{G} = (\mathcal{V}, \mathcal{C}, \mathcal{E})$ consists of a set of N_p variable nodes $\mathcal{V}$, a set of M_p check nodes $\mathcal{C}$, and a set of edges $\mathcal{E}$. Each edge $e_{j,i} \in \mathcal{E}$ connects a variable node $V_i \in \mathcal{V}$ to a check node $C_j \in \mathcal{C}$. Multiple parallel edges are permitted. A larger graph can be obtained by a copy-and-permute procedure: the protograph is copied Q times, and then the edges of the individual replicas are permuted among the Q replicas. The *derived graph* will consist of $N = N_p Q$ variable nodes and $M = M_p Q$ check nodes. A protograph can be described by a *base matrix* $\mathbf{B}$ of size $M_p \times N_p$. The element $b_{j,i}$ of $\mathbf{B}$ represents the number of edges connecting the variable node V_i to the check node C_j. Protographs are especially useful for the design of high-parallelism decoders relying on modular (elementary) blocks based on the code protograph [27].

The design of a protograph non-binary LDPC code may be summarized in three main steps:

1. Definition of the code protograph (equivalently, of the base matrix).
2. Expansion of the protograph (base matrix) into the code Tanner graph (associated with the code parity-check matrix $\mathbf{H}$).
3. Choice of the values of the non-zero entries of $\mathbf{H}$.

3.1. Definition of the code protograph

It is well established that regular distributions with variable node degree $d_v = 2$ provide excellent *iterative decoding thresholds* on the AWGN channel for sufficiently large field orders [29]. For large codeword lengths LDPC codes experience a threshold effect in terms of E_b/N_0 such that communication is reliable above the threshold and unreliable below it. As an example, the $(2,4)$-regular ensemble over GF(256) exhibits a threshold at $E_b/N_0 \simeq 0.45$ dB, only 0.27 dB away from the Shannon limit for rate-1/2 codes on the binary-input AWGN channel. Hence, we focus on regular protographs with (average) VN degree $d_v = 2$. Because of very small VN degrees, such graphs are called *ultra-sparse*. Examples are provided in Figure 2(a) and 2(b). A further remark deals with the design of low-rate codes. In the low code rate regime ($R < 1/3$), the regular protograph construction has to be dropped. A simple yet effective solution is given by the repetition-code-based approach of [30], where a design technique for low-rate non-binary LDPC codes based on protographs is presented. In particular, it is shown how an arbitrary low-rate non-binary LDPC code can be obtained from a higher rate one by repeating the codeword symbols by means of a non-binary repetition code (i.e. some codeword symbols are repeated, and the replicas are multiplied by non-zero GF elements). This allows an excellent flexibility in the code construction, supporting rate compatibility and maintaining the decoding complexity of the mother (higher-rate) code, with performance close to the theoretical bounds down to very low code rates and short codeword lengths. Accordingly, low-rate protographs are designed by repeating selected variable nodes of the protograph. An example is provided in Figure 2(c) where different branches of the graph may be added/removed to lower/increase the code rate. Let's consider now the base matrices

$$\mathbf{B}_1 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \quad \mathbf{B}_2 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \quad \mathbf{B}_3 = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

corresponding to the protographs of Figure 2 with rates 1/2, 1/3 and 1/4, respectively. In Table I, the iterative decoding thresholds over the binary-input AWGN channel for the three protograph ensembles
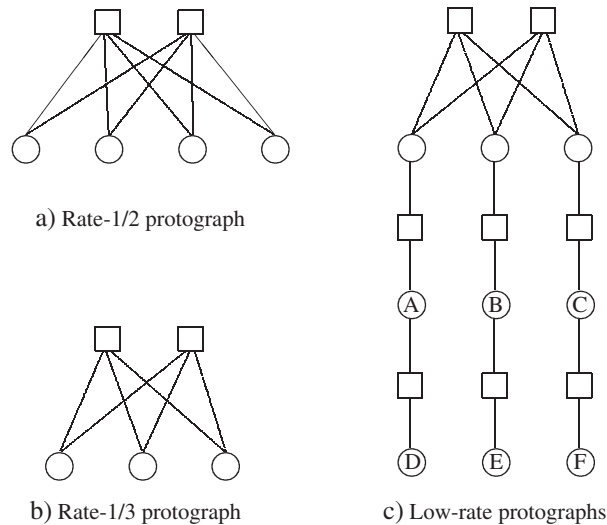
Figure 2. Protographs used for the code design. (a) Rate-1/2 regular protograph (base matrix $\mathbf{B}_1$). (b) Rate 1/3 regular protograph (base matrix $\mathbf{B}_2$). (c) Low-rate protographs obtained by multiplicative repetition of variable nodes [30]. A rate 1/4 protograph is obtained by adding to the rate-1/3 protograph the VN A and the CN connected to it (base matrix $\mathbf{B}_3$). The rate can be lowered to 1/6 by further adding VNs B and C. A rate 1/9 protograph is finally given by adding the VNs D, E and F.

are compared with the respective Shannon limits. As a main indicator of the code performance, the iterative decoding threshold can be derived via protograph-based DE. Thereto one tracks the probability densities of the messages passed along the edges of a cycle-free (infinite size) Tanner graph. The smallest value of E_b/N_0 such that the symbol error probability vanishes (as the number of iterations tends to infinity) corresponds to the iterative decoding threshold. To obtain the results in Table I for the three protographs, we used DE based on a Monte Carlo approach. For the first two ensembles, the decoding threshold is within 0.3 dB from the Shannon limit, whereas for the rate-1/4 ensemble, the gap is around 0.4 dB. Note that the threshold has been calculated for the ensemble where the parity-check matrix coefficients are selected with uniform distribution over $\mathrm{GF}(q)^*$, where $\mathrm{GF}(q)^*$ is the set of non-zero elements of $\mathrm{GF}(q)$. Refined ensembles based on an optimized choice of the parity-check matrix coefficients exhibit slightly improved thresholds [29].

3.2. Protograph expansion

The second step can be tackled by using tools available from the construction of binary LDPC codes. Hence, girth optimization techniques such as the progressive edge growth algorithm [31] can be adopted for the matrix construction. More specifically, the matrices have been constructed using a circulant version of the progressive edge growth algorithm, starting from the protograph and performing protograph expansions by means of circulant permutation matrices in either two or three stages. The resulting parity-check matrices are in block circulant form. This feature allows a compact description of the matrix structure, facilitating the decoder implementation.

3.3. Choice of the parity-check matrix coefficients

The third step may be pragmatically performed by selecting the non-zero entries of $\mathbf{H}$ with uniform probability over $\mathrm{GF}(q)^*$. This approach provides a satisfactory performance in most cases, especially

Table I. Thresholds computed for different protographs of Figure 2.

Protograph base matrix	Threshold, $(E_b/N_0)^*$	Shannon limit, $(E_b/N_0)^{sh}$
$\mathbf{B}_1$	0.48 dB	0.18 dB
$\mathbf{B}_2$	-0.21 dB	-0.49 dB
$\mathbf{B}_3$	-0.42 dB	-0.79 dB

for large GF orders. However, it has been pointed out that ultra-sparse ($d_v = 2, d_c$) non-binary LDPC code ensembles built with this approach tend to be affected by an error floor already at moderate error rates [29]. This phenomenon is related to the fact that their expected minimum distance grows sub-linearly with *n* [1]. An efficient approach for selecting the non-zero entries is proposed in [29]. The approach is based on the binary image of the non-binary parity-check equations. Note in fact that a degree-d_c equation over GF(2^p) is equivalent to *p* binary equations involving $p \cdot d_c$ bits and hence can be regarded as ($p \cdot d_c, p \cdot (d_c - 1)$) binary linear block code. In this view, the Tanner graph of a non-binary LDPC code can be described in terms of a generalized LDPC (G-LDPC) code graph. By judiciously selecting the coefficients for each equation, one can assure that the corresponding binary linear block code representation possesses a minimum distance larger than 2. If all *M* non-binary equations are designed in this manner, the overall result is an increased minimum distance for the non-binary LDPC code and hence a lower error floor. For the selection of the coefficients, we hence adopted the method of [29].

4. NUMERICAL RESULTS

The results presented in this section have been obtained by Monte Carlo simulations on the AWGN channel with $I_{max} = 200$ iterations. All simulated non-binary LDPC codes have been constructed on GF(256). We provide a comparison with binary codes in terms of codeword error rate (CER) versus E_b/N_0. The RCB and the sphere packing bound are shown for reference.

(a) CER for a GF(256) LDPC code and a protograph LDPC code from [19]. $R = 1/2$, $k = 64$ bits.

(b) CER for a GF(256) LDPC code and a protograph LDPC code from [19]. $R = 1/2$, $k = 128$ bits.

(c) CER for a GF(256) LDPC code and a protograph LDPC code from [19]. $R = 1/2$, $k = 256$ bits.

(d) CER for GF(256) LDPC codes, 3D-TC, DVB-RCS codes with $R = 1/2$ and $R = 1/4$. Information length $k = 448$ bits for the LDPC codes and $k = 456$ bits for 3D-TCs, the DVB-RCS code and the RCB.
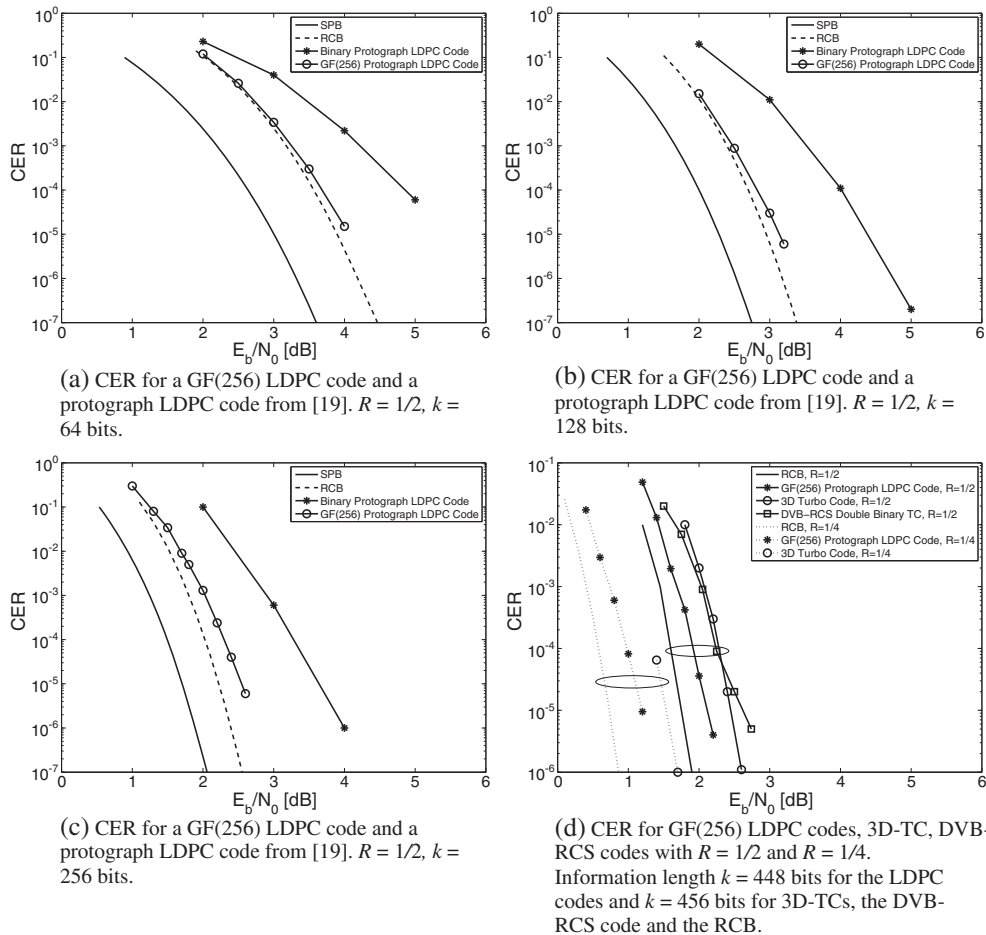
Figure 3. Performance comparisons among binary and non-binary low-density parity-check (LDPC) as well as turbo codes (TCs).

We first consider codes with rate 1/2 based on the protograph of Figure 2(a), with information block lengths $k = 64$, 128 and 256 bits. The performance of the designed non-binary LDPC codes is compared with that of the binary protograph LDPC codes recently proposed for the next generation up-link of the CCSDS standard [19]. The results are depicted in Figure 3(a), 3(b) and 3(c) for k equal to 64, 128 and 256 bits, respectively. Remarkably, the proposed non-binary LDPC codes perform very close to the RCB (within 0.3 dB down to low CERs) and gain ~ 1 dB over the binary protograph LDPC codes of [19].

A comparison between non-binary LDPC codes and some TCs is illustrated for $R = 1/2$ and $R = 1/4$ in Figure 3(d). Specifically, the double-binary TCs from the Digital Video Broadcasting - Return Channel via Satellite (DVB-RCS) standard [32] and the recently proposed 3D-TCs [33] are considered. Because of construction constraints, we have $k = 456$ for the TCs and $k = 448$ for the designed LDPC codes. From Figure 3(d), it can be seen that the non-binary LDPC codes outperform TCs for both code rates. At $CER = 10^{-5}$, the proposed codes gain more than 0.3 dB over their competitors.

5. CONCLUSIONS

We compared non-binary protograph LDPC constructions based on ultra-sparse matrices with binary LDPC and TCs, showing how remarkable coding gains can be achieved on the AWGN channel in the short block regime. The outcomes presented within this paper are in particular interesting for deep-space communications, as well as satellite applications, where the return link is targeted.

REFERENCES

1. Gallager R. *Low-Density Parity-Check Codes*. M.I.T. Press: Cambridge, MA, 1963.
2. Andrews K, Divsalar D, Dolinar S, Hamkins J, Jones C, Pollara F. The development of turbo and LDPC codes for deep-space applications. *Proc IEEE* 2007; **95**(11):2142–2156.
3. Calzolari GP, Chiani M, Chiaraluce F, Garello R, Paolini E. Channel coding for future space missions: New requirements and trends. *Proc IEEE* 2007; **95**(11):2157–2170.
4. Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications, ETSI, 2004.
5. Liva G, Papaleo M, Niebla C, Scalise S, Cioni S, Vanelli-Coralli A, Corazza GE, Kim P, Lee HJ. The very short frame of mobile DVB-RCS: Code design and QoS performance. *Int J Satellite Comm Network* 2010; **28**(3–4):209–231.
6. Richardson T, Shokrollahi M, Urbanke R. Design of capacity-approaching irregular low-density parity-check codes. *IEEE Trans Inf Theory* 2001; **47**(2):619–637.
7. Luby M, Mitzenmacher M, Shokrollahi MA, Spielman DA. Improved low-density parity-check codes using irregular graphs. *IEEE Trans Inf Theory* 2001; **47**(2):585–598.
8. Yang M, Li Y, Ryan W. Design of efficiently encodable moderate-length high-rate irregular LDPC codes. *IEEE Trans Commun* 2004; **52**(4):564–571.
9. Zhang Y, Ryan WE. Structured IRA codes: Performance analysis and construction. *IEEE Trans Commun* 2007; **55**(5):837–844.
10. Abbasfar A, Divsalar D, Yao K. Accumulate-repeat-accumulate codes. *IEEE Trans Commun* 2007; **55**(4):692–702.
11. Liva G, Ryan WE, Chiani M. Quasi-cyclic generalized LDPC codes with low error floors. *IEEE Trans Commun* 2008; **56**(1):49–57.
12. Ryan WE, Lin S. *Channel Codes—Classical and Modern*. Cambridge University Press: Cambridge, 2009.
13. Gallager RG. *Information Theory and Reliable Communication*. Wiley: New York, 1968.
14. Liva G, Paolini E, Scalise S, Chiani M. Turbo codes based on time-variant memory-1 convolutional codes over $\mathbb{F}_q$. *Proceedings of the 2011 IEEE International Conference on Communications*, Kyoto, Japan, Jun. 2011.
15. Davey M, MacKay D. Low density parity check codes over GF(q). *IEEE Commun Lett* 1998; **2**(6):70–71.
16. Barnault L, Declercq D. Fast decoding algorithm for LDPC over GF(2^q). *Proceedings of 2003 IEEE Information Theory Workshop*, Mar./Apr. 2003; 70–73.
17. Voicila A, Declercq D, Verdier F, Fossorier M, Urard P. Low complexity decoding for non-binary LDPC codes in high order fields. *IEEE Trans Commun* 2010; **58**(5):1365–1375.
18. Costantini L, Matuz B, Liva G, Paolini E, Chiani M. On the performance of moderate-length non-binary LDPC codes for space communications. *Proceedings 5th Advanced Satellite Mobile Systems Conference*, Cagliari, Italy, Sept. 2010.
19. Divsalar D, Dolinar S, Jones C. Short protograph-based LDPC codes. *Proceedings of 2007 IEEE MILCOM*, Orlando, Florida (US), 2007; 1–6.
20. Casini E, Gaudenzi RD, del Rio Herrero O. Contention resolution diversity slotted ALOHA (CRDSA): An enhanced random access scheme for satellite access packet networks. *IEEE Trans Wireless Comm* 2007; **6**:1408–1419.

21. De Gaudenzi R, del Rio Herrero O. Advances in random access protocols for satellite network. *Proceedings International Workshop on Satellite and Space Communications, IWSSC*, Sep. 2009.
22. Liva G. Graph-based analysis and optimization of contention resolution diversity slotted ALOHA. *IEEE Trans Commun* 2011; **59**(2):477–487.
23. Paolini E, Liva G, Chiani M. High throughput random access via codes on graphs: Coded slotted ALOHA. *Proceedings 2011 IEEE International Conference on Communications*, Kyoto, Japan, Jun. 2011.
24. MacKay D, Davey M. Evaluation of Gallager codes for short block length and high rate applications. In *Codes, Systems and Graphical Models*. Springer-Verlag: New York, 1999; 113–130.
25. Declercq D, Fossorier M. Decoding algorithms for non-binary LDPC codes over GF. *IEEE Trans Commun* 2007; **55**(4):633–643.
26. Mac Williams F, Sloane N. *The theory of error-correcting codes*, vol. **16**. North Holland Mathematical Libray: Amsterdam, 1977.
27. Thorpe J. Low-density parity-check (LDPC) codes constructed from protographs. JPL INP, Tech. Rep., Aug. 2003; 42–154.
28. Liva G, Song S, Lan L, Zhang Y, Ryan W, Lin S. Design of LDPC codes: A survey and new results. *J. Commun. Softw. Syst.* 2006; **2**(3):191–211. Invited paper.
29. Poulliat C, Fossorier M, Declercq D. Design of regular $(2, d_c)$-LDPC codes over GF(q) using their binary images. *IEEE Trans Commun* 2008; **56**(10):1626–1635.
30. Kasai K, Declercq D, Poulliat C, Sakaniwa K. Rate-compatible non-binary LDPC codes concatenated with multiplicative repetition codes. *Proceedings 2010 IEEE International Symposium on Information Theory*, Austin, Texas, USA, Jun. 2010.
31. Hu X-Y, Eleftheriou E, Arnold D. Regular and irregular progressive edge-growth Tanner graphs. *IEEE Trans Inf Theory* 2005; **51**(1):386–398.
32. Interaction channel for satellite distribution systems, ETSI EN 301 790 v1.5.1, DVB, 2009.
33. Berrou C, Graell i Amat A, Ould Cheikh Mouhamedou Y, Saouter Y. Improving the distance properties of turbo codes using a third component code: 3D turbo codes. *IEEE Trans Commun* 2009; **57**(9):2505–2509.

AUTHORS' BIOGRAPHIES
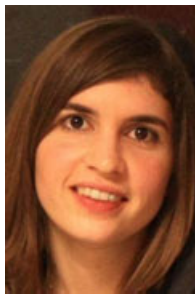
Laura Costantini received a Master's degree in Telecommunication engineering from the University of Bologna, Italy, in 2010. She carried out her Master's thesis about Non-binary LDPC decoding at DLR (German Aerospace Center) at the Institute of Communications and Navigation, Wessling, Germany. Laura Costantini has been employed as software and firmware consultant at several Italian companies. Currently she works on field of energy saving communication systems.
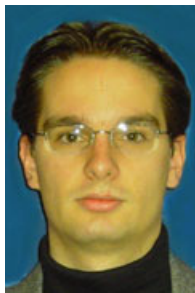
Balázs Matuz was born in Budapest, Hungary, in 1982. He received his Diploma degree in Electrical Engineering and Information Technology from the Technische Universität München (TUM), Germany in 2007. Since then he is enrolled in a PhD program at the German Aerospace Center (DLR) in Oberpfaffenhofen, Germany. Currently he is a scientific researcher at the Institute of Communications and Navigation where he mainly works on novel forward error correcting schemes (based on LPDC and turbo-like codes) for satellite and space systems. During the past years he has been involved in several national and international projects on channel coding and channel modeling. Amongst others he participated in development of a DVB-SH prototype system in the framework of the European Space Agency (ESA) financed projects Ortigia and J-Ortigia. He is an IEEE student member and he serves IEEE as a reviewer for Transactions, Journals and Conferences, as well as a technical program committee member.

Gianluigi Liva was born in Spilimbergo, Italy, on July 23rd, 1977. He received the Laurea in Electronic Engineering in 2002, and the Ph.D. degree in 2006 at DEIS, University of Bologna (Italy). His main research interests include satellite communication systems, random access techniques and error control coding. Since 2003 he has been involved in the research of channel codes for high data rate CCSDS (Consultative Committee for Space Data Systems) missions, in collaboration with the European Space Operations Centre of the European Space Agency (ESA-ESOC). From October 2004 to April 2005 he was researching at the University of Arizona as visiting student, where he was involved in the design of low-complexity coding systems for space communication systems. He is currently with the Institute of Communications and Navigation at the German Aerospace Center (DLR). He is active in the DVB-SH and in the

DVB-RCS Mobile standardization groups. In 2010 he has been appointed guest lecturer for channel coding at the Institute for Communications Engineering (LNT) of the Technische Universität München (TUM). He is IEEE member and he serves IEEE as reviewer for Transactions, Journals and Conferences.

Enrico Paolini was born in Fano, Italy, in 1977. He received the Dr. Ing. degree (with honors) in Telecommunications Engineering in 2003 and the Ph.D. degree in Electrical Engineering in 2007, both from the University of Bologna, Italy. While working toward the Ph.D. degree, he was Visiting Research Scholar with the University of Hawaii at Manoa. From 2007 to 2010, he held a postdoctoral position with the Department of Electronics, Computer Science and Systems (DEIS), University of Bologna. Currently, he is an Assistant Professor at the II Engineering Faculty, University of Bologna. His research interests include error-control coding (with emphasis on LDPC codes and their generalizations, iterative decoding algorithms, reduced-complexity maximum likelihood decoding for erasure channels), and radar sensor networks based on UWB. In the field of error correcting codes, has been involved since 2004 in several activities with the European Space Agency (ESA). Dr. Paolini served on the Technical Program Committee at several IEEE International Conferences, and on the Organizing Committee of the 2011 IEEE International Conference on Ultra-Wideband. He is member of the IEEE Communications Society and of the IEEE Information Theory Society.

Marco Chiani was born in Rimini, Italy, in April 1964. He received the Dr. Ing. degree (magna cum laude) in electronic engineering and the Ph.D. degree in electronic and computer science from the University of Bologna, Italy, in 1989 and 1993, respectively. He is a Full Professor of Telecommunications and the current Director of the Industrial Research Center on ICT, University of Bologna. During summer 2001, he was a Visiting Scientist with AT&T Research Laboratories, Middletown, NJ. He is a frequent visitor at the Massachusetts Institute of Technology (MIT), Cambridge, where he presently holds a Research Affiliate appointment. He is leading the research unit of the University of Bologna on cognitive radio and UWB (European project EUWB), on Joint Source and Channel Coding for wireless video (European projects Phoenix-FP6 and Optimix-FP7), and is a consultant to the European Space Agency (ESA-ESOC) for the design and evaluation of error correcting codes based on LDPCC for space CCSDS applications. His research interests include wireless communication systems, MIMO systems, wireless multimedia, low-density parity-check codes (LDPCC) and UWB. Prof. Chiani received the ICNEWS award "For Fundamental Contributions to the Theory and Practice of Wireless Communications" in January 2006. He was the recipient of the 2008 IEEE ComSoc Radio Communications Committee Outstanding Service Award. He has chaired, organized sessions, and served on the Technical Program Committees at several IEEE International Conferences. He is the past Chair (2002-2004) of the Radio Communications Committee of the IEEE Communication Society and past Editor of Wireless Communication (2000-2007) for the IEEE TRANSACTIONS ON COMMUNICATIONS. He is a Fellow of the IEEE.