# Simple Reconfigurable Low-Density Parity-Check Codes

Gianluigi Liva, Student Member, IEEE, Enrico Paolini, Student Member, IEEE, and Marco Chiani, Senior Member, IEEE

Abstract—Low-Density Parity-Check codes (LDPCC) have been recently investigated as a possible solution for high data rate applications, for both space and terrestrial wireless communications. A main issue is the research of low complexity encoding and decoding schemes. In this letter we present a class of reconfigurable LDPCC characterized by low encoding and decoding complexity: we call them Generalized Irregular Repeat-Accumulate (GeIRA) Codes.

Index Terms—LDPC codes, channel coding, satellite communications.

#### I. Introduction

RECENTLY, Low-Density Parity-Check Codes (LDPCC) [1] have been considered as a possible solution for near Shannon limit channel coding. For instance, their use is under investigation in both Near-Earth and Deep-Space missions requiring high data-rates and spectral efficiency. Satellite telecommunication systems have always traded complexity on the ground station for simplicity on-board. Therefore, a main issue is the design of low-complexity encoding schemes. Another issue to be taken into account in designing channel codes for such applications is the error floor [2].

Three main solutions can be found in literature for an efficient encoding of LDPCC: the algorithm proposed in [3], the finite-geometries based construction of [4], and the class of efficiently encodable LDPCC (eIRA) [5] related also to the concept of of Irregular Repeat-Accumulate (IRA) codes [6].

In this letter, we present a class of IRA-like LDPC codes with the same low encoding complexity as eIRA, that present some further interesting properties: first, respect to codes in [5], our solution (*Generalized Irregular Repeat-Accumulate Codes, GeIRA Codes*) gives a higher flexibility in the choice of the degree distributions (allowing for example the design of near-regular codes). More important, GeIRA show better performance in the high Signal-to-Noise Ratio (SNR) region. Moreover, the behavior of the code can be modified "on the fly" by a simple reconfiguration procedure.

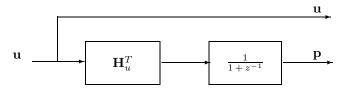
## II. EFFICIENT ENCODING OF LDPCC

The algorithm proposed in [3] is a general encoding procedure applicable in principle to any LDPCC; it consists in a

Manuscript received June 29, 2004. The associate editor coordinating the review of this letter and approving it for publication was Marc Fossorier. This work has been supported in part by ESA/ESOC.

The authors are with CNIT, DEIS, University of Bologna, Italy (e-mail: {gliva, epaolini, mchiani}@deis.unibo.it).

Digital Object Identifier 10.1109/LCOMM.2005.xxxxxx.



1

Fig. 1. Encoder structure for eIRA codes [5].

"reordering" of the parity check matrix  ${\bf H}$  through permutations of rows and columns, to transform  ${\bf H}$  in an approximate-triangular matrix. A parameter g (gap) is then defined that represents the "distance" of  ${\bf H}$  to an exact triangular form. The overall encoding complexity, in terms of number of multiplications, is  $O(n+g^2)$ , where n is the codeword length. Nevertheless, if g is a small fraction of n, the complexity of the encoding procedure can be maintained almost linear. However, only LDPCC characterized by small gap are suitable for this procedure, and this is not often the case.

LDPC Codes based on Finite Geometries [4] are cyclic or quasi-cyclic (by construction). Therefore they can be encoded through low-complexity circuits based on feedback shift registers. The main advantages of such codes are the above-mentioned reduced encoding complexity and good properties in terms of minimum distance. On the other hand, these codes exist only for precise values of parameters n and k, where k is the information block length.

Irregular Repeat-Accumulate (IRA) codes [6] are a particular class of serially concatenated turbo codes with an inner differential encoder and an outer repetition code. IRA codes can be encoded with the complexity O(n) proper of turbo codes and they can be decoded with LDPCC message passing algorithms. Extended IRA (eIRA) codes [5] extend the structure of IRA codes to high rate systematic LDPCC. The parity check matrix is partitioned as

$$\mathbf{H} = [\mathbf{H}_u | \mathbf{H}_p] , \qquad (1)$$

where  $\mathbf{H}_u$  is a  $(m \times k)$  matrix, while  $\mathbf{H}_p$  is a square  $(m \times m)$  matrix with m-1 columns of weight 2 and a weight 1 column. The resulting (systematic) encoder is depicted in Fig. 1 [5].

Therefore, for eIRA codes the variable nodes degree distribution is somewhat constrained since the number of weight-2 columns must be at least m-1.

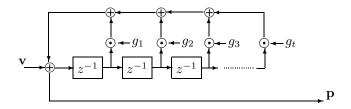


Fig. 2. Structure of rate-1 encoder.

#### III. THE PROPOSED NEW CODE STRUCTURE

In this section we describe our proposal (GeIRA) for extending the idea in [5]. We start the description of GeIRA codes from the (systematic) encoding algorithm. It can be summarized as follows:

- 1) Multiply the information vector  $\mathbf{u}$  for a  $(k \times m)$  Low-Density Generator Matrix  $\mathbf{H}_u^T$  (resulting in a m-bits vector  $\mathbf{v}$ ).
- 2) Input the *m*-bits vector **v** to a rate-1 encoder characterized by a transfer function

$$F(z) = \frac{1}{1 + \sum_{j=1}^{t} g_j z^{-j}}, \ 1 \le t \le m - 1, \quad (2)$$

with  $g_j \in GF(2)$  and define the m output bits of the rate-1 encoder to be the parity vector  $\mathbf{p}$ .

3) Pose the encoded codeword  $\mathbf{x} = [\mathbf{u} \mid \mathbf{p}].$ 

We denote by  $\{x_j\}$  a sequence of bits and with  $x_j$  the  $j^{\text{th}}$  element of the sequence. The rate-1 encoder can be realized through a recursive digital filter with the structure shown in Fig. 2. Its input/output relation in the discrete time domain is described by the difference equation  $p_i = v_i + \sum_{j=1}^{t} q_j v_{i-j}$ .

described by the difference equation  $p_i = v_i + \sum_{j=1}^t g_j p_{i-j}$ . Denoting the generic codeword as  $\mathbf{x} = [\mathbf{u} \mid \mathbf{p}]$ , the parity-check matrix of the code can be partitioned as in (1), with suitable  $\mathbf{H}_u$  and  $\mathbf{H}_p$ . Imposing the condition  $\mathbf{x} \mathbf{H}^T = \mathbf{0}$ , it immediately follows  $\mathbf{p} = \mathbf{u} \mathbf{H}_u^T \mathbf{H}_p^{-T}$ . Thus,  $\mathbf{H}_p^{-T}$  is the binary transformation matrix corresponding to the recursive digital filter with transfer function (2); its  $r^{\text{th}}$  row  $(r = 0, \dots, m-1)$  is then given by  $[0 \dots 0 \ f_0 \ f_1 \ \dots \ f_{m-1-r}]$ , where the number of 0s preceding  $f_0$  is r and  $\{f_q\}$  is the discrete impulse response of the digital filter. The following theorem gives the structure of sub-matrix  $\mathbf{H}_{\mathbf{p}}$ .

Theorem 1: Submatrix  $\mathbf{H}_p$  has the following structure (blanks represent zeros):

$$\mathbf{H_{p}} = \begin{bmatrix} 1 \\ g_{1} & 1 \\ g_{2} & g_{1} & \ddots \\ \vdots & g_{2} & \ddots & \ddots \\ g_{t} & \vdots & \ddots & \ddots & \ddots \\ g_{t} & \ddots & \ddots & \ddots & \ddots \\ & g_{t} & \ddots & \ddots & \ddots & \ddots \\ & & g_{t} & \dots & g_{2} & g_{1} & 1 \\ & & & g_{t} & \dots & g_{2} & g_{1} & 1 \end{bmatrix} . \tag{3}$$

*Proof:* It is sufficient to prove that the product  ${\bf A}$  between  ${\bf H}_p^{-T}$  and the transpose of the matrix given in (3) is the order-

m identity matrix  $I_m$ . Define the  $j^{th}$  element of  $\{x_i\}$  as:

$$x_j = \begin{cases} 1 & \text{if} \quad j = 0\\ g_j & \text{if} \quad 1 \le j \le t\\ 0 & \text{elsewhere} \end{cases}$$
 (4)

The  $j^{\text{th}}$  element of the  $r^{\text{th}}$  row of matrix  $\mathbf{A}$ ,  $A_{r,j}$ , can be written as

$$A_{r,j} = \sum_{l=-\infty}^{\infty} f_{l-r} x_{j-l} . {5}$$

By introducing the sequence  $\{\alpha_i^r\}$ , defined as

$$\alpha_j^r = \begin{cases} A_{r,j} & \text{if } 0 \le j \le m - 1\\ 0 & \text{otherwise} \end{cases}$$
 (6)

equation (5) can be also written as  $\{\alpha_j^r\} = \{f_{j-r}\} * \{x_j\}$ . By applying the z-transform to both terms it follows  $\alpha^r(z) = F(z)z^{-r} \ (1+\sum_{j=1}^t g_jz^{-j}) = z^{-r}$ , from which  $\alpha_j^r = \delta_{r-j}$ . Therefore, the (j,r) element of  $\mathbf A$  is a 1 if and only if j=r, 0 otherwise.

It is known that a condition to obtain good performance when using a Belief Propagation (BP) decoder, is that the bipartite graph [7] of the code must contain no short cycles (or at least a small number of short cycles). Recall that the length of a cycle is defined as its total number of edges. If F(z) is properly chosen, length 4 cycles involving columns of  $\mathbf{H}_p$  only can be avoided. In the following, we give a necessary and sufficient condition for that. Define  $g(z^{-1}) = \sum_{i=0}^t g_i z^{-i}$  ( $g_i \in \{0,1\}$  and  $g_0 = 1$ ), and denote with  $\Omega$  the ensemble of indexes of non-zero coefficients of  $g(z^{-1})$ . It is simple to prove that there are no length 4 cycles only involving columns of  $\mathbf{H}_p$ , if and only if for every choice of indexes  $i,j,\eta,\xi\in\Omega$  and  $i\neq j,\eta\neq i,\xi\neq j$  the following condition holds

$$i - j \neq \eta - \xi. \tag{7}$$

Once the rate-1 encoder has been chosen, the parity-check matrix can be then completed by constructing the systematic sub-matrix  $\mathbf{H}_u$ , according to a given degree distribution, possibly avoiding short cycles (also taking into account the 1s already present in  $\mathbf{H}_p$ ).

## IV. RECONFIGURABLE ENCODING AND DECODING

LDPC codes described in previous section are highly reconfigurable. On encoding side, the reconfigurability is guaranteed by the possibility of modifying the binary coefficients of polynomial  $g(z^{-1})$  with the exception of  $g_0$ . This implies the possibility of varying the weight distributions of both rows and columns in the parity-check matrix, according to the choice of  $g(z^{-1})$ . On decoding side, it must be first observed that each non zero coefficient in polynomial  $g(z^{-1})$  implies the presence of a certain number of edges in the bipartite graph associated to the parity-check matrix H, connecting some parity variable nodes and check nodes. In order to obtain a reconfigurable decoder, one possibility is to prearrange connections between variable and check nodes according to the case of  $g_i = 1$ , i = $1 \dots t$ , and then to force the messages received by variable and check nodes along inactive edges (i.e. edges associated to the forced to zero coefficients of  $g(z^{-1})$  to values that give no contribution to the decoding process. Although this

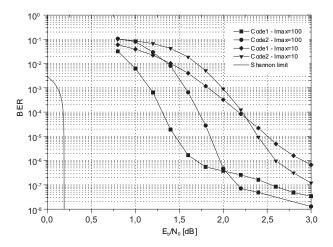


Fig. 3. Performance comparison between codes  $C_1$  and  $C_2$ .

solution for the decoder is in principle applicable to any set of codes (with the same number of variable and check nodes), in the case of GeIRA this does not imply an excessive increase of complexity, since only edges associated to coefficients of  $g(z^{-1})$  are involved in the procedure.

## V. NUMERICAL RESULTS

In this section we present some numerical results in terms of Bit Error Rate (BER) assuming BP decoding of GeIRA codes on the Binary-Input AWGN channel. Here, BER has been computed on information bits only; this has been made possible by the systematic structure of the code. For each value of  $E_b/N_0$  (where  $E_b$  denotes the energy per information bit and  $N_0$  is the one-sided noise power spectral density) simulation has been stopped as soon as achieving 100 wrong frames after decoding. We present the performance of a (4000, 2000) GeIRA code with two different choices of polynomial  $g(z^{-1})$ : in particular, code  $\mathcal{C}_1$  has  $g_1(z^{-1}) = 1 + z^{-1}$ , while code  $\mathcal{C}_2$  has  $g_2(z^{-1}) = 1 + z^{-1} + z^{-4}$ . The edge degree distributions [8] for  $\mathcal{C}_1$  are:

$$\lambda_1(x) = 0.0001 + 0.3077x + 0.2730x^2 + 0.4193x^6$$
  
 $\rho_1(x) = 0.4000x^5 + 0.6000x^6$ ,

and they are optimized for threshold according to density evolution [8]. The analogue edge degree distributions for  $\mathcal{C}_2$  are

$$\lambda_2(x) = 0.0001 + 0.0030x + 0.6330x^2 + 0.3639x^6$$
  
 $\rho_2(x) = 0.0004x^5 + 0.4070x^6 + 0.5926x^7$ .

No length 4 cycles are present in the bipartite graph of both codes. Note that it is possible to switch from one code to the other by simply modifying only one configuration bit in both encoder and decoder. In Fig. 3,  $C_1$  and  $C_2$  are compared setting the maximum number of iterations  $(I_{max})$  to 10 and 100. Consider first the case of  $I_{max} = 100$ . In the low Signal-to-Noise Ratio (SNR) region  $(E_b/N_0 < 2\text{dB})$  the performance of  $C_1$  is better than  $C_2$ , due to optimized distribution for the threshold; at BER =  $10^{-5}$  an additional coding gain of 0.4dB can be obtained by using  $C_1$  instead of  $C_2$ . Note that the gap between code  $C_1$  and the Shannon limit (for a binary input AWGN channel) at BER =  $10^{-4}$  is only

about 1.1 dB. For  $E_b/N_0>2$  dB,  $\mathcal{C}_2$  outperforms  $\mathcal{C}_1$ , due to its lower error floor. This behavior is to be related to the higher minimum distance of  $\mathcal{C}_2$ : codewords of weights 10,11,13,16 were found by BP decoder for code  $\mathcal{C}_1$ , while no undetected errors [2] occurred in the case of  $\mathcal{C}_2$ . This result could appear somewhat disappointing: in fact  $\mathcal{C}_2$ 's error floor gains only a factor of 6 with a sacrifice of 0.4 dB in the waterfall region. Anyway, the construction of code  $\mathcal{C}_2$  is constrained to that of code  $\mathcal{C}_1$ , whose distributions are designed for achieving good performance at the threshold. The above mentioned gain of a factor 6 in the error floor is thus achieved with a slightly modified distribution, preserving the reconfigurability. In this sense, these results can be considered interesting.

From Fig. 3 it can be noted that if  $I_{max}$  is reduced to 10, the BER crossover point is reached at BER  $\simeq 6 \cdot 10^{-5}$ instead of BER  $\simeq 4 \cdot 10^{-7}$ . Hence,  $C_2$  presents a higher decoding convergence speed than  $C_1$ . The reconfigurable decoding scheme made up of  $(C_1, C_2)$  could be interesting in scenarios characterized by a time varying channel. In such situation, if a feedback channel is available, for sufficiently high values of SNR  $C_2$  should be preferred. On the other hand, in the presence of a low SNR, it should be preferable to switch to  $C_1$ , exploiting its good behavior in the waterfall region. We found similar results for other values of coderates and codeword lengths, although the advantages of such a reconfigurable scheme seem to be more evident for not too high code-rates. This is probably due to the fact that in the case of high code-rates the edge degree distributions are less sensible to modifications of polynomial  $q(z^{-1})$ .

### VI. CONCLUSIONS

In this letter, we proposed a class of reconfigurable LDPC codes, GeIRA, that can be considered as a generalization of IRA codes, with the same low encoding complexity and further properties which could make them interesting in scenarios characterized by time varying channels. A possible encoding circuit and its implications in terms of parity-check matrix have been presented.

#### REFERENCES

- R. G. Gallager, Low-Density Parity-Check Codes. Cambridge, MA: M.I.T. Press, 1963.
- [2] M. Chiani and A. Ventura, "Design and performance evaluation of some high-rate irregular low-density parity-check codes," in *IEEE GLOBECOM*, 2001, vol. 2, pp. 990-994.
- [3] T. Richardson and R. Urbanke, "Efficient encoding of low-density parity-check codes," *IEEE Trans. Inform. Theory*, vol. 47, pp. 638-656, Feb. 2001.
- [4] Y. Kou, S. Lin, and M. P. C. Fossorier, "Low-density parity-check codes based on finite geometries: a rediscovery and new results," *IEEE Trans. Inform. Theory*, vol. 47, Nov. 2001.
- [5] M. Yang, Y. Li, and W. E. Ryan, "Design of efficiently encodable moderate-length high-rate irregular LDPC codes," *IEEE Trans. Commun.*, vol. 52, pp. 564-571, Apr. 2004.
- [6] H. Jin, A. Khandekar, and R. McEliece, "Irregular repeat-accumulate codes," in *Proc. 2nd Intern. Symp. on Turbo Codes and Related Topics*, Sept. 2000, pp. 1-8.
- [7] R. M. Tanner, "A recursive approach to low complexity codes," *IEEE Trans. Inform. Theory*, vol. 27, pp. 533-547, 1981.
- [8] T. Richardson, M. A. Shokrollahi, and R Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inform. Theory*, vol. 47, pp. 619-637, Feb. 2001.