Low-Density Parity-Check Codes for Nonergodic Block-Fading Channels

Joseph Jean Boutros, *Senior Member, IEEE*, Albert Guillén i Fàbregas, *Senior Member, IEEE*,
Ezio Biglieri, *Life Fellow, IEEE*, and Gilles Zémor, *Member, IEEE*

***Abstract*—We design powerful low-density parity-check (LDPC) codes with iterative decoding for the block-fading channel. We first study the case of maximum-likelihood decoding, and show that the design criterion is rather straightforward. Since optimal constructions for maximum-likelihood decoding do not perform well under iterative decoding, we introduce a new family of full-diversity LDPC codes that exhibit near-outage-limit performance under iterative decoding for all block-lengths. This family competes favorably with multiplexed parallel turbo codes for nonergodic channels.**

***Index Terms*—Block-fading (BF) channel, iterative decoding, low-density parity-check (LDPC) codes, maximum-likelihood (ML) decoding, maximum-distance separable (MDS) codes, outage probability.**

I. Introduction

THE block-fading (BF) channel model was first introduced in [20], and further elaborated upon in [2] (see also [1, p. 98 ff.]). This is a realistic and convenient model for a number of channels affected by slowly varying fading, and, as observed for example in [8], is especially relevant in wireless communications involving slow time–frequency hopping (e.g., cellular networks and wireless Ethernet) or multicarrier modulation using orthogonal frequency division multiplexing (OFDM). The design of error-control codes for BF channels offers a challenging problem, which differs greatly from its counterparts referred to additive white Gaussian noise (AWGN) or independent-fading channels (see [8] for a summary of recent results). The main reason for this major difference stems from the fact that in BF channels the random channel gains remain constant during a block of symbols (see below for additional details and definitions), and take independent values from block to block. As a result, while the word-error probability in independent-fading channels depends on the Hamming distances between code words, in BF channels it depends on a new parameter, the *blockwise Hamming distance*. Since codes exhibiting a large minimum Hamming distance may not have a large blockwise Hamming distance, codes that are good when used on the independent-fading channel may not be as good for a BF channel. In addition, over independently faded channels permutations of the symbols cause no variation of the code performance, but this property does no longer hold on the BF channel. Thus, if an off-the-shelf code, designed for the independent-fading channel, is used for transmission over the BF channel, it is important to carefully select the best permutation of its symbols. Finally, one must consider that the BF channel is nonergodic. As a consequence, to determine the information-theoretical rate limit which cannot be surpassed by the word error probability of any coding scheme, one cannot use channel capacity, but rather the *outage probability* [1], [2], [20]. Classical random-like codes, designed to approach ergodic capacity, cannot generally approach the ideal performance limits of BF channels, and, hence, code designs suited to the nonergodic nature of the channel are called for. This paper is devoted to this design problem.

Two main parameters that determine the error rate of coded BF channels for high signal-to-noise (SNR) ratios are the *diversity order* and the *coding gain*. The former determines the slope of the error-rate curve as a function of the SNR on a log-log scale.[1] Since the error probability of any coding scheme is lower-bounded by the outage probability, the diversity order is upper-bounded by the *intrinsic diversity* of the channel, which reflects the slope of the outage limit. When maximum diversity is achieved by a code, the coding gain yields a measure of SNR proximity to the outage limit. The maximum achievable diversity order with discrete input constellations is given by the Singleton bound [8], [14], [17], and codes achieving the Singleton bound are termed blockwise maximum-distance separable (MDS). Blockwise MDS codes are outage-achieving over the (noiseless) block-erasure channel [9], but may not achieve the outage-probability limit on noisy BF channels. As a matter of fact, as shown in [8], blockwise MDS codes are necessary, but not sufficient to approach the outage probability of the channel.

Manuscript received October 05, 2007; revised November 02, 2009. Date of current version August 18, 2010. The work of J. J. Boutros was supported by the Broadband Communications Systems project funded by Qatar Telecom (Qtel). The work of E. Biglieri was supported in part by the project INFSCO-ICT-216203 (DaVinci) within the 7th Framework Program of the European Commission and in part by the Spanish Ministry of Education and Science under Project CONSOLIDER-INGENIO 2010 CSD2008-00010 “COMONSENS”. The material in this paper was presented in part at the 2007 Information Theory and Applications Workshop, San Diego, CA, February 2007.

J. J. Boutros is with Texas A&M University at Qatar, Doha, Qatar (e-mail: boutros@ieee.org).

A. Guillén i Fàbregas is with the Department of Engineering, University of Cambridge, Cambridge, U.K. (e-mail: guillen@ieee.org).

E. Biglieri is with Universitat Pompeu Fabra, Barcelona, Spain (e-mail: e.biglieri@ieee.org).

G. Zémor is with the Institut de Mathématiques de Bordeaux, Université de Bordeaux 1, Bordeaux, France (e-mail: zemor@math.u-bordeaux1.fr).

Communicated by T. J. Richardson, Associate Editor for Coding Theory.

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIT.2010.2053890

[1] The diversity order is exactly the asymptotic slope for Rayleigh fading, while for other fading distributions it is only proportional to the slope. See [19], [27] for details. In this paper, we shall restrict our attention to Rayleigh fading.

Recent code designs for BF channels include near-outage schemes based on a suitable permutation of parallel turbo codes [3]–[5]. Multiplexers for convolutional, turbo and repeat-accumulate codes [3], [8], [14] appeared one decade after the analysis of random and periodic interleaving of convolutional codes on the block-erasure channel [16]. Random ensembles of low-density parity-check codes (LDPC) designed for ergodic AWGN channels [11], [23], in spite of the excellent decoding threshold of their irregular structures, do not have full-diversity, and hence exhibit a poor performance over a BF channel. Decoding thresholds of LDPC code ensembles over ergodic BF channels have been studied [12]. Unfortunately, these codes are not designed to be blockwise MDS, and therefore fail to achieve the outage limit in the nonergodic setup.

In this paper, we introduce a new family of blockwise MDS LDPC codes, the *root LDPC codes*, based on a special type of checknode that we call *rootchecks*.[2] Under iterative message-passing decoding, they achieve the outage-probability limit on block-erasure channels, and they perform close to that limit on Rayleigh BF channels. This paper is organized as follows. Section II introduces the channel model and the relevant notations. LDPC codes with full diversity under Maximum Likelihood (ML) decoding are discussed in Section III. Our new family of LDPC codes suited for iterative decoding is further described. Section V analyzes their density evolution in the presence of block fading. Conclusions are finally drawn in Section VI. Complementary support material is shown in the Appendices.

II. Channel Model and Notation

We consider codewords of N binary digits transmitted on a BF channel, where n_c independent fading gains (whose values form the *channel state*) affect each codeword. The length N is a multiple of n_c, with $\ell \triangleq N/n_c$ denoting the number of bits per fading block. The received signal when symbol x_i is transmitted is given by

$$y_i = \alpha_j x_i + z_i \tag{1}$$

where $y_i \in \mathbb{R}$, $i = 1 \ldots N$, and $j = 1 + [(i-1)/\ell]$, with $[r]$ denoting the integer part of a real number r. The nonnegative real number α_j is the fading gain at block j, $j = 1 \ldots n_c$. The symbols x_i are chosen from a BPSK alphabet $x_i = \pm\sqrt{E_s}$ where E_s is the average energy per symbol. The noise samples are i.i.d. with $z_i \sim \mathcal{N}(0, \sigma^2)$, $\sigma^2 = N_0/2$. We assume perfect channel state information (CSI) at the receiver, and channel gains which are i.i.d. Rayleigh-distributed from block to block and from codeword to codeword. Thus, when the information rate is R bits per channel use, the average SNR per symbol is given by $\gamma = E_\mathrm{s}/N_0$, and the average SNR per bit is $E_\mathrm{b}/N_0 = \gamma/R$. Fig. 1 illustrates the channel model for $n_c = 2$ and $\ell = N/2$.

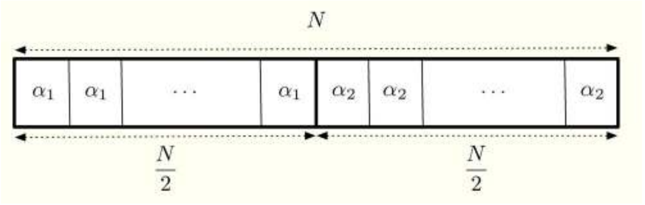

Fig. 1. Codeword representation for a BF channel with $n_c = 2$. The fading gains α_1, α_2 are independent between themselves and among codewords.

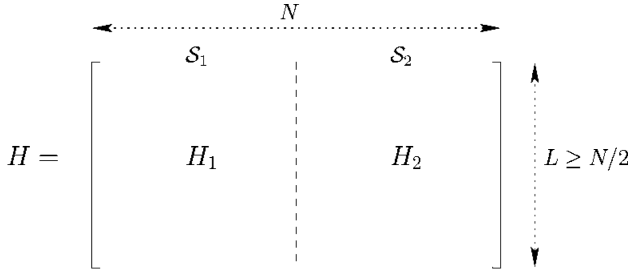

Fig. 2. Parity-check matrix notations for a block-fading channel with $n_c = 2$. The $L - N/2$ extra rows are added in order to enhance the coding gain of a full-diversity code.

In this paper, we focus on linear binary codes $C(N, K)_2$ with block length N, dimension K, and rate $R = K/N \leq 1/n_c \leq 1/2$. The code C is defined by an $L \times N$ parity-check matrix H (Fig. 2), or, equivalently, by the corresponding Tanner graph [1]. This has L single-parity checknodes. It is assumed that H has full rank L, so that $R = 1 - L/N$.

Let us recall that the diversity order attained by C is defined as [21], [25]

$$d = -\lim_{\gamma \to +\infty} \frac{\log P_\mathrm{ew}}{\log \gamma} \tag{2}$$

where P_ew is the word error probability at the decoder's output. Thus, the diversity order d depends on the decoding algorithm.

Definition 1: An error-correcting code is said to have full diversity if $d = n_c$.

The word error probability of a code with full diversity n_c decreases as $1/\gamma^{n_c}$ at high SNR [1], [21], [25], [27]. For a given codeword $c \in C$, we define the blockwise Hamming weight vector $(\omega_1(c), \ldots, \omega_{n_c}(c))$, where $\omega_j(c)$ is the Hamming weight of coded bits affected by fading α_j. Under maximum likelihood decoding, it is well known [3], [8], [14] that the diversity order is determined by

$$d = \min_{c \in C - \{0\}} |\{\omega_j(c) \neq 0\}|. \tag{3}$$

In words, the integer d is the minimum number of blocks that have nonzero Hamming weight. We refer to d as the blockwise minimum Hamming distance. Qualitatively, this implies that an ML decoder of C will be able to decode correctly in presence of $d - 1$ deep fades, which one can think of as block erasures. We also define the minimum blockwise Hamming weight as

$$\omega^\star = \min_{c \in C - \{0\}} \min_{j = 1 \ldots n_c} (\omega_j(c)). \tag{4}$$

[2] We hasten to observe that our definition of rootchecks can also be formulated in terms of stopping sets, as defined in [7] (see Definition 1.1 and Lemma 1.1) and in Section 3.22 of [24] in the context of binary erasure channels. Since the context is quite different in this paper, we deem it more natural to use our concept of rootchecks here.

Having $\omega^\star > 0$, i.e., nonzero weight in all blocks, implies that $d = n_c$ under ML decoding. Under these conditions, the pairwise error probability can be upper bounded by [14], [3]

$$P(0 \to c) \leq \frac{1}{2}\prod_{j=1}^{n_c} \frac{1}{1+\omega_j(c)\gamma} \approx \frac{1}{2\gamma^{n_c}\prod_{j=1}^{n_c}\omega_j(c)} \tag{5}$$

where the right approximation is valid at high SNR. The quantity $\prod_j \omega_j(c)$ is referred to as the *coding gain*. Since $\sum_j \omega_j(c)$ is constant for a given codeword c, then increasing $\omega^\star$ would lead to a higher coding gain.

The diversity order attained by C admits a Singleton-like bound [1], [8], [14], [17]

$$d \leq 1 + \lfloor n_c(1-R) \rfloor. \tag{6}$$

Consequently, $R = 1/n_c$ is the highest achievable rate for a full-diversity code.

The instantaneous mutual information of a block-fading channel depends on channel realization [2], [20], [25]. Such a quasi-static channel is not information stable [26]. Therefore, its Shannon capacity is zero since there is a nonvanishing probability that the decoder makes a *word error*. In the limit of large block length, this probability is the *information outage probability*, defined as [2], [20]

$$P_{\text{out}}(\gamma, R) \triangleq \mathbb{P}\{\mathcal{I}(\gamma, \boldsymbol{\alpha}) < R\} \tag{7}$$

where $\mathcal{I}(\gamma, \boldsymbol{\alpha})$ is the *instantaneous input–output mutual information* between the input and output of the channel, defined as

$$\mathcal{I}(\gamma, \boldsymbol{\alpha}) \triangleq \frac{1}{n_c}\sum_{i=1}^{n_c} I_{\text{AWGN}}\left(\gamma\alpha_i^2\right) \tag{8}$$

with $I_{\text{AWGN}}(s)$ the input–output mutual information of an AWGN channel with SNR per symbol equal to s. The BF channel is also commonly referred to as *nonergodic* since, for finite values of n_c, $\mathcal{I}(\gamma, \boldsymbol{\alpha})$ is a nonconstant random variable.

The information outage probability $P_{\text{out}}(\gamma, R)$ is the natural fundamental limit for the BF channel for sufficiently large word length, i.e., achievability and converse results hold for the outage probability [18] Therefore, any code approaching $P_{\text{out}}(\gamma, R)$ should have a word-error probability that, as N increases, becomes *independent* of the code length [4], [8].

Unless stated otherwise, we shall focus our study on a coding rate $R = \frac{1}{2}$ (or just slightly smaller than $\frac{1}{2}$) and a nonergodic Rayleigh fading channel with $n_c = 2$ blocks per codeword, as depicted in Figs. 1 and 2. However, most of our results can be easily generalized to $R = \frac{1}{n_c}$.

III. Full-Diversity LDPC Codes Under ML Decoding

In this section, we study LDPC codes in the presence of BF under ML decoding. As we shall see, the design of full-diversity LDPC codes under ML decoding is rather straightforward. We recognize that ML decoding is unfeasible in practice; however, it yields valuable insight into code structures suitable for nonergodic channels. The main result of this section is that, under iterative decoding, ML-designed full-diversity codes fail to guarantee diversity due to badly located pseudo-codewords.

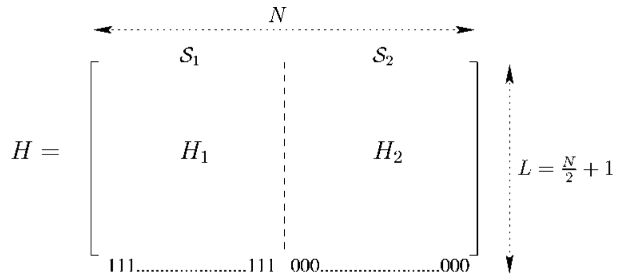

Fig. 3. ML-designed full-diversity LDPC code with $\omega^\star = 2$.

Following the notations defined in the previous section, the $L \times N$ parity-check matrix H is written in the form $H = [H_1 \,|\, H_2]$, where the left and right parts H_1, H_2 are $L \times N/2$. The vector space generated by the $N/2$ left columns is denoted $\mathcal{S}_1$. Similarly, $\mathcal{S}_2$ is the vector space generated by the $N/2$ right columns. Recall that the addition of redundant rows does not modify the code nor its Hamming weight distribution. Therefore, as stated in Section II, H can be assumed to have full rank L without any loss of generality.

Proposition 1: A binary code C with rate $R \leq \frac{1}{2}$, i.e., $L \geq N/2$, has full diversity if and only if H_1 and H_2 are both full-rank.

Proof: If $\dim \mathcal{S}_1 = N/2$, then a nonzero codeword cannot have its support on H_1, because all columns in H_1 are independent. Hence, $\omega_2 > 0$ for all nonzero codewords. Similarly, $\omega_1 > 0$ when $\dim \mathcal{S}_2 = N/2$. Finally, $\omega_1 > 0$ and $\omega_2 > 0$ for all nonzero codewords, which yields $\omega^\star > 0$. ■

The full-rank property of the above proposition was first observed in [10]. Its extension to coding rate $1/3$ with $H = [H_1 \,|\, H_2 \,|\, H_3]$ can be obtained by imposing that the matrices $[H_1 \,|\, H_2]$, $[H_1 \,|\, H_3]$, and $[H_2 \,|\, H_3]$ all have full rank. Generalization to any rate $R = \frac{1}{n_c}$ is straightforward.

Proposition 2: Consider a binary code C with rate $R = 1/2$, and hence with $L = K = N/2$. If C has full diversity, then $\omega^\star = 1$.

Proof: If C has full diversity, then $\dim \mathcal{S}_1 = \dim \mathcal{S}_2 = N/2$. Any column from H_1 can then be written as a linear combination of columns from H_2. This is also valid for any column belonging to H_2. Hence, nonzero codewords with $\omega_i = 1$ exist for both $i = 1$ and $i = 2$ if the coding rate is exactly equal to $1/2$. ■

The minimum blockwise Hamming weight must be increased in order to improve the coding gain of C. Proposition 2 states that to achieve this, one must decrease the coding rate. The next proposition shows that adding just one extra row is enough to improve ML decoding by moving from $\omega^\star = 1$ to $\omega^\star = 2$.

Proposition 3: There exists a binary code C of rate $R = 1/2 - 1/N$ that has full diversity with $\omega^\star = 2$.

Proof: The proof is based on the special parity-check matrix structure shown in Fig. 3 where H_2 is a full-rank matrix whose columns have odd Hamming weight (the identity matrix, for example). Let now H_1 be such that its first column is

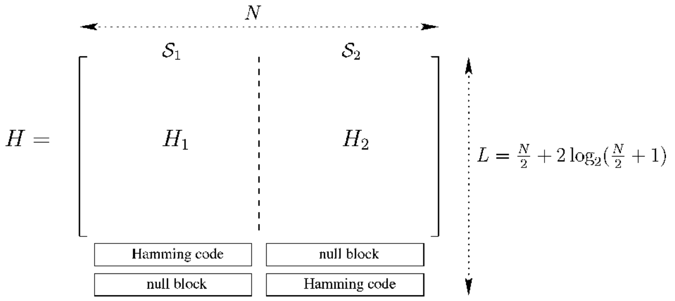

Fig. 4. ML-designed full-diversity LDPC code with $\omega^\star \geq 3$.

the all zero vector, and the remaining $N/2 - 1$ columns are all even-weight and full-rank.

Next, we show that the $\omega^\star$ corresponding to this construction is 2. Clearly, the first (leftmost) $N/2$ columns of H and the last (rightmost) $N/2$ columns of H have full rank, so that we have $\omega^\star \geq 1$.

None of the first $N/2$ columns of H can be a linear combination of the last $N/2$ columns of H, due to the 1 in the last position of each of the first columns. None of the last $N/2$ columns of H can be a linear combination of the first $N/2$ columns of H, because columns of H_2 have odd weight and any linear combination of columns of H_1 has even weight.

These last statements imply that $\omega^\star \geq 2$. ■

The rate reduction necessary to achieve $\omega^\star = 2$ is negligible for large code length N. If we now require $\omega^\star = 3$, the following result holds.

Proposition 4: Consider a binary code C with rate $R \leq 1/2$. The code has $\omega^\star = 3$ only if $R \leq 1/2 - (1/N)\log_2(1 + N/2)$.

Proof: Recall that $\mathcal{S}_2$ denotes the linear span of the set of columns of H_2. Consider the $1 + N/2$ sets consisting of $\mathcal{S}_2$ together with its translates $h_1 + \mathcal{S}_2$ for all columns h_1 of H_1. No two of these sets can intersect, otherwise either a column of H_1, or a sum of two columns of H_1, equals a sum of columns of H_2, which would imply the existence of a codeword of weight at most 2 on the first $N/2$ positions. Therefore we must have $2^L \geq (1 + N/2)2^{N/2}$. ■

Proposition 5: There exists a full-diversity binary code with $\omega^\star \geq 3$ and $R = 1/2 - (1/N)2\log_2(N/2 + 1)$.

Proof: The code has the parity-check matrix of Fig. 4. The presence of a Hamming code whose minimum distance is 3 rules out a blockwise Hamming weight equal to 2. ■

It is interesting to simulate iterative decoding of LDPC codes that are full-diversity for ML decoding, i.e., with $\omega^\star \geq 1$, and results are shown in Fig. 5, for $n_c = 2$ and the (3,6) ensemble. The code used is of the type guaranteed by Proposition 1, i.e., it is simply chosen so that H_1 and H_2 have full-rank. We see that this structure does not help the iterative decoder and that the code actually has diversity 1 for iterative decoding and not diversity 2 guaranteed by Proposition 1 for ML decoding. The performance is the same as that of randomly chosen (3,6) LDPC code (not shown in the figure). This effect is caused by the pseudocodewords [15] whose support is restricted to H_1 or H_2, and hence have a minimum blockwise pseudoweight equal to zero when belief propagation is applied.

To simulate ML decoding of this code we have used a "genie-aided" iterative decoder: this is an iterative decoder that considers that it has correctly decoded if there is no residual error in the positions corresponding to H_1 or to H_2. This is because we argue that if a suboptimal decoder is able to correct all errors in one block of positions, then the ML decoder should be able to remove all residual errors, because there is no codeword whose support belongs to a single block. Similarly, to simulate the case $\omega^* = 3$ guaranteed by Proposition 4, we have considered that the "genie-aided" decoder has correctly decoded if the number of residual errors in one position is less than 3.

Fig. 5 shows therefore that the structures investigated in this section do not improve the performance of belief propagation. To achieve this we have to introduce a new LDPC design: this is the object of the following section.

IV. Full-Diversity LDPC Codes for Iterative Belief Propagation Decoding

The results presented at the end of Section III show that, if iterative decoding is used, the design criteria derived under the assumption of ML decoding are irrelevant. In this section, we proceed to design LDPC codes with iterative decoding. Our design is based on a graphical representation [1], [24], which is then translated into a matrix description. We then analyze the construction by means of log-ratio probability-density evolution.

A. Limiting Case: Block-Erasure Channels

We illustrate our solution to the design problem by referring to a limiting case. Specifically, observe that, if the fading coefficients α_i belong to the set $\{0, +\infty\}$, the BF channel becomes a block-erasure channel [9], [16]. This corresponds to the large SNR regime. The reader is referred to Fig. 6, where the outage boundaries are illustrated (see [4] for more details).

In our approach, we need to find a graph whose topology yields full diversity. For simplicity, we illustrate the case of the (3,6) LDPC ensemble with $n_c = 2$ (generalizations to other degree distributions and rates will be treated *infra*). Fig. 7 shows the notation employed in this section. Two examples of local graphs whose diversity is not guaranteed are shown in Fig. 8. The checknodes defining an LDPC code are single-parity check codes, and hence they cannot tolerate more than one erased bit. For example, if $\alpha_1 = 0$ then the checknodes in Fig. 8 are not able to recover the erased bit, because it is connected to bitnodes which are also erased, because they are subject to the same fading coefficient. Notice also that the design must be symmetric, i.e., any analysis with respect to α_1 is valid for α_2, and hence permuting the order of the two fading gains should yield an equivalent design.

The two unique local graphs that guarantee full diversity in the presence of block erasures are illustrated in Fig. 9. The immediate consequence is the definition of *rootchecks*. We start by building a regular (3,6) structure where bitnodes have degree 3 and checknodes have degree 6, next we generalize to any $(\lambda(x), \rho(x))$ degree distribution [23]. A checknode Φ connected to bits $\vartheta_1, \vartheta_2, \ldots, \vartheta_6$ is written as $\Phi(\vartheta_1, \vartheta_2, \ldots, \vartheta_6)$.

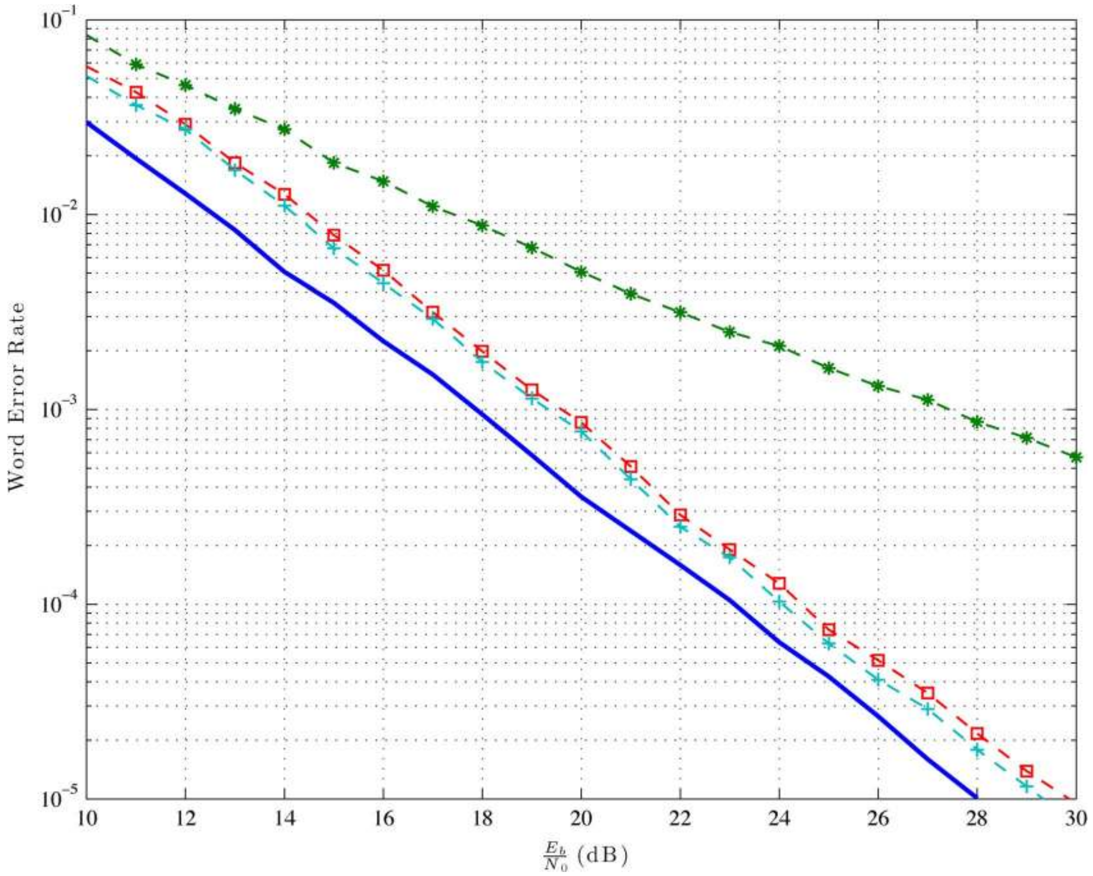

Fig. 5. Rate 1/2 ML-designed LDPC codes with iterative decoding on a Rayleigh block-fading channel with $n_c = 2$. The thick solid line corresponds to the outage probability with BPSK inputs, the dotted lines with $*$ markers corresponds to the ML-designed code with iterative decoding, the dotted lines with □ markers corresponds to the ML-designed code with $\omega^\star = 1$ using a genie ML decoder and the dotted lines with $+$ markers corresponds to the ML-designed code with $\omega^\star = 3$ using the genie ML decoder. The genie ML curves show the performance of a decoder that knows whether errors occur in positions corresponding to H_1 or H_2.

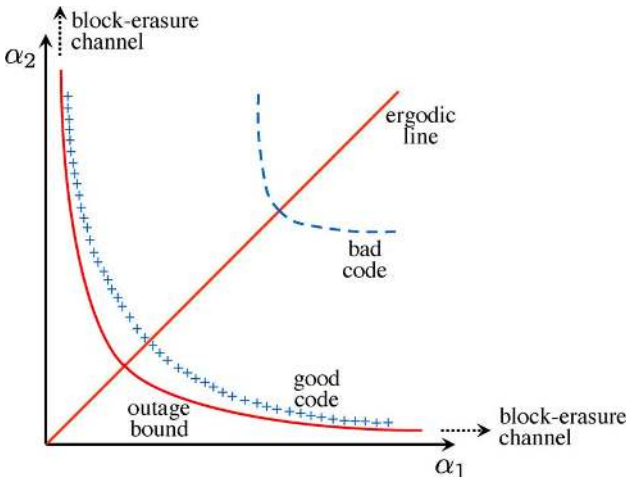

Fig. 6. Outage boundaries in the fading plane for a BF channel with $n_c = 2$. To approach the outage limit, one should: (a) reduce the gap on the ergodic line, which requires an excellent decoding threshold and (b) reduce the gap at infinity, which requires a full-diversity code (MDS) on a block-erasure channel.

Definition 2: Let ϑ be a binary element transmitted on fading α_1. A type-1 rootcheck for ϑ is a checknode $\Phi(\vartheta, \vartheta_1, \ldots, \vartheta_5)$ where all bits $\vartheta_1, \ldots, \vartheta_5$ are transmitted on fading α_2.

Type-2 rootchecks are defined similarly.

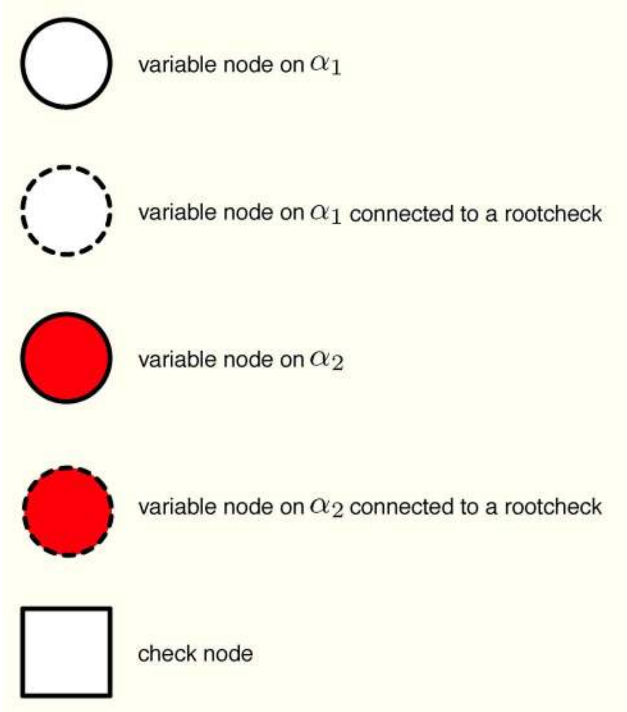
variable node on α_1
variable node on α_1 connected to a rootcheck
variable node on α_2
variable node on α_2 connected to a rootcheck
check node

Fig. 7. Notations for graph representation.

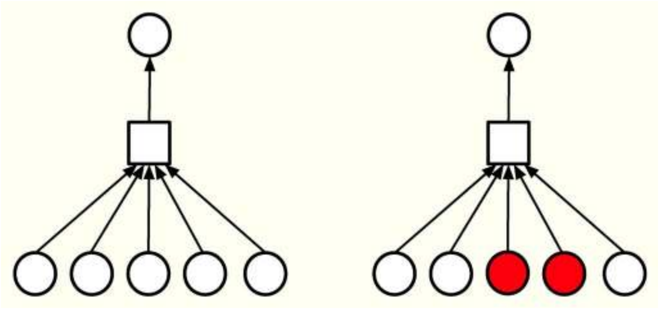

Fig. 8. Two examples of bad configurations under belief propagation decoding on a block-fading channel.

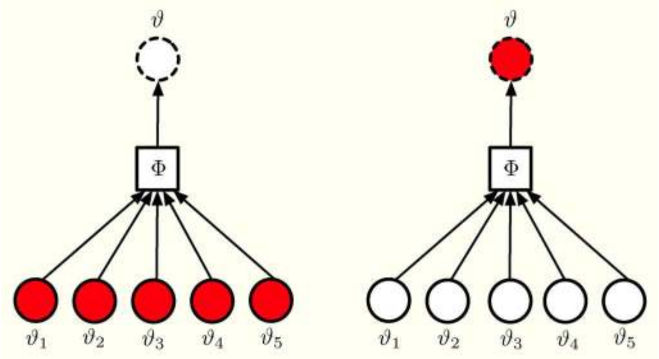
ϑ
Φ
ϑ
Φ
ϑ_1 ϑ_2 ϑ_3 ϑ_4 ϑ_5
ϑ_1 ϑ_2 ϑ_3 ϑ_4 ϑ_5

Fig. 9. Two unique good configurations (rootchecks) under belief propagation decoding on a block-fading channel.

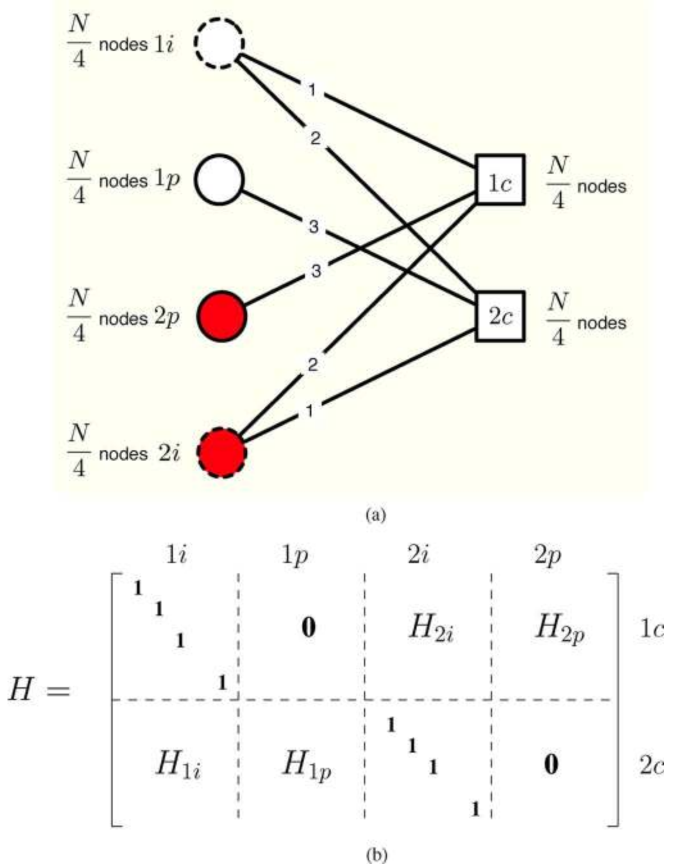

Fig. 10. Tanner graph and parity-check matrix for a regular (3,6) root-LDPC code of rate 1/2. An irregular structure $(\lambda(x), \rho(x))$ can be easily plugged on edges connected to nonroot checknodes. (a) Tanner graph. (b) Parity-check matrix.

Using Definition 2, consider a length-N, rate-$1/2$ LDPC code. Information bits are split into two classes: $N/4$ bits (tagged $1i$) are transmitted on α_1, while $N/4$ bits (tagged $2i$) are transmitted on α_2. Parity bits are also partitioned into two sets, say $1p$ and $2p$. Finally, we connect all information bits to rootchecks in order to guarantee full diversity when word error probability is measured on those bits. The protection of parity bits is not considered. More general structures with parity bit protection are considered in [6]. This design produces the bipartite Tanner graph drawn in Fig. 10(a). Its extension to rate 1/3 is portrayed in Fig. 11. Integers labeling edges indicate the degree of a node along those edges. The structure of H for a root-LDPC code is directly derived from its Tanner graph, and is shown in Fig. 10(b). The $N/4 \times N/4$ identity matrix is written twice in connections $1i \leftrightarrow 1c$ and $2i \leftrightarrow 2c$. Two all-zero $N/4 \times N/4$ submatrices prohibit any edge of type $1p \leftrightarrow 1c$ and $2p \leftrightarrow 2c$. The other four submatrices are all sparse, H_{1i} and H_{2i} are random sparse matrices of Hamming weight 2 per row and per column. Similarly, H_{1p} and H_{2p} are random sparse matrices of Hamming weight 3 per row and per column.

An irregular version of a root-LDPC code can be built from a left degree distribution $\lambda(x)$ and a right degree distribution $\rho(x)$ by appropriately modifying the weight distribution of the 4 submatrices H_{1i}, H_{2i}, H_{1p}, and H_{2p}. Equivalently, the degree distribution changes the distribution of edges connected to nonrootchecks in the Tanner graph. Irregularity has no influence on the diversity order because rootchecks are maintained. Irregularity should enhance the coding gain by pushing the code boundary near the outage capacity limit on the ergodic line.

Proposition 6: Consider a rate-$R = 1/2$ root-LDPC code with degree distribution $(\lambda(x), \rho(x))$ transmitted on a block-erasure channel with $n_c = 2$. Then, under iterative message passing decoding, the root-LDPC code has full-diversity.

Proof: The two fading coefficients α_1 and α_2 are independent and take two possible values $\{0, +\infty\}$. Examining the Tanner graph of Fig. 10(a), we observe that the only outage event occurs when $\alpha_1 = \alpha_2 = 0$ (both blocks erased). Indeed, when $\alpha_1 = 0$ and $\alpha_2 = +\infty$, it is straightforward to see that information bits $1i$ are determined using rootchecks $1c$. Similarly, when $\alpha_1 = +\infty$ and $\alpha_2 = 0$, information bits $2i$ are determined using rootchecks $2c$. ■

On a block-erasure channel, let ϵ be the probability that α_i be equal to 0. From the proof of Proposition 6 above, we find that the word error probability of a root-LDPC code is ϵ^2. As shown in [9], this is precisely the outage probability of the channel, and, therefore, full-diversity blockwise MDS codes are outage achieving in the block-erasure channel. As remarked in [9], blockwise MDS codes are necessary, but not sufficient to achieve the outage limit in noisy channels. In the following, we study the behavior of root-LDPC over general Rayleigh BF AWGN channels.

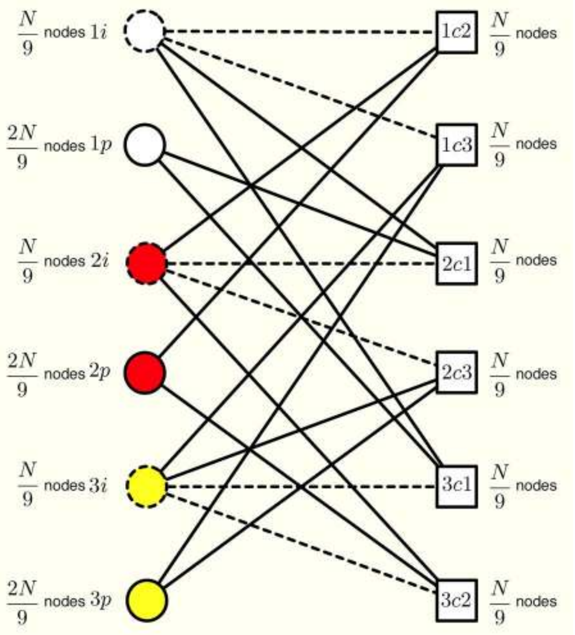
$\frac{N}{9}$ nodes $1i$
$\frac{2N}{9}$ nodes $1p$
$\frac{N}{9}$ nodes $2i$
$\frac{2N}{9}$ nodes $2p$
$\frac{N}{9}$ nodes $3i$
$\frac{2N}{9}$ nodes $3p$
$1c2$ $\frac{N}{9}$ nodes
$1c3$ $\frac{N}{9}$ nodes
$2c1$ $\frac{N}{9}$ nodes
$2c3$ $\frac{N}{9}$ nodes
$3c1$ $\frac{N}{9}$ nodes
$3c2$ $\frac{N}{9}$ nodes

Fig. 11. Tanner graph for a regular (4,6) root-LDPC code of rate 1/3. The introduction of any $(\lambda(x), \rho(x))$ irregularity is always possible on edges connected to nonroot checknodes.

B. The General Case

Now we study the general case of Rayleigh BF. Some simple facts about fourth-order χ^2 distributions are reviewed in Appendix I. In the sequel, we use the notations of Appendix I to analyze the diversity metric in log-ratio messages.

Proposition 7: Consider a rate-1/2 $(\lambda(x), \rho(x))$ root-LDPC code transmitted on a Rayleigh block-fading channel with $n_c = 2$. Then, under iterative belief propagation decoding, the root-LDPC code has full-diversity.

Proof: As indicated in the design of a root-LDPC code before Proposition 6, the diversity order of a root-LDPC code does not depend on its left or right degree distribution. This can also be proved via the evolution trees in the next section. Thus, we restrict this proof to a regular (3,6) LDPC. The extension to the irregular case is straightforward.

Let $\Lambda_i^a, i = 1 \ldots \delta - 1$, denote the input log-ratio probabilistic messages to a checknode Φ of degree δ. The output message Λ^e for belief propagation is

$$\Lambda^e = 2\mathrm{th}^{-1}\left(\prod_{i=1}^{\delta-1} \mathrm{th}\left(\frac{\Lambda_i^a}{2}\right)\right) \tag{9}$$

where $\mathrm{th}(x)$ denotes the hyperbolic-tangent function. Superscripts a and e stand for *a priori* and *extrinsic*, respectively. In order to simplify the proof, we will show that a suboptimal belief propagation decoder is able to achieve diversity order 2. Therefore, if a suboptimal decoder achieves full diversity, the optimal decoder also achieves full diversity. Consider the min-sum decoder. The output message produced by a checknode Φ is now approximated by

$$\Lambda^e = \min(|\Lambda_i^a|) \prod_{i=1}^{\delta-1} \mathrm{sign}\left(\Lambda_i^a\right) \tag{10}$$

a) First Decoding Iteration: We first study the output after one decoding iteration. We assume that the all-zero codeword has been transmitted. The channel crossover probability associated with fading α_j, $j = 1, 2$, is

$$\epsilon_j = Q\left(\sqrt{2\gamma\alpha_j^2}\right)$$

The channel message for a bit ϑ transmitted over fading coefficient α is

$$\Lambda_0 = \log\left(\frac{p(y \,|\, \vartheta = 0, \alpha)}{p(y \,|\, \vartheta = 1, \alpha)}\right) = \frac{2\alpha y}{\sigma^2} = \frac{2}{\sigma^2}(\alpha^2 + \alpha z) \tag{11}$$

where $y = \alpha + z$ and $z \sim \mathcal{N}(0, \sigma^2)$ (assuming $E_{\mathrm{s}} = 1$). At the first decoding iteration, all input messages Λ_i^a in (10) have an expression identical to (11).

An information bit ϑ of class $1i$ has $\Lambda_0 = \frac{2}{\sigma^2}(\alpha_1^2 + \alpha_1 z_0)$. It also receives 3 messages Λ_i^e, $i = 1 \ldots 3$ from its 3 neighboring checknodes. The total *a posteriori* message corresponding to ϑ is $\Lambda = \Lambda_0 + \Lambda_1^e + \Lambda_2^e + \Lambda_3^e$. Let Λ_1^e be the extrinsic message generated by the rootcheck of class $1c$ connected to ϑ. The error rate $P_e(1i)$ on class $1i$ is given by the negative tail of the density of Λ messages. The addition of $\Lambda_2^e + \Lambda_3^e$ to $\Lambda_0 + \Lambda_1^e$ cannot degrade $P_e(1i)$ because the convolution with the density of messages from nonrootchecks can only physically upgrade the resulting density. Thus, it is sufficient to prove that message $\Lambda_0 + \Lambda_1^e$ brings full diversity. The expression of Λ_1^e is found by applying (10). Input messages to the rootcheck are negative with probability ϵ_2. Then

$$\Lambda_1^e = S_1 \frac{2}{\sigma^2}\left(\alpha_2^2 + \alpha_2 z_1\right)$$

where

$$S_1 = \sum_{i \text{ even}} \binom{4}{i} \epsilon_2^i (1 - \epsilon_2)^{4-i} - \sum_{i \text{ odd}} \binom{4}{i} \epsilon_2^i (1 - \epsilon_2)^{4-i}.$$

We obtain

$$\Lambda_1^e = (1 - 2\epsilon_2)^4 \frac{2}{\sigma^2}\left(\alpha_2^2 + \alpha_2 z_1\right)$$

The partial *a posteriori* log-ratio message becomes

$$\Lambda_0 + \Lambda_1^e = \frac{2}{\sigma^2}\left(\alpha_1^2 + (1 - 2\epsilon_2)^4 \alpha_2^2\right.$$
$$\left. + \alpha_1 z_0 + (1 - 2\epsilon_2)^4 \alpha_2 z_1\right).$$

The embedded metric $Y = \alpha_1^2 + (1 - 2\epsilon_2)^4 \alpha_2^2$ guarantees full diversity. At high SNR (i.e., when $E_b/N_0 \to +\infty$), Y behaves exactly as $\alpha_1^2 + \alpha_2^2$.

b) Further Decoding Iterations: As can be seen from the decoding tree of a bitnode $1i$ in Fig. 14, the diversity order 2

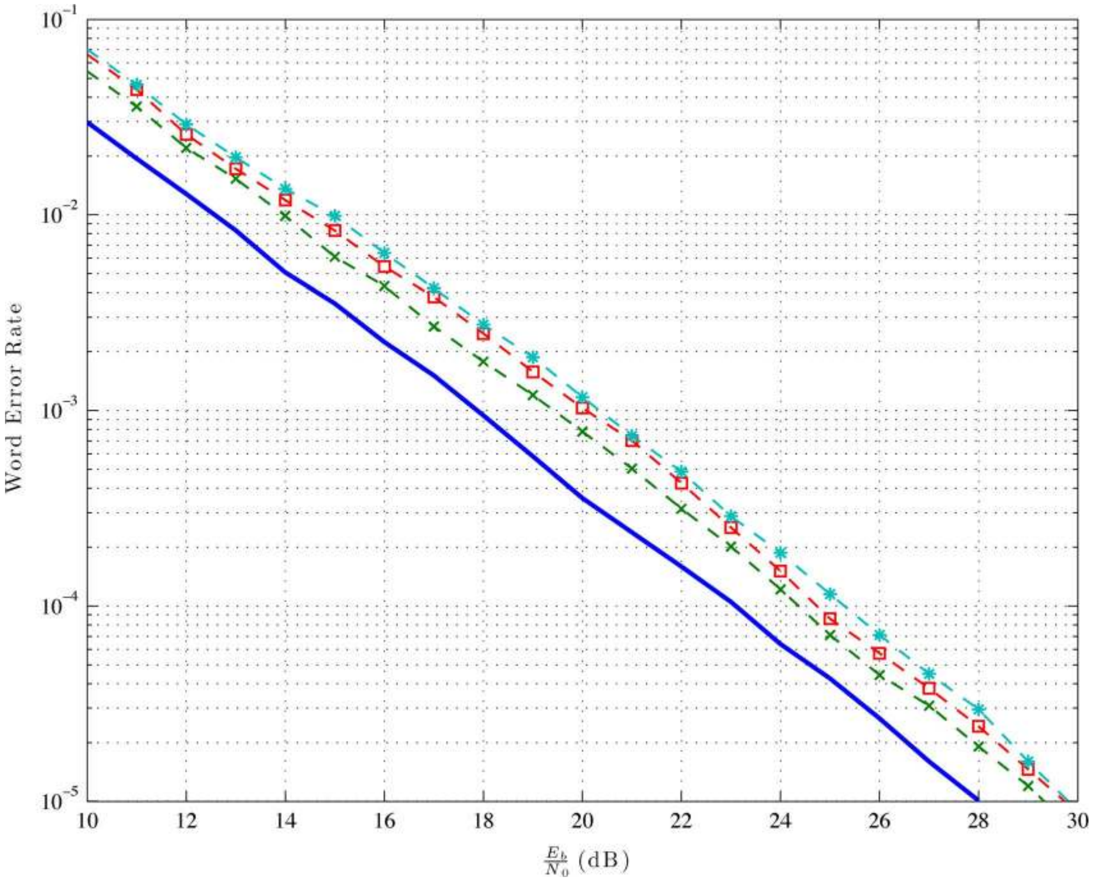

Fig. 12. Regular (3,6) root-LDPC codes with iterative decoding on a Rayleigh block-fading channel with $n_c = 2$. Word-error rate is measured on information bits. The thick solid line corresponds to the outage probability with BPSK, the dotted lines with × markers correspond to $N = 200$, the dotted lines with □ markers correspond to $N = 2000$ and the dotted lines with markers $*$ correspond to $N = 20000$.

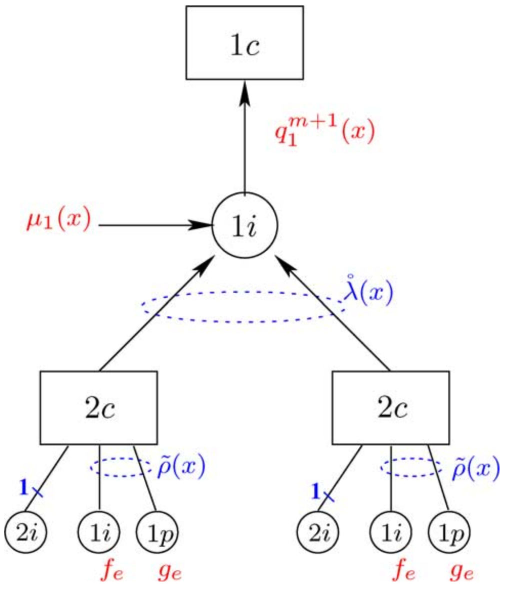

Fig. 13. Local neighborhood of bitnode $1i$. This tree is used to determine the evolution of messages $1i \rightarrow 1c$.

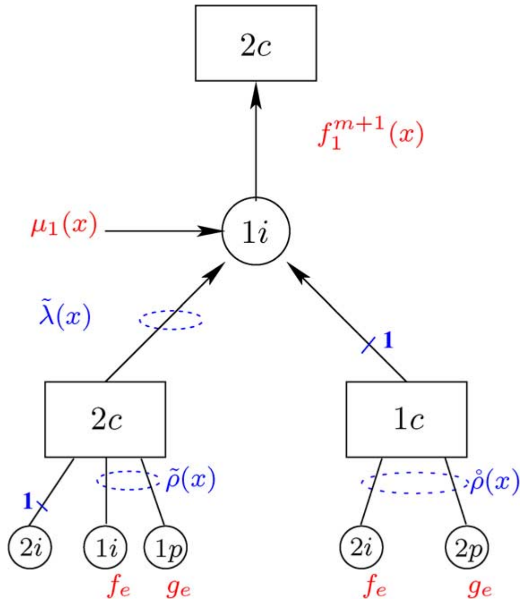

Fig. 14. Local neighborhood of bitnode $1i$. This tree is used to determine the evolution of messages $1i \rightarrow 2c$.

is maintained after the first iteration. Indeed, at the input of the rootcheck, information bits of class $2i$ have already full diversity and parity bits $2p$ bring always a term proportional to α_2^2. Due to the particular structure of root-LDPC codes, the density of message $\Lambda_0 + \Lambda_1^e$ can only be improved with respect to the first iteration. Hence, full diversity is preserved. ■

The proof of the previous proposition is based on showing that the information bits have diversity 2. In the following, we examine the diversity of the parity bits. A parity bit ϑ of class $1p$ has $\Lambda_0 = \frac{2}{\sigma^2}(\alpha_1^2 + \alpha_1 z_0)$. It also receives 3 messages Λ_i^e,

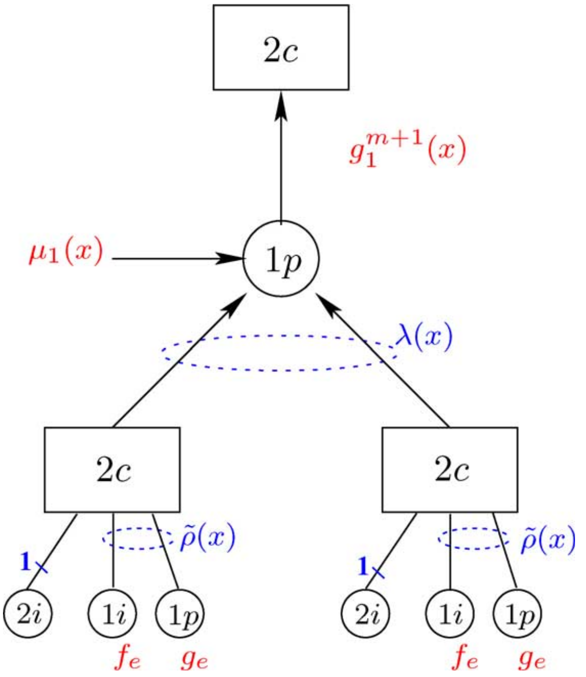

Fig. 15. Local neighborhood of bitnode $1p$. This tree is used to determine the evolution of messages $1p \rightarrow 2c$.

$i = 1 \ldots 3$ from its 3 neighboring checknodes all of class $2c$. The total *a posteriori* message of ϑ is $\Lambda = \Lambda_0 + \Lambda_1^e + \Lambda_2^e + \Lambda_3^e$. Now let us determine the nature of Λ_i^e based on input messages to a checknode Φ of class $2c$ as illustrated in Figs. 10(a) and 15. The node Φ is not a rootcheck. We need to determine the metric Y embedded in its output message. In the case $\alpha_2 \leq \alpha_1$ (this happens with probability $1/2$), it can be shown that, after one decoding iteration, the extrinsic message produced by Φ satisfies

$$\Lambda_i^e = \begin{cases} S_{\frac{2}{\sigma^2}}(\alpha_2^2 + \alpha_2 z) & \text{with probability } G^4 \geq \frac{1}{16} \\ S_{\frac{2}{\sigma^2}}(\alpha_1^2 + \alpha_1 z) & \text{with probability } 1 - G^4 \leq \frac{15}{16} \end{cases}$$

where the function G is defined in Appendix II. On the contrary, when $\alpha_2 \geq \alpha_1$, it can be shown that

$$\Lambda_i^e = \begin{cases} S_{\frac{2}{\sigma^2}}(\alpha_2^2 + \alpha_2 z) & \text{with probability } G^4 \leq \frac{1}{16} \\ S_{\frac{2}{\sigma^2}}(\alpha_1^2 + \alpha_1 z) & \text{with probability } 1 - G^4 \geq \frac{15}{16}. \end{cases}$$

We conclude that, for parity bits, with a probability greater than $\frac{1}{2} \times \frac{15}{16}$, the output message has diversity order one. In spite of the presence (with a nonzero probability) of diversity-2 messages, the error probability of parity bits will be dominated by weak messages with diversity 1. The above arguments are still valid for further decoding iterations.

Recall now that under ML decoding the coding gain is controlled by the quantity $\omega^\star$ which is the minimum blockwise Hamming weight defined in (4). Under iterative decoding we now use $\omega^\star$ to refer to the analogous quantity $\min(a, b)$ defined in Appendix I which controls the coding gain in the same way. We conclude this section by analyzing the behavior of this $\omega^\star$ in the case $R = 1/2$.

Corollary 1: A root-LDPC code with $R = 1/2$ satisfies $\omega^\star = 1$ under iterative belief propagation decoding.

Proof: Consider an information bit ϑ of class $1i$. Let $\delta_b \geq 2$ be the degree of ϑ. At high SNR, the log-ratio message produced by its rootcheck has an embedded metric $\alpha_1^2 + \alpha_2^2$. Consider the $\delta_b - 1$ nonroot checknodes connected to ϑ. Since parity bits of class $1p$ dominate the error probability at the input of $2c$ checknodes, then its metric will be α_1^2. Finally, the *a posteriori* log-ratio message associated to ϑ will contain a metric of the type $\delta_b\alpha_1^2 + \alpha_2^2$. Hence, the $\omega^\star$ parameter under iterative decoding is 1. ■

In Fig. 12, we illustrate the performance of the (3,6) root-LDPC ensemble. As we observe, the performance is similar for all ranges of N, and it is also close to the outage probability of the channel. This effect was first observed with blockwise-concatenated codes and repeat-accumulate codes in [8], and then in [3]–[5] for parallel turbo codes. For large N this effect is due to the threshold behavior of *good* codes, i.e., for a given channel realization, the code has a SNR threshold (independent of N) below which the decoder cannot decode successfully. Hence, whenever this threshold is larger than the SNR γ, the decoder will make an error for sufficiently large word length [8]. This is considered in more detail in the following section, where the analysis of the word error probability under iterative decoding for large N is done using density evolution.

V. Density Evolution in Presence of Block Fading

The evolution of message densities [22], [24] under iterative decoding is described through six evolution trees for a binary root-LDPC code. The evolution trees represent the local neighborhood of a bitnode in an infinite-length code whose graph has no cycles. Figs. 13, 14, and 15 show the local neighborhoods of classes $1i$ and $1p$. Similar evolution trees can be drawn for classes $2i$ and $2p$. Full diversity in the presence of fading is guaranteed, thanks to messages $1c \rightarrow 1i$ (respectively, $2c \rightarrow 2i$) as indicated in the proof of Proposition 7. Irregularity is defined in the standard way [23] through the polynomials $\lambda(x)$ and $\rho(x)$. Root-LDPC ensembles are a special case of multi-edge-type LDPC codes [24]. Nevertheless, we do not use the compact notation of multiedge-type codes as in [24, Ch. 7]. Indeed, root-LDPC codes have two specific properties which are not found in general ensembles.

- Nodes associated to information bits are clearly distinguished from those associated to parity bits. For each channel state, two classes must be created in order to separate parity nodes from information nodes.
- On a BF channel the root-LDPC ensemble is designed to ensure full diversity for information bits only. Hence, what mainly matters in Density Evolution is the convergence analysis of messages associated to information bits, mainly messages $1i \rightarrow 2c$ and $2i \rightarrow 1c$. This second property can be thought as an unequal error protection because parity bits will exhibit an average error probability with diversity order 1.

The following notations are used, where the superscript m is an integer denoting the decoding iteration order:

- $q_1^m(x)$ and $q_2^m(x)$: Probability density functions of log-ratio messages on the edges $1i \rightarrow 1c$ and $2i \rightarrow 2c$, respectively. See Fig. 13.
- $f_1^m(x)$ and $f_2^m(x)$: Probability density functions of log-ratio messages on the edges $1i \rightarrow 2c$ and $2i \rightarrow 1c$, respectively. See Fig. 14.

- $g_1^m(x)$ and $g_2^m(x)$: Probability density functions of log-ratio messages on the edges $1p \rightarrow 2c$ and $2p \rightarrow 1c$, respectively. See Fig. 15.
- Let $X_1 \sim p_1(x)$ and $X_2 \sim p_2(x)$ be two independent real random variables. The density function of $X_1 + X_2$ obtained by convolving the two original densities is written as $p_1(x) \otimes p_2(x)$. The notation $p(x)^{\otimes n}$ denotes the convolution of $p(x)$ with itself n times. The expression $\lambda(p(x))$ represents the density function $\sum_i \lambda_i p(x)^{\otimes i-1}$.
- Let $X_1 \sim p_1(x)$ and $X_2 \sim p_2(x)$ be two independent real random variables. The density function $p(y)$ of the variable $Y = 2\mathrm{th}^{-1}(\mathrm{th}(\frac{X_1}{2})\mathrm{th}(\frac{X_2}{2}))$ obtained through a checknode is written as $p_1(x) \odot p_2(x)$ and is called *R-convolution* [24]. The notation $p(x)^{\odot n}$ denotes the R-convolution of $p(x)$ with itself n times. The expression $\rho(p(x))$ represents the density function $\sum_i \rho_i p(x)^{\odot i-1}$.

The polynomial $\lambda(x)$ is replaced by $\tilde{\lambda}(x)$ each time an edge is isolated at the input of a bitnode. In addition, the polynomial $\rho(x)$ is replaced by $\tilde{\rho}(x)$ each time an edge is isolated at the input of a checknode. Also, the degree distribution of bitnodes and checknodes from a node perspective will be denoted by $\mathring{\lambda}(x)$ and $\mathring{\rho}(x)$, respectively. For regular ensembles, it is obvious that $\mathring{\lambda}(x) = \lambda(x)$, $\mathring{\rho}(x) = \rho(x)$, $\tilde{\lambda}(x) = \lambda(x)/x$, and $\tilde{\rho}(x) = \rho(x)/x$. Now, let d_b and d_c denote, respectively, the maximum left degree and the maximum right degree in the Tanner graph. If the original degree distribution polynomials are written as $\lambda(x) = \sum_{i=2}^{d_b} \lambda_i x^{i-1}$ and $\rho(x) = \sum_{j=2}^{d_c} \rho_j x^{j-1}$, then a straightforward edge counting in the Tanner graph leads to the general expressions of polynomials involved in the multiedge-type structure of root-LDPC ensembles

$$\begin{aligned}\mathring{\lambda}(x) &= \bar{d}_b \sum_{i=2}^{d_b} \lambda_i / i x^{i-1},\\ \mathring{\rho}(x) &= \bar{d}_c \sum_{j=2}^{d_c} \rho_j / j x^{j-1},\end{aligned} \tag{12}$$

and

$$\begin{aligned}\tilde{\lambda}(x) &= \frac{\bar{d}_b}{\bar{d}_b - 1} \sum_{i=1}^{d_b-1} i\lambda_{i+1}/(i+1)x^{i-1}\\ \tilde{\rho}(x) &= \frac{\bar{d}_c}{\bar{d}_c - 1} \sum_{j=1}^{d_c-1} j\rho_{j+1}/(j+1)x^{j-1}.\end{aligned} \tag{13}$$

where $\bar{d}_b = 1/\sum_{i=2}^{d_b} \lambda_i/i$ is the average degree of bitnodes and $\bar{d}_c = 1/\sum_{j=2}^{d_c} \rho_j/j$ is the average degree of checknodes. Keeping the above notations in mind, we can now state the density evolution equations for root-LDPC codes.

Proposition 8: Consider a nonergodic BF channel with $n_c = 2$. For fixed fading coefficients (α_1, α_2), the six density evolution equations of a $(\lambda(x), \rho(x))$ root-LDPC code are, for all m

$$\begin{aligned}q_1^{m+1}(x) &= \mu_1(x) \otimes \mathring{\lambda}(q_2^m(x) \odot \tilde{\rho}\,(f_e f_1^m(x) + g_e g_1^m(x)))\\ f_1^{m+1}(x) &= \mu_1(x) \otimes \tilde{\lambda}\,(q_2^m(x) \odot \tilde{\rho}\,(f_e f_1^m(x) + g_e g_1^m(x)))\\ &\qquad \otimes \mathring{\rho}\,(f_e f_2^m(x) + g_e g_2^m(x))\\ g_1^{m+1}(x) &= \mu_1(x) \otimes \lambda\,(q_2^m(x) \odot \tilde{\rho}\,(f_e f_1^m(x) + g_e g_1^m(x)))\end{aligned}$$

where the multi-edge-type fraction is

$$f_e = 1 - g_e = \frac{\bar{d}_b - 1}{2\bar{d}_b - 1}$$

and $\mu_1(x)$ is the Gaussian density at the output of the channel with fading α_1. The other three similar density evolution equations are obtained by permuting the two fading gains.

Proof: Let us carefully examine the set S_E of edges connecting $1i$ and $1p$ to $2c$ as in the Tanner graph of Fig. 10(a) that illustrates a regular root structure. For general irregular structures, the integers 2 and 3 indicating the number of edges should be replaced by degree distribution polynomials defined in (12) and (13), as clearly illustrated in the evolution trees in Figs. 13, 14, and 15. We have $S_E = S_{1i} \bigcup S_{1p}$, with $|S_{1p}|$ is the number of $1p-2c$ edges and $|S_{1i}| = \sum_i(\lambda_i|S_{1p}|/i)(i-1)$ is the number of $1i - 2c$ edges. Next, introduce the fraction f_e as

$$f_e = \frac{|S_{1i}|}{|S_{1i}| + |S_{1p}|} = \frac{\sum_i(i-1)\frac{\lambda_i}{i}}{\sum_i(i-1)\frac{\lambda_i}{i} + 1} = \frac{\bar{d}_b - 1}{2\bar{d}_b - 1}.$$

Now, the six density evolution equations can be directly derived from local neighborhoods of bitnodes in the graphical representation of the root-LDPC code. For example, as shown in Fig. 14, the message $f_1^{m+1}(x)$ is obtained by convolving the channel output density $\mu_1(x)$ with the outgoing message density from the set of $2c$ checknodes and then convolving with the single-edge density produced by $1c$ checknodes. Before applying the transformation $\tilde{\rho}()$ through $2c$ checknodes and the transformation $\mathring{\rho}()$ through $1c$ checknodes, input messages must be averaged via $f_e f_1^m(x) + g_e g_1^m(x)$ and $f_e f_2^m(x) + g_e g_2^m(x)$, respectively. ■

In the special case of regular root-LDPC ensembles, i.e., $\lambda(x)$ and $\rho(x)$ are monomials, density evolution will be described by four equations only since $\lambda(x) = \mathring{\lambda}(x)$ implies that $g_1^m(x) = q_1^m(x)$ and $g_2^m(x) = q_2^m(x)$, $\forall m$. A result on the ergodic threshold of regular ensembles follows.

Proposition 9: Consider an (ergodic) AWGN channel (i.e., assume $\alpha_1 = \alpha_2 = 1$). Under iterative decoding, a regular $(\lambda(x), \rho(x))$ root-LDPC code has the same decoding threshold as a random regular $(\lambda(x), \rho(x))$ LDPC code.

Proof: With the two fading gains equal to unity, the six evolution trees degenerate into a single tree, and all densities become identical: $q_1^m(x) = q_2^m(x) = f_1^m(x) = f_2^m(x) = g_1^m(x) = g_2^m(x)$ for any decoding iteration m. Thus, density evolution of a regular root-LDPC code reduces to a classical density evolution of a random code given by $p^{m+1}(x) = \mu(x) \otimes \lambda(\rho(p^m(x)))$, where $p^0(x) = \mu(x)$. ■

For irregular ensembles on the ergodic channel ($\alpha_1 = \alpha_2 = 1$), we have three distinct message densities $q_1^m(x) = q_2^m(x)$, $f_1^m(x) = f_2^m(x)$,, and $g_1^m(x) = g_2^m(x)$. It is difficult to determine the root-LDPC threshold as a function of the random ensemble threshold. Many numerical examples undertaken by the authors showed that there may be a slight loss in SNR, about 1 or 2 hundredths of a decibel. Surprisingly, in some irregular root-LDPC ensembles, there may be a slight gain in the ergodic

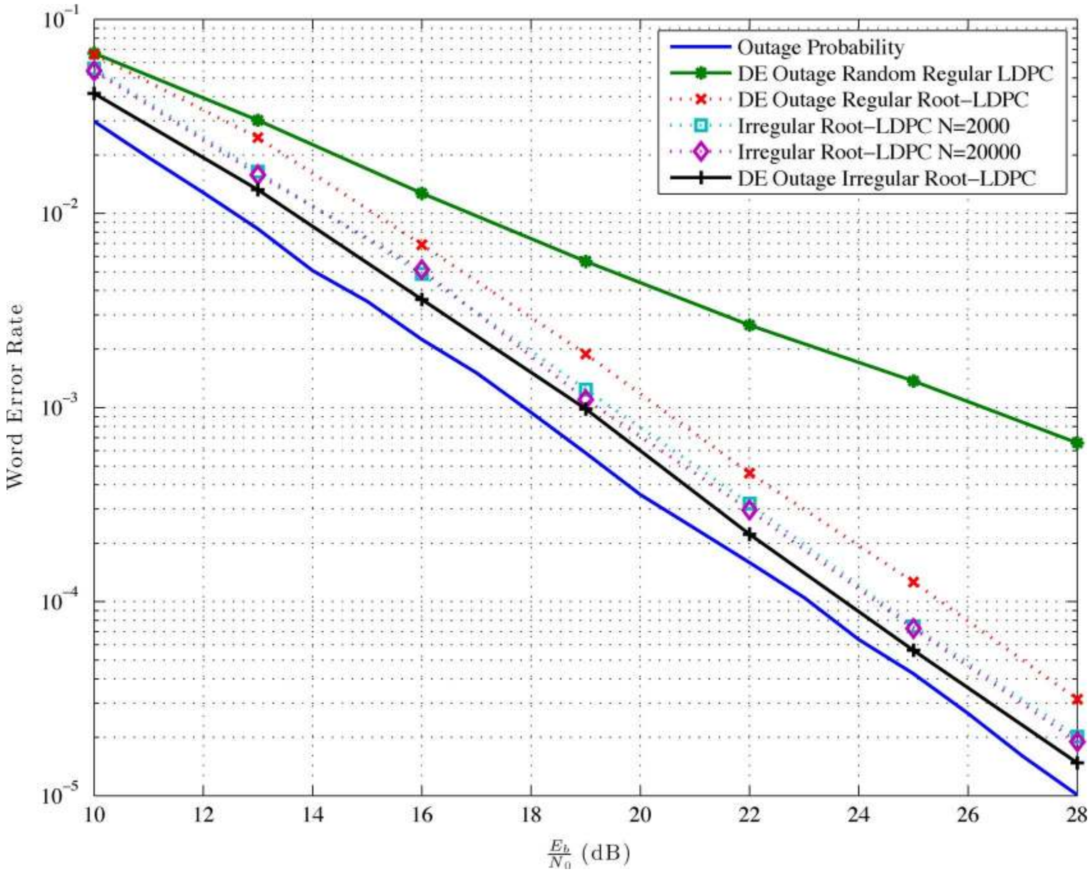

Fig. 16. Iterative decoding on a block-fading channel with $n_c = 2$. Density evolution of irregular root-LDPC and and its finite length performance. The irregular ensemble defined by (15) is also compared to a regular (3,6) ensemble and to the outage probability with BPSK.

threshold, about a couple of tenths of decibel. Thus, it should be possible to design root-LDPC codes for the block fading channel that are also efficient in the absence of fading. The irregular code given at the end of this section is one such example. A good ergodic threshold (i.e., an irregular LDPC structure) is also necessary to achieve near-outage performance on a nonergodic channel. Refer again to the outage boundary representation in the fading plane of Fig. 6. Let α_0 be the fading value defined by the intersection of the BPSK outage boundary and the ergodic line. For rate 1/2, this intersection point satisfies $I_b(\alpha_0^2 E_b/N_0) = 1/2$, where $I_b(x) \triangleq I_{\text{AWGN}}(Rx)$ is the average mutual information on an AWGN channel with a binary input and an SNR per bit equal to x.

Let α_{th} denote the fading value defined by the intersection of the LDPC code outage boundary and the ergodic line. Then we have

$$\alpha_{\text{th}}^2 = \frac{\left.\frac{E_b}{N_0}\right|_{\text{th}}}{\frac{E_b}{N_0}}$$

where $\frac{E_b}{N_0}|_{\text{th}}$ is the decoding threshold of the LDPC code over the ergodic AWGN channel. Finally, we obtain

$$\alpha_{\text{th}} = \alpha_0 \sqrt{\frac{\left.\frac{E_b}{N_0}\right|_{\text{th}}}{I_b^{-1}\left(\frac{1}{2}\right)}} = \alpha_0\sqrt{\Delta}$$

where Δ in the SNR gap separating the decoding threshold and the capacity limit on the Gaussian channel. To better understand the gain due to irregularity illustrated in Fig. 16, we evaluate the ratio $\alpha_{\text{th}}/\alpha_0$.

- For the regular (3,6) LDPC ensemble, the threshold is 1.10 dB over the Gaussian channel (ergodic line). Hence, $\alpha_{\text{th}}/\alpha_0 = 1.11$.
- For an irregular root-LDPC ensemble having a threshold of 0.38 dB over the Gaussian channel (ergodic line), we get $\alpha_{\text{th}}/\alpha_0 = 1.022$.

Using the best irregular code proposed in [23] with a threshold of 0.25 dB, we obtain $\alpha_{\text{th}}/\alpha_0 = 1.007$. Hence, with α_c/α_0 close to 1, the area between the outage capacity boundary and the code outage boundary is decreased in the neighborhood of the ergodic line. However, this does not ensure that, the code outage boundary would be close to the outage capacity boundary in the critical region between the ergodic line and the block-erasure channel. Therefore, in order to approach the outage probability limit, a full-diversity capacity-achieving code is necessary, but may not be sufficient. The numerical optimization of an ensemble degree distribution in order to fully match the BPSK outage boundary is outside the scope of this paper. Nevertheless, we describe below an irregular ensemble with excellent performance on the block-fading channel. Before completing this section with the irregular root-LDPC example, let us briefly describe how Proposition 8 is used to estimate the asymptotic performance.

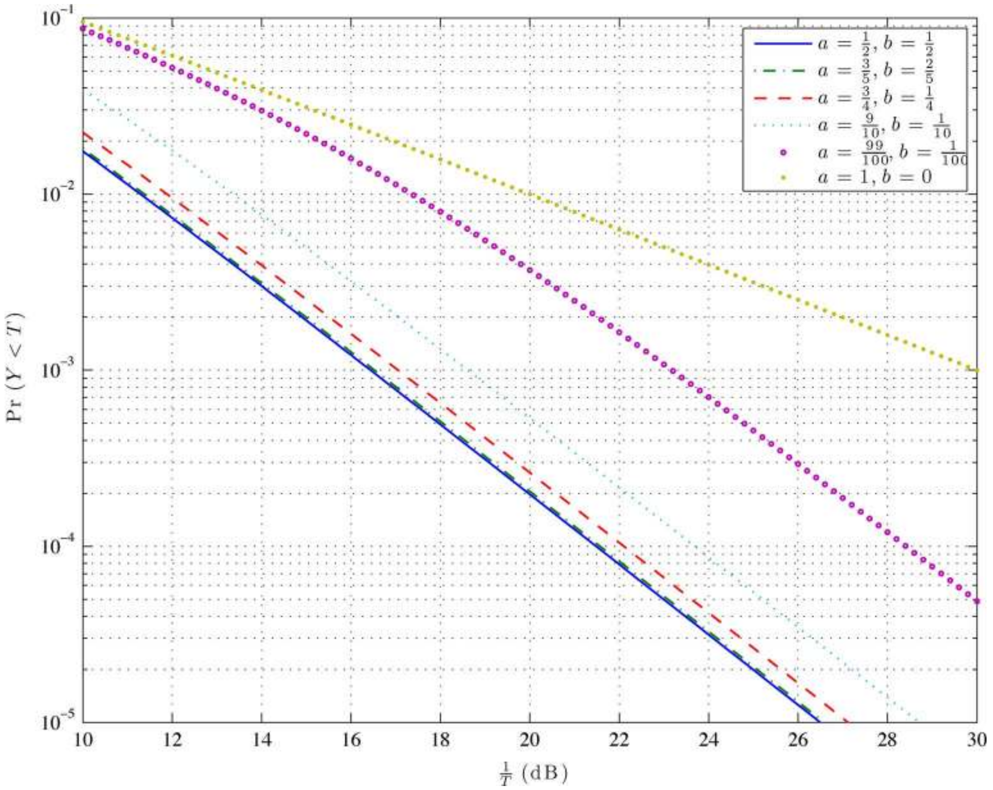

Fig. 17. Coding gain and diversity order of $Y = a\alpha_1^2 + b\alpha_2^2$ (χ^2 of fourth order) where α_1 and α_2 are Rayleigh distributed.

Let us assume that the root-LDPC ensemble is well defined, i.e., the pair $(\lambda(x), \rho(x))$ is given. Thanks to Proposition 8, for a fixed fading pair (α_1, α_2) it is possible to determine whether the information bit error probability converges to 0 or not. We refer to the event where the bit error probability does not converge to 0 by *Density Evolution Outage* (DEO). Thus, at a fixed SNR, it is possible to determine the probability of a Density Evolution Outage P_{DEO} by averaging over a sufficient number of fading instances. Now, it is possible to write the word error probability of the ensemble as

$$P_{\text{ew}} = P_{ew\,|\,\text{DEO}} \times P_{\text{DEO}} + P_{ew\,|\,\text{CONV}} \times (1 - P_{\text{DEO}}) \quad (14)$$

where $P_{ew\,|\,\text{DEO}}$ is the word error probability given a DEO event and $P_{ew\,|\,\text{CONV}}$ is the word error probability when DE converges. It is obvious that $P_{ew\,|\,\text{DEO}} = 1$. On the other hand, $P_{ew\,|\,\text{CONV}}$ depends on the speed of convergence of density evolution and the population expansion of the ensemble with the number of decoding iterations [13]. For any root-LDPC ensemble, we will simply use the following inequality directly derived from (14)

$$P_{\text{DEO}} \leq P_{\text{ew}}.$$

Thus, the performance estimated via density evolution is a lower bound for the word error probability.

Finally, we illustrate in Fig. 16 some performance results of an irregular rate-$1/2$ LDPC ensemble with the following degree distribution:

$$\lambda(x) = 0.285486x + 0.313850x^2 + 0.199606x^7 + 0.201058x^{14}, \quad \rho(x) = x^6. \quad (15)$$

On an ergodic Gaussian channel, the threshold of a random ensemble based on the above degree distribution is 0.63 dB. The root-LDPC ensemble based on the same degree distribution has a better threshold equal to 0.38 dB. The results shown in Fig. 16 can be compared to those of the best parallel turbo codes on block fading channels reported in [3], [4]. Our proposed root-LDPC codes compete favorably with turbo codes since the performance is within a 2-dB gap from the outage probability limit. Notice that the range of SNR on fading channels is 10 times larger than the standard scale of turbo and LDPC codes on ergodic Gaussian channels. Consequently, a 2-dB gap on the nonergodic channel is comparable to a 0.2-dB gap on the Gaussian channel.

VI. Conclusion

We have studied LDPC codes in the block-fading channel under both ML and iterative decoding. We have shown that constructions designed for ML decoders fail to guarantee diversity under iterative decoding. Driven by this restriction, we have introduced the new family of root-LDPC codes, which achieve full

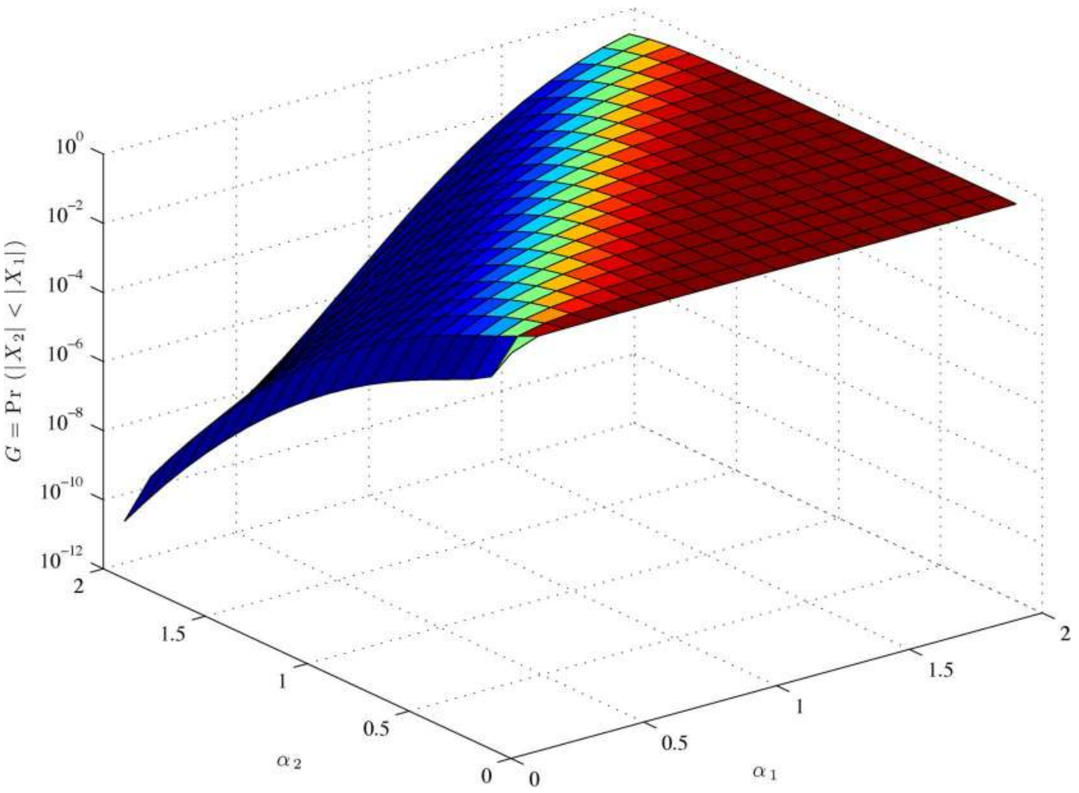

Fig. 18. 3-D plot of $G = \Pr(|X_2| < |X_1|)$ versus α_1 and α_2 for a variance $\sigma^2 = 1/10$.

diversity under iterative decoding. We have shown both finite- and infinite-length performance, and we have illustrated how the error-rate performance of root-LDPC is close to the outage probability limit and almost insensitive to the block-length. This makes root-LDPC codes attractive for slowly varying wireless communications scenarios.

Appendix I
Coding Gain of a Fourth-Order Unbalanced χ^2 Distribution

Here we limit our description to a diversity order of 2, but all results are easily extendable to rate-$1/n_c$ coding on a channel with diversity order n_c. In the context of ML decoding, the Euclidean distance between two codewords is proportional to $\omega_1\alpha_1^2 + \omega_2\alpha_2^2$. As fading α_i have a Rayleigh density, their squares are exponentially distributed, i.e., $p_{\alpha_i^2}(x) = e^{-x}$. The latter is a central χ^2 distribution of order 2 with parameter $\sigma^2 = 1/2$ [21]. Diversity 2 is achieved with a χ^2 distribution of order 4. Hence, a full-diversity code must satisfy $\omega_1 > 0$ and $\omega_1 > 0$ in order to get the order-4, χ^2 distributed, metric $\omega_1\alpha_1^2 + \omega_2\alpha_2^2$. Once maximum diversity is guaranteed, the maximization of the product $\omega_1\omega_2$ increases the coding gain.

The above simple facts are still valid in the context of iterative probabilistic decoding. Let Λ be the *a posteriori* probability log-ratio of a binary element. Achieving full diversity under iterative decoding is equivalent to letting Λ behave as the metric $Y = a\alpha_1^2 + b\alpha_2^2$, where a and b are two positive real numbers. The energy of Y is normalized, $a+b=1$. The exact mathematical expression relating Λ to Y depends on the type of iterative algorithm used for decoding, e.g., $\Lambda \propto Y + \nu$ where ν is an additive noise. To understand the influence of the product ab on the performance, one should study the error probability associated with Y, i.e., $P(Y < T) = F(a,b,T)$. When $a = b = 1/2$, the order-4 χ^2 distribution is balanced, and its probability density function is

$$p_Y(y) = 4ye^{-2y}. \quad (16)$$

When $a \neq b = 1 - a$, the order-4 χ^2 distribution is unbalanced, and its probability density function is

$$p_Y(y) = \frac{(e^{-y/a} - e^{-y/b})}{2a-1}. \quad (17)$$

The expression of $P(Y < T) = F(a,b,T)$ is obtained after integrating $p_Y(y)$. The diversity order and the coding gain embedded in Y appear when $T \ll 1$. For a balanced χ^2 distribution, we have

$$F(a,b,T) = 1 - e^{-2T}(1+2T) = 2T^2 + \mathrm{o}(T^2). \quad (18)$$

For an unbalanced χ^2 distribution, we obtain

$$F(a,b,T) = 1 - \frac{ae^{-T/a} - be^{-T/b}}{2a-1} = \frac{T^2}{2ab} + \mathrm{o}(T^2). \quad (19)$$

In Fig. 17, the performance function $F(a,b,T)$ is plotted versus $\gamma = 1/T$ on a double logarithmic scale for different values of

a and b. The slope is always 2 (i.e., $F(a,b,T) \propto 1/\gamma^2$) for all positive values of a and b. The function F degenerates to $T + \mathrm{o}(T)$ when $b = 0$ (diversity order equal to 1 instead of 2). Notice also that an unbalanced χ^2 distribution with $a = 3/4$ and $b = 1/4$ generates a coding loss about 0.65 dB. This loss is slightly higher (about 0.75 dB) when considering $P(\Lambda < 0)$ for $\Lambda \propto Y + \nu$ since additive noise depends on the fading coefficients as shown in Section IV.

Appendix II
Bidimensional Cumulative Density Function $G = \Pr(|X_2| < |X_1|)$

Consider two real independent Gaussian random variables $X_1 \sim \mathcal{N}(\alpha_1^2, \alpha_1^2\sigma^2)$ and $X_2 \sim \mathcal{N}(\alpha_2^2, \alpha_2^2\sigma^2)$. We define the multivariate function $G(\alpha_1, \alpha_2, \sigma^2) \triangleq \mathbb{P}(|X_2| < |X_1|)$. The G function is given by the integral expression

$$G = 1 - \int_0^{\infty} \frac{dt}{\sqrt{2\pi\alpha_1^2\sigma^2}} \left(e^{-\frac{(t-\alpha_1^2)^2}{2\alpha_1^2\sigma^2}} + e^{-\frac{(t+\alpha_1^2)^2}{2\alpha_1^2\sigma^2}} \right) \times \left(Q\left(\frac{t-\alpha_2}{\alpha_2\sigma}\right) + Q\left(\frac{t+\alpha_2}{\alpha_2\sigma}\right) \right) \quad (20)$$

where $Q(x)$ is the Gaussian tail function. A 3-D plot of G is illustrated in Fig. 18. The main properties of G are:

- $G(\alpha, \alpha, \sigma^2) = 1/2$ for all $\sigma^2 > 0$.
- G is a nondecreasing function of α_1 and a decreasing function of α_2. Hence, $G \leq 1/2$ if $\alpha_1 \leq \alpha_2$ and $G \geq 1/2$ if $\alpha_2 \leq \alpha_1$.
- For fixed σ^2 and α_2, $G \to 1$ as $\alpha_1 \to +\infty$.
- For fixed σ^2 and α_1, $G \to 0$ as $\alpha_2 \to +\infty$.

Acknowledgment

The authors would like to thank D. Duyck from Ghent University for his detailed and precious comments.

References

[1] E. Biglieri, *Coding for Wireless Channels*. New York: Springer, 2005.

[2] E. Biglieri, J. Proakis, and S. Shamai (Shitz), "Fading channels: Information-theoretical and communications aspects," *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2619–2692, Oct. 1998.

[3] J. J. Boutros, E. C. Strinati, and A. Guillén i Fàbregas, "Turbo code design for block fading channels," in *Proc. 2004 Allerton Conf. Commun., Contr. Comput.*, Monticello, IL, Sep. 2004 [Online]. Available: http://.josephboutros.org

[4] J. J. Boutros, A. Guillén i Fàbregas, and E. Calvanese Strinati, "Analysis of coding on non-ergodic channels," in *Proc. 2005 Allerton Conf. Commun., Contr. Comput.*, Monticello, IL, Sep. 2005 [Online]. Available: http://.josephboutros.org

[5] J. J. Boutros, G. M. Kraidy, and N. Gresset, "Near outage limit space-time coding for MIMO channels," in *Inaugural ITA Workshop*, San Diego, CA, Feb. 2006 [Online]. Available: http://.josephboutros.org, UCSD

[6] J. J. Boutros, "Diversity and coding gain evolution in graph codes," in *ITA Workshop*, San Diego, CA, Feb. 2009 [Online]. Available: http://.josephboutros.org, UCSD

[7] 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. Inf. Theory*, vol. 48, no. 6, pp. 1570–1579, Jun. 2002.

[8] A. Guillén i Fàbregas and G. Caire, "Coded modulation in the block-fading channel: Coding theorems and code construction," *IEEE Trans. Inf. Theory*, vol. 52, no. 1, pp. 91–114, Jan. 2006.

[9] A. Guillén i Fàbregas, "Coding in the block-erasure channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 11, pp. 5116–5121, Nov. 2006.

[10] S. Hirst and A. Burr, "Design of low density parity check codes for space–time coding," in *Proc. 3rd Int. Symp. Turbo Codes and Related Topics*, Brest, France, Sep. 1–5, 2003, pp. 315–318.

[11] J. Hou, P. H. Siegel, and L. B. Milstein, "Performance analysis and code optimization of low density parity-check codes on Rayleigh fading channels," *IEEE J. Sel. Areas Commun.*, vol. 19, no. 5, pp. 924–934, May 2001.

[12] X. Jin, A. W. Eckford, and T. E. Fuja, "Analysis of LDPC decoding for correlated and uncorrelated block fading channels," in *Proc. 2004 IEEE Int. Symp. Inf. Theory*, Chicago, IL, 2004.

[13] H. Jin and T. Richardson, "Block error iterative decoding capacity for LDPC codes," in *Proc. IEEE Int. Symp. Inf. Theory*, Adelaide, Australia, Sep. 2005.

[14] R. Knopp and P. A. Humblet, "On coding for block fading channels," *IEEE Trans. Inf. Theory*, vol. 46, no. 1, pp. 189–205, Jan. 2000.

[15] R. Koetter and P. O. Vontobel, "Graph covers and iterative decoding of finite-length codes," in *Proc. 3rd Int. Symp. Turbo Codes and Rel. Topics*, Brest, France, Sep. 1–5, 2003, pp. 75–82.

[16] A. Lapidoth, "The performance of convolutional codes on the block erasure channel using various finite interleaving techniques," *IEEE Trans. Inf. Theory*, vol. 40, no. 5, pp. 1459–1473, Sep. 1994.

[17] E. Malkamäki and H. Leib, "Evaluating the performance of convolutional codes over block fading channels," *IEEE Trans. Inf. Theory*, vol. 45, no. 5, pp. 1643–1646, Jul. 1999.

[18] E. Malkamäki and H. Leib, "Coded diversity on block-fading channels," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 771–781, Mar. 1999.

[19] K. D. Nguyen, A. Guillén i Fàbregas, and L. K. Rasmussen, "A tight lower bound to the outage probability of discrete-input block-fading channels," *IEEE Trans. Inf. Theory* vol. 53, no. 11, Nov. 2007 [Online]. Available: http://arxiv.org/abs/0707.1588

[20] L. H. Ozarow, S. Shamai (Shitz), and A. D. Wyner, "Information theoretic considerations for cellular mobile radio," *IEEE Trans. Veh. Technol.*, vol. 43, no. 2, pp. 359–378, May 1994.

[21] J. G. Proakis, *Digital Communications*, 4th ed. New York: McGraw-Hill, 2000.

[22] T. J. Richardson and R. L. Urbanke, "The capacity of low-density parity-check codes under message-passing decoding," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 599–618, Feb. 2001.

[23] T. J. Richardson, M. A. Shokrollahi, and R. L. Urbanke, "Design of capacity-approaching irregular low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, pp. 619–637, Feb. 2001.

[24] T. Richardson and R. Urbanke, *Modern Coding Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2008.

[25] D. N. C. Tse and P. Viswanath, *Fundamentals of Wireless Communication*. Cambridge , U.K.: Cambridge Univ. Press, 2005.

[26] S. Verdú and T. S. Han, "A general formula for channel capacity," *IEEE Trans. Inf. Theory*, vol. 40, no. 4, pp. 1147–1157, Jul. 1994.

[27] Z. Wang and G. B. Giannakis, "A simple and general parameterization quantifying performance in fading channels," *IEEE Trans. Commun.*, vol. 51, no. 8, pp. 1389–1398, Aug. 2003.

Joseph Jean Boutros (M'94–SM'09) received the M.S. degree in electrical engineering in 1992 and the Ph.D. degree in 1996, both from Ecole Nationale Supérieure des Télécommunications (ENST, Telecom ParisTech), Paris, France.

From 1996 to 2006, he was with the Communications and Electronics Department, ENST, as an Associate Professor. He was also a member of the research unit UMR-5141 of the French National Scientific Research Center (CNRS). In 2007, he joined Texas A&M University at Qatar (TAMUQ) as a full Professor in the electrical engineering program. He has been a scientific consultant for Alcatel Espace, Philips Research, and Motorola Semiconductors, and was a member of the Digital Signal Processing team of Juniper Networks Cable. His fields of interest are codes on graphs, iterative decoding, joint source-channel coding, space-time coding, and lattice sphere packings.

Albert Guillén i Fàbregas (S'01–M'05–SM'09) was born in Barcelona, Catalunya, Spain, in 1974. He received the telecommunication engineering degree and the electronics engineering degree from the Universitat Politècnica de Catalunya, Barcelona, and the Politecnico di Torino, Torino, Italy, respectively, in 1999, and the Ph.D. degree in communication systems from Ecole Polytechnique Fédérale de Lausanne (EPFL), Lausanne, Switzerland, in 2004.

From August 1998 to March 1999, he conducted his Final Research Project at the New Jersey Institute of Technology, Newark, NJ. He was with Telecom Italia Laboratories, Italy, from November 1999 to June 2000, and with the European Space Agency (ESA), Noordwijk, The Netherlands, from September 2000 to May 2001. During his doctoral studies, from 2001 to 2004, he was a Research and Teaching Assistant with the Institut Eurécom, Sophia-Antipolis, France. From June 2003 to July 2004, he was a Visiting Scholar with EPFL. From September 2004 to November 2006, he was a Research Fellow with the Institute for Telecommunications Research, University of South Australia, Mawson Lakes. Since 2007, he has been a Lecturer with the Department of Engineering, University of Cambridge, Cambridge, U.K., where he is also a Fellow of Trinity Hall. He has held visiting appointments with Ecole Nationale Supérieure des Télécommunications (ENST), Paris, France; Texas A&M University, Doha, Qatar; Universitat Pompeu Fabra, Barcelona, Spain; and the University of South Australia. His research interests are in communication theory, information theory, coding theory, digital modulation, and signal processing techniques with wireless applications.

Dr. Guillén i Fàbregas is currently an Editor of the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. He received a pre-Doctoral Research Fellowship of the Spanish Ministry of Education to join ESA. He received the Young Authors Award of the 2004 European Signal Processing Conference EUSIPCO 2004, Vienna, Austria, and the 2004 Nokia Best Doctoral Thesis Award in Mobile Internet and 3rd Generation Mobile Solutions from the Spanish Institution of Telecommunications Engineers. He is also a member of the ARC Communications Research Network (ACoRN) and a Junior Member of the Isaac Newton Institute for Mathematical Sciences.

Ezio Biglieri (M'73–SM'82–F'89–LF'10) was born in Aosta, Italy. He received the Dr. Engr. degree in 1967 in electrical engineering from the Politecnico di Torino, Torino, Italy.

He is presently an Adjunct Professor of Electrical Engineering at the University of California, Los Angeles (UCLA), and an honorary Professor with the Universitat Pompeu Fabra, Barcelona, Spain. Previously, he was a Professor with the University of Napoli, Napoli, Italy, with the Politecnico di Torino, and with UCLA. He has held visiting positions with the Department of System Science, UCLA; the Mathematical Research Center, Bell Laboratories, Murray Hill, NJ; Bell Laboratories, Holmdel, NJ; the Department of Electrical Engineering, UCLA; the Telecommunication Department of The Ecole Nationale Supérieure des Télécommunications, Paris, France; the University of Sydney, Australia; the Yokohama National University, Japan; the Electrical Engineering Department, Princeton University, Princeton, NJ; the University of South Australia, Adelaide; the University of Melbourne, Australia; the Institute for Communications Engineering, Munich Institute of Technology, Germany; the Institute for Infocomm Research, National University of Singapore; the National Taiwan University, Taipei, Taiwan, R.O.C.; the University of Cambridge, U.K.; and ETH Zurich, Switzerland.

Prof. Biglieri was elected three times to the Board of Governors of the IEEE Information Theory Society, and he served as its President in 1999. He was the Editor-in-Chief of the IEEE TRANSACTIONS ON INFORMATION THEORY and is the Editor-in-Chief of the *Journal of Communications and Networks*. Among other honors, in 2000, he received the IEEE Third-Millennium Medal and the IEEE Donald G. Fink Prize Paper Award, in 2001 the IEEE Communications Society Edwin Howard Armstrong Achievement Award, and a Best Paper Award from WPMC01, Aalborg, Denmark, and in 2004, the *Journal of Communications and Networks* Best Paper Award.

Gilles Zémor (M'92) was born in Paris, France, in 1963. He received the Agrégation de Mathmatiques degree in 1984, the Ph.D. degree in computer science from Ecole Nationale Supérieure des Télécommunications (ENST), Paris, France, in 1989, and the Habilitation Diriger des Recherches degree in mathematics from Paris 6 University, in 2002.

From 1990 to 2006, he was an Associate Professor with the Computer Science and Network Department, ENST. Since 2006, he has been a Professor with the Mathematics Institute of Bordeaux University, Bordeaux, France. His research interests include combinatorial mathematics, coding theory, additive number theory, and cryptography.

Prof. Zémor was an Associate Editor for Coding Theory for the IEEE TRANSACTIONS ON INFORMATION THEORY from 2003 to 2006.