# On the Performance of Moderate-Length Non-Binary LDPC Codes for Space Communications 

Laura Costantini*, Balazs Matuz ${ }^{\dagger}$, Gianluigi Liva ${ }^{\dagger}$, Enrico Paolini* and Marco Chiani*<br>*DEIS/WiLAB, University of Bologna, via Venezia 52, 47521 Cesena (FC), Italy<br>${ }^{\dagger}$ Institute of Communications and Navigation, German Aerospace Center (DLR), Oberpfaffenhofen, 82234 Wessling, Germany Email: laura.costantini4@studio.unibo.it, \{e.paolini, marco.chiani\}@unibo.it, \{Balazs.Matuz,Gianluigi.Liva\}@dlr.de


#### Abstract

In this paper, an overview of recent achievements in the design and decoding of non-binary low-density paritycheck (LDPC) codes is provided. Non-binary constructions based on ultra-sparse matrices are compared with binary low-density parity-check codes and turbo codes from satellite communication standards, to show that larger coding gains (outperforming the binary competitors by at least $0.3 \mathbf{d B}$ ) can be achieved on the AWGN channel, especially in the moderate/short block regimes. Thanks to this excellent performance, non-binary LDPC codes represent an appealing solution for space communications.

Index Terms-Belief propagation, non-binary LDPC codes, space communications, satellite communications.


## I. Introduction

Thanks 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 [2]-[5]. Their application ranges from deep-space communications [2], [3] to satellite broadcasting services [4] and up-link for interactive satellite systems [5].

In the past decade, LDPC code constructions were proposed approaching the Shannon limit within few tens of dB for large block lengths $(n>10000)$ [6], [7]. In the moderate block size regime ( $1000<n<10000$ ), structured constructions with low error floors were proposed, for example, in [8]-[12]. These constructions achieve low codeword error rates, e.g. $\sim 10^{-6}$, within $0.5 \div 1 \mathrm{~dB}$ from the random coding bound (RCB) ${ }^{1}$ [14].

To enhance the code performance for short/moderate block sizes, LDPC codes over non-binary Galois fields (GFs) were proposed in [15]. The performance gain, however, has the drawback of an increased decoding complexity. As for binary LDPC codes, decoding is based belief propagation (BP), that is on message passing (MP) along the edges of the Tanner graph. The decoding complexity is dominated by the check node ( CN ) operations and scales with $\mathcal{O}\left(q^{2}\right)$, where $q$ is the order of the GF. However, the probability-domain decoding algorithm can be simplified by using fast Fourier transforms

[^0](FFTs) to perform the CN elaborations, reducing the complexity to $\mathcal{O}\left(q \log _{2}(q)\right)$ [16]. Further complexity reductions for non-binary LDPC decoders were achieved in [17], while a construction technique for ultra-sparse non-binary LDPC codes (i.e., LDPC codes with regular variable and check node degrees $\left(d_{v}=2, d_{c}\right)$ ) was proposed in [18], which is based on the binary image of the parity-check equations for the selection of the equation coefficients. The method in [18] is effective in reducing the error floor of ultra-sparse non-binary LDPC codes, even if for these LDPC code ensembles the minimum distance grows sub-linearly with $n$.

Non-binary LDPC codes possess a large potential for space/satellite communications systems. In particular, their applicability seems to be tailored to:

- Deep-space communications down-links. Here, the typical data-rates are still moderate [2], reducing the impact of a higher decoding complexity. Moreover, the decoder is located in the ground station.
- Up-link in interactive satellite communications. In this context short or moderate-size packets have to be sent by fixed/mobile terminals to a gateway through a satellite link. The terminals may have power constraints (due to either regulatory issues / cost of amplifiers) and hence large coding gains are essential for achieving reasonable bandwidth efficiencies. The data rates are moderate, and the decoder is located in the gateway.
In this paper, we provide an overview of recent achievements in the design/decoding of non-binary LDPC codes. We also provide numerical evidence on the gain of non-binary LDPC codes over both well-established and recently-proposed binary LDPC counterparts. The work is organized as follows. Reduced-complexity decoding for non-binary LDPC codes is illustrated in Section II. Insights on the code design are given in Section III, before presenting simulation results in Section IV. Section V concludes the paper.


## II. Belief Propagation Decoding of Non-Binary LDPC Codes

In this paper we always refer to GFs of order $q=2^{p}, p>1$. The parity-check matrix of a $(n, k)$ LDPC code on $\mathrm{GF}\left(2^{p}\right)$ possesses $N=n / p$ columns, $M=(n-k) / p$ rows and
each entry takes a value in $\operatorname{GF}\left(2^{p}\right)$. The corresponding Tanner graph is composed of a set $\left\{V_{i}\right\}_{i=0, \ldots, N-1}$ of $N$ variable nodes (VNs) and a set $\left\{C_{j}\right\}_{j=0, \ldots, M-1}$ of $M$ CNs. A variable node $V_{i}$ is connected by an edge to the check node $C_{j}$ iff $h_{j, i} \neq 0$, i.e. if the corresponding element of $\mathbf{H}$ is non-zero.

Probability-domain BP decoding of non-binary LDPC codes on the additive white Gaussian noise (AWGN) channel was investigated in [15]. Due to a complexity scaling with $\mathcal{O}\left(q^{2}\right)$, 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], [19], [20], leading to a complexity scaling with $\mathcal{O}\left(q \log _{2}(q)\right)$. A log-domain implementation of the algorithm was proposed in [21].

Next, the probability-domain BP decoding algorithm is reviewed. Apart from the initialization step, the decoding steps are repeated until a valid codeword is found or a maximum number of iterations $\left(I_{\max }\right)$ is reached. 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.

## A. Initialization

The first message $\mathbf{v}_{i, j}^{\text {out }}$ from the $\mathrm{VN} V_{i}$ to the $\mathrm{CN} C_{j}$ coincides with $\mathbf{m}_{i}$, a vector of the $q$ symbol probabilities given the observation from the channel. Assuming AWGN channel and BPSK modulation, a codeword symbol $c_{i} \in \mathrm{GF}(q)$ is represented by a binary sequence $\mathbf{c}_{i}=\left(c_{i, 0}, c_{i, 1}, \ldots, c_{i, p-1}\right)$ of $p$ bits. Each bit is mapped according to an antipodal modulation, i.e. $\mathbf{x}_{i}=1-2 \mathbf{c}_{i}$, of which a noisy version $\mathbf{y}_{i}=\mathbf{x}_{i}+\mathbf{n}_{i}$ is received. Here, $\mathbf{n}_{i}$ is a vector of $p$ independent and identically-distributed (i.i.d.) zero-mean Gaussian noise samples, each with variance $\sigma^{2}=\left(2 R \cdot E_{b} / N_{0}\right)^{-1}$, where $E_{b}$ is the energy per bit (associated with an information symbol), $N_{0}$ is the one-sided noise power spectral density and $R=k / n$ is the code rate. The $w$ th element of $\mathbf{m}_{i}, w \in\{0, \ldots, q-1\}$, is the probability of $c_{i}$ being equal to the $w$ th $\operatorname{symbol}$ in $\operatorname{GF}(q)$, $a_{w}$, given the received vector $\mathbf{y}_{i}$. It may be expressed as

$$
\begin{equation*}
m_{i, w}=\operatorname{Pr}\left(c_{i}=a_{w} \mid \mathbf{y}_{i}\right)=\prod_{l=0}^{p-1} \operatorname{Pr}\left(c_{w, l}=a_{w, l} \mid y_{i, l}\right) \tag{1}
\end{equation*}
$$

where $c_{w, l}$ is the $l$ th bit of the binary representation $\mathbf{c}_{i}$ of $c_{i}$ and $a_{w, l}$ is the $l$ th bit of the binary representation $\mathbf{a}_{w}$ of $a_{w}$. Under the assumption that all symbols in $\mathrm{GF}(q)$ are equiprobable, $m_{i, w}$ may be expressed as

$$
\begin{equation*}
m_{i, w}=\frac{\exp \left(-\frac{\left|\mathbf{y}_{i}-\tilde{\mathbf{x}}_{w}\right|^{2}}{2 \sigma^{2}}\right)}{\sum_{w=0}^{q-1} \exp \left(-\frac{\left|\mathbf{y}_{i}-\tilde{\mathbf{x}}_{w}\right|^{2}}{2 \sigma^{2}}\right)} \tag{2}
\end{equation*}
$$

where $\tilde{\mathbf{x}}_{w}=1-2 \mathbf{a}_{w}$.

## B. Permutation of Outgoing VN Messages

The entries $h_{j, i}$ of the parity-check matrix are elements of $\mathrm{GF}(q)$. The $j$ th parity check equation can be described as

$$
\begin{equation*}
\sum_{i=0}^{N-1} h_{j, i} c_{i}=0 \tag{3}
\end{equation*}
$$

The multiplication of $c_{i}$ with $h_{j, i}$ in (3) entails a permutation of the entries of $\mathbf{v}_{i, j}^{\text {out }}$. For sake of clarification, let's take a non-zero entry $h_{j, i}$ and define $z_{i}=h_{j, i} c_{i}$. For the symbol probabilities we obtain $\operatorname{Pr}\left(z_{i}=a_{w}\right)=\operatorname{Pr}\left(c_{i}=h_{j, i}^{-1} a_{w}\right)$, where $h_{j, i}^{-1}$ is the multiplicative inverse of $h_{j, i}$. This means that the corresponding probabilities have to be mapped accordingly. Following that, the permuted message form $\mathrm{VN}(i)$ to $\mathrm{CN}(j)$ is given by

$$
\begin{equation*}
\mathbf{v}_{i, j}^{\Pi}=\mathbf{v}_{i, j}^{\text {out }} \cdot \boldsymbol{\Pi}_{j, i}, \tag{4}
\end{equation*}
$$

where $\boldsymbol{\Pi}_{j, i}$ is a $q \times q$ permutation matrix associated with $h_{j, i}$.

## C. CN Message Processing

Modeling each $z_{i}=h_{j, i} c_{i} \in \mathrm{GF}(q)$ as a discrete random variable (RV) and under independence assumption, the lefthand side in (3) is a RV whose PMF is given by the convolution in $\mathrm{GF}(q)$ 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 $\mathrm{VN} V_{i}$ as $\mathbf{u}_{j, i}^{\text {out }}$. We then obtain

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

where $\circledast$ denotes the convolution of the PMFs. By applying the Hadamard transform (HT), $\mathcal{H}\{\cdot\}$, the discrete convolution turns into an element-wise multiplication. This yields to

$$
\begin{equation*}
\mathcal{H}\left\{\mathbf{u}_{j, i}^{\text {out }}\right\}=\prod_{l \in \mathcal{I}_{j} \backslash\{i\}} \mathcal{H}\left\{\mathbf{v}_{l, j}^{\Pi}\right\} . \tag{5}
\end{equation*}
$$

The right-hand side of (5) can be efficiently implemented via the fast Hadamard transform (FHT) as a recursive application of sums and differences. This allows lowering the complexity of the CN elaboration to $\mathcal{O}\left(q \log _{2}(q)\right)$. Moreover, since the Hadamard transform coincides with its inverse, we have

$$
\mathbf{u}_{j, i}^{\text {out }}=\mathcal{H}\left\{\prod_{l \in \mathcal{I}_{j} \backslash\{i\}} \mathcal{H}\left\{\mathbf{v}_{l, j}^{\Pi}\right\}\right\}
$$

## D. De-permutation of outgoing $C N$ messages

The output message $\mathbf{u}_{j, i}^{\text {out }}$ has to be de-permuted, before it can be passed to the VN $V_{i}$. In a similar way as (4) the depermutation may be written as

$$
\mathbf{u}_{j, i}^{\Pi}=\mathbf{u}_{j, i}^{\text {out }} \cdot \boldsymbol{\Pi}_{j, i}^{-1}
$$

Here, $\boldsymbol{\Pi}_{j, i}^{-1}$ is a $(q \times q)$ permutation matrix related to $h_{j, i}^{-1}$.

## E. VN Messages Processing

The generic VN $V_{i}$ computes the outgoing message towards its neighboring $\mathrm{CN} C_{j}$ by multiplying (element-wise) $\mathbf{m}_{i}$ by the product of all incoming messages (each of which consists of a PMF) but the message from $C_{j}$. For a VN $V_{i}$, let us denote as $\mathcal{J}_{i}$ the set of its neighboring CNs. Then, the message from VN $V_{i}$ to $\mathrm{CN} C_{j}$ is given by

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

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

## F. Hard Decision and Stopping Criterion Step

The algorithm stops when a given maximum number $I_{\max }$ of iterations is reached or if a codeword is found at the end of any iteration. At the end of each iteration, the a posteriori probabilies of symbol $c_{i}$ are obtained by multiplying elementwise all messages incoming towards the $\mathrm{VN} V_{i}$, including $\mathbf{m}_{i}$ :

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

The message $\mathbf{v}_{i}$ is a vector of $q$ elements (one for each possible value of $c_{i}$ ) and provides an estimation of the a posteriori probabilities $\operatorname{Pr}\left(c_{i}=a_{w} \mid \mathbf{y}\right)$, where $\mathbf{y}=\left(\mathbf{y}_{1}, \mathbf{y}_{2}, \ldots, \mathbf{y}_{N}\right)$ is the vector of all received soft values from the channel. The decision on $c_{i}$ is given by $\hat{c}_{i}=a_{\hat{w}}$ with $\hat{w}=\arg \max _{w} v_{i, w}$, where $v_{i, w}$ is the $w$ th element of $\mathbf{v}_{i}$.

## III. Non-Binary LDPC Code Designs

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

1) Definition of the degree distribution pair to be used for the parity-check matrix construction.
2) Construction of a parity-check matrix $\mathbf{H}$ whose Tanner graph possesses a large girth.
3) Choice of the values of the non-zero entries of $\mathbf{H}$.

The first step is rather unexplored in the non-binary LDPC context. It is however established that regular distributions with variable node degree $d_{v}=2$ provide an excellent iterative decoding thresholds on the AWGN channel, especially for sufficiently large field orders. As an example, the (2,4)-regular ensemble over $\operatorname{GF}(256)$ exhibits a threshold at $E_{b} / N_{0} \simeq 0.45 \mathrm{~dB}$, only 0.27 dB away from the Shannon limit for rate- $1 / 2$ codes on the binary input AWGN channel. This justifies the increasing attention recently gained by the design of non-binary LDPC codes with ultra-sparse paritycheck matrices [18].

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 (PEG) algorithm [22] can be adopted for the matrix construction.

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 an acceptable performance in most cases, especially for large Galois field 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 [18]. This has to be related to the fact that their minimum distance grows sub-linearly with $n$ [1].

An efficient approach for selecting the non-zero entries is proposed in [18]. 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 $\operatorname{GF}\left(2^{p}\right)$ is equivalent to $p$ binary equations involving $p d_{c}$ bits, and hence can be regarded as $\left(p d_{c}, p\left(d_{c}-1\right)\right)$ 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 equations coefficients, one can assure that the corresponding binary linear block code representation possesses a minimum distance larger than 2 . If all the $M$ nonbinary 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.

In [23] an approach for the design of low-rate non-binary LDPC codes based on protographs [24], [25] is presented. In particular, it is shown how an arbitrary low-rate non-binary LDPC code can be obtained from an 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 Galois field 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 block sizes.

Next, we will show the performance of some non-binary LDPC codes constructed by means of some of the techniques mentioned above. We will focus on ultra-sparse matrices with $d_{v}=2$. The matrices have been constructed using a circulantversion of the PEG algorithm, starting from a small base matrix (protograph) and performing protograph expansions by means of circulant permutation matrices in either 2 or 3 stages. The resulting parity-check matrices are in block circulant form. This feature allows a compact description of the matrix structure, facilitating the decoder implementations. The choice of the non-zero coefficients has been performed according to the criteria of [18]. For low-rate codes ( $R<1 / 2$ ), the repetition-code-based approach of [23] has been adopted. The protographs used for the code design, together with extensions for achieving low-rates, are depicted in Fig. 1.


Fig. 1. Protographs used for the code design. a) Rate- $1 / 2$ regular protograph. b) Rate $1 / 3$ regular protograph. c) Low-rate protographs obtained by multiplicative repetition of variable nodes [23]. A rate $1 / 4$ protograph is obtained by adding to the rate- $1 / 3$ protograph the VN type A . The rate can be lowered to $1 / 6$ by further adding VNs of type B and C . A rate $1 / 9$ protograph if finally given by adding the VNs of type D,E and F.

## IV. Numerical Results

The results presented in this section have been obtained by Monte Carlo simulation on the AWGN channel with $I_{\max }=200$ iterations. All simulated non-binary LDPC codes have been constructed on $\operatorname{GF}(256)$. We provide a comparison with binary codes and with the RCB, for the same $(n, k)$ parameters (in bits). We evaluated the codeword error rate (CER) vs. $E_{b} / N_{0}$ for non-binary protograph-based codes and for binary irregular repeat accumulate (IRA) codes with constant information node degree 4 . This choice for IRA codes is dictated by the need to trade-off the error floor and the waterfall performance [8]. The RCB is provided as well.

Fig. 2 and Fig. 3 show the results for $R=1 / 2$ codes with information lengths $k=256$ and $k=1024$, respectively. At CER $=10^{-5}$, the gap between the RCB and the LDPC codes over $\mathrm{GF}(256)$ is less than 0.3 dB in both cases. By contrary the IRA code shows a gap of 0.9 dB for $k=1024$ and around 1.3 dB for $k=256$.

Fig. 4 and Fig. 5 show the CER vs. $E_{b} / N_{0}$ for $R=1 / 3$ codes with $k=256$ and $k=1024$, respectively. The codes under investigation are non-binary LDPC codes and (again) IRA codes with information node degree 4 . Similarly to $R=$ $1 / 2$ codes above, also for lower code rates the gap to the RCB at $\mathrm{CER}=10^{-5}$ is less than 0.3 dB for the non-binary codes, whereas for the IRA codes its always greater than 1 dB .

Next, a comparison between non-binary LDPC codes and state-of-the-art turbo codes (TCs) (specifically, TCs from the DVB-RCS standard [26] and 3D-TCs [27]) is illustrated for $R=1 / 2$ and $R=1 / 4$. In this latter low-rate case, TCs usually express excellent performance. Due to construction constraints, we have $k=456$ for the TCs (and for the RCB), while $k=448$ for the LDPC codes (this is reflected in a slightly shorter block length for $n$ for the non-binary LDPC codes). From Fig. 6 it can be seen that the non-binary LDPC codes ouperform TCs at both code rates. At CER $=10^{-5}$, the 3D-TCs have a performance loss with respect to their LDPC competitors of about $0.3 \div 0.4 \mathrm{~dB}$.

## V. Conclusions

In this paper, we provided an overview of recent achievements in the design and in the decoding of non-binary LDPC codes. We compared non-binary constructions based on ultrasparse matrices with binary LDPC and turbo codes, showing how remarkable coding gains can be achieved on the AWGN channel, especially 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.

## Acknowledgment

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


Fig. 2. CER of GF(256) LDPC code, binary IRA code and RCB over $E_{b} / N_{0}$ with $R=1 / 2, k=256$.


Fig. 3. CER of GF(256) LDPC code, binary IRA code and RCB over $E_{b} / N_{0}$ with $R=1 / 2, k=1024$.

## REFERENCES

[1] R. Gallager, Low-Density Parity-Check Codes. Cambridge, MA: M.I.T. Press, 1963.
[2] G. P. Calzolari, M. Chiani, F. Chiaraluce, R. Garello, and E. Paolini, "Channel coding for future space missions: New requirements and trends," Proc. IEEE, vol. 95, no. 11, pp. 2157-2170, Nov. 2007.
[3] K. Andrews, D. Divsalar, S. Dolinar, J. Hamkins, C. Jones, and F. Pollara, "The development of turbo and LDPC codes for deep-space applications,"" Proc. IEEE, vol. 95, no. 11, pp. 2142-2156, Nov. 2007.
[4] "Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications," ETSI, 2004.
[5] G. Liva, M. Papaleo, C. Niebla, S. Scalise, S. Cioni, A. Vanelli-Coralli, G. E. Corazza, P. Kim, and H. J. Lee, "The very short frame of mobile DVB-RCS: Code design and QoS performance," Int. J. of Satellite Communications and Networking, vol. 28, no. 3-4, pp. 209-231, 2010.


Fig. 4. CER of GF(256) LDPC code, binary IRA code and RCB over $E_{b} / N_{0}$ with $R=1 / 3, k=256$.


Fig. 5. CER of GF(256) LDPC code, binary IRA code and RCB over $E_{b} / N_{0}$ with $R=1 / 3, k=1024$.
[6] T. Richardson, M. Shokrollahi, and R. Urbanke, "Design of capacityapproaching irregular low-density parity-check codes," IEEE Trans. Inf. Theory, vol. 47, no. 2, pp. 619-637, Feb. 2001.
[7] M. Luby, M. Mitzenmacher, M. A. Shokrollahi, and D. A. Spielman, "Improved low-density parity-check codes using irregular graphs," IEEE Trans. Inf. Theory, vol. 47, no. 2, pp. 585-598, Feb. 2001.
[8] M. Yang, Y. Li, and W. Ryan, "Design of efficiently encodable moderatelength high-rate irregular LDPC codes," IEEE Trans. Commun., vol. 52, no. 4, pp. 564-571, Apr. 2004.
[9] Y. Zhang and W. E. Ryan, "Structured IRA codes: Performance analysis and construction," IEEE Trans. Commun., vol. 55, no. 5, pp. 837-844, May 2007.
[10] A. Abbasfar, K. Yao, and D. Disvalar, "Accumulate repeat accumulate codes," in Proc. IEEE Globecomm, Dallas, Texas, Nov. 2004.
[11] 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.


Fig. 6. CER of GF (256) LDPC code, 3D-TC, DVB-RCS code and RCB over $E_{b} / N_{0}$ with $R=1 / 2$ and $R=1 / 4$. Information length $k=448$ for the LDPC code and $k=456$ for 3D-TC, DVB-RCS code and RCB.
[12] W. E. Ryan and S. Lin, Channel Codes - Classical and Modern. Cambridge University Press, 2009.
[13] S. Dolinar, D. Divsalar, and F. Pollara, "Code performance as a function of block size," JPL INP, Tech. Rep., Mar. 1998, TMO PR 42-133.
[14] R. G. Gallager, Information Theory and Reliable Communication. New York: Wiley, 1968.
[15] M. Davey and D. MacKay, "Low density parity check codes over GF (q)," IEEE Commun. Lett., vol. 2, no. 6, pp. 70-71, Jun. 1998.
[16] L. Barnault and D. Declercq, "Fast decoding algorithm for LDPC over GF $\left(2^{q}\right)$," in Proc. of 2003 IEEE Inf. Theory Workshop, Mar./Apr. 2003, pp. 70-73.
[17] A. Voicila, D. Declercq, F. Verdier, M. Fossorier, and P. Urard, "Low complexity decoding for non-binary LDPC codes in high order fields," IEEE Trans. Commun., vol. 58, no. 5, pp. 1365-1375, May 2010.
[18] C. Poulliat, M. Fossorier, and D. Declercq, "Design of regular $\left(2, d_{c}\right)$ LDPC codes over GF $(q)$ using their binary images," IEEE Trans. Commun., vol. 56, no. 10, pp. 1626-1635, Oct. 2008.
[19] D. MacKay and M. Davey, "Evaluation of Gallager codes for short block length and high rate applications," in In Codes, Systems and Graphical Models. Springer-Verlag, 1999, pp. 113-130.
[20] D. Declercq and M. Fossorier, "Decoding algorithms for non-binary ldpc codes over GF," IEEE Trans. Commun., vol. 55, no. 4, pp. 633-643, Apr. 2007.
[21] H. Song and J. Cruz, "Reduced-complexity decoding of $q$-ary LDPC codes for magnetic recording," IEEE Trans. Magn., vol. 39, no. 2, pp. 1081-1087, Mar. 2003.
[22] X.-Y. Hu, E. Eleftheriou, and D. Arnold, "Regular and irregular progressive edge-growth Tanner graphs," IEEE Trans. Inf. Theory, vol. 51, no. 1, pp. 386-398, Jan. 2005.
[23] K. Kasai, D. Declercq, C. Poulliat, and K. Sakaniwa, "Rate-Compatible Non-Binary LDPC Codes Concatenated with Multiplicative Repetition Codes," in Proc. IEEE International Symposium on Information Theory, Austin, Texas, USA, Jun. 2010.
[24] J. Thorpe, "Low-density parity-check (LDPC) codes constructed from protographs," JPL INP, Tech. Rep., Aug. 2003, 42-154.
[25] G. Liva, S. Song, L. Lan, Y. Zhang, W. Ryan, and S. Lin, "Design of LDPC codes: A survey and new results," J. Commun. Softw. Syst., vol. 2, no. 3, pp. 191-211, Sep. 2006, invited paper.
[26] "Interaction channel for satellite distribution systems," ETSI EN 301 790 v1.5.1, DVB, 2009.
[27] C. Berrou, A. Graell i Amat, Y. Ould Cheikh Mouhamedou, and Y. Saouter, "Improving the distance properties of turbo codes using a third component code: 3D turbo codes," IEEE Trans. Commun., vol. 57, no. 9 , pp. 2505-2509, Sep. 2009.


[^0]:    ${ }^{1}$ In the moderate-block size regime we compare the code performance with the RCB, rather than the Shannon limit, to take into account the block size. Although the RCB is an upper bound on the performance achievable by a $(n, k)$ linear block code, for input block sizes $k>200$ bits it is a valid benchmark [13].

