Binary Codes in the Block-Fading Channel

Joseph J. Boutros
Ecole Nationale Supérieure
des Télécommunications
46 Rue Barrault, Paris
boutros@enst.fr

Albert Guillén i Fàbregas
Institute for Telecommunications Research
University of South Australia
Mawson Lakes SA 5095
albert.guillen@unisa.edu.au

Emilio Calvanese Strinati
Ecole Nationale Supérieure
des Télécommunications
46 Rue Barrault, Paris
strinati@enst.fr

***Abstract*— We study coding for the non-ergodic block-fading channel. In particular, we analyze the error probability of full-diversity binary codes, and we elaborate on how to approach the outage probability limit. In so doing, we introduce the concept outage boundary region, which is a graphical way to illustrate failures in the decoding process. We show that outage achieving codes have a frame error probability which is independent of the block length. Conversely, we show that codes that do not approach the outage probability have an error probability that grows logarithmically with the block length.**

I. Introduction and model

The block-fading channel is a simplified channel model that characterizes delay-constrained communication over slowly-varying fading channels [1], [2]. Particular instances of the block-fading channel are orthogonal-frequency multiplexing modulation (OFDM) and frequency-hopping systems, such as the Global System for Mobile Communications (GSM) or the Enhanced Data GSM Envronment (EDGE). Despite its simplification, it captures the essential characteristics of delay-constrained wireless communication and yields useful code design criteria. More specifically, we consider a block-fading channel with n_c fading blocks, whose discrete-time channel output at block i is given by

$$\mathbf{y}_i = \sqrt{\gamma}\,\alpha_i\,\mathbf{x}_i + \mathbf{z}_i, \quad i = 1\dots n_c \tag{1}$$

where $\mathbf{y}_i, \mathbf{x}_i \in \mathbb{R}^L$ are the received and transmitted signal vectors at block i, $\alpha_i \in \mathbb{R}$ is the i-th fading coefficient, $\mathbf{z}_i \in \mathbb{R}^L$ is the i-th noise vector, with i.i.d. samples $\sim \mathcal{N}(0,\sigma^2)$, with $\sigma^2 = 1/2$, and L is the *block* length. Let $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \dots, \alpha_{n_c}) \in \mathbb{R}^{n_c}$ denote the vector of fading coefficients, fixed for the duration of a *frame* (or codeword). Therefore, the transmission of one frame involves $N_f = n_c L$ channel uses. In compact matrix form we write

$$\mathbf{Y} = \sqrt{\gamma}\,\mathrm{diag}(\boldsymbol{\alpha})\mathbf{X} + \mathbf{Z} \tag{2}$$

where $\mathbf{Y} = [\mathbf{y}_1, \dots, \mathbf{y}_{n_c}]^T \in \mathbb{R}^{n_c \times L}$, $\mathbf{X} = [\mathbf{x}_1, \dots, \mathbf{x}_{n_c}]^T \in \mathbb{R}^{n_c \times L}$ and $\mathbf{Z} = [\mathbf{z}_1, \dots, \mathbf{z}_{n_c}]^T \in \mathbb{R}^{n_c \times L}$. We assume that the fading coefficients are Rayleigh distributed [3] and i.i.d. from block to block and from frame to frame. Thus, the *average* received signal-to-noise ratio (SNR) is γ. Furthermore, we assume perfect channel state information (CSI) at the receiver and no CSI at the transmitter, namely, the receiver has perfectly estimated the fading coefficients. We consider binary transmission only, i.e., $\mathbf{x}_i \in \{+1, -1\}^L$ for $i = 1, \dots, n_c$. In particular, we consider linear binary codes $\mathcal{C} \subseteq \mathbb{F}_2^{N_f}$ of length N_f, dimension K_f and rate $R = \frac{K_f}{N_f}$. Thus, $\gamma = R\frac{E_b}{N_0}$. Throughout the paper we will use the standard notation $\mathcal{C} = (n, k, d_{\min})$ to denote a code of length n, dimension k and minimum distance $d_{\min}$.

[1]The work by A. Guillén i Fàbregas has been supported by the Australian Research Council (ARC) Communications Research Network (ACoRN) under ARC grant RN0459498 and by ARC Grants DP0344856 and DP0558861.

In this paper we study the error probability binary codes in the block-fading channel. We first review the fundamental limits of the channel, namely the *information outage probability*. In passing, we introduce the concept of outage boundary region, which is a graphical way to illustrate failures in the decoding process. We study algebraic binary block codes and parallel turbo codes, and we will discuss on their respective capabilities of approaching the fundamental limits of the channel.

II. Outage Probability and Outage Boundaries in the Fading Space

For a particular channel realization $\boldsymbol{\alpha}$ and SNR γ, the *instantaneous* mutual information between the input and output of the channel is given by

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

where $I_{\mathrm{AWGN}}(s)$ is the mutual information of an AWGN channel with SNR s. 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. Therefore, strictly speaking, the capacity of the block-fading channel is zero since there is an irreducible probability that the decoder makes a *frame error*. In the limit of large frame length, this probability is the *information outage probability* defined as [1], [2],

$$P_{\mathrm{out}}(\gamma, R) = \Pr\{\mathcal{I}(\gamma, \boldsymbol{\alpha}) \le R\} \tag{4}$$

where R is the transmission rate in bits per channel use.

Remark 1: The information outage probability $P_{\mathrm{out}}(\gamma, R)$ represents the best achievable frame error rate for large enough frame length. Therefore, any code aiming at approaching $P_{\mathrm{out}}(\gamma, R)$ should have a frame error probability that, for large enough frame length, becomes *independent* of the frame length [4]. Conversely, if the frame error probability of a given code grows with the frame length it cannot aproach the limit established by $P_{\mathrm{out}}(\gamma, R)$ in a meaningful way.

For large SNR, $P_{\mathrm{out}}(\gamma, R) \sim \kappa\gamma^d$, where κ is the optimal *coding gain* independent of γ and d is referred to as SNR exponent or *diversity* [4]. The optimal exponent corresponds to full diversity, i.e., $d_{\mathrm{gauss}} = n_c$ and it is achieved by Gaussian inputs [4, Lem. 1]. Under the assumption of binary phase shift-keying (BPSK) inputs, the best possible achievable

SNR exponent for large enough frame length is given by the Singleton bound [4, Cor. 1]

$$d_{\rm bpsk} \triangleq 1 + \lfloor n_c(1-R) \rfloor. \tag{5}$$

The Singleton bound thus establishes the *optimal rate-diversity tradeoff* and dictates that the diversity achieved by *any* binary coding scheme $\mathcal{C}$ will be at most $d_{\rm bpsk}$. Interstingly, the Singleton bound is also the largest possible minimum distance (also commonly referred to as *block diversity*) of $\mathcal{C}$ interpreted as a code of length n_c constructed over an alphabet of size 2^L [5]. Eq. (5) also imples that good codes should be able to decode under any combination of $d_{\rm bpsk}+1$ *deep fades*.

In order to better understand how to approach the outage probability limit, we here introduce the concept of *outage region* and *outage boundary* [2].

Definition 1: The outage region for a given SNR γ and transmission rate R, denoted by $\mathcal{R}_{\rm out}(\gamma,R)$ is

$$\mathcal{R}_{\rm out}(\gamma,R) \triangleq \left\{\boldsymbol{\alpha} \in \mathbb{R}_+^{n_c} \quad : \quad \mathcal{I}(\gamma,\boldsymbol{\alpha}) \geq R\right\}$$

in the Euclidean space defined by the fading coefficients $\boldsymbol{\alpha}$. The outage probability is thus given by

$$P_{\rm out}(\gamma,R) = \int_{\boldsymbol{\alpha}\in\mathcal{R}_{\rm out}(\gamma,R)} p(\boldsymbol{\alpha})d\boldsymbol{\alpha}. \tag{6}$$

Definition 2: The outage boundary for a given SNR γ and transmission rate R, denoted by $\mathcal{B}_{\rm out}(\gamma,R)$ is given by the boundary of $\mathcal{R}_{\rm out}(\gamma,R)$

$$\mathcal{B}_{\rm out}(\gamma,R) \triangleq \left\{\boldsymbol{\alpha} \in \mathbb{R}_+^{n_c} \quad : \quad \mathcal{I}(\gamma,\boldsymbol{\alpha}) = R\right\}$$

in the Euclidean space defined by the fading coefficients $\boldsymbol{\alpha}$. Therefore we have the following results.

Proposition 1: The optimal outage boundary $\mathcal{B}_{\rm out}^{\rm gauss}(\gamma,R)$ achievable by Gaussian channel inputs is given by the set of fading points satisfying

$$\prod_{i=1}^{n_c}\left(1+2\gamma\alpha_i^2\right) = 2^{2Rn_c}$$

Proof: $\mathcal{B}_{\rm out}^{\rm gauss}(\gamma,R)$ is simply given by the points satisfying $\mathcal{I}(\gamma,\boldsymbol{\alpha}) = R$. Using the fact that for real Gaussian inputs $I_{\rm AWGN}(s) = \frac{1}{2}\log_2(1+2s)$ the result follows. ■

Proposition 2: The outage boundary $\mathcal{B}_{\rm out}^{\rm bpsk}(\gamma,R)$ achievable with BPSK channel inputs is given by the set of fading points satisfying

$$\mathbb{E}_Z\left[\log_2\left(\prod_{i=1}^{n_c}\left(1+e^{-2(\gamma\alpha_i^2+\sqrt{\gamma}\alpha_i Z)}\right)\right)\right] = n_c(1-R)$$

where $Z \sim \mathcal{N}(0,1)$.

Proof: $\mathcal{B}_{\rm out}^{\rm bpsk}(\gamma,R)$ is simply given by the points satisfying $\mathcal{I}(\gamma,\boldsymbol{\alpha}) = R$. Using the fact that for real BPSK inputs

$$I_{\rm AWGN}(s) = 1 - \mathbb{E}_Z\left[\log_2\left(1+e^{-2(s+\sqrt{s}Z)}\right)\right]$$

where $Z \sim \mathcal{N}(0,1)$, the result follows. ■

Figure 1 shows the outage boundaries $\mathcal{B}_{\rm out}^{\rm gauss}(\gamma,R)$ and $\mathcal{B}_{\rm out}^{\rm bpsk}(\gamma,R)$ in a block-fading channel with $n_c=2$, $R=\frac{1}{2}$ and $\frac{E_{\rm b}}{N_0} = 8$ dB. We also show the line $\alpha_1 = \alpha_2 = \cdots = \alpha_{n_c}$ which we call *ergodic line*. This line corresponds to an ergodic AWGN channel with SNR$=\gamma\alpha_1^2$. The first observation is that, since the fading coefficients are i.i.d., $\mathcal{B}_{\rm out}^{\rm gauss}(\gamma,R)$ and $\mathcal{B}_{\rm out}^{\rm bpsk}(\gamma,R)$ are symmetric with respect to the ergodic line. We also observe that $\mathcal{B}_{\rm out}^{\rm gauss}(\gamma,R)$ and $\mathcal{B}_{\rm out}^{\rm bpsk}(\gamma,R)$ have essentially much different shapes. This is due to the fact that $R=\frac{1}{2}$ is the largest possible rate for binary codes with full diversity. Since for BPSK $I_{\rm AWGN}(s) \to 1$ only for $s\to\infty$, we see from (3) that when one of the fading coefficients is very small, the other has to be very large in order to make $\mathcal{I}(\gamma,\boldsymbol{\alpha}) = R$. Thus, $\mathcal{B}_{\rm out}^{\rm bpsk}(\gamma,\frac{1}{n_c})$ will only touch the axis in the limit.

[2]These concepts were first introduced in [6]. However, the authors did not not use these regions to analyze practical code constructions.

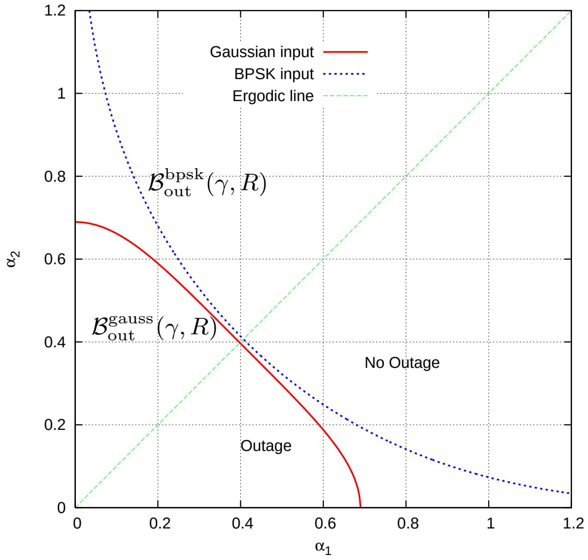

Fig. 1. Outage boundaries $\mathcal{B}_{\rm out}^{\rm gauss}(\gamma,R)$ and $\mathcal{B}_{\rm out}^{\rm bpsk}(\gamma,R)$ if a block-fading channel with $n_c=2$ with $R=\frac{1}{2}$ and $\frac{E_{\rm b}}{N_0}=8$ dB.

III. Code Outage Boundaries and Channel Multiplexers

In this section we introduce outline the basic code design guidelines and we will introduce the code outage boundaries. As mentioned in the previous section, we can interpret the diversity as the minimum Hamming distance of a code of length n_c contructed over an alphabet of size 2^L [5]. Formally we have,

Definition 3: We define the *block diveristy* of $\mathcal{C}$ as

$$\delta \triangleq \min_{\substack{\mathbf{x}\in\mathcal{C}\\ \mathbf{x}\neq\mathbf{0}}} |\{i \in (1,\ldots,n_c) \ \mid \ \mathbf{x}_i \neq \mathbf{0}\}|. \tag{7}$$

In words, δ represents the limit number of deep faded blocks that $\mathcal{C}$ can tolerate. Obviously $\delta \leq d_{\rm bpsk}$. Eq. (5) reveals that the largest rate that can achieve full diversity is $R=\frac{1}{n_c}$. In this work, we focus on full diversity codes[3]. Codes for the more general setting are studied in [5], [8], [4].

[3]In order to achieve full diversity with higher rates, one should construct full diversity binary codes and *expand* the signal constellation [4]. For example, the standard bit-interleaved coded modulation (BICM) [7] is shown to be a practical means of achieving the optimal rate-diversity tradeoff and to have negligible loss in outage probability compared with standard coded modulation [4]. Therefore, constructing full diversity binary codes is the key enabler to transmit higher rates as reliably as possible.

The frame error probability of a code $\mathcal{C}$ is given by

$$P_e^{\mathcal{C}}(\gamma) = \mathbb{E}\left[P_e^{\mathcal{C}}(\gamma|\boldsymbol{\alpha})\right] \tag{8}$$

where $P_e^{\mathcal{C}}(\gamma|\boldsymbol{\alpha})$ is the *conditional* error probability. Using the tight upper bound of Malkamaki and Leib in [9], we can write

$$P_e^{\mathcal{C}}(\gamma) \leq \mathbb{E}\left[\min\left\{1, \sum_{\mathbf{w}} A_{\mathbf{w}} P_e^{\mathcal{C}}(\gamma, \mathbf{w}, \boldsymbol{\alpha})\right\}\right] \tag{9}$$

where $\mathbf{w} = (w_1, \ldots, w_{n_c})$ is the Hamming weight vector, $A_{\mathbf{w}}$ is the number of codewords of $\mathcal{C}$ that have Hamming weight vector $\mathbf{w}$, which we nickname the *multiplexed weight enumerator*, and

$$P_e^{\mathcal{C}}(\gamma, \mathbf{w}, \boldsymbol{\alpha}) = Q\left(\sqrt{2\gamma \sum_{i=1}^{n_c} w_i \alpha_i^2}\right) \tag{10}$$

$$\leq \frac{1}{2}\exp\left(-\gamma \sum_{i=1}^{n_c} w_i \alpha_i^2\right) \tag{11}$$

is the corresponding pairwise error probability. We can now easily define the *code outage region* and *code outage boundary* as[4]

Definition 4: The outage region for a given code $\mathcal{C}$ and SNR γ, denoted by $\mathcal{R}_{\rm out}(\gamma, \mathcal{C})$ is defined as

$$\mathcal{R}_{\rm out}(\gamma, \mathcal{C}) \triangleq \left\{\boldsymbol{\alpha} \in \mathbb{R}_+^{n_c} \;\;:\;\; \sum_{\mathbf{w}} A_{\mathbf{w}} P_e^{\mathcal{C}}(\gamma, \mathbf{w}, \boldsymbol{\alpha}) \geq 1\right\}$$

in the Euclidean space defined by the fading coefficients $\boldsymbol{\alpha}$.

Definition 5: The outage boundary for a given code $\mathcal{C}$ and SNR γ, denoted by $\mathcal{B}_{\rm out}(\gamma, \mathcal{C})$ is defined as the boundary of $\mathcal{R}_{\rm out}(\gamma, \mathcal{C})$

$$\mathcal{B}_{\rm out}(\gamma, \mathcal{C}) \triangleq \left\{\boldsymbol{\alpha} \in \mathbb{R}_+^{n_c} \;\;:\;\; \sum_{\mathbf{w}} A_{\mathbf{w}} P_e^{\mathcal{C}}(\gamma, \mathbf{w}, \boldsymbol{\alpha}) = 1\right\}$$

in the Euclidean space defined by the fading coefficients $\boldsymbol{\alpha}$. The previous definition separates the code outage region $\mathcal{R}_{\rm out}(\gamma, \mathcal{C})$ and the *noise region* defined as its complement. The error probability is thus dominated by code outages when $\boldsymbol{\alpha} \in \mathcal{R}_{\rm out}(\gamma, \mathcal{C})$ and by noise elsewhere. In order to achieve reliable communication over the block-fading channel, we will design codes that achieve the optimal tradeoff given by the Singleton bound and have a coding gain that is as close as possible to κ. This implies that, the code outage boundary $\mathcal{B}_{\rm out}(\gamma, \mathcal{C})$ should be as close to $\mathcal{B}_{\rm out}^{\rm bpsk}(\gamma, R)$ as possible and, as the block length grows, the contribution of the noise region should be negligible. This unveils some sort of *threshold effect* which, as we shall see in the following, is the key to approach the outage probability limit. Figure 1 also implies that a given code has full diversity if and only if its corresponding boundary approaches all the n_c axis.

Constructing full diversity codes is however non trivial, as illustrated by the following example. Consider a repetition code of length $N_f = 8$ and rate $R = \frac{1}{2}$, to be transmitted over a block-fading channel with $n_c = 2$. Obviously there are multiple ways of allocating its coded bits to the channel blocks. One such method is to alternatively allocate one coded bit to each block. This method obviously benefits from the inherent diversity in the repetition code, since in case of one block in deep fade the decoder can still correctly decode. However, consider for example the case where the first 4 coded bits are mapped onto the first block and the rest to the second. In this case, if one block is in deep fade it might happen that the decoder has more than one codeword to choose from, and thus, will make an error. In the following, we generalize this idea and introduce the notion of *channel multiplexer*, which is a particular type of interleaver that maps the output of the encoder to the n_c different channel coefficients. A channel multiplexer allocates the bits at the output of the encoder to the matrix $\mathbf{X}$. Once the coded bit has been allocated a channel block, since the channel is fixed for L consecutive coded bits and the noise is indepnedent, the actual time index is irrelevant for diversity purposes.

Definition 6: A channel multiplexer is a bijection from the set $\{1, \ldots, N_f\}$ to the set $\{1, \ldots, n_c\}^L$, where the superscript denotes cartesian product.

The channel multiplexers corresponding to the previous example are $(1\ 2\ 1\ 2\ 1\ 2\ 1\ 2)$ and $(1\ 1\ 1\ 1\ 2\ 2\ 2\ 2)$ respectively. For a given code $\mathcal{C}$ transmitted over a block-fading channel with n_c states, the total number of multiplexers is $(N_f)!/(L!)^{n_c}$. A multiplexer is said to be *regular* if it is has a periodical pattern. The number of regular multiplexers of period p reduces then to $(p!)/((p/n_c)!)^{n_c}$. The two multiplexers of the previous example are obviously regular. Note that the channel multiplexer is therefore a key element in the system: it *enables* the code to achieve diversity.

In the following sections, we study specific code constructions. In particular we consider algebraic binary block codes and parallel turbo codes combined with a variety of channel multiplexers.

IV. Binary Block Codes

In this section we study the error probability of binary block codes in the block-fading channel. We construct $\mathcal{C}$ as the direct sum of N small block codes of the same rate $\mathcal{C}_0 = (n, k, d_{\min})$. Thus $N_f = nN$ and $K_f = kN$. For such a construction, we can upperbound the error probability of $\mathcal{C}$ as

$$P_e^{\mathcal{C}}(\gamma) = \mathbb{E}\left[1 - (1 - P_e^{\mathcal{C}_0}(\gamma|\boldsymbol{\alpha}))^N\right] \tag{12}$$

where $P_e^{\mathcal{C}_0}(\gamma|\boldsymbol{\alpha})$ is the conditional error probability of the short block code $\mathcal{C}_0$. We can thus, upperbound (9) as

$$P_e^{\mathcal{C}}(\gamma) \leq \mathbb{E}\left[\min\left\{1, N\sum_{\mathbf{w}} A_{\mathbf{w}}^{\mathcal{C}_0} P_e^{\mathcal{C}_0}(\gamma, \mathbf{w}, \boldsymbol{\alpha})\right\}\right] \tag{13}$$

where $A_{\mathbf{w}}^{\mathcal{C}_0}$ is the number of codewords of $\mathcal{C}_0$ with Hamming weight vector $\mathbf{w}$ and $P_e^{\mathcal{C}_0}(\gamma, \mathbf{w}, \boldsymbol{\alpha})$ is the corresponding pairwise error probability. Thus, in this case, the outage region and boundary can be written as

$$\mathcal{R}_{\rm out}(\gamma, \mathcal{C}) = \left\{\boldsymbol{\alpha} \in \mathbb{R}_+^{n_c} \;\;:\;\; \sum_{\mathbf{w}} A_{\mathbf{w}}^{\mathcal{C}_0} P_e^{\mathcal{C}_0}(\gamma, \mathbf{w}, \boldsymbol{\alpha}) \geq \frac{1}{N}\right\}$$

$$\mathcal{B}_{\rm out}(\gamma, \mathcal{C}) = \left\{\boldsymbol{\alpha} \in \mathbb{R}_+^{n_c} \;\;:\;\; \sum_{\mathbf{w}} A_{\mathbf{w}}^{\mathcal{C}_0} P_e^{\mathcal{C}_0}(\gamma, \mathbf{w}, \boldsymbol{\alpha}) = \frac{1}{N}\right\}.$$

[4]These correspond to the outage region and boundaries with maximum-likelihood (ML) decoding. In the case where the ML decoder is too complex and iterative decoders are used instead, in Section V we will appropriately define the outage region and boundaries.

Using these definitions, we can rewrite (13) as

$$P_e^{\mathcal{C}}(\gamma) \leq \int_{\boldsymbol{\alpha}\in\mathcal{R}_{\rm out}(\gamma,\mathcal{C})} p(\boldsymbol{\alpha})d\boldsymbol{\alpha} \tag{14}$$

$$+ \int_{\boldsymbol{\alpha}\notin\mathcal{R}_{\rm out}(\gamma,\mathcal{C})} N\, P_e^{\mathcal{C}_0}(\gamma|\boldsymbol{\alpha})\, p(\boldsymbol{\alpha})d\boldsymbol{\alpha} \tag{15}$$

$$\leq \int_{\boldsymbol{\alpha}\in\widetilde{\mathcal{R}}_{\rm out}(\gamma,\mathcal{C})} p(\boldsymbol{\alpha})d\boldsymbol{\alpha} \tag{16}$$

$$+ \int_{\boldsymbol{\alpha}\notin\widetilde{\mathcal{R}}_{\rm out}(\gamma,\mathcal{C})} \frac{N}{2}\sum_{\mathbf{w}} A_{\mathbf{w}}^{\mathcal{C}_0} e^{-\gamma\sum_{i=1}^{n_c} w_i\alpha_i^2}\, p(\boldsymbol{\alpha})d\boldsymbol{\alpha} \tag{17}$$

$$\triangleq \mathcal{P}_{\rm out}^{\mathcal{C}}(\gamma) + \mathcal{P}_{\rm noise}^{\mathcal{C}}(\gamma) \tag{18}$$

where

$$\widetilde{\mathcal{R}}_{\rm out}(\gamma,\mathcal{C}) \triangleq \left\{\boldsymbol{\alpha}\in\mathbb{R}_+^{n_c} \;:\; \sum_{\mathbf{w}} A_{\mathbf{w}}^{\mathcal{C}_0} e^{-\gamma\sum_{i=1}^{n_c} w_i\alpha_i^2} \geq \frac{2}{N}\right\} \tag{19}$$

is the code outage region using the exponential function. Obviously we have that $\mathcal{R}_{\rm out}(\gamma,\mathcal{C}) \subseteq \widetilde{\mathcal{R}}_{\rm out}(\gamma,\mathcal{C})$. Equation (18) defines the integrals $\mathcal{P}_{\rm out}^{\mathcal{C}}(\gamma)$ and $\mathcal{P}_{\rm noise}^{\mathcal{C}}(\gamma)$ to be the contributions of code outages due to fading and noise respectively. Let now

$$A^{\mathcal{C}_0}(W) = \sum_w A_w^{\mathcal{C}_0} W^w$$

denote the weight enumerator polynomial of $\mathcal{C}_0$ [10] and let

$$A^{\mathcal{C}_0}(\mathbf{W}) = \sum_{\mathbf{w}} A_{\mathbf{w}}^{\mathcal{C}_0} W_1^{w_1}\dots W_{n_c}^{w_{n_c}}$$

denote the multiplexed weight enumerator polynomial, where $\mathbf{W} = (W_1,\dots,W_{n_c})$ denotes the vector of dummy variables and $A_{\mathbf{w}}^{\mathcal{C}_0}$ is the number of codewords of $\mathcal{C}_0$ of Hamming weight $w = \sum_{i=1}^{n_c} w_i$ for which the multiplexer assigns Hamming weight w_i to channel block i, for $i = 1,\dots,n_c$. Obviously, $A^{\mathcal{C}_0}(W,\dots,W) = A^{\mathcal{C}_0}(W)$. A code $\mathcal{C}_0$ associated to a given channel multiplexer has full block diversity if and only if $A^{\mathcal{C}_0}(\mathbf{W}) - 1$ is divisible by $\mathbf{W}$. The number of distinct multiplexed weight enumerators $A^{\mathcal{C}_0}(\mathbf{W})$ depends on the algebraic structure of $\mathcal{C}_0$. Some examples are given in Table I, e.g. the $(6,3,3)$ code obtained by shortening the $(7,4,3)$ Hamming code has 3 distinct $A^{\mathcal{C}_0}(\mathbf{W})$ polynomials. The 70 multiplexers of the $(8,4,4)$ extended Hamming codes are grouped in two classes only, with two distinct $A^{\mathcal{C}_0}(W_1,W_2)$ polynomials. The first with diversity 1 is

$$A^{\mathcal{C}_0}(W_1,W_2) = 1 + W_2^4 + 12W_1^2W_2^2 + W_1^4 + W_1^4W_2^4 \tag{20}$$

and the second with diversity 2 is

$$A^{\mathcal{C}_0}(W_1,W_2) = 1 + 6W_1^2W_2^2 + 4W_1^3W_2 + 4W_1W_2^3 + W_1^4W_2^4. \tag{21}$$

Figure 2 shows the outage boundaries $\mathcal{B}_{\rm out}(\gamma,\mathcal{C})$ for the extended Hamming code $\mathcal{C}_0 = (8,4,4)$ with $N = 100, 1000, 10000$ and multiplexer (21) in a block-fading channel with $n_c = 2$ and $\frac{E_{\rm b}}{N_0} = 8$ dB. We observe that the outage region remarkably increases with N, which implies that the error probability increases with N, and thus this construction cannot be outage achieving. In the light of these results, we are interested in knowing the growth rate with N. Since the weight enumerator grows linearly with N, at a first glance, one might argue that the growth is linear with N. This is precisely the answer for ergodic channels, but in non-ergodic channels, as we will show in the following, the growth is logarithmic. Throughout this section we will use $\mathcal{C}_0 = (8,4,4)$ extensively, as it is a simple case that captures the essential behavior of this family of codes. To illustrate the logarithmic growth, Figure 3 illustrates the simulated frame error probability for the $\mathcal{C}_0 = (8,4,4)$ code. For a fixed $\frac{E_{\rm b}}{N_0}$, as N increases, the error probability does not grow linearly but logarithmically.

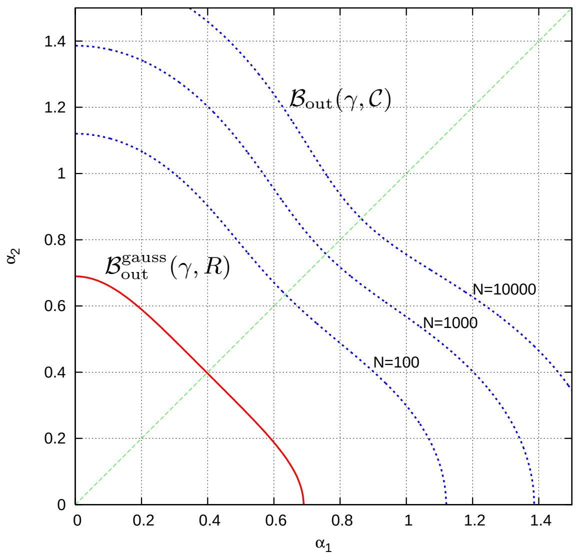

Fig. 2. Code outage boundaries in the fading plane for binary block codes with $R = \frac{1}{2}$ obtained from the extended Hamming code $\mathcal{C}_0 = (8,4,4)$ with $N = 100, 1000, 10000$, in a block-fading channel with $n_c = 2$ and $\frac{E_{\rm b}}{N_0} = 8$ dB.

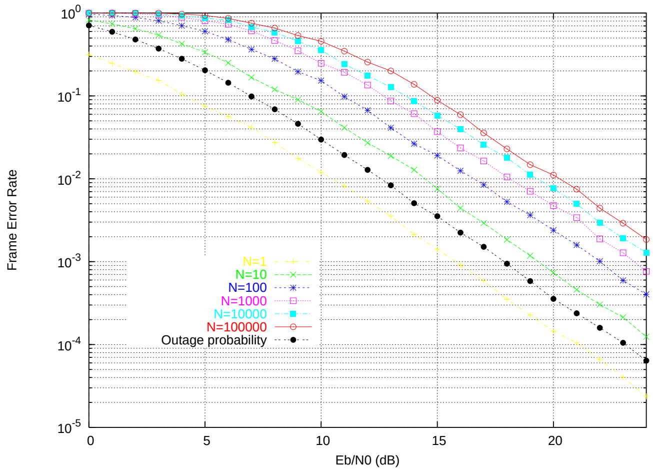

Fig. 3. Frame error rate versus $\frac{E_{\rm b}}{N_0}$ for $n_c = 2$ and $\mathcal{C}_0 = (8,4,4)$.

In order to analyze the growth behavior with N, we introduce some new definitions.

Definition 7: We define

$$\mathcal{S}_i(\gamma,\mathcal{C}) \triangleq \left\{\boldsymbol{\alpha}\in\mathbb{R}_+^{n_c} \;|\; \|\boldsymbol{\alpha}\|^2 \leq R_i^2\right\} \tag{22}$$

where

$$R_i^2 \triangleq \frac{1}{\gamma w_{i,\min}} \log\left(\frac{N A_{w_{i,\min}}^{\mathcal{C}_0}}{2}\right), \tag{23}$$

TABLE I

SOME RATE 1/2 BLOCK CODES FOR $n_c = 2$ BLOCK FADING CHANNELS.

Block code $(n, k, d_{\min})$	Total number of multiplexers	Number of multiplexing classes	Population per class	Diversity order
$(10, 5, 4)$	252	14	$6^2, 12^4, 24^4 \mid 24^4$	$1 \mid 2$
$(8, 4, 4)$	70	2	$14^1 \mid 56^1$	$1 \mid 2$
$(8, 4, 3)$	70	13	$1^2, 4^4, 8^3 \mid 4^1, 8^3$	$1 \mid 2$
$(6, 3, 3)$	20	3	$4^2 \mid 12^1$	$1 \mid 2$

$w_{i,\min}$ is the absolute minimum Hamming weight allocated to block i and $A^{\mathcal{C}_0}_{w_{i,\min}}$ is the corresponding total number of codewords in $\mathcal{C}_0$ that allocate weight $w_{i,\min}$ to block i. We denote by $\mathcal{S}_{\max}(\gamma, \mathcal{C})$ the sphere of radius

$$R^2_{\max} = \max_{1,\dots,n_c} \{R^2_1, \dots, R^2_{n_c}\} = R^2_\iota \tag{24}$$

with

$$\iota = \arg \min_{1,\dots,n_c} \{w_{1,\min}, \dots, w_{n_c,\min}\}. \tag{25}$$

In words, definition 7 defines n_c spheres with radiuses are obtained by solving (19) for α_i by letting $\alpha_j = 0$ for $j \neq i$ and γ large enough.

Proposition 3: For large enough γ, $\widetilde{\mathcal{R}}_{\text{out}}(\gamma, \mathcal{C}) \subseteq \mathcal{S}_{\max}(\gamma, \mathcal{C})$.

Proof: Let $\mathcal{C}'_0$ denote a code whose multiplexed weight enumerator is given by

$$A^{\mathcal{C}'_0}(\mathbf{W}) = \sum_{\mathbf{w}} A^{\mathcal{C}_0}_{\mathbf{w}} W_1^{\omega_{\mathbf{w}}} \dots W_{n_c}^{\omega_{\mathbf{w}}} \tag{26}$$

where every possible Hamming weight vector $\mathbf{w}$ of $\mathcal{C}_0$ is replaced in $\mathcal{C}'_0$ by a vector $\boldsymbol{\omega}_{\mathbf{w}} = (\omega_{\mathbf{w}}, \dots, \omega_{\mathbf{w}})$ with

$$\omega_{\mathbf{w}} \triangleq \min_{1,\dots,n_c} \{w_1, \dots, w_{n_c}\}. \tag{27}$$

That is, $\mathcal{C}'_0$ has Hamming weight vectors with equal weight (the minimum component of $\mathbf{w}$) on every block with the same coefficients $A^{\mathcal{C}_0}_{\mathbf{w}}$. Therefore,

$$\widetilde{\mathcal{R}}_{\text{out}}(\gamma, \mathcal{C}') = \left\{ \boldsymbol{\alpha} \in \mathbb{R}^{n_c}_+ : \sum_{\mathbf{w}} A^{\mathcal{C}_0}_{\mathbf{w}} e^{-\gamma \omega_{\mathbf{w}} \sum_{i=1}^{n_c} \alpha_i^2} \geq \frac{2}{N} \right\} \tag{28}$$

Then, for large γ $\widetilde{\mathcal{R}}_{\text{out}}(\gamma, \mathcal{C}') \to \mathcal{S}_{\max}(\gamma, \mathcal{C})$. Since the boundary $\widetilde{\mathcal{B}}_{\text{out}}(\gamma, \mathcal{C}')$ is defined as the $\boldsymbol{\alpha} \in \mathbb{R}^{n_c}_+$ satisfying that

$$\frac{2}{N} = \sum_{\mathbf{w}} A^{\mathcal{C}_0}_{\mathbf{w}} e^{-\gamma \omega_{\mathbf{w}} \sum_{i=1}^{n_c} \alpha_i^2} \tag{29}$$

and we have that

$$\sum_{\mathbf{w}} A^{\mathcal{C}_0}_{\mathbf{w}} e^{-\gamma \omega_{\mathbf{w}} \sum_{i=1}^{n_c} \alpha_i^2} \geq \sum_{\mathbf{w}} A^{\mathcal{C}_0}_{\mathbf{w}} e^{-\gamma \sum_{i=1}^{n_c} w_i \alpha_i^2} \tag{30}$$

for every $\boldsymbol{\alpha} \in \mathbb{R}^{n_c}_+$, if we want the condition of $\widetilde{\mathcal{B}}_{\text{out}}(\gamma, \mathcal{C})$

$$\frac{2}{N} = \sum_{\mathbf{w}} A^{\mathcal{C}_0}_{\mathbf{w}} e^{-\gamma \sum_{i=1}^{n_c} w_i \widetilde{\alpha}_i^2} \tag{31}$$

to be met for a given fading vector $\widetilde{\boldsymbol{\alpha}}$, we need that $\widetilde{\alpha}_i \leq \alpha_i$ for $i = 1, \dots, n_c$. Summarizing, we have that the vector $\widetilde{\boldsymbol{\alpha}} \in \widetilde{\mathcal{B}}_{\text{out}}(\gamma, \mathcal{C})$ has to be componentwise smaller than or equal to $\boldsymbol{\alpha} \in \widetilde{\mathcal{B}}_{\text{out}}(\gamma, \mathcal{C}')$. Since for large γ, $\widetilde{\mathcal{R}}_{\text{out}}(\gamma, \mathcal{C}') \to \mathcal{S}_{\max}(\gamma, \mathcal{C})$ we have that for large γ $\widetilde{\mathcal{R}}_{\text{out}}(\gamma, \mathcal{C}) \subseteq \mathcal{S}_{\max}(\gamma, \mathcal{C})$. Using similar arguments it is not difficult to prove that $\mathcal{R}_{\text{out}}(\gamma, \mathcal{C})$ satisfies an identical property with a sphere of smaller radius. ∎

We have the following result,

Proposition 4: The contribution of code outages satisfies that

$$\lim_{N \to \infty} \lim_{\gamma \to \infty} \frac{\mathcal{P}^{\mathcal{C}}_{\text{out}}(\gamma)}{\left(\frac{\log N}{\gamma}\right)^{n_c}} = a \tag{32}$$

where a is a constant independent of γ and N.

Proof: Using proposition 3, we have that

$$\lim_{\gamma \to \infty} \mathcal{P}^{\mathcal{C}}_{\text{out}}(\gamma) = \int_{\boldsymbol{\alpha} \in \widetilde{\mathcal{R}}_{\text{out}}(\gamma, \mathcal{C})} p(\boldsymbol{\alpha}) d\boldsymbol{\alpha} \tag{33}$$

$$\leq \int_{\boldsymbol{\alpha} \in \mathcal{S}_{\max}(\gamma, \mathcal{C})} p(\boldsymbol{\alpha}) d\boldsymbol{\alpha} \tag{34}$$

$$= \Pr\left\{ \sum_{i=1}^{n_c} \alpha_i^2 \leq R^2_{\max} \right\} \tag{35}$$

Since the variable $\chi = \sum_{i=1}^{n_c} \alpha_i^2$ is a chi-squared random variable with $2n_c$ degrees of freedom we write (35) as [3]

$$\lim_{\gamma \to \infty} \mathcal{P}^{\mathcal{C}}_{\text{out}}(\gamma) \leq 1 - e^{-R^2_{\max}} \sum_{k=0}^{n_c - 1} \frac{1}{k!} R^{2k}_{\max} \tag{36}$$

$$\leq 1 - (1 - R^2_{\max}) \sum_{k=0}^{n_c - 1} \frac{1}{k!} R^{2k}_{\max} \tag{37}$$

$$= R^2_{\max} - \sum_{k=1}^{n_c - 1} \frac{R^{2(k-1)}_{\max} - R^{2k}_{\max}}{k!} \tag{38}$$

Thus, the dominant term in (38) is readily seen to be $R^{2n_c}_{\max}$ and we have that $\mathcal{P}^{\mathcal{C}}_{\text{out}}(\gamma)$ behaves as $R^{2n_c}_{\max}$ for large enough γ, which completes the proof. ∎

As we observe, code outages are mainly due to the codewords with minimum weight in any block, and the corresponding number of codewords. Hence, for such direct sum of short block codes, the code outages scale as $\left(\frac{\log N}{\gamma}\right)^{n_c}$ for a fixed (large enough) γ. In fact, this result is still valid for *any* code construction such that the multiplexed weight enumerator grows linearly with N. Therefore, binary block codes obtained from trellis-terminated convolutional codes will mimic this behavior [11].

We now consider the noise integral $\mathcal{P}^{\mathcal{C}}_{\rm noise}(\gamma)$. We can write

$$\begin{aligned}\mathcal{P}^{\mathcal{C}}_{\rm noise}(\gamma) &= \frac{N}{2}\sum_{\mathbf{w}} A^{\mathcal{C}_0}_{\mathbf{w}} \int_{\boldsymbol{\alpha}\notin\tilde{\mathcal{R}}_{\rm out}(\gamma,\mathcal{C})} e^{-\gamma\sum_{i=1}^{n_c} w_i\alpha_i^2}\, p(\boldsymbol{\alpha})d\boldsymbol{\alpha}\\ &= \frac{N}{2}\sum_{\mathbf{w}} A^{\mathcal{C}_0}_{\mathbf{w}} \int_{\boldsymbol{\alpha}\in\mathbb{R}_+^{n_c}} e^{-\gamma\sum_{i=1}^{n_c} w_i\alpha_i^2}\, p(\boldsymbol{\alpha})d\boldsymbol{\alpha}\\ &\quad -\frac{N}{2}\sum_{\mathbf{w}} A^{\mathcal{C}_0}_{\mathbf{w}} \int_{\boldsymbol{\alpha}\in\tilde{\mathcal{R}}_{\rm out}(\gamma,\mathcal{C})} e^{-\gamma\sum_{i=1}^{n_c} w_i\alpha_i^2}\, p(\boldsymbol{\alpha})d\boldsymbol{\alpha}\\ &= \frac{N}{2}\sum_{\mathbf{w}} A^{\mathcal{C}_0}_{\mathbf{w}} \prod_{i=1}^{n_c}\frac{1}{1+w_i\gamma}\\ &\quad -\frac{N}{2}\sum_{\mathbf{w}} A^{\mathcal{C}_0}_{\mathbf{w}} \int_{\boldsymbol{\alpha}\in\tilde{\mathcal{R}}_{\rm out}(\gamma,\mathcal{C})} e^{-\gamma\sum_{i=1}^{n_c} w_i\alpha_i^2}\, p(\boldsymbol{\alpha})d\boldsymbol{\alpha}\end{aligned} \tag{39}$$

where the first term in (39) is the classical union bound [5].

We illustrate the impact of $\mathcal{P}^{\mathcal{C}}_{\rm noise}(\gamma)$ by means of an example. Consider the $(8,4,4)$ extended Hamming code transmitted over the block-fading channel with $n_c = 2$. We will bound the contribution of every pairwise error event separately. In particular, we will use the ellipsoid

$$\mathcal{E}_1(\gamma,\mathcal{C}) = \left\{\boldsymbol{\alpha}\in\mathbb{R}_+^{n_c} : 3\alpha_1^2+\alpha_2^2 = R^2_{\max}\right\}$$

to bound the second pairwise term in (21) and the ellipsoid (see Figure 4)

$$\mathcal{E}_2(\gamma,\mathcal{C}) = \left\{\boldsymbol{\alpha}\in\mathbb{R}_+^{n_c} : \alpha_1^2+3\alpha_2^2 = R^2_{\max}\right\}$$

to bound the third pairwise term in (21). The other two terms are bounded using a sphere of radius $R_{\rm ergodic}$ such that

$$\sum_{\mathbf{w}} A^{\mathcal{C}_0}_{\mathbf{w}} e^{-\gamma\frac{R^2_{\rm ergodic}}{\sqrt{n_c}}w} = \frac{2}{N}$$

where $w = \sum_{i=1}^{n_c} w_i$. Some tedious but otherwise straightforward algebra leads to (for large enough γ),

$$\mathcal{P}^{\mathcal{C}}_{\rm noise}(\gamma) \le \frac{3/7\log 7N + 2\log(2N) + 24/7}{\gamma^2} \tag{40}$$

Therefore, the dominant term becomes $\mathcal{P}^{\mathcal{C}}_{\rm out}(\gamma)$. The ratio of the simulated error rate by the upper bounds on $P_e^{\mathcal{C}}(\gamma)$ is shown in Figure 5.

V. Parallel Turbo Codes

So far, we have characterized the diversity of parallel turbo codes under a variety of channel multiplexers and ML decoding. In practice, turbo-codes are decoded iteratively, using the forward-backward algorithm [13] on each component code and exchanging extrinsic information through the iterations [12]. Using iterative decoding, it is well known that turbo-codes exhibit a threshold behavior in ergodic channels. In the non-ergodic case, this threshold behavior implies that code outages are the only cause of error for sufficiently large frame length. Thus,

$$P_e^{\mathcal{C}}(\gamma) = \int_{\boldsymbol{\alpha}\in\mathcal{R}_{\rm out}(\gamma,\mathcal{C})} p(\boldsymbol{\alpha})\; d\boldsymbol{\alpha} \tag{41}$$

where

$$\mathcal{R}_{\rm out}(\gamma,\mathcal{C}) = \left\{\boldsymbol{\alpha}\in\mathbb{R}_+^{n_c} \;\middle|\; \lim_{n_{\rm it}\to\infty}\lim_{K_f\to\infty} P_e^{\mathcal{C}}(\gamma|\boldsymbol{\alpha},K_f,n_{\rm it}) = 1\right\} \tag{42}$$

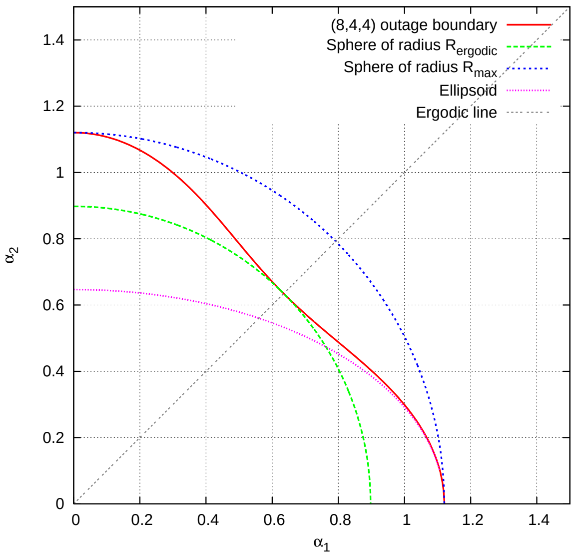

Fig. 4. Outage boundary $\mathcal{B}_{\rm out}(\gamma,\mathcal{C})$, the spheres with radius $R_{\rm ergodic}$, the sphere with radius $R_{\max}$ and the ellipsoid $\mathcal{E}_2(\gamma,\mathcal{C})$ defined by one monomial in $A(W_1,W_2)$. $\frac{E_b}{N_0} = 8$ dB.

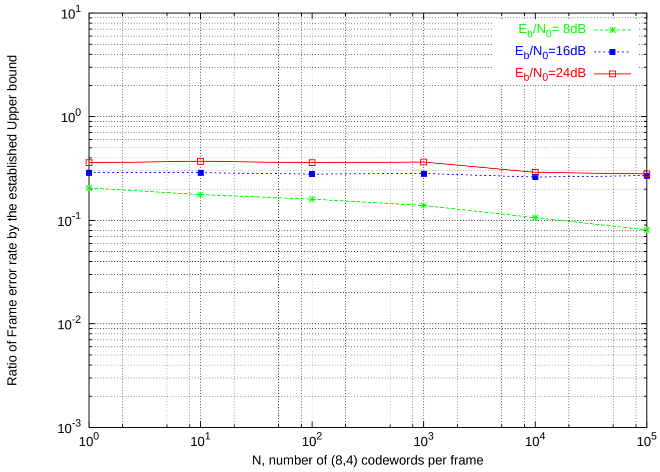

Fig. 5. Ratio of the Monte Carlo simulated frame error rate by the upper bounds on $\mathcal{P}^{\mathcal{C}}_{\rm out}(\gamma)$ and $\mathcal{P}^{\mathcal{C}}_{\rm noise}(\gamma)$, $\mathcal{C}_0 = (8,4,4)$.

denotes the outage region of the turbo code, $P_e^{\mathcal{C}}(\gamma|\boldsymbol{\alpha},K_f,n_{\rm it})$ is the conditional error probability and $n_{\rm it}$ denotes the number of iterations of the iterative decoder. In words, $\mathcal{R}_{\rm out}(\gamma,\mathcal{C})$ is the fading region such that, for a fixed SNR γ the iterative decoder will not be able to decode. Thus, the error probability for large frame length is given by the distribution of the decoding threshold as a function of the fading.

It is possible to efficiently compute the outage boundary $\mathcal{B}_{\rm out}(\gamma,\mathcal{C})$. Figure 6 clearly illustrates the process. We take a grid of fading coefficients orthogonal to the BPSK outage curve and compute density evolution in all of them. If for a given fading the density evolution algorithm does not converge (thin dots), we move to the next point in the grid and run it again. The first point where the algorithm converges defines the boundary.

Brute force computation of the threshold distribution can be very complex, as for every fading realization we need a run of the density evolution algorithm. In order to reduce the complexity of the brute force density evolution algorithm we only run the algorithm whenever there is no BPSK outage and when $\alpha_{\min}\frac{E_b}{N_0} > \frac{E_b}{N_0}\big|_{\rm th}$, where $\alpha_{\min} = \min\alpha$ and $\frac{E_b}{N_0}\big|_{\rm th}$

is the iterative decoding threshold of the turbo-code in the AWGN channel. This preprocessing stage severely accelerates the overall algorithm and makes it practical.

Figures 7 and 8 illustrate the density evolution method used to compute the error probability. As we observe, the h-π-diag channel multiplexer (see [11] for details) is about 0.8 dB from the outage probability limit. Note that this density evolution method for very large block length gives the same results as the finite-length simulations. Therefore, this turbo-code and multiplexer can approach the outage probability limit for *any* block length.

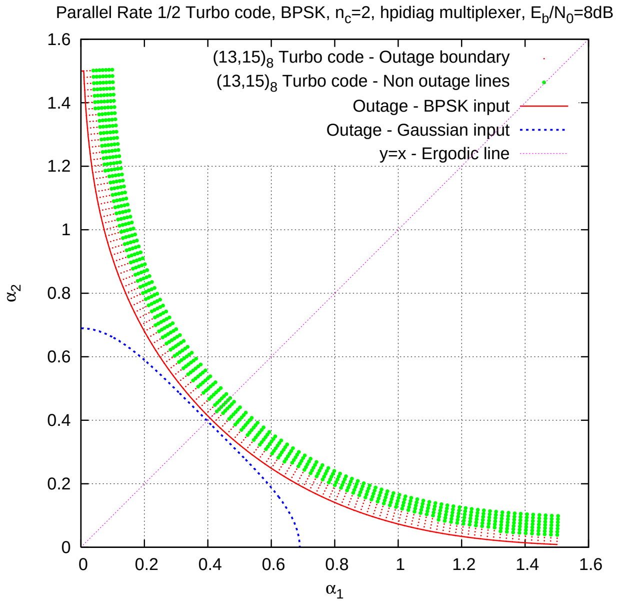

Fig. 6. Boundary region $\mathcal{B}_{\text{out}}(\gamma, \mathcal{C})$ for the turbo-code of rate $R = 1/2$ with iterative decoding in the block-fading channel with $n_c = 2$ and $\frac{E_b}{N_0} = 8$ dB. The thin dots denote the fading values where the density evolution does not converge. The thick dots denote the fading values where the algorithm converges.

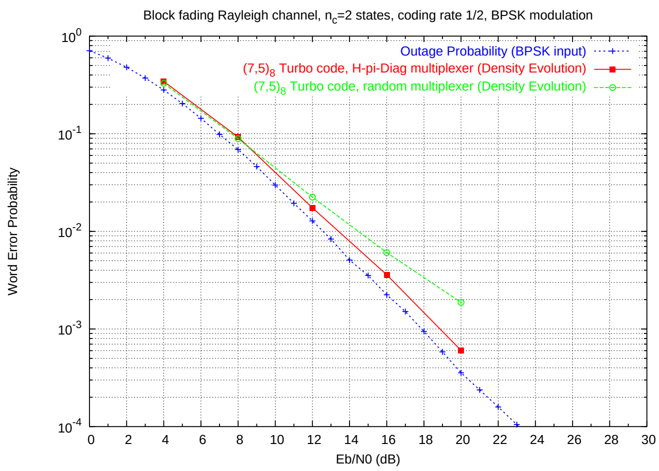

Fig. 7. Error probability computed with the density evolution algorithm for $n_c = 2$ and the rate $R = 1/2$ turbo code with generators $(7, 5)_8$ with random and h-π-diag channel multiplexers.

VI. Conclusions

We have studied the error probability of binary codes in the block-fading channel and we have shown that short block codes and convolutional codes cannot achieve the outage probability limit as their frame error rate grows as the block length increases. We have also shown that the growth rate is logarithmic. In so doing, we have introduced the outage boundary regions, which are a useful graphical tool to understand the source of errors in the decoding process. Furthermore, we show that turbo-codes with good channel multiplexers have frame error probability independent of the block-length and we have computed the asymptotic limit using density evolution.

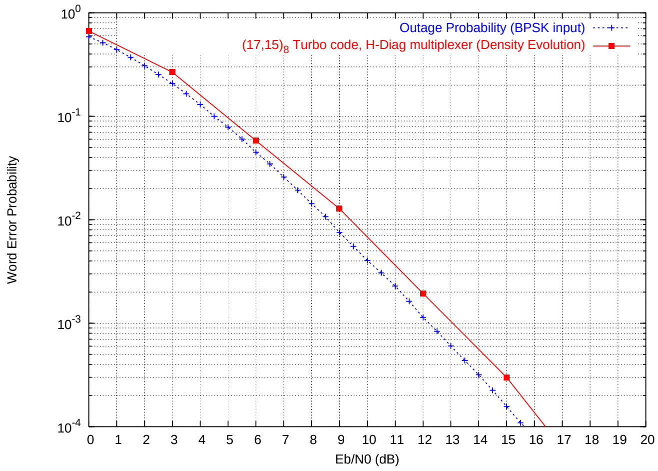

Fig. 8. Error probability computed with the density evolution algorithm for $n_c = 3$ and the rate $R = 1/3$ turbo code with generators $(17, 15)_8$ with the h-diag channel multiplexer.

Acknowledgment

We would like to thank Mr Nicolas Gresset for his precious help during the research work reported in this paper.

References

[1] L. H. Ozarow, S. Shamai 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.

[2] E. Biglieri, J. Proakis and S. Shamai, "Fading channels: information-theoretic and communications aspects," *IEEE Trans. on Inform. Theory*, vol. 44, no. 6, pp. 2619 –2692, Oct. 1998.

[3] J. Proakis, *Digital Communications*, McGraw-Hill, 4th edition, 2001.

[4] A. Guillén i Fàbregas and G. Caire, "Coded modulation in the block-fading channel: Coding theorems and code construction," *IEEE Trans. on Information Theory*, vol. 52, no. 1, Jan. 2006.

[5] R. Knopp and P. Humblet, "On coding for block fading channels," *IEEE Trans. on Inform. Theory*, vol. 46, no. 1, pp. 1643–1646, July 1999.

[6] G. Caire, G. Taricco and E. Biglieri, "Optimum power control over fading channels," *IEEE Trans. on Inform. Theory*, vol. 45, no. 5, pp. 1468–1489, July 1999.

[7] G. Caire, G. Taricco, and E. Biglieri, "Bit-interleaved coded modulation," *IEEE Trans. on Inform. Theory*, vol. 44, no. 3, pp. 927–946, May 1998.

[8] M. Chiani, A. Conti and V. Tralli, "Further results on convolutional code search for block fading channels," *IEEE Trans. on Inform. Theory*, vol. 50, no. 6, pp. 1312–1318, Jun. 2004.

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

[10] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*, North-Holland, 8th impression (1991), 1977.

[11] J.J. Boutros, E.Calvanese Strinati, A. Guillen i Fabregas, "Turbo code design in the block fading channel," *Allerton Conference on Communication, Control and Computing*, Monticello, Illinois, Sept 2004. Available at `http://www.comelec.enst.fr/~boutros`

[12] C. Berrou, A. Glavieux and P. Thitimajshima, "Near shannon limit error correcting coding and decoding: Turbo codes," in *Proc. IEEE Int. Conference on Communications, Geneva, Switzerland*, 1993.

[13] L. Bahl, J. Cocke, F. Jelinek and J. Raviv, "Optimal decoding of linear codes for minimizing the symbol error rate," *IEEE Trans. on Inform. Theory*, vol. 20, pp. 284–287, Mar. 1974.