Generalized IRA Erasure Correcting Codes for Hybrid Iterative/Maximum Likelihood Decoding

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

***Abstract*— The design of low-density parity-check (LDPC) codes under hybrid iterative / maximum likelihood decoding is addressed for the binary erasure channel (BEC). Specifically, we focus on generalized irregular repeat-accumulate (GeIRA) codes, which offer both efficient encoding and design flexibility. We show that properly designed GeIRA codes tightly approach the performance of an ideal maximum distance separable (MDS) code, even for short block sizes. For example, our $(2048, 1024)$ code reaches a codeword error rate of 10^{-5} at channel erasure probability $\epsilon = 0.450$, where an ideal $(2048, 1024)$ MDS code would reach the same error rate at $\epsilon = 0.453$.**

***Index Terms*— LDPC codes, binary erasure channel, maximum likelihood decoding, iterative decoding, packet erasure correcting codes.**

I. Introduction

ITERATIVE (IT) decoding based on belief propagation has been shown to provide very effective error correction capability over a wide range of communication channels when applied to LDPC codes. In the particular case of the BEC, it allows also to asymptotically approach the capacity with arbitrarily small gap for some LDPC ensembles (see e.g. the codes proposed in [1]).

However, the performance of a finite length (n, k) LDPC code under IT decoding may be quite different from the performance of the same code under maximum likelihood (ML) decoding. At high error rates (waterfall region) the IT performance curve usually exhibits a non-negligible performance degradation with respect to that of the same code under ML decoding. Moreover, at low error rates the IT performance curve usually exhibits a higher error floor. Over the BEC this is due to the presence of stopping sets [2] not associated with codeword ambiguity, and thus resolvable by the ML decoder.

The existence of patterns of variable nodes (VNs) representing stopping sets for the IT decoder, but not for the ML decoder, suggests a possible hybrid erasure correction strategy which consists of performing IT decoding and, upon a decoder failure, employing the ML decoder to resolve the residual maximum stopping set. This hybrid iterative/maximum likelihood (HIML) decoder achieves the same performance as ML but with a lower complexity, as some of the unknowns are recovered iteratively. Moreover, reduced-complexity ML decoding for the BEC can be used [3], [4].

In this letter we address the design of LDPC codes for HIML decoding over the BEC. We first propose code design guidelines that allow near-optimum performance and a manageable encoding/decoding complexity. We then adopt GeIRA codes [5] as a simple solution for satisfying such guidelines.

II. Efficient ML Decoding for LDPC Codes

ML decoding of binary linear block codes is known to be in general an NP-hard problem [6]. However, for the BEC it is equivalent to solving the linear equation

$$\mathbf{x}_{\overline{K}}\,\mathbf{H}_{\overline{K}}^{T} = \mathbf{x}_{K}\,\mathbf{H}_{K}^{T},$$

where $\mathbf{x}_{\overline{K}}$ ($\mathbf{x}_K$) denotes the set of erased (correctly received) encoded bits and $\mathbf{H}_{\overline{K}}$ ($\mathbf{H}_K$) the submatrix composed of the corresponding columns of the parity-check matrix $\mathbf{H}$. Then, ML decoding for the BEC can be implemented as a Gaussian elimination (GE) performed on the binary matrix $\mathbf{H}_{\overline{K}}$: its complexity is cubic in the codeword length [7].

Recently, the problem of performing ML decoding of LDPC codes in a more efficient way than with a full GE has been considered [3]. There, the sparseness of the parity-check matrix is exploited to put $\mathbf{H}_{\overline{K}}$ into an approximate triangular form through row/column permutations only (this technique is reminiscent of the triangulation procedure proposed in [8]). The encoded bits corresponding to the columns of $\mathbf{H}_{\overline{K}}$ which cannot be put into triangular form are named *reference bits*. In order to resolve the whole set of unknowns $\mathbf{x}_{\overline{K}}$, it is sufficient to apply GE to these columns only: provided that GE is successful, the remaining unknown bits are recovered by low-complexity back-substitution. While the overall complexity remains cubic in the codeword length, this algorithm is efficient as long as the number of reference bits is kept small.

III. The Design of LDPC Codes for HIML Decoding

A. Design guidelines

The design of LDPC codes for HIML decoding requires consideration of severe constraints and complexity issues. The aim is to generate codes with a manageable encoding/decoding complexity and exhibiting a near-optimum performance down to low error rates. For given k and n we use as a benchmark the performance of an ideal MDS code with minimum distance $d_{\min} = n - k + 1$ under ML decoding[1].

The following general requirements should be fulfilled.

R1. The code shall be systematic.

[1]The expression "ideal MDS code" is used as in general such a code does not exist in the binary case.

Manuscript received February 12, 2008. The associate editor coordinating the review of this letter and approving it for publication was G. Taricco. This work has been supported by the EC-IST SatNEx-II project (IST-27393) and by the EC-IST Optimix project (IST-214625). The authors wish to thank Prof. W. E. Ryan for his feedback on this work.

E. Paolini and M. Chiani are with DEIS/WiLAB, University of Bologna, Cesena, Italy (e-mail: {e.paolini, marco.chiani}@unibo.it).

G. Liva and B. Matuz are with the Deutsches Zentrum fur Luft- und Raumfahrt (DLR), 82234 Wessling, Germany (e-mail: {Gianluigi.Liva, Balazs.Matuz}@dlr.de).

Digital Object Identifier 10.1109/LCOMM.2008.080221.

1089-7798/08$25.00 © 2008 IEEE

Authorized licensed use limited to: Universita degli Studi di Bologna. Downloaded on April 15, 2009 at 08:06 from IEEE Xplore. Restrictions apply.

R2. Low-complexity encoding shall be guaranteed.
R3. The frequency of ML decoding usage shall be as small as possible even for large erasure probabilities.
R4. When the ML decoder is used, the number of reference bits shall be as small as possible.
R5. The ML performance shall closely match that of an ideal MDS code in the waterfall region.
R6. The code shall exhibit a low error floor.

Systematic codes allow delivery of the correctly received information bits even in case of decoding failure (R1). Efficient encoding is required to obtain a coding scheme easy to implement (R2). The code shall be designed in order to minimize the decoding complexity (R3 and R4). From a code design point of view, the requirements R3 and R4 imply that the LDPC code shall exhibit a good IT decoding threshold ϵ^*_{IT} as a larger ϵ^*_{IT} is usually associated with a smaller number of reference bits. We observe that, while under IT decoding ϵ^*_{IT} is related to the waterfall performance of the LDPC code, when using HIML decoding larger ϵ^*_{IT} implies reduced decoding complexity. In order to have a close-to-ideal waterfall performance (R5) we need to design LDPC codes with ML threshold ϵ^*_{ML} close to $1-R$, which usually requires large check node (CN) degrees. Since $d_{\min} < n-k+1$, the performance deviates from that of an ideal MDS code due to the error floor only depending on the code distance spectrum. Such an error floor appears at low error rates (R6) if the designed code has a good (large) minimum distance.

Note that some of these requirements are conflicting (e.g. R3/R4 and R6), imposing a tradeoff. For short n (e.g., a few hundreds of bits) the requirements R3 and R4 (decoding complexity, related to ϵ^*_{IT}) can be relaxed. In fact, due to the short codeword length, a more frequent use of ML decoding and a larger fraction of reference bits can be afforded. On the other hand, the requirement R6 (minimum distance) may become an issue. Therefore, we propose to use near-regular LDPC codes in this regime, where ϵ^*_{ML} for the near regular distribution shall be very close to $1-R$. This requires a larger CN degree than is usually done for IT decoding, e.g., degree 8 instead of 6 for $R=1/2$. For longer codes, the requirements on the decoding complexity (R3/R4) shall be favored, which imposes consideration of irregular LDPC codes with a larger ϵ^*_{IT}. Again, ϵ^*_{ML} shall be very close to $1-R$.

B. GeIRA approach

Concerning R1 and R2, there are several solutions for a systematic and efficient LDPC encoding. Among them, a very simple one is represented by systematic IRA (SIRA) encoding [9], [10]. The major drawback of this coding technique is poor minimum distance (see [11, Theorem 23]). In order to preserve the extremely simple SIRA-like encoding while improving the minimum distance, GeIRA codes are considered [5]. They fulfill R1 and R2 while, as shown in the next section, offering a good compromise between R3, R4, R5 and R6.

GeIRA codes are systematic LDPC codes that generate the parity bits by a serial concatenation of an outer low-density generator matrix (LDGM) code with an inner rate-1 recursive convolutional code (RCC). Decomposing the parity-check matrix as $\mathbf{H}=[\mathbf{H}_u|\mathbf{H}_p]$, where $\mathbf{H}_u$ corresponds to the k systematic bits and $\mathbf{H}_p$ to the $m=n-k$ parity bits, we have that $\mathbf{H}_u^T$ is the outer LDGM code generator matrix. Moreover, $\mathbf{H}_p$ is specified by the feedback polynomial $g(D)=\sum_{j=0}^{t} g_j D^j$ of the inner rate-1 RCC (where $g_j \in \{0,1\}$ and $g_0=g_t=1$). Correspondingly, $\mathbf{H}_p$ is lower triangular and its '1's have a multi-diagonal structure, where the number of all-'1' diagonals equals the number of non-null coefficients of $g(D)$ (see example in Fig. 1). Note that a SIRA code can be seen as a GeIRA code with $g(D)=1+D$.

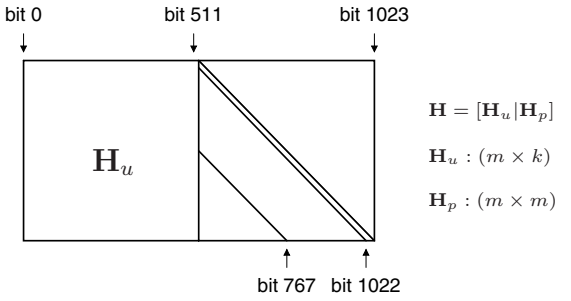

Fig. 1. Parity check matrix of a $(1024, 512)$ GeIRA code with $g(D)=1+D+D^{256}$ ($\mathbf{H}_p$ with three all-'1' diagonals). The diagonal corresponding to the bit 767 is associated with the term D^{256} (767=1023-256).

While for SIRA codes the number of degree-2 VNs is constrained to be not smaller than the number m of CNs, this is not required for GeIRA codes. Allowing multiple diagonals in $\mathbf{H}_p$ enables to still employ a highly efficient SIRA-like encoding but with a smaller number of degree-2 VNs, and also gaining flexibility in the choice of the VN degrees. The reduced number of degree-2 VNs is beneficial in terms of $d_{\min}$ [12]: as shown in Section IV, it is possible to generate both irregular codes with controlled $d_{\min}$ and near-regular codes exhibiting good $d_{\min}$ even for short block lengths.

Given $g(D)$, the CNs distribution and the systematic VNs distribution, the GeIRA code can be constructed with the following algorithm. The connections for the parity VNs are first drawn according to the multi-diagonal structure of $\mathbf{H}_p$. The bipartite graph is then completed with the PEG algorithm [13] for the systematic VNs.

IV. Numerical Results

Examples of design and performance analysis for $R=1/2$ codes with short and moderate lengths are provided. Specifically, we focus on codeword lengths 512, 1024 and 2048 bits. For each length we construct an irregular GeIRA code with uniform CN degree 9 and feedback polynomial $g(D)=1+D+D^{\lfloor 0.24\,n\rfloor}$: for each code $\mathbf{H}_p$ has three diagonals and the fraction of degree-2 VNs is 0.24. The systematic VN distribution is given by

$$\Lambda(x)=0.7813x^3+0.1914x^{49}+0.0195x^{53}+0.0078x^{54},$$

the coefficient of x^i being the fraction of systematic VNs of degree i. The corresponding ensemble is characterized by $\epsilon^*_{IT}=0.480$ and $\epsilon^*_{ML}=0.498$. For $n=512$, a near-$[4,8]$ regular GeIRA code is also considered, with constant $\mathbf{H}_u$ column weight 4 and feedback polynomial $g(D)=1+D+D^4+D^{10}$. We have in this case $\epsilon^*_{IT}=0.383$ and $\epsilon^*_{ML}=0.497$.

Authorized licensed use limited to: Universita degli Studi di Bologna. Downloaded on April 15, 2009 at 08:06 from IEEE Xplore. Restrictions apply.

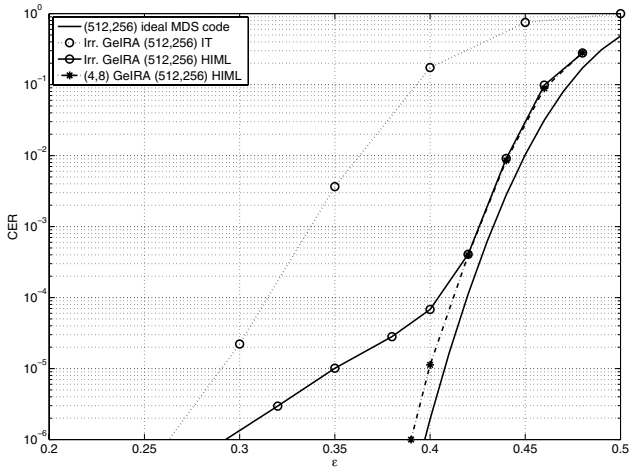

Fig. 2. Performance of $(512, 256)$ GeIRA codes compared to the performance of an ideal MDS code.

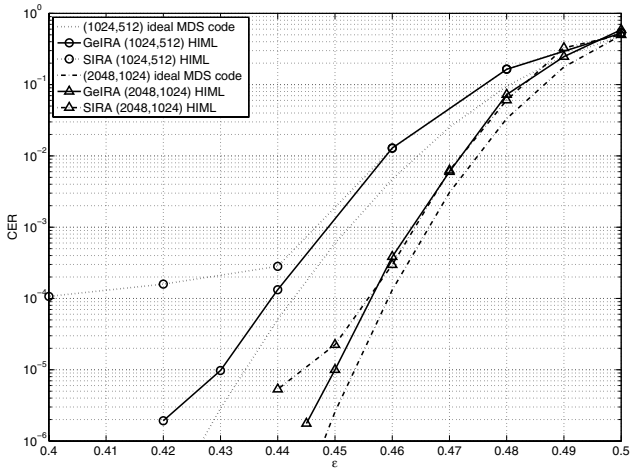

Fig. 3. Performance of $(1024, 512)$ and $(2048, 1024)$ GeIRA and SIRA codes compared to the performance of ideal MDS codes.

In Fig. 2 the performance under HIML decoding of the $(512, 256)$ irregular and of the $(512, 256)$ near-regular GeIRA codes, in terms of codeword error rate (CER) versus the BEC erasure probability ϵ, are compared to the performance of an ideal $(512, 256)$ MDS code. For the irregular GeIRA code the IT performance curve is also shown. For both codes, the HIML curve has a nearly-MDS behavior down to $\mathsf{CER} \simeq 10^{-4}$. At lower error rates the irregular code deviates remarkably, due to the presence of a codeword of weight 11. On the other hand, using the algorithm described in [14] we estimated $d_{\min} = 40$ (with multiplicity 2) for the near-regular code: the error floor is expected at $\mathsf{CER} \simeq 10^{-20}$ in this case.

A comparison between the performance of the $(1024, 512)$ and $(2048, 1024)$ irregular GeIRA codes and that of SIRA codes with same (n, k) parameters is presented in Fig. 3. The SIRA codes have a regular CN degree 9, $g(D) = 1 + D$ and systematic VN distribution given by

$$\Lambda(x) = \begin{array}{l} 0.6485x^3 + 0.0371x^7 + 0.2168x^8 + 0.0254x^{18} \\ +0.0371x^{19} + 0.0351x^{54}, \end{array}$$

leading to $\epsilon^*_{IT} = 0.496$ and $\epsilon^*_{ML} = 0.499$.

While presenting nearly the same performance in the waterfall region, there is a clear advantage with GeIRA design in the error floor region, especially for the $n = 1024$ case, where the SIRA error floor is above $\mathsf{CER} = 10^{-4}$. The irregular GeIRA code provides nearly-MDS performance down to $\mathsf{CER} \simeq 10^{-6}$. The high value of ϵ^*_{IT} is effective in reducing the fraction of reference bits. For instance, in the $(2048, 1024)$ case, the average fraction of reference bits at $\epsilon = 0.5$ is approximately 0.016 meaning that, on average, GE is applied to a submatrix with only 33 columns.

V. Conclusion

In this paper the design guidelines for LDPC codes with hybrid iterative / maximum likelihood decoding over the BEC have been investigated. The design requirements involve waterfall and error floor performance, encoding and decoding complexity. GeIRA codes have been shown to represent a simple solution to satisfy such requirements for both short and moderate codeword lengths, due to their very limited encoding complexity and their flexibility in terms of code design.

References

[1] H. D. Pfister, I. Sason, and R. Urbanke, "Capacity-achieving ensembles for the binary erasure channel with bounded complexity," *IEEE Trans. Inform. Theory*, vol. 51, no. 7, pp. 2352–2379, July 2005.

[2] C. Di, D. Proietti, I. E. Telatar, T. J. Richardson, and R. L. Urbanke, "Finite-length analysis of low-density parity-check codes on the binary erasure channel," *IEEE Trans. Inform. Theory*, vol. 48, no. 6, pp. 1570–1579, June 2002.

[3] D. Burshtein and G. Miller, "An efficient maximum likelihood decoding of LDPC codes over the binary erasure channel," *IEEE Trans. Inform. Theory*, vol. 50, no. 11, pp. 2837–2844, Nov. 2004.

[4] H. Pishro-Nik and F. Fekri, "On decoding of low-density parity-check codes over the binary erasure channel," *IEEE Trans. Inform. Theory*, vol. 50, no. 3, pp. 439–454, Mar. 2004.

[5] G. Liva, E. Paolini, and M. Chiani, "Simple reconfigurable low-density parity-check codes," *IEEE Commun. Lett.*, vol. 9, no. 3, pp. 258–260, Mar. 2005.

[6] E. R. Berlekamp, R. J. McEliece, and H. C. A. van Tilborg, "On the inherent intractability of certain coding problems," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 384–386, May 1978.

[7] Y. Han, W. E. Ryan, and R. D. Wesel, "Dual-mode decoding of product codes with application to tape storage," in *Proc. IEEE 2005 Global Communications Conf.*, vol. 3, St. Louis, USA, Nov. 2005.

[8] T. J. Richardson and R. L. Urbanke, "Efficient encoding of low-density parity-check codes," *IEEE Trans. Inform. Theory*, vol. 47, no. 2, pp. 638–656, Feb. 2001.

[9] H. Jin, A. Khandekar, and R. McEliece, "Irregular repeat-accumulate codes," in *Proc. Int. Symp. on Turbo codes and Related Topics*, Brest, France, Sept. 2000, pp. 1–8.

[10] M. Yang, Y. Li, and W. E. Ryan, "Design of efficiently encodable moderate-length high-rate irregular LDPC codes," *IEEE Trans. Commun.*, vol. 52, no. 4, pp. 564–571, Apr. 2004.

[11] C. Di, T. Richardson, and R. Urbanke, "Weight distribution of low-density parity-check codes," *IEEE Trans. Inform. Theory*, vol. 52, no. 11, pp. 4839–4855, Nov. 2006.

[12] S. Johnson and S. Weller, "Combinatorial interleavers for systematic regular repeat-accumulate codes," *IEEE Trans. Commun.*, to appear.

[13] X. Hu, E. Eleftheriou, and D. Arnold, "Regular and irregular progressive edge-growth Tanner graphs," *IEEE Trans. Inform. Theory*, vol. 51, no. 1, pp. 386–398, Jan. 2005.

[14] X.-Y. Hu, M. Fossorier, and E. Eleftheriou, "On the computation of the minimum distance of low-density parity-check codes," in *Proc. IEEE Int. Conf. on Communications*, vol. 2, Paris, France, June 2004, pp. 767–771.

Authorized licensed use limited to: Universita degli Studi di Bologna. Downloaded on April 15, 2009 at 08:06 from IEEE Xplore. Restrictions apply.