Design and Analysis of Low-Density Parity-Check Codes for Block-Fading Channels

Joseph J. Boutros
ENST
Paris, France
boutros@ieee.org

Albert Guillén i Fàbregas
University of Cambridge
Cambridge, UK
guillen@ieee.org

Ezio Biglieri
Universitat Pompeu Fabra
Barcelona, Spain
e.biglieri@ieee.org

Gilles Zémor
University of Bordeaux 1
Bordeaux, France
zemor@math.u-bordeaux1.fr

***Abstract*— We solve the problem of designing powerful low-density parity-check (LDPC) codes with iterative decoding for the block-fading channel. We present a new family of full-diversity LDPC codes that exhibit near outage limit performance. This family competes with multiplexed parallel turbo codes suitable for non-ergodic channels and recently reported in the literature.**

I. Introduction

The block-fading channel, first introduced in [14] and further elaborated in [1], is a channel model which is particularly relevant in wireless communications situations involving slow time-frequency hopping (e.g., cellular networks and wireless Ethernet) or multicarrier modulation using orthogonal frequency division multiplexing (OFDM). Therefore, the design of error-correcting codes for such channels is a relevant and challenging problem. The outage probability defines the information-theoretical limit on such non-ergodic wireless channels and cannot be surpassed by the word error probability of any coding scheme [14][1]. Classical random-like capacity-achieving graph codes cannot approach the outage limit and specifically designed codes become a must.

Two main parameters characterize the error rate performance on block-fading channels: the diversity order and the coding gain. The diversity order defines the slope of the error-rate curve as a function of the signal-to-noise ratio on a double logarithmic scale. 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 given by the slope of the outage limit. When full diversity is attained, the coding gain yields a measure of signal-to-noise ratio distance to the outage limit.

It has been proven in [6] that the optimal achievable diversity order with discrete input constellations is given by the Singleton bound [13][10]. Coding schemes achieving the Singleton bound are termed blockwise maximum-distance separable (MDS). Blockwise MDS codes are outage-achieving over the (noiseless) block-erasure channel [7]. However, blockwise MDS codes are only necessary, but not sufficient to achieve the outage probability limit in noisy block-fading channels.

Recently, a near-outage coding scheme has been proposed based on a special permutation, the so-called *h-π-diagonal multiplexer* [3][4][5], in conjunction with parallel turbo codes. Multiplexers for convolutional and turbo codes [3] appeared one decade after the analysis of random and periodic interleaving of convolutional codes on the block-erasure channel [12]. Random ensembles of low-density parity-check codes designed for ergodic additive white gaussian noise channels [17][9], despite the excellent decoding threshold of their irregular structures, are not full-diversity, and hence exhibit a poor performance in presence of block-fading. Repeat-accumulate codes that allocate bits to different channel states are full-diversity [6], but they suffer from a poor coding gain and cannot compete with multiplexed turbo codes.

In this work, we design a new family of LDPC codes based on a special type of checknodes called *rootchecks*. These *root-LDPC* codes are maximum-distance separable. Under iterative message passing decoding, they achieve the outage probability limit on block-erasure channels and they perform close to that limit on Rayleigh block-fading channels.

The paper is organized as follows. Section II introduces the channel model and the notations. LDPC codes with full diversity under Maximum Likelihood (ML) decoding are discussed in section III. The new family of root-LDPC codes suited for iterative decoding is described in the fourth section. Section V presents the density evolution analysis of root-LDPC in presence of block fading. The conclusions are finally drawn in section VI.

II. Channel Model and Notations

We consider codewords of length N bits transmitted on a block-fading channel with n_c fading coefficients per codeword. The length N is taken to be a multiple of n_c. Let $\ell = N/n_c$ be the number of bits per fading block and let $[r]$ denote the integer part of a real r. Then, the received signal for a transmitted symbol x_i is

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

where $y_i \in \mathbb{R}$, $i = 1 \dots N$, and $j = 1 + [\frac{i-1}{\ell}]$. The positive real number α_j is the fading coefficient at block j, $j = 1 \dots n_c$. The symbols x_i belong to 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 $z_i \sim \mathcal{N}(0, \sigma^2)$, $\sigma^2 = \frac{N_0}{2}$. We assume perfect channel state information (CSI) at the receiver and that the channel coefficients 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

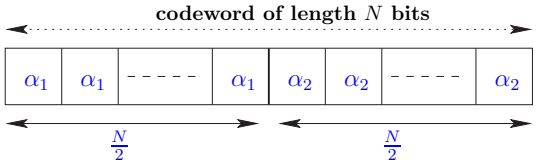

Fig. 1. Codeword representation for a block-fading channel with $n_c = 2$ states. Fading coefficients are independent from one codeword to another.

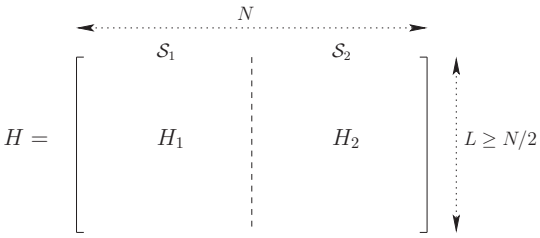

Fig. 2. Parity-check matrix notations for a block-fading channel with $n_c = 2$ states. The $L - N/2$ extra rows are added in order to enhance the coding gain of a full-diversity code.

per symbol is given by $\gamma = \frac{E_s}{N_0}$ and the average SNR per bit is $\frac{E_b}{N_0} = \gamma/R$. Fig. 1 gives an illustration for $n_c = 2$ and $\ell = N/2$.

In this work, we consider linear binary codes $C(N, K)_2$ of length N, dimension K, and rate $R = \frac{K}{N} \leq \frac{1}{n_c} \leq \frac{1}{2}$. The code C is defined by its $L \times N$ parity-check matrix H. The graph representation of C has L single-parity checknodes. It is assumed that H has always full rank L, i.e. $R = 1 - \frac{L}{N}$.

For a given non-zero codeword $c \in C$, we define the Hamming weight vector $(\omega_1, \ldots, \omega_{n_c})$, where ω_j is the partial Hamming weight of coded bits undergoing fading α_j. We also define the minimum partial Hamming weight as

$$\omega^\star = \min_{c \in C - \{0\}} (\omega_1, \ldots, \omega_{n_c}).$$

Definition 1: An error-correcting code is said to be *full-diversity* if $\omega^\star > 0$.

The highest achievable rate for a full-diversity code is $R = \frac{1}{n_c}$ determined from the Singleton bound [13][10][6]. Furthermore, the word error probability of a n_c-diversity code decreases as $1/\gamma^{n_c}$ at high SNR [15].

The block-fading channel is not information stable [19], and therefore its Shannon capacity is zero since there is an irreducible probability that the decoder makes a *word error*. In the limit of large block length, this probability is the *information outage probability* defined as [14][1]

$$P_{\text{out}}(\gamma, R) = \Pr\{\mathcal{I}(\gamma, \boldsymbol{\alpha}) < R\} \tag{2}$$

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

$$\mathcal{I}(\gamma, \boldsymbol{\alpha}) = \frac{1}{n_c} \sum_{i=1}^{n_c} I_{\text{AWGN}}(\gamma \alpha_i^2), \tag{3}$$

$I_{\text{AWGN}}(s)$ is the input-output mutual information of an AWGN channel with SNR s per symbol. The block-fading channel is also commonly referred to as *non-ergodic* since, as n_c does not tend to infinity, $\mathcal{I}(\gamma, \boldsymbol{\alpha})$ is a random variable.

The information outage probability $P_{\text{out}}(\gamma, R)$ represents the best achievable word error rate for large enough word length. Therefore, any code aiming at approaching $P_{\text{out}}(\gamma, R)$ should have a word error probability that, for large enough length, becomes *independent* of the code length [4][6].

Unless otherwise stated, we will focus our study to a coding rate $R = 1/2$ (or slightly smaller than $1/2$) and a non-ergodic Rayleigh fading channel with $n_c = 2$ states per codeword, as depicted in Figures 1 and 2. Most of our results are easily extendable to $n_c \geq 3$ and $R \leq 1/3$.

III. Full-diversity LDPC codes under Maximum Likelihood decoding

In this section, we study LDPC codes in presence of block-fading under maximum likelihood decoding. It is shown that designing full-diversity LDPC codes under ML decoding is straightforward. Although ML decoding is unfeasible in practice, it gives a valuable insight for the coding structure suitable for non-ergodic channels. This section terminates with the negative result that ML-designed full-diversity codes, under iterative decoding, fail to guarantee diversity due to badly located pseudo-codewords.

Following the notations given in the previous section, the $L \times N$ parity-check matrix H is written as $H = [H_1 \mid H_2]$. The left and right parts H_1 and H_2 are $L \times \frac{N}{2}$. The vector space generated by the $\frac{N}{2}$ left columns is denoted $\mathcal{S}_1$. Similarly $\mathcal{S}_2$ is the vector space generated by the $\frac{N}{2}$ right columns.

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

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

The full-rank property of the above proposition has been firstly published in [8]. Its extension to coding rate $1/3$ with $H = [H_1 \mid H_2 \mid H_3]$ is obtained by imposing that all matrices $[H_1 \mid H_2]$, $[H_1 \mid H_3]$, and $[H_2 \mid H_3]$ have a full rank. Generalization to $R = \frac{1}{n_c}$ is straightforward.

Proposition 2: Consider a binary code C with rate $R = \frac{1}{2}$, i.e. $L = K = N/2$. If C is full-diversity then $\omega^\star = 1$.

Proof: If C is full-diversity then $\dim \mathcal{S}_1 = \dim \mathcal{S}_2 = \frac{N}{2}$. 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 non-zero 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 partial Hamming weight must be increased in order to improve the coding gain of C. Proposition 2 suggests that the only solution is to slightly decrease the coding rate.

For example, adding two extra rows to H yields $\omega^\star = 2$ under ML decoding.

Proposition 3: Consider a binary code C with rate $R \leq 1/2$. If C is full-diversity then $R = \frac{1}{2} - \frac{2}{N}$ attains $\omega^\star = 2$.

Proof: The proof is based on the special parity-check matrix structure given in Fig. 3. Adding a single parity checknode to all columns of H_1 and another checknode to all columns of H_2 makes $\omega^\star \geq 2$. Proposition 4 proves that $\omega^\star$ cannot exceed 2 by the addition of 2 extra rows only. ■

The price of $\omega^\star = 2$ is negligible for large code length N. If we now require $\omega^\star = 3$ we have the following result.

Proposition 4: Consider a binary code C with rate $R \leq 1/2$. If $\omega^\star = 3$ then $R \leq \frac{1}{2} - \frac{\log_2(N/2)}{N}$.

Proof: Let $h_1, h_2 \in \mathcal{S}_1$ be two distinct columns in H_1. If $\omega^\star = 3$ then $h_1 + h_2$ does not belong to $\mathcal{S}_2$. Hence h_1 must not belong to $h_2 + \mathcal{S}_2$. This is possible only if 2^L is greater than $|h_2 + \mathcal{S}_2| = \frac{N}{2} \times 2^{N/2}$. ■

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

Proof: The proof is trivial. Such a code is defined by the parity-check matrix depicted in Fig. 4. The presence of a Hamming code whose minimum distance is 3 prevents a partial Hamming weight equal to 2. ■

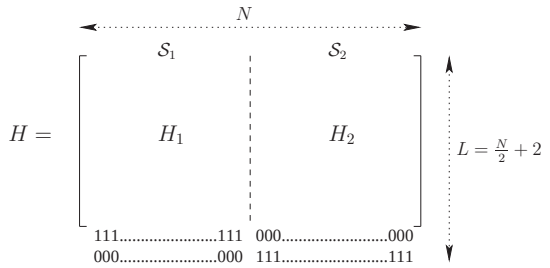

Fig. 3. ML-designed full-diversity LDPC code with $\omega^\star = 2$.

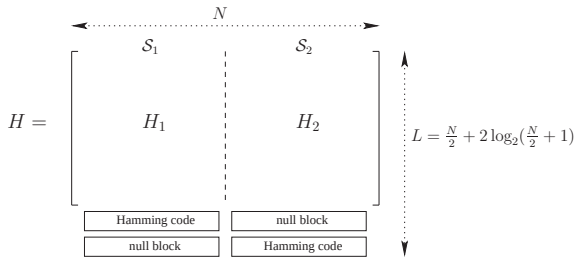

Fig. 4. ML-designed full-diversity LDPC code with $\omega^\star \geq 3$.

We now show the word error rate performance of ML-designed full-diversity LDPC codes and compare it to the outage capacity limit. The results are illustrated in Figure 5 for $n_c = 2$, and the $(3, 6)$ ensemble using the constructions outlined above. As we can see, under iterative decoding, an ML-designed LDPC code does not guarantee diversity and shows a unit slope. This is caused by pseudo-codewords [11] whose support is restricted to H_1 or H_2. Hence, the minimum partial pseudo-weight is zero when iterative belief propagation decoding is applied. On the other hand, full diversity is guaranteed when a fake ML decoder is used.

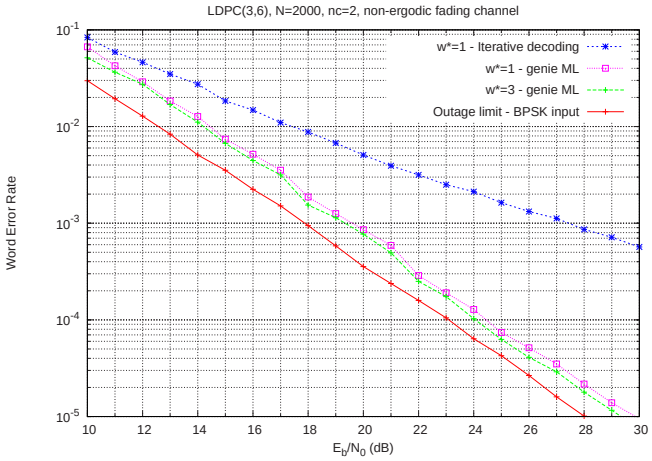

Fig. 5. Rate $1/2$ ML-designed LDPC codes with iterative decoding on a Rayleigh block-fading channel. A random LDPC code (not shown above) performs as poor as an ML-designed code with $\omega^\star = 1$. The genie ML is a fake decoder that knows if errors occur on H_1 or H_2 positions.

IV. Full-diversity LDPC codes for iterative belief propagation decoding

The design of low-density parity-check codes suitable for iterative decoding is based on graphical tools [2][18]. The graphical representation can then be translated into a matrix description or a log-ratio probability density evolution.

The solution is simple when starting to solve an extremal case. Let us assume that the fading coefficients α_i belong to the set $\{0, +\infty\}$. In this case, the block-fading channel is converted into a block-erasure channel. The reader may refer to Fig. 6 where the outage boundaries are illustrated (see [4] for more details).

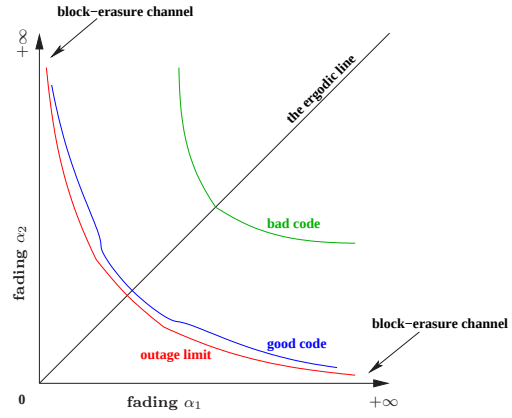

Fig. 6. Outage boundaries in the fading plane for a 2-state block-fading channel. Two conditions are necessary in order to approach the outage limit: a- Reducing the gap on the ergodic line requires an excellent decoding threshold, b- Reducing the gap at infinity requires a full-diversity code (Maximum Distance Separable) on a block-erasure channel.

Our approach is to find a graph construction with bitnodes and checknodes such that the connecting edges guarantee full diversity. For simplicity, we consider the case of the $(3,6)$ LDPC ensemble with $n_c = 2$. Generalizations to other degree distributions and rates will be treated further on. The reader is referred to Fig. 7 for more details on the notation employed in this section. Two examples of local graphs where diversity is not guaranteed are shown in Fig. 8. The checknodes defining an LDPC code are single-parity check codes, and hence they cannot afford more than one erased bit. For example, if $\alpha_1 = 0$ then the checknodes in Fig. 8 are not able to recompute the erased bit because it is connected to bitnodes which are also erased (i.e., undergoing 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 permuting the two fading coefficients yields an equivalent design.

The two unique local graphs that guarantee full diversity in presence of block erasures are drawn 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, and then we generalize to any $(\lambda(x), \rho(x))$ degree distribution [17]. A checknode Φ connected to bits $\vartheta_1, \vartheta_2, \ldots, \vartheta_6$ is written as $\Phi(\vartheta_1, \vartheta_2, \ldots, \vartheta_6)$.

Definition 2: Let ϑ be a binary element transmitted on fading α_1. A rootcheck of type 1 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.

We define similarly rootchecks of type 2.

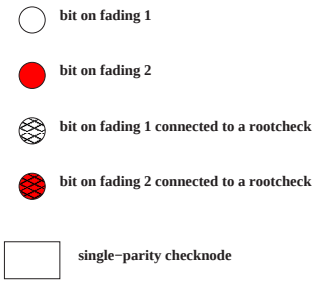

Fig. 7. Notations for graph representation.

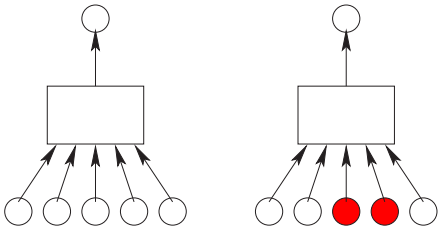

Fig. 8. Two examples of bad configurations under belief propagation decoding on a block-fading channel.

Using definition (2), we consider a rate $1/2$ LDPC code of length N. Information bits are splitted into two classes,

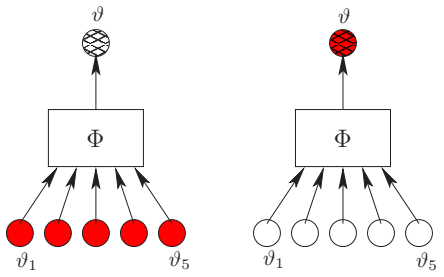

Fig. 9. The two unique good configurations (rootchecks) under belief propagation decoding on a block-fading channel.

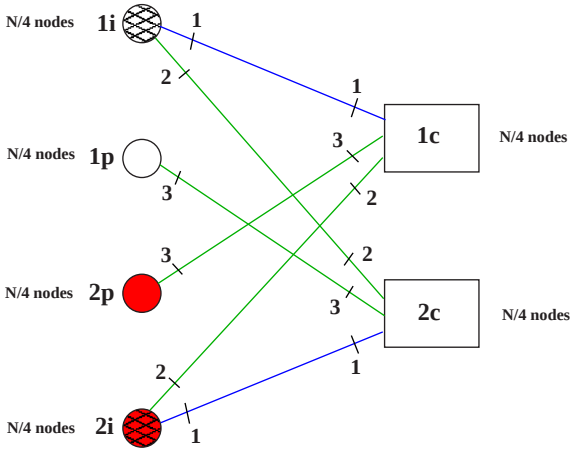

Fig. 10. Tanner graph for a regular (3,6) root-LDPC code of rate $1/2$. An irregular structure $(\lambda(x), \rho(x)$ can be easily plugged on edges connected to non-root checknodes.

$N/4$ bits called $1i$ are transmitted on α_1 and $N/4$ bits called $2i$ are transmitted on α_2. Parity bits are also partitioned into two sets $1p$ 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 abandoned. This design produces the bipartite Tanner graph drawn in Fig. 10. Its extension to rate $1/3$ is portrayed in Fig. 12. Integers positioned near 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 given in Fig. 11. The $N/4 \times N/4$ identity matrix is written twice in connections $1i \leftrightarrow 1c$ and $2i \leftrightarrow 2c$. Two all-zero

$$H = \begin{array}{c} \begin{array}{cccc} 1i & 1p & 2i & 2p \end{array} \\ \left[\begin{array}{cccc} \mathbf{1} & \mathbf{0} & H_{2i} & H_{2p} \\ H_{1i} & H_{1p} & \mathbf{1} & \mathbf{0} \end{array}\right] \end{array} \begin{array}{l} 1c \\ 2c \end{array}$$

Fig. 11. Parity-check matrix for a regular (3,6) root-LDPC code of rate $1/2$.

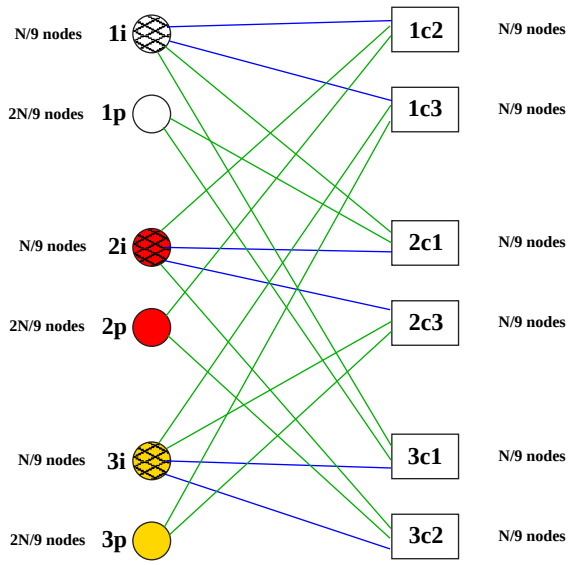

Fig. 12. Tanner graph for a regular (4,6) root-LDPC code of rate 1/3. The introduction of any $(\lambda(x), \rho(x)$ irregularity is always possible on edges connected to non-root checknodes.

$N/4 \times N/4$ sub-matrices prohibit any edge of type $1p \leftrightarrow 1c$ and $2p \leftrightarrow 2c$. The other 4 sub-matrices 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 sub-matrices H_{1i}, H_{2i}, H_{1p}, and H_{2p}. Equivalently, the degree distribution changes the distribution of edges connected to non-rootchecks 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 $R = \frac{1}{2}$ root-LDPC code with degree distribution $(\lambda(x), \rho(x))$ transmitted on a 2-state block-erasure channel. Then, under iterative message passing decoding, the root-LDPC code is full-diversity.

Proof: The two fading coefficients α_1 and α_2 are independent and take two possible values $\{0, +\infty\}$. Examinig the Tanner graph in Fig. 10, we observe that only outage event occurs when $\alpha_1 = \alpha_2 = 0$ (both blocks erased). Indeed, when $\alpha_1 = 0$ and $\alpha_2 = +\infty$, it is straighdforward 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 of α_i being equal to 0. From the proof of proposition (6) above, we find that the outage probability of a root-LDPC code is ϵ^2, i.e. the code attains the outage limit of the block-erasure channel. In general, it has been shown in [7] that a full-diversity code on a block-erasure channel is outage achieving.

Now we study the general case of Rayleigh block-fading. Some simple facts from communication theory on the 4th order χ^2 distribution are exposed in Appendix A. In the sequel, we use the notations of Appendix A when analyzing the diversity metric in log-ratio messages.

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

Proof: As indicated in the design of a root-LDPC 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 trivial.

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

$$\Lambda^e = 2 \ \text{th}^{-1}\left(\prod_i \text{th}\left(\frac{\Lambda_i^a}{2}\right)\right) \tag{4}$$

where $\text{th}(x)$ is 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 sub-optimal belief propagation decoder is able to achieve diversity order 2. Therefore, if a sub-optimal decoder achieves full-diversity, the optimal decoder also achieves full-diversity. We consider the min-sum decoder. The output message produced by a checknode Φ is now approximated by

$$\Lambda^e = \min(|\Lambda_i^a|) \prod_i \text{sign}(\Lambda_i^a) \tag{5}$$

a) First decoding iteration: We first study the output after one decoding iteration. The all-zero codeword is assumed to be transmitted. The channel cross-over probability associated to 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

$$\Lambda_0 = \log\left(\frac{p(y|\vartheta = 0, \alpha)}{p(y|\vartheta = 1, \alpha)}\right) = \frac{2\alpha y}{\sigma^2} = \frac{2}{\sigma^2}(\alpha^2 + \alpha z) \tag{6}$$

where $y = \alpha + z$ and $z \sim \mathcal{N}(0, \sigma^2)$ (assuming $E_s = 1$). At the first decoding iteration, all input messages Λ_i^a in (5) have an expression identical to (6).

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 non-rootchecks 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 (5). Input messages to the rootcheck are negative with probability ϵ_2. Then

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

where

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

We obtain

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

The partial *a posteriori* log-ratio message becomes

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

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

b) Further decoding iterations: As can be seen from the decoding tree of a bitnode $1i$ in Fig. 15 the diversity order 2 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. The density of message $\Lambda_0 + \Lambda_1^e$ can only be upgraded with respect to the first iteration. Hence, full diversity is preserved. ■

The proof of the previous proposition is based in 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, $i = 1 \ldots 3$ 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 Figures 10 and 16. 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 satsifies

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

where the function G is defined in Appendix B. On the opposite, 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. Despite the presence (with a non-zero 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.

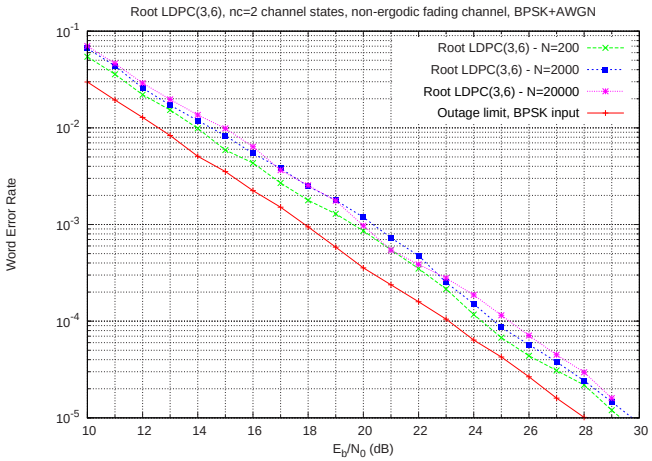

Fig. 13. Regular (3,6) root-LDPC codes with iterative decoding on a 2-state Rayleigh block-fading channel. Word error rate is measured on information bits. 100 erroneous words have been counted for each point.

Finally, we look at the minimum partial Hamming weight $\omega^\star$ under belief propagation decoding.

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 $\delta_b - 1$ non-root 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 $\delta_b \alpha_1^2 + \alpha_2^2$. Hence, the equivalent $\omega^\star$ parameter under iterative decoding is 1. ■

In Fig. 13, 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 also observed with repeat-accumulate codes [6] and parallel turbo codes [3][4][5].

V. Density evolution in presence of block-fading

The evolution of message densities [16][18] under iterative decoding is described with the means of six evolution trees for a binary root-LDPC code. The evolution trees represent the local neighbourhood of a bitnode in an infinite length code without graph cycles. Figures 14, 15, and 16 show the local neighbourhoods of classes $1i$ and $1p$. Similar evolution trees can be drawn for classes $2i$ and $2p$. Full-diversity is guaranteed in presence of fading thanks to messages $1c \to 1i$ (resp. $2c \to 2i$) as indicated in the proof of proposition 7. Irregularity is defined by the standard polynomials $\lambda(x)$ and $\rho(x)$ [17]. The polynomial $\lambda(x)$ is replaced by $\tilde{\lambda}(x) = \lambda(x)/x$ each time an edge is isolated at the input of a bitnode. In addition, the polynomial $\rho(x)$ is replaced by $\tilde{\rho}(x) = \rho(x)/x$ each time an edge is isolated at the input of a checknode. The following notations are used in root-LDPC density evolution where the superscript integer m denotes the decoding iteration:

- $q_1^m(x)$ 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. 14.
- $f_1^m(x)$ 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. 15.
- $g_1^m(x)$ 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. 16.
- 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 $Y = 2th^{-1}(th(\frac{X_1}{2})th(\frac{X_2}{2}))$ obtained through a checknode is written as $p_1(x) \odot p_2(x)$ and is called *R-convolution*. 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 $\sum_i \rho_i \, p(x)^{\odot i-1}$.

Proposition 8: Consider an ergodic additive white gaussian noise channel (i.e. $\alpha_1 = \alpha_2 = 1$). Under iterative decoding, a $(\lambda(x), \rho(x))$ root-LDPC code has the same decoding threshold as a random $(\lambda(x), \rho(x))$ LDPC code.

Proof: The two fading coefficients are equal to unity. One can notice that the six evolution trees degenerate to a unique 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 root-LDPC code reduces to a classical density evolution of a random code given by $p^{m+1}(x) = \lambda(\rho(p^m(x)))$. ■

Proposition 9: Consider a non-ergodic block-fading channel with two states. For fixed fading coefficients (α_1, α_2), density evolution equations of a $(\lambda(x), \rho(x))$ root-LDPC code are

$$\begin{aligned} q_1^{m+1}(x) &= \mu_1(x) \\ &\quad \otimes \lambda\left(q_2^m(x) \odot \tilde{\rho}\left(f_e \; f_1^m(x) + g_e \; g_1^m(x)\right)\right) \\ f_1^{m+1}(x) &= \mu_1(x) \\ &\quad \otimes \tilde{\lambda}\left(q_2^m(x) \odot \tilde{\rho}\left(f_e \; f_1^m(x) + g_e \; g_1^m(x)\right)\right) \\ &\quad \otimes \rho\left(f_e \; f_1^m(x) + g_e \; g_1^m(x)\right) \\ g_1^m(x) &= q_1^m(x) \quad \forall m \end{aligned}$$

where the multi-edge type fraction is

$$f_e = 1 - g_e = \frac{\sum_i \frac{\lambda_i}{i}}{\sum_i \frac{\lambda_i}{(i-1)} + \sum_i \frac{\lambda_i}{i}}$$

and $\mu_1(x)$ is the gaussian density at the output of the channel with fading α_1. Similar density evolution equations are obtained after the permutation of the two fading numbers.

Proof: The above equations are directly derived from local neighbourhoods of bitnodes in the graph representation of the LDPC code. ■

To demonstrate the performance of LDPC codes via density evolution in presence of non-ergodic fading, we illustrate the

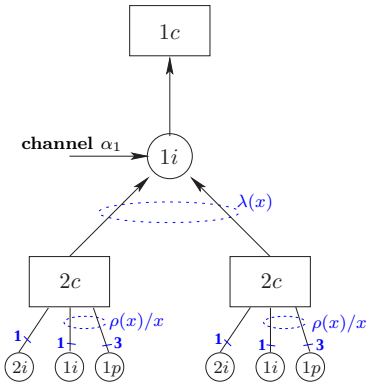

Fig. 14. Local neighbourhood of bitnode $1i$. This tree is used to determine the evolution of messages $1i \rightarrow 1c$.

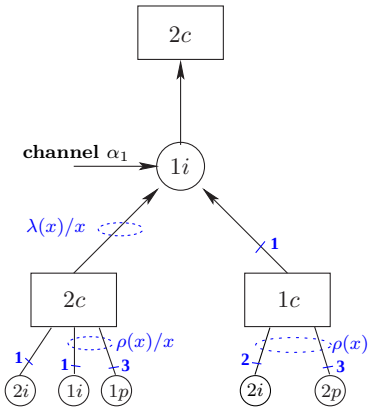

Fig. 15. Local neighbourhood of bitnode $1i$. This tree is used to determine the evolution of messages $1i \rightarrow 2c$.

results from proposition 9 versus the outage capacity limit. Three codes are shown in Fig. 17: a random regular (3,6) code, a root regular (3,6) code, and an irregular root LDPC with left and right degree distributions from [17] given by the polynomials $\lambda(x) = 0.24426x + 0.25907x^2 + 0.01054x^3 + 0.05510x^4 + 0.01455x^7 + 0.01275x^9 + 0.40373x^{11}$ and $\rho(x) = 0.25475x^6 + 0.73438x^7 + 0.01087x^8$.

We now refer back to the outage boundary representation in the fading plane (see 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 satsifies $I_b(\alpha_0^2 \frac{E_b}{N_0}) = \frac{1}{2}$, where $I_b(x) = I_{\text{AWGN}}(Rx)$ is the average mutual information on an additive white gaussian noise channel with a binary input and a signal-to-noise ratio per bit 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

$$\alpha_{\text{th}}^2 = \frac{\frac{E_b}{N_0}_{\text{th}}}{\frac{E_b}{N_0}},$$

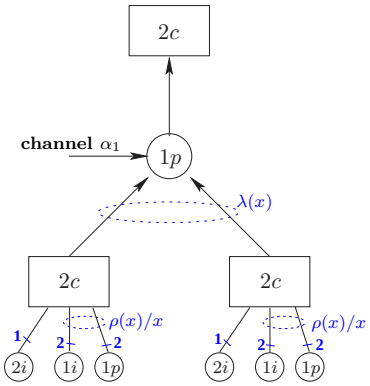

Fig. 16. Local neighbourhood of bitnode $1p$. This tree is used to determine the evolution of messages $1p \rightarrow 2c$.

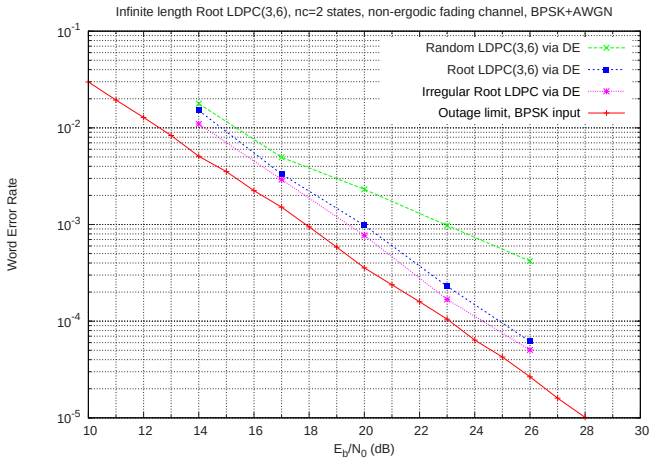

Fig. 17. Infinite length random-LDPC versus root-LDPC codes under iterative decoding on a block-fading channel with $n_c = 2$.

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

$$\alpha_{\text{th}} \;=\; \alpha_0 \sqrt{\frac{\frac{E_b}{N_0\,\text{th}}}{I_b^{-1}(\frac{1}{2})}} \;=\; \alpha_0\sqrt{\Delta}$$

where Δ in the signal-to-noise ratio gap separating the decoding threshold and the capacity limit on the ergodic gaussian channel. To better understand the gain due to irregularity illustrated in Fig. 17, we evaluate the ratio $\frac{\alpha_{\text{th}}}{\alpha_0}$.

- For the regular (3,6) LDPC code, the threshold is 1.09dB on the ergodic gaussian channel. Hence, $\frac{\alpha_{\text{th}}}{\alpha_0} = 1.107$.
- For the irregular LDPC code given above, the threshold is 0.37dB on the ergodic gaussian channel. Hence, $\frac{\alpha_{\text{th}}}{\alpha_0} = 1.045$.

Using the best irregular code proposed in [17] with a threshold of $0.25dB$ yields $\frac{\alpha_{\text{th}}}{\alpha_0} = 1.007$. Hence, with α_c/α_0 close to 1, the area between the outage capacity boundary and the code outage boundary reduces in the neighbourhood of the ergodic line. Nevertheless, the code outage boundary is still uncontrolled in the critical region between the ergodic line and the block-erasure channel. In order to achieve the outage probability limit, a full-diversity capacity-achieving code is necessary but may not be sufficient.

VI. Conclusions

We designed a new family of outage-approaching full-diversity LDPC codes, the *root-LDPC* codes. The design of this family was motivated by the failure of both ML-designed and irregular capacity-approaching LDPC codes to guarantee diversity under iterative decoding. As in the case of multiplexed parallel turbo codes, the word error rate of root-LDPC is quasi-insensitive to block length.

Appendix A: Coding gain of a 4th order unbalanced χ^2 distribution

Without loss of generality, we limit our description to a diversity order of 2. 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 $\omega_1\alpha_1^2 + \omega_2\alpha_2^2$. A fading α_i^2 is Rayleigh distributed, i.e. $p_{\alpha^2}(x) = e^{-x}$. The latter is a central χ^2 distribution of order 2 with parameter $\sigma^2 = 1/2$ (see [15]). 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 $\omega_1\omega_2$ improves 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 b. 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 to 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

$$p_Y(y) \;=\; 4ye^{-2y} \tag{7}$$

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

$$p_Y(y) \;=\; \frac{(e^{-y/a} - e^{-y/b})}{2a-1} \tag{8}$$

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 $T << 1$. For a balanced χ^2 distribution, we have

$$F(a, b, T) \;=\; 1 - e^{-2T}(1 + 2T) \;=\; 2T^2 \;+\; o(T^2) \tag{9}$$

For an unbalanced χ^2 distribution, we obtain

$$F(a, b, T) \;=\; 1 - \frac{ae^{-T/a} - be^{-T/b}}{2a-1} \;=\; \frac{T^2}{2ab} \;+\; o(T^2) \tag{10}$$

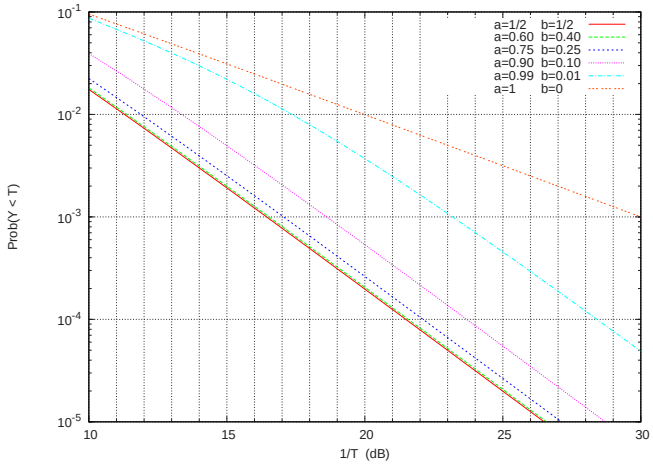

Fig. 18. Coding gain and diversity order of $Y = a\alpha_1^2 + b\alpha_2^2$ (χ^2 of 4th order) where α_1 and α_2 are Rayleigh distributed.

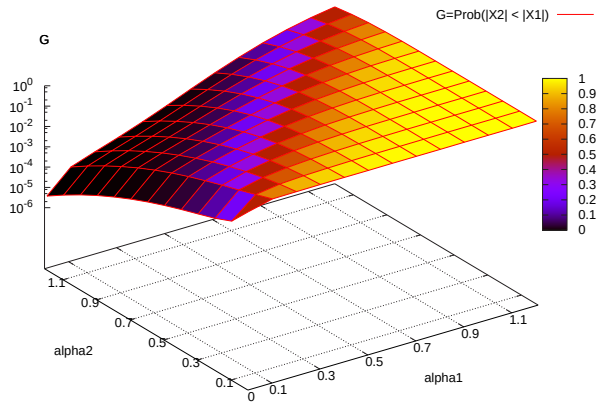

Fig. 19. A 3D plot of $G = P(|X_2| < |X_1|)$ versus α_1 and α_2 for a variance $\sigma^2 = 1/10$.

In Fig. 18, 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. $\propto 1/\gamma^2$) for all positive values of a and b. The function F degenerates to $T + o(T)$ 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 0.75dB) when considering $P(\Lambda < 0)$ for $\Lambda \propto Y + \nu$ since additive noise depends on the fading coefficients as shown in section IV.

Appendix B: The bidimensional cumulative density function $G = P(|X_2| < |X_1|)$

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

$$G = 1 - \int_0^\infty \frac{dt}{\sqrt{2\pi\alpha_1^2\sigma^2}} \left(e^{-\frac{(t-\alpha_1^2)^2}{2\alpha_1^2\sigma^2}} + e^{-\frac{(t+\alpha_1^2)^2}{2\alpha_1^2\sigma^2}} \right) \left(Q\left(\frac{t-\alpha_2}{\alpha_2\sigma}\right) + Q\left(\frac{t+\alpha_2}{\alpha_2\sigma}\right) \right) \quad (11)$$

where $Q(x)$ is the gaussian tail function. A 3D plot of G is illustrated in Fig. 19. The main properties of G are:

- $G(\alpha, \alpha, \sigma^2) = 1/2$ for all $\sigma^2 > 0$.
- G is a non-decreasing 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, $G \to 1$ when $\alpha_1 \to +\infty$.
- For fixed σ^2 and α_1, $G \to 0$ when $\alpha_2 \to +\infty$.

References

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

[2] E. Biglieri, Coding for Wireless Channels, Springer, May 2005.

[3] J.J. Boutros, E. Calvanese Strinati, and A. Guillén i Fàbregas, "Turbo code design for block fading channels," *Allerton's Conference*, Monticello, Illinois, Sept 2004. Downloadable at `www.josephboutros.org`.

[4] J.J. Boutros, A. Guillén i Fàbregas, and E. Calvanese Strinati, "Analysis of coding on non-ergodic channels," *Allerton's Conference*, Monticello, Illinois, Sept 2005. Downloadable at `www.josephboutros.org`.

[5] J.J. Boutros, G.M. Kraidy, and N. Gresset,"Near outage limit space-time coding for MIMO channels," *Inaugural ITA workshop*, UCSD, San Diego, California, Feb. 2006. Downloadable at `www.josephboutros.org`.

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

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

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

[9] 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. Selec. Areas in Commun.*, vol. 19, no. 5, pp. 924-934, May 2001.

[10] 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.

[11] R. Koetter and P.O. Vontobel, "Graph covers and iterative decoding of finite-length codes," *Proc. 3rd International Symposium on Turbo Codes and Related Topics*, Brest, France, pp. 75-82, Sep. 1-5, 2003.

[12] 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, Sept. 1994.

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

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

[15] J.G. Proakis, *Digital Communications*, McGraw-Hill, 4th ed., 2000.

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

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

[18] T.J. Richardson and R.L. Urbanke, *Modern Coding Theory*, Cambridge University Press, Jan. 2007.

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