

On Improved Bounds on the Decoding Error Probability of Block Codes over Interleaved Fading Channels, with Applications to Turbo-Like Codes

Igal Sason and Shlomo Shamai (Shitz)
Department of Electrical Engineering
Technion–Israel Institute of Technology
Haifa 32000, Israel

March 1, 2001

Abstract

We derive here improved upper bounds on the error probability of block codes which are transmitted over fully interleaved Rician fading channels, coherently detected and maximum likelihood decoded. We assume that the fading coefficients during each symbol are statistically independent (due to a perfect channel interleaver), and that perfect estimates of these fading coefficients are provided to the receiver. The improved upper bounds on the block and bit error probabilities are derived for fully interleaved fading channels with various orders of space diversity, and are found by generalizing some recently introduced upper bounds for the binary-input AWGN channel. The advantage of these bounds over the ubiquitous union bound is demonstrated for some ensembles of turbo codes and low-density parity check codes, and it is especially pronounced in a portion of the rate region exceeding the cutoff rate. Our generalization of the Duman and Salehi bound which is based on certain variations of Gallager's bounding technique, is demonstrated to be the tightest reported upper bound. We therefore apply it to calculate numerically upper bounds on the thresholds of some ensembles of turbo-like codes, referring to the optimal maximum likelihood decoding. For certain ensembles of uniformly interleaved turbo codes, the upper bounds derived here also indicate good match with computer simulation results of efficient iterative decoding algorithms.

Index terms: block codes, bounds, decoding error probability, distance spectrum, fading channels, input-output weight distribution, maximum likelihood decoding, thresholds, turbo-like codes.

I. Introduction

Channel coding is a necessary tool for designing reliable wireless communication systems over fading channels (see [4] and references therein). As the error performance of efficiently coded communication systems rarely admit exact expressions, tight analytical bounds emerge as a useful theoretical and engineering tool for assessing performance and to gain insight into the effect of the main system parameters. Since the advent of information theory, the search for efficient coding systems has motivated the introduction of efficient bounding techniques tailored to specific codes or some carefully chosen ensembles of codes. The motivation for introducing and applying such bounds has increased with the recent introduction of turbo codes [3] and the rediscovery of the low density parity check (LDPC) codes [19]. Clearly, the sought for bounds must not be subject to the union bound limitation, as for long block length these families of codes perform reliably at rates above the cutoff rate (R_0) of the channel. Although the maximum likelihood (ML) decoding is mostly prohibitively complex for long enough codes, the derivation of upper bounds on the ML decoding error probability is of interest, providing an ultimate indication on the system performance. Further, the fine structure of efficient coding families is usually not available, necessitating efficient bounds to rely only on basic features, such as the distance spectrum or the input-output weight distribution of the codes, which can usually be found by some analytical methods (e.g, [20]).

Improved upper bounds on the ML decoding error probability for a binary-input additive white Gaussian noise (AWGN) channel were reported in the literature (e.g, [7], [9], [11], [16], [22], [23], [24]) with a variety of applications to efficient coding techniques. However, most of the bounds on the ML decoding error probability that have been reported so far for interleaved fading channels were mainly based on the union bound (e.g, [1], [10], [15]).

In this paper, we derive new rigorous analytical upper bounds on the ML decoding error probability of binary linear block codes, operating over fully interleaved (memoryless) Rician fading channels. These bounds are applied in several ensembles of turbo-like codes, demonstrating their significant advantage over the ubiquitous union bounds in a portion of the rate region above R_0 . Throughout the paper, we assume a perfect side information on the channel i.i.d fading coefficients which are available to the receiver. The theoretical implications of this assumption are discussed in [18].

Two bounding techniques are proposed here: The first upper bound is a modified and generalized version of the Duman and Salehi bounds for a binary-input AWGN channel ([9], [11]), which are based on modifying the classical Gallager bound [14]. We undertake this generalization and modify the derivation of the Duman and Salehi upper bound on the bit error probability, as to tighten the bound further. The second version of Duman and Salehi bounds [11] for a binary-input AWGN channel is generalized for fully interleaved fading channels, and that generalization yields

the *tightest* reported upper bound on the ML decoding error probability for coded communications over interleaved fading channels (see also [28]). This bounding technique is also amenable for calculations of upper bounds on the thresholds for ensembles of efficient codes, such as the regular LDPC codes ([13]) and the regular ‘repeat and accumulate’ (RA) codes ([6]). The second upper bound derived here is a generalization of the Engdahl and Zigangirov bound [12] for fully interleaved fading channels, where this bound was originally derived for a binary-input AWGN channel.

In parallel to our study here, upper bounds for coded communications over fully interleaved fading channel were derived by Divsalar and Biglieri ([8]), and also by Sason, Shamai and Divsalar ([27]). It is demonstrated in our paper that the bounds proposed here (especially, the bound that stems from the generalization of the Duman and Salehi bounds) compete favorably with the other reported upper bounds (see also [28], [29]). For long enough block codes, the tightness of the upper bounds proposed here is especially pronounced in a portion of the rate region exceeding the cutoff rate. By generalizing the framework of the Duman and Salehi bounding technique, upper bounds on the decoding error probability are studied for the mismatched case, where inaccurate estimates of the independent fading coefficients are provided to the receiver (see [26] and [28]).

The paper is organized as follows: The model of the considered coded communication system and further details which makes the presentation self-contained are introduced in section II. The improved upper bounds on the ML decoding error probability and the approach for calculating upper bounds on the thresholds of block codes which are transmitted over fully interleaved fading channels is introduced in section III. In section IV, these bounds are applied to several ensembles of turbo-like codes and for various orders of space diversity. These bounds are also compared to computer simulation results of efficient iterative decoding algorithms, and a good match is demonstrated in our examples. Section V concludes the paper.

II. Model and Preliminaries

A. The System Model

The model of the communication system is the following: The information bits are encoded, fully interleaved and BPSK modulated. Then, the modulated signal is transmitted through a frequency non-selective fading channel. We discuss in this paper fully interleaved Rician fading channels and also Rayleigh fading channels where the latter may be combined with space diversity of order L , based on the maximum ratio combining (MRC) principle. As a consequence of a perfect channel interleaver (which clearly differs from the interleaver of the code), the fading coefficients which correspond to the interleaved coded bits are assumed to be i.i.d. The noise added to the signal is

an additive white Gaussian noise (AWGN) with a zero mean and a double-side spectral density of N_0 . At the receiver, assumed to be equipped with ideal channel state information (realizations of the fading values), we assume that the fading coefficients received by these L antennas are statistically independent. The received signal is coherently detected. Finally, the demodulated bits are deinterleaved (according to the inverse permutation of the channel interleaver) and ML decoded.

Considering a turbo code, we assume a termination to the all-zero state at the end of each frame (block). Clearly, no termination is required for block codes in general and for LDPC codes and RA codes in particular.

B. The Capacity and the Cutoff-Rate of Binary-Input Fully interleaved Fading Channels

We denote the pdf of the non-negative¹ fading a by $p(a)$. Clearly, with a (ideally given to the receiver) interpreted as part of the measurements and independent of the transmitted signals, it follows:

$$\begin{aligned} p_0(y, a) &= \frac{1}{\sqrt{2\pi}} \cdot \exp \left[-\frac{(y - a\sqrt{2E_s/N_0})^2}{2} \right] \cdot p(a) \\ p_1(y, a) &= \frac{1}{\sqrt{2\pi}} \cdot \exp \left[-\frac{(y + a\sqrt{2E_s/N_0})^2}{2} \right] \cdot p(a) \end{aligned}, \quad \begin{array}{l} -\infty < y < \infty \\ a \geq 0 \end{array}, \quad (1)$$

where $\frac{E_s}{N_0}$ stands for the energy per symbol to the spectral noise density.

For the binary-input, memoryless and symmetric channels in (1), the probability distribution of the input which achieves the channel capacity is clearly symmetric: $\text{Prob}(x = 0) = \text{Prob}(x = 1) = \frac{1}{2}$. A straightforward calculation of the channel capacity (C) of the fully interleaved fading channels in (1) provides the following equality:

$$C = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \int_0^{\infty} p(a) \exp \left[-\frac{1}{2} \left(y + a\sqrt{\frac{2E_s}{N_0}} \right)^2 \right] \log_2 \left(\frac{2}{1 + \exp \left(2ay\sqrt{\frac{2E_s}{N_0}} \right)} \right) da dy, \quad (2)$$

in units of bits per channel use.

¹The effect of the phases of the fading measurements is eliminated at the receiver and the fades during each symbol are treated as non-negative random variables.

For a fully interleaved Rician fading channel, the probability density function of the amplitudes of the i.i.d fading coefficients is:

$$p(a) = \begin{cases} 2a(K+1) \exp(-(K+1)a^2 - K) I_0\left(2\sqrt{K(K+1)}a\right) & a \geq 0 \\ 0 & a < 0 \end{cases}, \quad (3)$$

where the Rician parameter K stands for the power ratio of the direct to the diffused received path of the fading channel, and $I_0(x)$ designates the Modified Bessel function of order zero:

$$I_0(x) = \frac{1}{\pi} \int_0^\pi \exp(x \cos \theta) d\theta, \quad (-\infty < x < \infty).$$

The probability density function of the i.i.d fading coefficients of a fully interleaved Rayleigh fading channel with MRC diversity of order L admits the form:

$$p(a) = \begin{cases} \frac{2L^L a^{2L-1} \exp(-La^2)}{(L-1)!} & a \geq 0 \\ 0 & a < 0 \end{cases}. \quad (4)$$

Clearly, for coded communications: $E_s = RE_b$ where E_s , E_b designate the energies per coded symbol and information bit, respectively, and R is the rate of the code (in bits per channel use).

The value of $\frac{E_b}{N_0}$ which corresponds to the channel capacity for a certain code rate R is calculated numerically by solving the implicit equation: $C = R$, where C is expressed in (14), associated with the appropriate expression for the probability density function $p(a)$ of the fading coefficients.

When the bit error probability is allowed not to exceed a certain value P_b , then by applying the rate-distortion theory with the Hamming distance between two binary codewords as a distortion measure, the minimal theoretical value of $\frac{E_b}{N_0}$ is found by solving numerically the implicit equation:

$$C = R (1 - h_2(P_b)), \quad (5)$$

where $h_2(x)$ designates the binary entropy function: $h_2(x) = -x \log_2(x) - (1-x) \log_2(1-x)$ and the capacity C of the considered fully interleaved fading channels is expressed in (2).

The cutoff rate (in bits per channel use) of a fully interleaved Rayleigh fading channel with MRC space diversity of order L admits the form:

$$R_0 = 1 - \log_2 \left(1 + \left(1 + \frac{E_s}{LN_0} \right)^{-L} \right),$$

or $\frac{E_b}{N_0}$ in terms of R is given by:

$$\frac{E_b}{N_0} = \frac{L}{R} \left[\left(2^{1-R} - 1 \right)^{-\frac{1}{L}} - 1 \right]. \quad (6)$$

A straightforward calculation of the cutoff rate of a fully interleaved Rician fading channel yields:

$$R_0 = 1 - \log_2(1 + Z), \quad (7)$$

where:

$$\begin{aligned} Z &= \int_0^\infty \exp\left(-\frac{a^2 E_s}{N_0}\right) p(a) da \\ &= \sqrt{\frac{4K(K+1)^3}{\pi \left(K+1 + \frac{E_s}{N_0}\right)^3}} \cdot \int_0^\pi \exp\left(-\frac{K(K+1)\sin^2\theta + \frac{KE_s}{N_0}}{K+1 + \frac{E_s}{N_0}}\right) \cos\theta Q\left(\frac{\sqrt{2K(K+1)}\cos\theta}{\sqrt{K+1 + \frac{E_s}{N_0}}}\right) d\theta \\ &\quad + \frac{(K+1)\exp(-K)}{K+1 + \frac{E_s}{N_0}}, \end{aligned} \quad (8)$$

where the last transition in (8) results in by the substitution of $p(a)$ in (3).

C. The Pairwise Error Probability and Union Bounds

For a fully interleaved Rician fading channel with a Rician factor K , the expression of the pairwise ML decoding error probability for two codewords which differ in d symbols was derived in [30]. This derivation relied on the Craig's identity [5] for the Q -function:

$$Q(x) = \frac{1}{\pi} \int_0^{\frac{\pi}{2}} \exp\left(-\frac{x^2}{2\sin^2\theta}\right) d\theta, \quad x \geq 0,$$

where $Q(u) = \frac{1}{\sqrt{2\pi}} \int_u^\infty e^{-t^2/2} dt$ is the probability that a zero mean and unit variance Gaussian RV exceeds an arbitrary value u ($-\infty < u < \infty$).

Under the assumptions in subsection A, the following expressions for the pairwise error probability refer to the case where the Hamming distance between the transmitted codeword (x) and another competitive codeword (\hat{x}) is d .

For of a fully interleaved Rician fading channel whose Rician factor is K , the expression for the pairwise error probability results in by combining equations (25),(38) in [30]:

$$\text{Prob}(x \rightarrow \hat{x} \mid W_H(x, \hat{x}) = d) = \frac{1}{\pi} \int_0^{\frac{\pi}{2}} \left(\frac{1+K}{1+K + \frac{E_s/N_0}{\sin^2\theta}}\right)^d \exp\left(-\frac{Kd}{1 + \frac{(1+K)\sin^2\theta}{E_s/N_0}}\right) d\theta, \quad (9)$$

where $W_H(x, \hat{x})$ designates the Hamming distance between the two binary codewords x and \hat{x} .

For fully interleaved Rayleigh fading channels with MRC space diversity of order L (where the fading coefficients received by the L antennas are assumed to be i.i.d), the expression for the pairwise ML decoding error probability results in by substituting $K = 0$ in (9), and by also replacing E_s and d in the left hand side of (9) with $\frac{E_s}{L}$ and dL , respectively:

$$\text{Prob}(x \rightarrow \hat{x} \mid W_H(x, \hat{x}) = d) = \frac{1}{\pi} \int_0^{\frac{\pi}{2}} \left(\frac{1}{1 + \frac{E_s/N_0}{L \sin^2 \theta}} \right)^{dL} d\theta . \quad (10)$$

The union bound on the block error probability for a ML decoded linear and binary block code (designated by P_e) admits the form:

$$P_e \leq \sum_{d=d_{\min}}^n S_d \text{Prob}(x \rightarrow \hat{x} \mid W_H(x, \hat{x}) = d) , \quad (11)$$

where d_{\min} denotes the minimal Hamming weight of the nonzero codewords of the code C , and the expressions of the pairwise error probability for the fully interleaved fading channels studied here are provided in (9), (10). Here, S_d is the appropriate coefficient of the distance spectrum of the code, which designates the number of codewords whose Hamming weight equals d .

Similarly, the union bound on the bit error probability admits the form:

$$P_b \leq \sum_{d=d_{\min}}^n S'_d \text{Prob}(x \rightarrow \hat{x} \mid W_H(x, \hat{x}) = d) , \quad (12)$$

where:

$$S'_d \triangleq \sum_{\omega=1}^k \left\{ \binom{\omega}{k} \cdot A_{\omega,d} \right\} , \quad (13)$$

and where $A_{\omega,d}$ is the appropriate coefficient of the input-output weight distribution (enumeration) of the considered systematic block code, and it denotes the number of codewords of the code C possessing an overall Hamming weight d and a Hamming weight ω for the information (systematic) bits.

III. Improved Upper Bounds

A. Generalization and modification of the Duman and Salehi upper bounds ([9], [11])

The first type of improved upper bounds on the ML decoding error probability are derived here by generalizing and modifying the Duman and Salehi bounds, which were specifically derived for the binary-input AWGN channel. In this section, we introduce a generalization of these improved upper bounds for fully interleaved fading channels.

Let C be a binary and linear block code of length n and rate $R = \frac{k}{n}$, and suppose that its distance spectrum $\{S_d\}_{d=1}^n$ is available. Without loss of generality, we assume that the all-zero codeword is transmitted (based on the linearity of the code C and the symmetry of the channel). Clearly, $E_s = RE_b$, where E_s , E_b designate the energies per coded symbol and information bit, respectively. The binary-input channel is memoryless (due to a perfect channel interleaver) and also has a symmetric output, which yields that the following equation holds for the conditional probability density functions (pdf) with binary inputs: $p_0(y, a) = p_1(-y, a)$, where $y_i = a_i x_i + \nu_i$ ($i = 1, 2, \dots, n$) are the components of the demodulated signal, corresponding to antipodal signaling $x_i \in \{+\sqrt{E_s}, -\sqrt{E_s}\}$, i.i.d fading coefficients (a_i) and samples (ν_i) of a zero-mean Gaussian noise with variance $\frac{N_0}{2}$.

For the derivation of the upper bound on the block error probability, the block code C is partitioned into a set of subcodes $\{C_d\}_{d=1}^n$, where every subcode C_d includes all the codewords which possess a constant Hamming weight d ($d = 1, 2, \dots, n$) and also the all-zero codeword.

Let $P_e(d)$ designate the conditional block error probability associated with the ML decoding of the subcode C_d , when the all-zero codeword is transmitted. Based on the union bound as applied to the subcodes, we get an upper bound on the ML decoding error probability of the block code C :

$$P_e \leq \sum_{d=d_{\min}}^n P_e(d), \quad (14)$$

where $d = d_{\min} \dots, n$ is the Hamming weight of the non-zero codewords of the subcode C_d .

The generalization of the second version of Duman and Salehi bounds [11] relies on the classical Gallager's bounding technique [14] and yields the following upper bound on $P_e(d)$ (see Appendix A):

$$P_e(d) \leq (S_d)^\rho \left\{ \left(\int_{-\infty}^{\infty} \int_0^{\infty} \psi(y, a)^{1-\frac{1}{\rho}} p_0(y, a)^{\frac{1}{\rho}} da dy \right)^{(1-\delta)\rho} \cdot \left(\int_{-\infty}^{\infty} \int_0^{\infty} \psi(y, a)^{1-\frac{1}{\rho}} p_0(y, a)^{\frac{1-\lambda\rho}{\rho}} p_1(y, a)^\lambda da dy \right)^{\delta\rho} \right\}^n, \quad \begin{matrix} 0 < \rho \leq 1 \\ \lambda \geq 0 \end{matrix}, \quad (15)$$

where $\delta \triangleq \frac{d}{n}$ is the normalized Hamming weight ($0 \leq \delta \leq 1$), and ψ is an arbitrary non-negative function which satisfies the equation:

$$\int_{-\infty}^{\infty} \int_0^{\infty} \psi(y, a) da dy = 1. \quad (16)$$

The function ψ can be regarded as a tilting measure which depends on the measurements y, a , which are perfectly available to the receiver. Resorting to calculus of variations, we obtain the following form for the optimal function ψ , as to provide the tightest upper bound of the family above:

$$\psi(y, a) = \beta p_0(y, a) \cdot \left(1 + \alpha \left[\frac{p_1(y, a)}{p_0(y, a)} \right]^\lambda \right)^\rho, \quad \begin{matrix} -\infty < y < \infty \\ a \geq 0 \end{matrix}, \quad (17)$$

where α, β are non-negative numbers (see Appendix A).

For specific values of λ, ρ and δ , the parameter α is optimally determined as to satisfy the implicit equation:

$$\frac{\int_{-\infty}^{\infty} \int_0^{\infty} p_0(y, a) \cdot \left(1 + \alpha \left[\frac{p_1(y, a)}{p_0(y, a)} \right]^\lambda \right)^{\rho-1} da dy}{\int_{-\infty}^{\infty} \int_0^{\infty} p_0(y, a) \cdot \left(1 + \alpha \left[\frac{p_1(y, a)}{p_0(y, a)} \right]^\lambda \right)^\rho da dy} = 1 - \delta. \quad (18)$$

The parameter β is then optimally determined by the following relation (which stems directly from (16) and (17)):

$$\beta = \left\{ \int_{-\infty}^{\infty} \int_0^{\infty} p_0(y, a) \cdot \left(1 + \alpha \left[\frac{p_1(y, a)}{p_0(y, a)} \right]^\lambda \right)^\rho da dy \right\}^{-1}. \quad (19)$$

We note here that the left hand side of (18) is a decreasing function of the non-negative parameter α , and it also admits every value between zero and unity (corresponding to $\alpha \rightarrow \infty$ and $\alpha = 0$, respectively). Therefore, the existence and uniqueness of a solution α for (18) is assured for any δ (as $0 < \delta < 1$), and this solution can be determined numerically (e.g, by the bisection method).

We observe from our discussion so far that the minimization of the above upper bound on the block error probability (which is based on the minimization of the upper bound on $P_e(d)$ in (15) and the calculation of the bound (14)) involves a numerical minimization over the parameters λ and ρ (where $\lambda \geq 0$ and $0 < \rho \leq 1$), for every particular subcode C_d ($d = 1, 2, \dots, n$). The optimal values of α and β which are related to the optimal tilting measure ψ in (17) are numerically evaluated from (18), (19) as a function of the two optimized parameters λ and ρ . That minimization is performed separately for every subcode (where the number of the subcodes C_d doesn't exceed the length n of the block code C , and clearly we are interested only on the subcodes C_d for which $S_d > 0$, as otherwise $P_e(d) = 0$).

Suppose we wish to calculate an upper bound on the block error probability for an ensemble of linear block codes whose *average* distance spectrum is calculable. Then, by applying the Jensen inequality to the right hand side of (15), one gets: $E[(S_d)^\rho] \leq (E[S_d])^\rho$, where $0 \leq \rho \leq 1$. The upper bound (15) stays therefore valid by also replacing S_d in its right hand side with the statistical expectation $E[S_d]$ (as was first noted in [9]).

Let C be a binary, *systematic* and linear block code (the fact that the code is systematic is necessary for the derivation of the upper bound on the *bit* error probability, although that property was clearly irrelevant for the derivation of the upper bound on the block error probability). Similarly to (14), the upper bound on the bit error probability with ML decoding is:

$$P_b \leq \sum_{d=d_{\min}}^n P_b(d), \quad (20)$$

where $P_b(d)$ designates the conditional bit error probability of the subcode C_d with ML decoding, when the all-zero vector is the transmitted codeword. We note that since the subcode C_d usually forms a non-linear block code, then the conditional upper bound on the block/ bit error probabilities may depend on the transmitted codeword in the subcode C_d (as opposed to the case for the linear block code C , for which the conditional error probability doesn't depend on the transmitted codeword).

Our generalization and modification of the Duman and Salehi bound on the bit error probability ([9], [11]) is presented in appendix A, which finally results in the following form for the upper bound on the conditional bit error probability:

$$P_b(d) \leq (S'_d)^\rho \left\{ \left(\int_{-\infty}^{\infty} \int_0^{\infty} \psi(y, a)^{1-\frac{1}{\rho}} p_0(y, a)^{\frac{1}{\rho}} da dy \right)^{(1-\delta)\rho} \cdot \left(\int_{-\infty}^{\infty} \int_0^{\infty} \psi(y, a)^{1-\frac{1}{\rho}} p_0(y, a)^{\frac{1-\lambda\rho}{\rho}} p_1(y, a)^\lambda da dy \right)^{\delta\rho} \right\}^n, \quad \begin{matrix} 0 < \rho \leq 1 \\ \lambda \geq 0 \end{matrix}, \quad (21)$$

where S'_d is introduced in (13).

The concept of the minimization of the upper bound on the bit error probability is similar to the concept which was described above for the upper bound on the block error probability. Also here, the two parameters λ and ρ are optimized for every subcode C_d for which $S_d > 0$ (where $d = 1, 2, \dots, n$), and the parameters α and β which are related to the optimal tilting measure ψ in (17) are calculated numerically as a function of the other two parameters λ and ρ , based on (18), (19) (where these equations are also valid for the optimized upper bound on the bit error probability).

The main modification of the above upper bound on the *bit* error probability is that the union

bound (20) is applied here to a significantly reduced number of subcodes, as compared to the number of subcodes that were involved in the derivation of the Duman and Salehi bounds on the bit error probability (see [9], [11]). The union bound (20) is applied to the constant Hamming weight subcodes C_d (as is also the case for the derivation of the upper bound on the block error probability), instead of applying the union bound on the subcodes which possess a constant information Hamming weight (w) and also a constant overall Hamming weight (d) (as was the case in the derivation of the Duman and Salehi upper bound on the bit error probability). That reduces considerably the number of terms in the union bound (20) (as the reduced number of subcodes grows here linearly with n , while it grows like n^2 in the corresponding derivation of the Duman and Salehi upper bound on the bit error probability). Clearly, that modification tightens the overall upper bound on the bit error probability (20), as compared to the Duman and Salehi bound on the bit error probability.

Another modification performed in the derivation of the above bounds on the block and bit error probabilities (as compared to the second version of Duman and Salehi bounds [11]) is connected to equations (18) and (19) which facilitate to determine numerically the values of α and β which are related to the optimal function $\psi(y, a)$ in (17), and hence reduces considerably the complexity of the optimization process over the remaining parameters (λ, ρ) in the upper bounds (15) and (21). The reasonable complexity involved in the numerical two-parameters optimizations (which are involved in the calculation of the proposed upper bounds) was demonstrated by an efficient Matlab computer program. The numerical computation of the proposed upper bounds involves relatively short run-times for the numerical calculation of the upper bounds derived here, even for long block codes (such as the ensembles of turbo-like codes which are considered in section IV).

Following [9], we compare the partial bounds in (15),(21) with the corresponding union bounds for every Hamming weight d , and then minimize between the two values for every term of the bounds (14),(20) (see section 2).

The general features of our generalization of the Duman and Salehi bounding technique has been addressed in [28], [29].

B. Generalization of Engdahl-Zigangirov upper bound [12]

Assume a binary and linear block code of length n and dimension k is BPSK modulated and transmitted over a fully interleaved fading channel. As noted in section II, we assume throughout the paper that a perfect channel side information (CSI) is available to the receiver. Let the vector $\mathbf{a} = (a_1, a_2, \dots, a_n)$ denote the perfect measurements of the i.i.d. fading samples, where $E[a_i^2] = 1$.

We assume that the symbols ‘0’ and ‘1’ are mapped by the BPSK modulation to $+\sqrt{E_s}$ and $-\sqrt{E_s}$, respectively. As before, we also assume without loss of generality that the all-zero codeword is

transmitted (due to the linearity of the code and the symmetry of the channel). The components of the demodulated signal (\mathbf{y}) are:

$$y_i = a_i \sqrt{E_s} + \nu_i \quad i = 1, 2, \dots, n, \quad (22)$$

where $\{a_i\}_{i=1}^n$ are the i.i.d fading coefficients and $\{\nu_i\}_{i=1}^n$ are the i.i.d. zero-mean Gaussian noise samples with variance $E[\nu_i^2] = \frac{N_0}{2}$.

Define:

$$\begin{aligned} z &= \sum_{i=1}^n a_i y_i \\ &= \sum_{i=1}^n \left(a_i^2 \sqrt{E_s} + a_i \nu_i \right). \end{aligned} \quad (23)$$

Similarly to our approach in the derivation of the previous upper bound, the binary and linear block code C is partitioned into constant Hamming weight subcodes (C_d), where the subcode C_d ($d = 1, 2, \dots, n$) includes all the codewords with a Hamming weight d and also the all-zero codeword.

The fading samples of the channel are i.i.d random variables (RVs), so the pairwise ML decoding error probability stays constant for all the competitive codewords of the same Hamming weight d . As the binary-input symmetric-output channel is memoryless, we assume without any loss of generality that a competitive codeword of Hamming weight d differs from the transmitted all-zero codeword in its first d coordinates, i.e, the first d coordinated of the competitive codeword are ones and the succeeding $n - d$ components are zeros.

Let W_d (where $d = 1, 2 \dots n$) be the RV:

$$W_d = \sum_{i=1}^d \left(a_i^2 \sqrt{E_s} + a_i \nu_i \right). \quad (24)$$

If $W_d < 0$, then the codeword of Hamming weight d is preferred by the ML decoder (rather than the all-zero codeword).

The case where z is small enough may yield an unreliable decision of the ML decoder (it may happen for example when the channel undergoes a severe fade). We therefore introduce a threshold η_z and we wish to optimize it in order to get the tightest upper bound among the following family of upper bounds on the ML decoding error probability:

$$P_e \leq \sum_{d=1}^n \left\{ S_d \cdot \text{Prob} \left(W_d < 0, z \geq \eta_z \right) \right\} + \text{Prob} \left(z < \eta_z \right), \quad (25)$$

where $\{S_d\}_{d=1}^n$ is the distance spectrum of the block code C .

In the asymptotic case where $\eta_z \rightarrow -\infty$, the upper bound (14) turns to be the well known union

bound. Therefore, an optimization over the parameter η_z yields an upper bound which is uniformly tighter than the ubiquitous union bound.

Let $p_{W_d|z, \mathbf{a}}(w|z, \mathbf{a})$ denote the conditional pdf of the random variable W_d , given the measurements z, \mathbf{a} . By Bayes' rule, we get the equality:

$$p_{W_d|z, \mathbf{a}}(w|z, \mathbf{a}) = \frac{p_{W_d|\mathbf{a}}(w|\mathbf{a}) \cdot p_{z|W_d, \mathbf{a}}(z|w, \mathbf{a})}{p_{z|\mathbf{a}}(z|\mathbf{a})}. \quad (26)$$

The following probability density functions which appear in the right hand side of (26) possess normal distributions:

$$p_{z|\mathbf{a}}(z|\mathbf{a}) = \frac{1}{\left(\pi N_0 \sum_{i=1}^n a_i^2\right)^{1/2}} \cdot \exp \left\{ -\frac{\left(z - \sqrt{E_s} \sum_{i=1}^n a_i^2\right)^2}{N_0 \sum_{i=1}^n a_i^2} \right\}, \quad (27)$$

$$p_{W_d|\mathbf{a}}(w|\mathbf{a}) = \frac{1}{\left(\pi N_0 \sum_{i=1}^d a_i^2\right)^{1/2}} \cdot \exp \left\{ -\frac{\left(w - \sqrt{E_s} \sum_{i=1}^d a_i^2\right)^2}{N_0 \sum_{i=1}^d a_i^2} \right\}, \quad (28)$$

$$p_{z|W_d, \mathbf{a}}(z|w, \mathbf{a}) = \frac{1}{\left(\pi N_0 \sum_{i=d+1}^n a_i^2\right)^{1/2}} \cdot \exp \left\{ -\frac{\left(z - w - \sqrt{E_s} \sum_{i=d+1}^n a_i^2\right)^2}{N_0 \sum_{i=d+1}^n a_i^2} \right\}. \quad (29)$$

Based on Eqs. (26)-(29), we obtain the equality:

$$\begin{aligned} p_{W_d|z, \mathbf{a}}(w|z, \mathbf{a}) &= \frac{1}{\left(\pi N_0\right)^{1/2}} \cdot \left(\frac{1}{\sum_{i=1}^d a_i^2} + \frac{1}{\sum_{i=d+1}^n a_i^2} \right)^{1/2} \\ &\cdot \exp \left\{ -\frac{1}{N_0} \left(\frac{1}{\sum_{i=1}^d a_i^2} + \frac{1}{\sum_{i=d+1}^n a_i^2} \right) \left(w - \frac{z \cdot \sum_{i=1}^d a_i^2}{\sum_{i=1}^n a_i^2} \right)^2 \right\}. \end{aligned} \quad (30)$$

Therefore, the conditional probability that W_d is negative, given the measurements z, \mathbf{a} is:

$$\text{Prob}(W_d < 0 | z, \mathbf{a}) = \int_{-\infty}^0 p_{W_d | z, \mathbf{a}}(w | z, \mathbf{a}) dw = Q \left(\sqrt{\frac{2}{N_0} \left(\frac{1}{\sum_{i=d+1}^n a_i^2} - \frac{1}{\sum_{i=1}^n a_i^2} \right)} z \right). \quad (31)$$

We introduce now the RVs:

$$u(d) = \sum_{i=1}^d a_i^2, \quad v(d) = \sum_{i=d+1}^n a_i^2, \quad (32)$$

where $d = 1, 2 \dots n$ is the Hamming weight of the competitive codeword (for $d = n : v(d) \triangleq 0$). The RVs $u(d), v(d)$ are statistically independent, as the fading coefficients are i.i.d RVs. The conditional probability in (31) can be rewritten in the form:

$$\text{Prob}(W_d < 0 | z, \mathbf{a}) = Q \left(\sqrt{\frac{2}{N_0} \left(\frac{1}{v(d)} - \frac{1}{u(d) + v(d)} \right)} z \right). \quad (33)$$

The joint conditional probability that W_d is negative and z exceeds an arbitrary threshold η_z when the vector \mathbf{a} is perfectly known to the receiver is calculated from (27), (32), (33):

$$\begin{aligned} & \text{Prob}(W_d < 0, z \geq \eta_z | \mathbf{a}) \\ &= \int_{\eta_z}^{\infty} \text{Prob}(W_d < 0 | z, \mathbf{a}) \cdot p_{z | \mathbf{a}}(z | \mathbf{a}) dz \\ &= \int_{\eta_z}^{\infty} Q \left(\sqrt{\frac{2}{N_0} \left(\frac{1}{v(d)} - \frac{1}{u(d) + v(d)} \right)} z \right) \cdot \frac{1}{(\pi N_0 (u(d) + v(d)))^{1/2}} \\ & \quad \cdot \exp \left(-\frac{(z - (u(d) + v(d)))^2}{N_0 (u(d) + v(d))} \right) dz. \end{aligned} \quad (34)$$

From (32), (34) and the substitutions: $z = \sqrt{E_s} t$ and $\eta = \frac{\eta_z}{\sqrt{E_s}}$, one obtains the following expression for the joint probability that W_d is negative and z exceeds the threshold η_z :

$$\begin{aligned} & \text{Prob}(W_d < 0, z \geq \eta_z) \\ &= \sqrt{\frac{E_s}{\pi N_0}} \int_0^{\infty} \int_0^{\infty} \int_{\eta}^{\infty} Q \left(\sqrt{\frac{2E_s}{N_0} \left(\frac{1}{v} - \frac{1}{u+v} \right)} t \right) \cdot \frac{p_{u(d)}(u) p_{v(d)}(v)}{\sqrt{u+v}} \\ & \quad \cdot \exp \left(-\frac{E_s}{N_0} \frac{(t - (u+v))^2}{u+v} \right) dt du dv, \end{aligned} \quad (35)$$

where $p_{u(d)}$ and $p_{v(d)}$ designate the probability density functions of the *statistically independent* RVs $u(d)$ and $v(d)$, respectively (note that the vector \mathbf{a} also dictates the exact values of the RVs $u(d)$, $v(d)$, where $d = 1, 2, \dots, n$).

From (27), it can be easily verified that:

$$\text{Prob}(z \leq \eta_z | \mathbf{a}) = \int_{-\infty}^{\eta_z} p_{z|\mathbf{a}}(z|\mathbf{a}) dz = Q \left(\sqrt{\frac{2E_s}{N_0}} \left(\sqrt{\frac{\sum_{i=1}^n a_i^2}{\sum_{i=1}^n a_i^2}} - \frac{\eta}{\sqrt{\sum_{i=1}^n a_i^2}} \right) \right), \quad (36)$$

where $\eta \triangleq \frac{\eta_z}{\sqrt{E_s}}$.

From (32): $u(n) = \sum_{i=1}^n a_i^2$, and therefore (36) yields the equality:

$$\text{Prob}(z \leq \eta_z) = \int_0^\infty Q \left(\sqrt{\frac{2E_s}{N_0}} \left(\sqrt{u} - \frac{\eta}{\sqrt{u}} \right) \right) p_{u(n)}(u) du. \quad (37)$$

The substitution of (35),(37) in the right hand side of (25) finally leads to the following upper bound on the ML decoding error probability, which is formulated in terms of the average distance spectrum of the ensemble of codes:

$$P_e \leq \sum_{d=1}^n \left\{ S_d \cdot \sqrt{\frac{E_s}{\pi N_0}} \int_0^\infty \int_0^\infty \int_\eta^\infty Q \left(\sqrt{\frac{2E_s}{N_0}} \left(\frac{1}{v} - \frac{1}{u+v} \right) t \right) \cdot \frac{p_{u(d)}(u)p_{v(d)}(v)}{\sqrt{u+v}} \right. \\ \left. \cdot \exp \left(-\frac{E_s}{N_0} \frac{(t - (u+v))^2}{u+v} \right) dt du dv \right\} + \int_0^\infty Q \left(\sqrt{\frac{2E_s}{N_0}} \frac{u - \eta}{\sqrt{u}} \right) p_{u(n)}(u) du. \quad (38)$$

The tightest upper bound in (38) results by nulling the derivative of the upper bound with respect to η , which yields the following implicit equation for the optimized parameter η :

$$\sum_{d=1}^n \left\{ S_d \int_0^\infty \int_0^\infty Q \left(\sqrt{\frac{2E_s}{N_0}} \left(\frac{1}{v} - \frac{1}{u+v} \right) \eta \right) \frac{p_{u(d)}(u)p_{v(d)}(v)}{\sqrt{u+v}} \right. \\ \left. \cdot \exp \left(-\frac{E_s}{N_0} \frac{(\eta - (u+v))^2}{u+v} \right) du dv \right\} = \int_0^\infty \frac{p_{u(n)}(u)}{\sqrt{u}} \cdot \exp \left(-\frac{E_s}{N_0} \frac{(u - \eta)^2}{u} \right) du. \quad (39)$$

The existence and uniqueness of a solution η of (39) is proved in Appendix B, and the proof also leads to a constructive algorithm which facilitate to evaluate numerically the optimal η in (38).

An upper bound on the *bit* error probability (with the ML decoding) for an ensemble of linear, binary block codes results in by simply replacing the average distance spectrum $\{S_d\}_{d=1}^n$ of the ensemble of codes by the sequence $\{S'_d\}_{d=1}^n$ as defined in Eq. (13) (similarly to the first bounding technique presented here).

The upper bound (38) with the optimal η in (39) forms a generalization of the upper bound which was derived by Engdahl & Zigangirov ([12]), as for the special case of a binary-input AWGN channel:

$$p_{u(d)}(u) = \delta(u - d), \quad p_{v(d)}(v) = \delta(v - (n - d)), \quad d = 1, 2, \dots, n, \quad (40)$$

where δ denotes the Dirac delta function. For this specific channel, the substitution of (40) in (38) yields the upper bound:

$$P_e \leq \sum_{d=1}^n \left\{ S_d \sqrt{\frac{E_s}{\pi N_0}} \frac{1}{\sqrt{n}} \int_{\eta}^{\infty} Q \left(\sqrt{\frac{2E_s}{N_0}} \frac{d}{n(n-d)} t \right) \cdot \exp \left(-\frac{E_s}{N_0} \frac{(t-n)^2}{t} \right) dt \right\} + Q \left(\sqrt{\frac{2E_s}{N_0}} \frac{n-\eta}{\sqrt{n}} \right), \quad (41)$$

which coincides with the Engdahl & Zigangirov upper bound [12] for the binary-input AWGN channel. The substitution of (40) in the optimization equation (39) for the threshold η , yields the simplified optimization equation:

$$\sum_{d=1}^n S_d Q \left(\sqrt{\frac{2E_s}{N_0}} \frac{d}{n(n-d)} \eta \right) = 1, \quad (42)$$

which also agrees with the optimization equation in [12], derived for the particular case of a binary-input AWGN channel.

Further algebraic simplifications of the upper bound expressed in Eqs. (38),(39) for fully interleaved fading channels are proposed in Appendix C.

C. A calculation of an upper bound on the threshold for a general ensemble of codes over fully interleaved fading channels

Let C be an ensemble of binary, linear (or geometrically uniform) block codes of length n and rate R . In this section, we calculate an upper bound on the threshold of the energy per bit to spectral-noise-density $\left(\frac{E_b}{N_0}\right)$ which ensures a vanishing ML decoding error probability over fully interleaved fading channels, as the block length (n) tends asymptotically to infinity.

Based on the above generalization and modification of Duman and Salehi upper bounds (see (14)–(19)), we define the following expressions:

$$\begin{aligned} A &\triangleq \int_{-\infty}^{+\infty} \int_0^{\infty} \psi(y, a)^{1-\frac{1}{\rho}} p_0(y, a)^{\frac{1}{\rho}} da dy \\ B &\triangleq \int_{-\infty}^{+\infty} \int_0^{\infty} \psi(y, a)^{1-\frac{1}{\rho}} p_0(y, a)^{\frac{1-\lambda\rho}{\rho}} p_1(y, a)^{\lambda} da dy \end{aligned} \quad , \quad \begin{array}{l} \lambda > 0 \\ 0 < \rho \leq 1 \end{array} \quad ,$$

where the optimal function ψ which is expressed in (17)–(19) depends on the three parameters λ, ρ, δ .

We also define the following notations which are related to the exponential behavior of the distance spectrum of the code (or ensemble of codes):

$$r_{\delta, n} \triangleq \frac{\ln(S_d)}{n} \quad , \quad r_{\delta} \triangleq \lim_{n \rightarrow \infty} r_{\delta, n} \quad , \quad \delta \triangleq \frac{d}{n} \quad (0 \leq \delta \leq 1).$$

The optimized upper bound (15) gets the following form when the block-length n tends to infinity:

$$\begin{aligned} P_e(d) &\leq \min_{\lambda > 0, 0 < \rho \leq 1} \left\{ (S_d)^{\rho} \left[A^{(1-\delta)\rho} B^{\delta\rho} \right]^n \right\} \\ &= \min_{\lambda > 0, 0 < \rho \leq 1} e^{-n \left[-(1-\delta)\rho \ln A - \delta\rho \ln B - \rho r_{\delta} \right]} \\ &= e^{-nE\left(\delta, R, \frac{E_b}{N_0}\right)} \quad , \quad d = 1, 2 \dots n \quad , \end{aligned}$$

where $E\left(\delta, R, \frac{E_b}{N_0}\right) = \max_{\lambda > 0, 0 < \rho \leq 1} \left\{ -(1-\delta)\rho \ln A - \delta\rho \ln B - \rho r_{\delta} \right\}$.

Based on the union bounding technique which yields inequality (14), we derive the following upper bound on the ML decoding error probability:

$$P_e \leq n e^{-nE\left(R, \frac{E_b}{N_0}\right)} \doteq e^{-nE\left(R, \frac{E_b}{N_0}\right)} \quad , \quad (43)$$

where

$$\begin{aligned} E\left(R, \frac{E_b}{N_0}\right) &= \min_{0 < \delta \leq 1} E\left(\delta, R, \frac{E_b}{N_0}\right) \\ &= \min_{0 < \delta \leq 1} \max_{0 < \rho \leq 1, \lambda > 0} \left\{ -(1-\delta)\rho \ln A - \delta\rho \ln B - \rho r_{\delta} \right\} \quad . \end{aligned} \quad (44)$$

Then, we calculate numerically the minimal value of $\frac{E_b}{N_0}$ which ensures that $E\left(R, \frac{E_b}{N_0}\right) > 0$.

The minimization with respect to δ in (44) is over the range $0 < \delta \leq 1$ (excluding $\delta = 0$). However, if for $\delta = 0$: $E\left(\delta, R, \frac{E_b}{N_0}\right) = 0$, then it implies that the ML decoding error probability vanishes polynomially (and not exponentially) when the block-length tends to infinity, as was also proved

analytically for the ensemble of the regular RA codes [6].

The above condition ensures reliable communications for asymptotically large block length and $\frac{E_b}{N_0}$ values above the minimal value calculated above. A similar approach was suggested by Divsalar [7] as to determine thresholds for ensembles of codes operating over the AWGN channel. Since various reported upper bounds on the ML decoding error probability can be derived as particular cases of the generalization of the Duman and Salehi bound (see [28], [29]), our approach then furnishes an upper bound on the thresholds with the aid of the generic generalized bound, as to provide the tightest alternative.

As the above generalization of the Duman and Salehi bounds was based on Gallager's bounding technique, it should therefore achieve the channel capacity for the ensemble of fully random block codes. In order to verify it numerically (based on the above condition which is related to (44)) for fully interleaved fading channels (and for any rate R of that ensemble codes), we express the distance spectrum of this ensemble of codes:

$$S_d = 2^{-n(1-R)} \cdot \binom{n}{d} \doteq 2^{-n(1-R)} 2^{nh_2(\delta)}, \quad (45)$$

where $h_2(\delta) = -\delta \log_2(\delta) - (1 - \delta) \log_2(1 - \delta)$ is the binary entropy function. Then, the following exponential behavior of the distance spectrum for that ensemble of codes results:

$$r_\delta = \frac{\ln(S_d)}{n} \doteq [h_2(\delta) - (1 - R)] \ln 2,$$

where \doteq designates exponential equivalence. Finally, the substitution of the asymptotic expression for $\{r_d\}$ into (44) verifies numerically that the generalization of the Duman & Salehi bound achieves the channel capacity for ensembles of fully random block codes with asymptotically infinite block length. This result was proved theoretically in [29] without any decomposition of the random-like code to equi-distance subcodes. It was noted in [8] that for the ensemble of rate- $\frac{1}{2}$ fully random block code, the bound derived by Divsalar and Biglieri ensures (for large enough block length) reliable communications over fully interleaved Rayleigh fading channels for $\frac{E_b}{N_0}$ values above 3.06 dB, which falls short by 1.2 dB of channel capacity. It was also noted in [8] that for a zero-rate code ($R \rightarrow 0$), the bound of Divsalar and Biglieri ensures reliable communications for $\frac{E_b}{N_0}$ above -1 dB, falling short by about 0.6 dB of channel capacity. This demonstrates the superiority of the generalized Duman and Salehi bounds also at low rates where the relative tightness of the Divsalar and Biglieri bound is enhanced.

We consider here thresholds for ensembles of structured codes operating over fully interleaved fading channels. The first ensemble of structured codes considered here is the ensemble of uniformly interleaved regular RA codes, which was proposed by Divsalar, Jin and McEliece [6]. This ensemble

of serially concatenated codes (see Fig. 1a) consists of a repetition code (where each bit is repeated q times), followed by a uniform interleaver and a differential encoder (accumulator). The exponent of the distance spectrum of long enough RA codes (where the code rate is $R = \frac{1}{q}$) is determined in [17]:

$$r_\delta \doteq \max_{0 \leq u \leq \min(2\delta, 2-2\delta)} \left\{ \left(f(u, \delta) + \frac{h_2(u)}{q} \right) \ln 2 \right\}, \quad (46)$$

where

$$f(u, \delta) = -h_2(u) + (1 - \delta) h_2\left(\frac{u}{2(1 - \delta)}\right) + \delta h_2\left(\frac{u}{2\delta}\right). \quad (47)$$

We simplified the numerical maximization expressed in (46), by nulling the derivative with respect to u and the substitution $v = \left(\frac{u}{1-u}\right)^{\frac{1}{q}}$, which yields the polynomial equation:

$$(1 - a)v^{2q} + 2(1 - a)v^q + v^2 - a = 0, \quad (48)$$

where $a = 4\delta(1 - \delta)$. Since in the maximization above $0 \leq u \leq \min(2\delta, 2 - 2\delta)$, u then lies between zero and unity and $v \geq 0$. The polynomial equation (48) has a single non-negative real root (as $0 \leq a \leq 1$), and finally the inverse substitution $u = \frac{v^q}{1+v^q}$ yields the value of the parameter u which maximizes the right hand side of equation (46). This procedure simplifies the numerical calculation of the asymptotic exponential behavior of the distance spectrum of regular RA codes. Since the ensemble of RA codes is amenable to analysis, $\frac{E_b}{N_0}$ thresholds for fully interleaved fading channels are numerically derived here for $q \geq 3$ and asymptotically infinite block length (it was proved in [6] that the block error probability with ML decoding tends to zero for an asymptotically large block length if $q \geq 3$, and we therefore consider the case where $q \geq 3$).

The second ensemble of structured codes considered here comprises the ensemble of regular LDPC codes, which was proposed by Gallager [13]. This ensemble of codes is specified by a sparse parity check matrix containing mostly 0's and only a relatively small number of 1's. An (n, j, k) LDPC code is a block code of length n with a parity check matrix H , where each column contains a small fixed number j ($j \geq 3$) of 1's and each row contains a small fixed number k of 1's (where $k > j$). It easily follows from this definition that the rate R of an (n, j, k) LDPC code satisfies the inequality $R \geq 1 - \frac{j}{k}$ [13], which is also a good approximation for large blocks n and relatively small values of j, k . More specifically the parity check matrix H in the ensemble of (n, j, k) LDPC codes are constructed as follows: Divide the matrix into j sub-matrices, each containing a single 1 in each column. The first of these sub-matrices contains all its 1's in descending order: that is, the i -th row contains 1's in columns $(i - 1)k + 1$ to ik . The other sub-matrices are column permutations of the first. The ensemble of (n, j, k) LDPC codes discussed here is then the ensemble of all codes resulting from random permutations of the columns of each of the bottom $j - 1$ sub-matrices in

the matrix H , with equal probability. This definition was proposed by Gallager for mathematical convenience, which enabled the derivation of an upper bound on the distance spectrum of such ensembles of LDPC codes, which is also asymptotically tight for an infinite block length [13].

According to the analysis in [13], we invoke the following expression for the asymptotic exponent of the distance spectrum for the ensemble of the regular (n, j, k) LDPC codes:

$$r_\delta = \frac{\ln(S_d)}{n} \doteq -(j-1)H(\delta) + j \left(\frac{\mu(s)}{k} + \frac{(k-1)\ln 2}{k} - s\delta \right) \quad (49)$$

where $\mu(s) = \ln \left[\left(\frac{1+e^s}{2} \right)^k + \left(\frac{1-e^s}{2} \right)^k \right]$ and s is a real number, determined by solving the equation $\delta \triangleq \frac{d}{n} = \frac{\mu'(s)}{k}$. By substituting $s = \ln \left(\frac{1-u}{1+u} \right)$, the equation is converted to the polynomial form:

$$(1-2\delta)u^k - u^{k-1} - u + (1-2\delta) = 0, \quad (50)$$

where $\delta \triangleq \frac{d}{n}$ is the normalized Hamming weight ($0 \leq \delta \leq 1$). Moreover, the polynomial equation has a single real root u in the interval $(-1 \leq u \leq 1)$ for even values of k , yielding a single real solution s for equation (50). For odd values of k , equation (50) has a single real root u in the interval $[-1, 1]$ for $\delta \leq \frac{j}{k}$; if $\delta > \frac{j}{k}$, then the limit case where $s \rightarrow \infty$ is the appropriate choice of s in (49) for the calculation of r_δ .

IV. Results

We examine here improved upper bounds on the ML decoding error probability for fully interleaved fading channels with perfect CSI. These bounds are evaluated for certain ensembles of turbo-like codes, and they are also compared with computer simulation results of suboptimal and practical iterative decoding algorithms. As is demonstrated in the following, the tightness of these bounds is especially pronounced in the rate region exceeding the cutoff rate, where the performance of turbo-like codes is most appealing.

The first ensemble of codes which is considered here is the ensemble of the regular RA codes [6] (see Fig. 1a). We examine here the case where the information block length is $N = 1000$ and the number of repetitions of the outer code is $q = 4$, which yields a rate $-1/4$ turbo-like code. For the calculations of the improved upper bounds on the bit error probability which were derived in section III, the sequence $\{S'_d\}_{d=1}^n$ in (13) (where $n = qN$ is the block length of these RA codes) is calculated, based on the prior calculation of the input-output weight distribution of this ensemble of codes in [6] (see Fig. 1b). The two bounds derived in section III and also the upper bound of Divsalar and Biglieri in [8] are depicted in Fig. 2 for a fully interleaved Rayleigh fading channel. The

union bound is regarded here as a benchmark, to assess the usefulness of all the improved bounding techniques at rates beyond the cutoff rate. It is demonstrated here that the generalization of the second version of Duman and Salehi bound ([9], [11]) yields the tightest reported bound. It is also reflected in Fig. 2 that the generalization of the Engdahl & Zigangirov bound [12], results in an upper bound which falls very close to the bound evaluated by Divsalar and Biglieri in [8]. Based on the results depicted in Fig. 2, we get an upper bound on the bit error probability of 10^{-5} at energy per bit to spectral noise density ratios $\left(\frac{E_b}{N_0}\right)$ of 1.85, 2.13, 2.15 and 2.85 dB corresponding to curves 1, 2, 3, 4 respectively. It is evidenced that the generalization of the second version of Duman and Salehi bound yields here a coding gain of 1.00 dB over the ubiquitous union bound, while the other two improved upper bounds (Divsalar & Biglieri bound [8] and the generalized Engdahl & Zigangirov bound) yield a coding gain of about 0.7 dB (with respect to the union bound). Although the outer and inner component codes of these RA codes possess a very simple structure, the improved upper bounds indicate their remarkable performance at rates considerably beyond the cutoff rate, as is also demonstrated by computer simulation results of sum-product iterative decoding algorithm (with 20 iterations). It is also reflected in Fig. 2 that the generalization of the second version of Duman and Salehi upper bound falls below the simulated results of the iterative decoding algorithm above for $\frac{E_b}{N_0} \geq 1.63$ dB, which is markedly below the $\frac{E_b}{N_0}$ value corresponding to the cutoff rate of a fully interleaved Rayleigh fading channel (2.71 dB, based on (6) with $L = 1$ and $R = \frac{1}{4}$). That observation demonstrates the mild sub-optimality of the iterative decoding algorithm.

In order to assess the performance of ensembles of rate-1/3 turbo codes, rate-distortion curves are depicted in Fig. 3, corresponding to rate-1/3 random block codes which operate over fully interleaved Rayleigh fading channels with several orders of MRC space diversity (L). These curves serve for estimating the closeness of the performance of the examined rate-1/3 ensemble of turbo codes to the theoretical rate-distortion limits. By examining also the rate-distortion curves which corresponds to fully interleaved Rician fading channels with perfect CSI at the receiver, we have chosen to examine the value of $K = 2.33$ dB, as the rate-distortion curve for this channel falls exactly between the rate-distortion curves for the two extreme cases (which refer to the fully interleaved Rayleigh fading channel where $K = 0$ and the Gaussian channel, where $K \rightarrow \infty$).

We examine here upper bounds on the ML decoding error probability of the ensemble of rate-1/3 uniformly interleaved turbo codes depicted in Fig. 4a, when these codes operate over fully interleaved fading channels with perfect CSI. That ensemble of the turbo codes consists of two identical recursive systematic convolutional (RSC) codes whose generators are $G_1(D) = G_2(D) = \left[1, \frac{1+D^4}{1+D+D^2+D^3+D^4}\right]$ and a uniform interleaver of length $N = 1000$. As in Fig. 1a, the components

of that ensemble of codes are fixed and the interleaving is uniformly weighted over all possible permutations of length N . For the calculation of the upper bounds on the bit error probability in section III and the upper bound of Divsalar and Biglieri in [8], we first need to calculate the sequence $\{S'_d\}_{d=1}^n$ in (13) (where $n = 3008$ is the block length of the terminated turbo code to the all-zero state). To that end, we first calculated the input-output weight distribution of the two identical RSC component codes above (based on the general technique which was proposed by McEliece in [20]), then we calculated the input-output for the considered ensemble of uniformly interleaved turbo codes (based on the relation between the input-output weight distribution of *uniformly* interleaved turbo codes and the input-output weight distributions of its component codes [2]) and finally applied (13) to the calculation of the sequence $\{S'_d\}_{d=1}^n$ (see Fig. 4b).

The improved upper bounds on the bit error probability which were derived in section III are presented in Fig. 5a for the ensemble of the uniformly interleaved turbo codes depicted in Fig. 4a, when the transmission takes place over a fully interleaved Rayleigh fading channel with perfect CSI. These bounds on the ML decoding error probability are also compared in Fig. 5a with the union bound and with computer simulation results of the Log-MAP iterative decoding algorithm (with up to 10 iterations). Based on Fig. 5a, the two improved bounds that were derived in section III by generalizing the Duman & Salehi bound and the Engdahl & Zigangirov bound yield upper bounds on the bit error probability of 10^{-4} at $\frac{E_b}{N_0} = 2.08$ and 2.55 dB, and the union bound achieves the same bit error probability at $\frac{E_b}{N_0} = 3.25$ dB (which results in coding gains of 1.17 and 0.70 dB as compared to the union bound). Similarly to Fig. 2, the generalized second version of Duman and Salehi bound provides here the tightest upper bound for ML decoding. Based on the iterative decoding simulation results, the generalized Duman and Salehi bound falls very close to simulation results of the Log-MAP iterative decoding algorithm for $\frac{E_b}{N_0} \geq 2.0$ dB (which is 1.24 dB below the value of $\frac{E_b}{N_0}$ which corresponds to the channel cutoff rate for a rate-1/3 code).

For the ensemble of turbo codes depicted in Fig. 4a, it is reflected in Figs. 5(a)-(c) that there is a good match between the generalization of the second version of Duman and Salehi upper bound and the computer simulation results of the Log-MAP iterative decoding algorithm (with 10 iterations). This match is demonstrated for fully interleaved Rayleigh fading channels with various orders of space diversity (based on the MRC principle) and perfect CSI. For fully interleaved Rayleigh fading channels with a sufficiently high order of diversity (where the channels become more Gaussian in nature), the generalization of the Engdahl & Zigangirov bound falls very close to the generalization of the second version of Duman and Salehi bound (as is reflected in Figs. 5(b), 5(c)). It is note that the complexity in the calculation of the generalized Engdahl & Zigangirov bound is significantly lower than that of the generalized Duman & Salehi bound (since in the former bound, an optimization over a single parameter is performed with respect to the whole code). Hence,

the generalization of the Engahl & Zigangirov bound can be especially applied to fully interleaved fading channels with a large order of space diversity.

It is demonstrated in Figs. 5(b),5(c) and 6 that the generalization of the second version of Duman and Salehi bound yields remarkable coding gains as compared to the union bound, referring to the ensemble of rate-1/3 turbo codes (depicted in Fig. 4a), operating over fully interleaved Rayleigh fading channels with several orders of MRC diversity (L). As reflected in Fig. 6, we get an upper bound on the bit error probability of 10^{-4} at $\frac{E_b}{N_0} = 2.05, 1.51, 1.34$ and 1.25 dB for $L = 1, 2, 3$ and 4 respectively. The corresponding union bounds with the same bit error probability are achieved at $\frac{E_b}{N_0} = 3.25, 2.66, 2.45$ and 2.36 dB. These remarkable coding gains (which lie in the range between 1.1 and 1.2 dB) demonstrate the usefulness of our generalized second version of Duman and Salehi bound at a portion of the rate region between the cutoff rate and the capacity. Based on Eqs. (2), (4), the Shannon capacity corresponds to $\frac{E_b}{N_0} = 0.49, -0.01, -0.17$ and -0.25 dB for $L = 1, 2, 3$ and 4 , respectively (see also the rate-distortion curves in Fig. 3 for fully interleaved Rayleigh fading channels with MRC diversity). Hence, the improved upper bounds are within 1.5 to 1.6 dB from capacity.

The ensemble performance of the uniformly interleaved turbo codes depicted in Fig. 4a is studied in Fig. 7 for a fully interleaved Rician fading channel with a Rician factor of $K = 2.33$ dB. The generalized Duman and Salehi bound and the ubiquitous union bound yield upper bounds on the bit error probability of 10^{-4} at $\frac{E_b}{N_0} = 1.59$ and 2.65 dB respectively (see Fig. 7). Based on the rate distortion theory, for an acceptable bit error probability of 10^{-4} , the theoretical limit for a rate-1/3 code operating over the considered fully interleaved Rician fading channel with perfect CSI at the receiver corresponds to $\frac{E_b}{N_0} = 0.02$ dB (as can be verified from Eqs. (2), (3) with $K = 2.33$ dB). The generalized Duman and Salehi bound is then 1.57 dB above the $\frac{E_b}{N_0}$ which corresponds to that theoretical limit and 1.06 dB below the $\frac{E_b}{N_0}$ value which corresponds to the channel's cutoff rate (2.65 dB, as can be verified from (7), (8)). These results also demonstrate the uselessness of the union bound for long enough codes at rates above the cutoff rate of the channel.

In Fig. 8, we compare Gallager's upper bound on the exponent of the distance spectrum of two ensembles of (n, j, k) LDPC codes (which is $\frac{r_\delta}{\ln 2}$ with r_δ in (49)) with the exact exponent of the distance spectrum for the ensemble of uniformly interleaved turbo codes which is depicted in Fig. 4a. The exponent of the ensemble distance spectrum of these turbo codes (see curve 1) is based on the numerical calculation of the distance spectrum of the uniformly interleaved turbo codes (with the aid of the technique introduced in [2] and [20], which was explained above while referring to Fig. 4b). The three ensembles of turbo-like codes considered in Fig. 8 possess almost the same rate ($\frac{1}{3}$) and the same block length (3000). As was noted in [13], (49) is the *exact* asymptotic

exponent of the ensemble distance spectrum of (n, j, k) LDPC codes when the block length n tends to infinity. For any pair of (j, k) , the minimal Hamming weight is typically increased linearly with n . This observation is also reflected in curves 2, 3 of Fig. 8, as the exponent r_δ gets negative values for $\delta < \delta_{j,k}$ (where $\delta_{j,k}$ depends on j, k [13]), and therefore the number of codewords which possess a Hamming weight below $n\delta_{j,k}$ tends asymptotically to zero as $n \rightarrow \infty$). Moreover, it is demonstrated in Fig. 8 that for relatively small values of j, k , the increase in the values of j and k such that the ratio $\frac{j}{k}$ is kept fixed (which implies that the lower bound on the code rate $(1 - \frac{j}{k})$ stays constant [13]) reduces the number of codewords characterized by low Hamming weights and therefore also reduces the error floor which is theoretically associated with the ML decoding for these ensembles of LDPC codes. That phenomenon is demonstrated in Figs. 9(a),(b) for some fully interleaved fading channels with several orders of space diversity ($L = 1, 4$). Increasing the value of j and k (as above) for a fixed block length n , affects therefore the upper bound on the distance spectrum of the ensemble of (n, j, k) LDPC codes in a similar manner to the “spectral thinning” effect [21], which characterizes the influence of increasing the interleaver length on the distance spectrum of turbo codes. It is also demonstrated in Fig. 8 that the “spectral thinning” for the considered ensembles of regular LDPC codes (see curves 2, 3) is more pronounced than for the ensemble of turbo codes depicted in Fig. 4a (see curve 1). That justifies the superiority of the ML bounds for the ensembles of $(3000, 4, 6)$ and $(3000, 6, 9)$ LDPC codes over the ML bounds for the uniformly interleaved turbo code depicted in Fig. 4a, which is also evidenced in Fig. 9(a), 9(b) for fully interleaved Rayleigh fading channels with or without diversity. These upper bounds on the block error probability which are associated with the ML decoding relies on the generalization of the second version of the Duman and Salehi bounds in section III.

The generalization of the second version of Duman & Salehi bounds was also applied to uniformly interleaved turbo codes with interleavers of length not exceeding 1024 uncoded (information) bits, because of inherent overflow limitations associated with the numerical calculation of the distance spectrum of these ensembles of codes. However, this difficulty is circumvented by employing the existing exponential upper bound on the ensemble distance spectrum of the (n, j, k) binary LDPC codes [13]. Hence, for these ensembles of LDPC codes, we combine here the Gallager’s upper bound on the distance spectrum with the generalization of the second version of Duman & Salehi bounds, which yields a tight upper bound on the block error probability for these ensembles of codes, coherently detected and ML decoded. Pursuing that approach, upper bounds on the block error probability for regular LDPC codes of block length 3000–40000 are depicted in Figs. 10(a),(b) for some fully interleaved Rayleigh fading channels with or without space diversity (based on the MRC principle). These upper bounds on the ML decoding error probability indicate the unprecedented performance of LDPC codes of length 5000–40000 coded bits as reflected by their closeness to the ultimate Shannon capacity limit. That conclusion also conforms with the results depicted in

[24] referring to the tangential sphere upper bounds on the ensemble performance of ML decoded LDPC codes in the binary-input AWGN channel. The ML bounds on the block error probability of regular LDPC codes (see Fig. 10(a), 10(b)) substantiate the conclusion that like turbo codes, LDPC codes are strong alternatives for high performance communication systems, striving to approach the ultimate limit of channel capacity.

Upper bounds on thresholds for ensembles of RA and regular LDPC codes (where the block length tends to infinity) are depicted in Figs. 11(a),(b). These thresholds (which refer to the optimal ML decoding) are calculated based on the approach discussed in section III (which relies on the generalization of the second version of Duman & Salehi bounds). It is demonstrated that (n, j, k) LDPC codes (with a sufficiently large value of n) nearly achieve the channel capacity for some fully interleaved Rayleigh fading channels with or without space diversity (based on the MRC principle). It is also demonstrated that by increasing the value of j and k (where the ratio $\frac{j}{k}$ is kept constant), the resulting upper bounds on the threshold values for long enough (n, j, k) LDPC codes approach remarkably the channel capacity. These observations, demonstrated in Figs. 11(a),(b) for some fully interleaved fading channels, conform with similar conclusion made by Gallager for the BSC case [13]. As expected, the upper bounds on the thresholds which are numerically calculated for the ensemble of the regular RA codes (based on the approach in section IIIc) are considerably away from the Shannon capacity limit as compared to the corresponding upper bounds on the thresholds which were calculated by the same approach for regular LDPC codes (see Figs. 11(a),(b)). Obviously, the degradation in performance of the RA codes as compared to LDPC codes (of the same rate) is attributed to the extremely simple structure of the RA codes. On the other hand, RA codes are demonstrated as efficient codes at rates considerably beyond the channel cutoff rate and since they possess a simple and efficient iterative decoding algorithm, they constitute an attractive alternative for ensuring reliable communication in a portion of the rates exceeding the channel cutoff rate. It is also indicated in Figs. 11(a),(b), that for zero approaching rates, RA codes closely approach the channel capacity, as was established in [17].

V. Summary and Conclusions

We introduce here tight rigorous upper bounds on the block and bit error probabilities of ML decoded block codes, operating over fully interleaved fading channels with or without diversity. We assume throughout perfect fading side information available to the receiver. The two improved bounding techniques proposed here are modified and generalized versions of the recently introduced bounds for the AWGN channel by Duman & Salehi ([9], [11]) and Engdahl & Zigangirov [12] (see section III). The improved upper bounds on the block and bit error probabilities with ML decoding

rely solely on the distance spectrum and the input-output weight distribution of the codes (or ensembles of codes) and, to that end, we apply the general distance spectrum evaluation technique introduced in [20]. These improved upper bounds are applied to uniformly interleaved turbo codes [2] (with a termination at the all-zero state), regular low-density parity check (LDPC) codes [13] and some other ensembles of turbo-like codes [6], operating over fully interleaved fading channels with several orders of space diversity. These bounds (referring to ML decoding) are observed also to closely approximate the unprecedented performance achieved by sub-optimal and practical iterative decoding algorithms. Hence, the improved upper bounds studied here can be also applied as a fast technique to approximately assess the performance of iterative decoding.

We apply the generalized Duman & Salehi version II bound (derived in section III) to determine upper bounds on the thresholds of some ensembles of codes operating over interleaved fading channels and ML decoded. This bound achieves the channel capacity for fully random block codes [29], and in this respect it outperforms a recent bound by Divsalar and Biglieri [8] even at low rates. We also apply the generalized Duman & Salehi second version bound to regular LDPC codes and numerically determine their thresholds for some parameters of the codes and for some orders of space diversity (based on the MRC principle). The thresholds for the regular LDPC codes fall very close to channel capacity, as demonstrated in Figs. 11a, 11b. This bounding technique is applied in particular to regular rate $-\frac{1}{3}$ LDPC codes with block length 3K–40K coded bits, operating over fully interleaved fading channels (see Figs. 10a, 10b). These bounds demonstrate that for the considered ensemble of regular LDPC codes with a block length of 10K coded bits, a block error probability of 10^{-5} is ensured at energy per bit to a noise spectral density $\left(\frac{E_b}{N_0}\right)$ of about 0.8 dB away from the channel capacity (either without diversity or with MRC diversity of order 4).

This bound also provides upper bounds on thresholds for ML decoding of the regular repeat-accumulate (RA) codes [6]. Although the thresholds for RA codes are less impressive than those corresponding to regular LDPC codes (see Figs. 11a, 11b), the simple encoding and the low-complexity of the iterative decoding algorithm for RA codes compensate in certain cases for the degradation in their performance. The second bounding technique which is proposed here is a generalization of the Engdahl & Zigangirov bound for the AWGN channel ([12]). It depends on a single parameter that is determined by a numerical solution of an optimization equation (see Eq. (28) and Appendix B (proving the existence and uniqueness of a solution for this equation and also providing an efficient algorithm for solving it). The optimization for this bound is performed once as it applies to the whole block code, without partitioning the block code to constant Hamming weight subcodes and optimizing the parameter for every subcode separately (we demonstrated that for the generalized Engdahl & Zigangirov bound, the partitioning of the linear block code to subcodes results in a looser upper bound). Surprisingly, this bound is approximately as tight as

the Divsalar & Biglieri bound [8] (see Fig. 2) and is considerably easier for numerical evaluation (a numerical optimization of three parameters in the Divsalar and Biglieri [8] is required for every constant Hamming subcode separately). We note that the more Gaussian in nature the channel is, the smaller the gap between the generalized Engdahl & Zigangirov bound and the generalized second version of the Duman & Salehi bound. This phenomenon is reflected by comparing Figs. 5a, 5b and 5c and noticing that increasing the order of the receiver's space diversity (based on the MRC principle) for a fully interleaved fading channel, implies that the probability density function of the channel resembles more strongly the AWGN channel (including LDPC codes and terminated turbo codes) operating over fading channels with relatively large space diversity order (of at least 4 in the examples here).

It is demonstrated here that the second version of Duman & Salehi bound yields the tightest reported upper bound for fully interleaved fading channels (see Figs. 2, 5–7), and its calculation requires modest complexity (as it involves a numerical optimization over two instead of three parameters for every constant Hamming weight subcode separately).

The results of our ML decoding bounding techniques are put in perspective by comparison with the associated Shannon channel capacity of those fading channels with a binary input (see Fig. 3) and with simulated results of efficiently iterative decoded turbo codes (employing the Log-MAP based iterative decoding algorithm). The comparison shows that the considered uniformly interleaved turbo code (depicted in Fig. 4a) with a relatively moderate interleaver length ($N = 1000$), operates 1.55 and 1.75 dB away from the channel capacity (referring to a bit error probability of 10^{-4}) for a Rayleigh fading channel without or with diversity (of order 4) respectively (see Figs. 3, 5a and 5b). As expected, the performance of the considered turbo codes and regular LDPC codes in a fully interleaved Rayleigh fading channel is significantly improved by diversity. For example, for the considered ensemble of uniformly interleaved turbo codes, the improved upper bounds which are based on the generalized Duman & Salehi bounding technique predict a bit error probability of 10^{-4} at $\frac{E_b}{N_0}$ of 2.05, 1.57, 1.35, 1.28 and 1.17 dB for respective diversity orders of 1, 2, 3, 4 and 6 (see Figs. 5(c) and 6).

The generalization of the second version of the Duman and Salehi bounds provides the natural bridge between the 1963 and 1965 Gallager bounds ([13],[14]), and it is suitable for both random and fixed codes (as evidenced in [28], [29]). Many recent useful bounds were demonstrated in [28] and [29] as special cases of the generalization of the Duman and Salehi bounds, which was applied here to certain ensembles of codes operating over fully interleaved fading channels with perfect channel state information. By generalizing the framework of the Duman and Salehi bounding technique, upper bounds on the decoding error probability for the mismatched case, where inaccurate estimates of the independent fading samples are provided to the receiver, are studied in [26], [28].

Appendix A: The Generalized Duman & Salehi Bounding Technique for Fully Interleaved Fading Channels – Technical Details:

Let \mathbf{y} and \mathbf{a} denote the received signal sequence and the perfect measurements of the i.i.d. fades respectively (as mentioned in section III, the effect of the phase is eliminated according to the assumption of perfect CSI). Let $\mathbf{r} = (\mathbf{y}, \mathbf{a})$ denote the $(2n)$ -dimensional vector, where n is the code's block-length. The upper bound (15) is based on Gallager's bounding technique [14], which yields:

$$P_e(d) \leq \underbrace{\int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty}}_{\substack{\text{n-dimensions} \\ \text{(w.r.t. } \mathbf{y})}} \underbrace{\int_0^{\infty} \cdots \int_0^{\infty}}_{\substack{\text{n-dimensions} \\ \text{(w.r.t. } \mathbf{a})}} [p(\mathbf{r}|\mathbf{0})]^{1-\lambda\rho} \left\{ \sum_{\substack{\mathbf{c} \in C_d \\ \mathbf{c} \neq \mathbf{0}}} [p(\mathbf{r}|\mathbf{c})]^\lambda \right\}^\rho d\mathbf{a} d\mathbf{y}, \quad (\text{A.1})$$

where $\lambda \geq 0$, $0 \leq \rho \leq 1$ and $d = 1, 2 \dots n$.

By introducing an arbitrary non-negative function of the form:

$$\Psi(\mathbf{r}) = \prod_{i=1}^n \psi(y_i, a_i), \quad (\text{A.2})$$

which also satisfies equality (16), we get from (A.1):

$$P_e(d) \leq \underbrace{\int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty}}_{\text{n-dimensions}} \underbrace{\int_0^{\infty} \cdots \int_0^{\infty}}_{\text{n-dimensions}} \prod_{i=1}^n \psi(y_i, a_i) \left\{ \sum_{\substack{\mathbf{c} \in C_d \\ \mathbf{c} \neq \mathbf{0}}} \prod_{i=1}^n \psi(y_i, a_i)^{-\frac{1}{\rho}} p_0(y_i, a_i)^{\frac{1-\lambda\rho}{\rho}} \cdot [p_{c_i}(y_i, a_i)]^\lambda \right\}^\rho d\mathbf{a} d\mathbf{y}, \quad (\text{A.3})$$

where c_i equals '1' or '0' for d and $n - d$ indices of i respectively, and the probability density functions p_0, p_1 are expressed in (1). By applying Jensen inequality to the right hand side of (A.3), as ψ in (4) is an arbitrary probability density function, we find for $0 \leq \rho \leq 1$ and $\lambda \geq 0$ that:

$$\begin{aligned} P_e(d) &\leq \left\{ \sum_{\substack{\mathbf{c} \in C_d \\ \mathbf{c} \neq \mathbf{0}}} \underbrace{\int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty}}_{\text{n-dimensions}} \underbrace{\int_0^{\infty} \cdots \int_0^{\infty}}_{\text{n-dimensions}} \prod_{i=1}^n \psi(y_i, a_i)^{1-\frac{1}{\rho}} p_0(y_i, a_i)^{\frac{1-\lambda\rho}{\rho}} \cdot [p_{c_i}(y_i, a_i)]^\lambda d\mathbf{a} d\mathbf{y} \right\}^\rho \\ &= \left\{ S_d \left(\int_{-\infty}^{+\infty} \int_0^{\infty} \psi(y, a)^{1-\frac{1}{\rho}} p_0(y, a)^{\frac{1-\lambda\rho}{\rho}} p_1(y, a)^\lambda da dy \right)^d \cdot \left(\int_{-\infty}^{+\infty} \int_0^{\infty} \psi(y, a)^{1-\frac{1}{\rho}} p_0(y, a)^{\frac{1}{\rho}} da dy \right)^{n-d} \right\}^\rho \\ &= (S_d)^\rho \left(\int_{-\infty}^{+\infty} \int_0^{\infty} \psi(y, a)^{1-\frac{1}{\rho}} g_1(y, a) da dy \right)^{(n-d)\rho} \left(\int_{-\infty}^{+\infty} \int_0^{\infty} \psi(y, a)^{1-\frac{1}{\rho}} g_2(y, a) da dy \right)^{d\rho}, \end{aligned} \quad (\text{A.4})$$

where $\{S_d\}_{d=1}^n$ denotes the distance spectrum of the considered linear block code C (S_d is also the number of non-zero codewords of the constant Hamming weight subcode C_d defined in section 3) and:

$$\begin{aligned} g_1(y, a) &= p_0(y, a)^{\frac{1}{\rho}} \\ g_2(y, a) &= p_0(y, a)^{\frac{1}{\rho}} \left[\frac{p_1(y, a)}{p_0(y, a)} \right]^\lambda, \end{aligned} \quad \begin{array}{l} -\infty < y < +\infty \\ a \geq 0 \end{array}. \quad (\text{A.5})$$

The upper bound (15) results from (A.4) and (A.5), by substituting $\delta = \frac{d}{n}$ (where δ is the normalized Hamming weight).

Resorting to calculus of variations, we obtain the following implicit equation for the optimal function ψ which yields the tightest upper bound on the conditional block error probability ($P_e(d)$) within the family of bounds in (A.4):

$$\left(\frac{(1-\delta)\left(1-\frac{1}{\rho}\right)g_1(y, a)}{\int_{-\infty}^{+\infty} \int_0^\infty \psi(y, a)^{1-\frac{1}{\rho}} g_1(y, a) da dy} + \frac{\delta\left(1-\frac{1}{\rho}\right)g_2(y, a)}{\int_{-\infty}^{+\infty} \int_0^\infty \psi(y, a)^{1-\frac{1}{\rho}} g_2(y, a) da dy} \right) \psi(y, a)^{-\frac{1}{\rho}} + \zeta = 0, \quad (\text{A.6})$$

where ζ designates the Lagrange multiplier.

Based on (A.6), it follows that the optimal ψ in (A.4) is of the form:

$$\psi(y, a) = \left(k_1 g_1(y, a) + k_2 g_2(y, a) \right)^\rho, \quad (\text{A.7})$$

where k_1 and k_2 are non-negative constants.

The substitution of g_1, g_2 in (A.5) into (A.7) yields equation (17), where α and β are non-negative numbers (as by comparing (A.7) and (17), one gets: $\alpha = \frac{k_2}{k_1}$ and $\beta = (k_1)^\rho$ for some non-negative numbers k_1, k_2).

The optimal ratio $\frac{k_2}{k_1}$ in the function ψ (A.7) satisfies from (A.6) and (A.7) the implicit equation:

$$\frac{k_2}{k_1} = \frac{\delta}{1-\delta} \frac{\int_{-\infty}^{+\infty} \int_0^\infty \psi(y, a)^{1-\frac{1}{\rho}} g_1(y, a) da dy}{\int_{-\infty}^{+\infty} \int_0^\infty \psi(y, a)^{1-\frac{1}{\rho}} g_2(y, a) da dy}. \quad (\text{A.8})$$

The substitution of g_1, g_2 from (A.5) with the optimal function ψ into the right hand side of (A.8), and the substitution of the relation $\alpha = \frac{k_2}{k_1}$ into the left hand side of (A.8) yields the equation:

$$\alpha = \frac{\delta}{1-\delta} \frac{\int_{-\infty}^{+\infty} \int_0^\infty p_0(y, a) \left(1 + \alpha \left[\frac{p_1(y, a)}{p_0(y, a)} \right]^\lambda \right)^{\rho-1} da dy}{\int_{-\infty}^{+\infty} \int_0^\infty p_0(y, a) \left(1 + \alpha \left[\frac{p_1(y, a)}{p_0(y, a)} \right]^\lambda \right)^{\rho-1} \left[\frac{p_1(y, a)}{p_0(y, a)} \right]^\lambda da dy},$$

or alternatively:

$$\begin{aligned}
& \frac{1-\delta}{\delta} \\
&= \frac{\int_{-\infty}^{+\infty} \int_0^{\infty} p_0(y, a) \left(1 + \alpha \left[\frac{p_1(y, a)}{p_0(y, a)}\right]^\lambda\right)^{\rho-1} da dy}{\int_{-\infty}^{+\infty} \int_0^{\infty} p_0(y, a) \left(1 + \alpha \left[\frac{p_1(y, a)}{p_0(y, a)}\right]^\lambda\right)^{\rho-1} \alpha \left[\frac{p_1(y, a)}{p_0(y, a)}\right]^\lambda da dy} \\
&= \frac{\int_{-\infty}^{+\infty} \int_0^{\infty} p_0(y, a) \left(1 + \alpha \left[\frac{p_1(y, a)}{p_0(y, a)}\right]^\lambda\right)^{\rho-1} da dy}{\int_{-\infty}^{+\infty} \int_0^{\infty} p_0(y, a) \left(1 + \alpha \left[\frac{p_1(y, a)}{p_0(y, a)}\right]^\lambda\right)^\rho da dy - \int_{-\infty}^{+\infty} \int_0^{\infty} p_0(y, a) \left(1 + \alpha \left[\frac{p_1(y, a)}{p_0(y, a)}\right]^\lambda\right)^{\rho-1} da dy} \\
&= \frac{1}{\frac{\int_{-\infty}^{+\infty} \int_0^{\infty} p_0(y, a) \left(1 + \alpha \left[\frac{p_1(y, a)}{p_0(y, a)}\right]^\lambda\right)^\rho da dy}{\int_{-\infty}^{+\infty} \int_0^{\infty} p_0(y, a) \left(1 + \alpha \left[\frac{p_1(y, a)}{p_0(y, a)}\right]^\lambda\right)^{\rho-1} da dy} - 1},
\end{aligned}$$

which then yields (18).

For the derivation of the upper bound on the bit error probability (21), let $C_{w,d}$ designate the subcode of the considered systematic and linear block code C which in addition to the all-zero codeword also consists all the codewords which exhibit information (systematic) bits with a Hamming weight w and an overall Hamming weight d (where $w = 1, 2, \dots, k$ and $d = 1, 2, \dots, n$). By Gallager's bounding technique [14], we find:

$$\begin{aligned}
& P_b(d) \\
&\leq \underbrace{\int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty}}_{\substack{\text{n-dimensions} \\ \text{(w.r.t. } \mathbf{y})}} \underbrace{\int_0^{\infty} \cdots \int_0^{\infty}}_{\substack{\text{n-dimensions} \\ \text{(w.r.t. } \mathbf{a})}} p(\mathbf{r}|\mathbf{0}) \left\{ \sum_{w=1}^k \frac{w}{k} \sum_{\substack{\mathbf{c} \in C_{w,d} \\ \mathbf{c} \neq \mathbf{0}}} \left[\frac{p(\mathbf{r}|\mathbf{c})}{p(\mathbf{r}|\mathbf{0})}\right]^\lambda \right\}^\rho da dy \\
&= \underbrace{\int_{-\infty}^{+\infty} \cdots \int_{-\infty}^{+\infty}}_{\substack{\text{n-dimensions} \\ \text{(w.r.t. } \mathbf{y})}} \underbrace{\int_0^{\infty} \cdots \int_0^{\infty}}_{\substack{\text{n-dimensions} \\ \text{(w.r.t. } \mathbf{a})}} [p(\mathbf{r}|\mathbf{0})]^{1-\lambda\rho} \left\{ \sum_{w=1}^k \frac{w}{k} \sum_{\substack{\mathbf{c} \in C_{w,d} \\ \mathbf{c} \neq \mathbf{0}}} [p(\mathbf{r}|\mathbf{c})]^\lambda \right\}^\rho da dy,
\end{aligned} \tag{A.9}$$

Similarly to the derivation of the upper bound on the block error probability from (A.1), we derive the upper bound (21) on $P_b(d)$ from (A.9) (which is similar to (15) but for the replacement of the distance spectrum $\{S_d\}_{d=1}^n$ by $\{S'_d\}_{d=1}^n$ as expressed in (13)).

The main difference in the derivation of the above upper bound on the bit error probability as

compared to the derivation of the Duman and Salehi bound in [9] is explained in section III (which further tightens the bound).

Appendix B: On the existence and uniqueness of a solution to the optimization equation (39)

It is proved here that there always exists a unique solution to the optimization Eq. (39), derived in section III. This statement holds for every distance spectrum of a linear block code C . It is also independent of the block length n , the code's rate R and the energy per bit to spectral noise density ratio $\frac{E_b}{N_0}$.

To that end, we denote by $R(\eta)$ the right hand side of the optimization Eq. (39):

$$R(\eta) = \int_0^\infty \frac{p_{u(n)}(t)}{\sqrt{t}} \cdot \exp\left(-\frac{E_s}{N_0} \frac{(t-\eta)^2}{t}\right) dt. \quad (\text{B.1})$$

Based on the statistic independence of the non-negative RVs: $u(d), v(d)$ introduced in Eq. (32) (where $d = 1, 2, \dots, n$) and the equality: $u(n) = u(d) + v(d)$, we get:

$$\begin{aligned} p_{u(n)}(t) &= (p_{u(d)} * p_{v(d)})(t) \\ &= \int_0^t p_{u(d)}(u) \cdot p_{v(d)}(t-u) du, \end{aligned} \quad (\text{B.2})$$

where ‘*’ stands for the convolution operation.

Combining Eqs. (B.1),(B.2) with the substitution $t = uv$, the function $R(\eta)$ admits the expression:

$$R(\eta) = \int_0^\infty \int_0^\infty \frac{p_{u(d)}(u) \cdot p_{v(d)}(v)}{\sqrt{u+v}} \cdot \exp\left(-\frac{E_s}{N_0} \frac{(\eta - (u+v))^2}{u+v}\right) du dv, \quad (\text{B.3})$$

for $-\infty < \eta < +\infty$.

We denote here by $L(\eta)$ the left hand side of the optimization Eq. (39), and based on Eq. (B.3) we find the equality:

$$\frac{L(\eta)}{R(\eta)} = \sum_{d=1}^n S_d f_d(\eta), \quad (\text{B.4})$$

where $\{S_d\}_{d=1}^n$ denotes the distance spectrum of the linear block code C and

$$f_d(\eta) = \frac{\int_0^\infty \int_0^\infty Q\left(\sqrt{\frac{2E_s}{N_0}}\left(\frac{1}{v} - \frac{1}{u+v}\right)\eta\right) \frac{p_{u(d)}(u) \cdot p_{v(d)}(v)}{\sqrt{u+v}} \cdot \exp\left(-\frac{E_s}{N_0} \frac{(\eta - (u+v))^2}{u+v}\right) du dv}{\int_0^\infty \int_0^\infty \frac{p_{u(d)}(u) \cdot p_{v(d)}(v)}{\sqrt{u+v}} \cdot \exp\left(-\frac{E_s}{N_0} \frac{(\eta - (u+v))^2}{u+v}\right) du dv}, \quad (\text{B.5})$$

for $d = 1, 2, \dots, n$ and $-\infty < \eta < +\infty$.

Based on some elementary properties of the Q -function, it can be verified by Eq. (B.5) that $f_d(\eta)$ is a monotonic decreasing and non-negative function, which also satisfies the equalities:

$$\lim_{\eta \rightarrow -\infty} f_d(\eta) = 1, \quad f_d(0) = \frac{1}{2}, \quad \lim_{\eta \rightarrow +\infty} f_d(\eta) = 0. \quad (\text{B.6})$$

Therefore, by Eqs. (B.4),(B.6), we conclude the following:

$$\lim_{\eta \rightarrow -\infty} \frac{L(\eta)}{R(\eta)} = \sum_{d=1}^n S_d, \quad \frac{L(0)}{R(0)} = \frac{1}{2} \sum_{d=1}^n S_d, \quad \lim_{\eta \rightarrow +\infty} \frac{L(\eta)}{R(\eta)} = 0. \quad (\text{B.7})$$

Since $\{f_d(\eta)\}_{d=1}^n$ (where $-\infty < \eta < +\infty$) are non-negative and decreasing functions of η and also $\{S_d\}_{d=1}^n$ is a non-negative sequence, we get from Eq. (B.4) that also the function: $\frac{L(\eta)}{R(\eta)}$ is a monotonic decreasing and non-negative function of η . Moreover, based on Eq. (B.7), we get by the mean value theorem for continuous functions, that the equation $\frac{L(\eta)}{R(\eta)} = 1$ has a solution η , which is also unique (because of the monotonicity of the function $\frac{L(\eta)}{R(\eta)}$). We also note that the Eq. (39) is equivalent to the equation: $\frac{L(\eta)}{R(\eta)} = 1$, and that completes our proof for the existence and uniqueness of a solution to the optimization Eq. (39).

Moreover, under the mild condition $\sum_{d=1}^n S_d \geq 2$ (which states that there are at least two non-zero codewords of the considered block code C), we get from Eq. (B.7) that the unique solution of Eq. (39) is non-negative.

Appendix C: Simplifications of the Generalized Engdahl-Zigangirov Bound [12]

In this appendix we simplify by some algebraic manipulations the upper bound and its corresponding optimization equation, which are derived in section III as a generalization of Engdahl-Zigangirov

bound.

Let the function J be the inner integral of the triple integrals introduced in the upper bound (38):

$$J\left(u, v, \eta, \frac{E_s}{N_0}\right) = \sqrt{\frac{E_s}{\pi N_0}} \int_{\eta}^{\infty} Q\left(\sqrt{\frac{2E_s}{N_0}} \left(\frac{1}{v} - \frac{1}{u+v}\right) \eta\right) \exp\left(-\frac{E_s}{N_0} \frac{(t - (u+v))^2}{u+v}\right) dt, \quad (\text{C.1})$$

where $u, v \geq 0$ and based on our comment in Appendix B, $\eta \geq 0$.

By applying Craig's identity ([5]) to the evaluation of J , we reach the equality:

$$\begin{aligned} J\left(u, v, \eta, \frac{E_s}{N_0}\right) & \quad (\text{C.2}) \\ &= \frac{\sqrt{2(u+v)}}{\pi} \int_0^{\frac{\pi}{2}} \frac{\sin \phi}{A(\phi)} \cdot \exp\left(-\frac{2E_s}{N_0} \frac{u + \frac{u^2}{v}}{A^2(\phi)}\right) Q\left(\sqrt{\frac{E_s}{(u+v)N_0}} \frac{\eta A^2(\phi) - 2(u+v) \sin^2 \phi}{A(\phi) \sin \phi}\right) d\phi, \end{aligned}$$

where $A(\phi) = \sqrt{\frac{2u}{v} + 2 \sin^2 \phi}$ and u, v, η are non-negative.

The upper bound in (38) admits the following form (based on Eq. (C.1)):

$$P_e \leq \sum_{d=1}^n \left\{ S_d \int_0^{\infty} \int_0^{\infty} p_{u(d)}(u) \cdot p_{v(d)}(v) \cdot \frac{J\left(u, v, \eta, \frac{E_s}{N_0}\right)}{\sqrt{u+v}} du dv \right\} + \int_0^{\infty} Q\left(\sqrt{\frac{2E_s}{N_0}} \frac{u - \eta}{\sqrt{u}}\right) p_{u(n)}(u) du. \quad (\text{C.3})$$

The transformations $t = u + v$, $u = \alpha t$ (where $t \geq 0$ and $0 \leq \alpha \leq 1$), further simplifies the upper bound in Eq. (C.3) and the optimization equation (39) (for the parameter η), reading now:

$$P_e \leq \sum_{d=1}^n \left\{ S_d \int_0^{\infty} \int_0^1 g_1\left(t, \alpha, d, \eta, \frac{E_s}{N_0}\right) d\alpha dt \right\} + \int_0^{\infty} Q\left(\sqrt{\frac{2E_s}{N_0}} \frac{u - \eta}{\sqrt{u}}\right) p_{u(n)}(u) du. \quad (\text{C.4})$$

where:

$$g_1\left(t, \alpha, d, \eta, \frac{E_s}{N_0}\right) = \sqrt{t} p_{u(d)}(\alpha t) p_{v(d)}((1-\alpha)t) J\left(\alpha t, (1-\alpha)t, \eta, \frac{E_s}{N_0}\right),$$

and $t \geq 0$, $0 \leq \alpha \leq 1$.

By the same substitutions, the optimization equation for the parameter η admits the simplified form:

$$\sum_{d=1}^n \left\{ S_d \int_0^{\infty} \int_0^1 g_2\left(t, \alpha, d, \eta, \frac{E_s}{N_0}\right) d\alpha dt \right\} = \int_0^{\infty} \frac{p_{u(n)}(u)}{\sqrt{u}} \cdot \exp\left(-\frac{E_s}{N_0} \frac{(u - \eta)^2}{u}\right) du, \quad (\text{C.5})$$

where:

$$g_2\left(t, \alpha, d, \eta, \frac{E_s}{N_0}\right) = \sqrt{t} p_{u(d)}(\alpha t) p_{v(d)}((1-\alpha)t) \exp\left(-\frac{E_s}{N_0} \frac{(\eta-t)^2}{t}\right) Q\left(\sqrt{\frac{2E_s}{N_0} \frac{\alpha}{(1-\alpha)t}} \eta\right), \quad (\text{C.6})$$

and $t \geq 0, 0 \leq \alpha \leq 1$.

In the special case of a fully interleaved Rayleigh fading channel with MRC space diversity of order L , we get the following pdf for the RVs introduced in Eq. (32):

$$\begin{aligned} p_{u(d)}(u) &= \frac{L^{dL} u^{dL-1} e^{-Lu}}{(dL-1)!} \quad u \geq 0, \quad d = 1, 2, \dots, n \\ p_{v(d)}(v) &= \frac{L^{(n-d)L} v^{(n-d)L-1} e^{-Lv}}{((n-d)L-1)!} \quad v \geq 0, \quad d = 1, 2, \dots, n-1. \end{aligned} \quad (\text{C.7})$$

If $d = n$, then $v(d) = 0$, which yields that $p_{v(d)}(v) = \delta(v)$. Based on Eqs. (C.4),(C.5), and by substituting the pdf in (C.7), we finally get the following upper bound on the ML decoding error probability:

$$P_e \leq \int_0^\infty \frac{x^{nL-1} e^{-x}}{(nL-1)!} \cdot g(x, \eta) dx, \quad (\text{C.8})$$

where the optimized value of η satisfies the equation:

$$\int_0^\infty \frac{x^{nL-1} e^{-x}}{(nL-1)!} \cdot h(x, \eta) dx = 0, \quad (\text{C.9})$$

and where,

$$\begin{aligned} g(x, \eta) &= f_1(x, \eta) + f_2(x, \eta), \\ f_1(x, \eta) &= (nL-1) \cdot \sqrt{\frac{L}{x}} \int_0^1 J\left(\frac{\alpha x}{L}, \frac{(1-\alpha)x}{L}, \eta, \frac{E_s}{N_0}\right) P(\alpha) d\alpha, \\ f_2(x, \eta) &= Q\left(\sqrt{\frac{2E_s}{N_0} \frac{x-L\eta}{\sqrt{Lx}}}\right). \end{aligned} \quad (\text{C.10})$$

The function J is introduced in Eqs. (C.1),(C.2) and $P(\alpha) \triangleq P\left(\alpha, \{S_d\}_{d=1}^n\right)$ is the polynomial function:

$$P(\alpha) = \sum_{d=1}^{n-1} \left\{ S_d \binom{nL-2}{dL-1} \alpha^{dL-1} (1-\alpha)^{(n-d)L-1} \right\}. \quad (\text{C.11})$$

The function h in Eq. (C.9) admits the form:

$$h(x, \eta) = f_3(x, \eta) + f_4(x, \eta),$$

where

$$\begin{aligned}
f_3(x, \eta) &= (nL - 1) \sqrt{\frac{L}{x}} \cdot \exp\left(-\frac{E_s}{LN_0} \frac{(L\eta - x)^2}{x}\right) \int_0^1 P(\alpha) Q\left(\sqrt{\frac{2E_s}{N_0} \frac{\alpha}{1-\alpha} \frac{x}{L} \eta}\right) d\alpha, \\
f_4(x, \eta) &= \sqrt{\frac{L}{x}} \exp\left(-\frac{E_s}{LN_0} \frac{(L\eta - x)^2}{x}\right). \tag{C.12}
\end{aligned}$$

It can be analytically shown that the functions h, g expressed in Eqs. (C.10),(C.12) are bounded on the interval $[0, \infty)$. Since the function $f(x) = \frac{x^{nL-1} e^{-x}}{(nL-1)!}$ (where $x \geq 0$) is a pdf, the integrals in Eqs. (C.8),(C.9) are interpreted as statistical means.

Acknowledgement We thank the Neaman Institute at Technion and the Israeli Software Radio Consortium for their support in this research project.

References

- [1] F. Babich, G. Montorsi and F. Vatta, “Transfer function bounds on turbo codes performance in the Rician fading channel”, *Proceedings 1999 IEEE International Conference on Communications (ICC’99)*, pp. 108–112, Vancouver, British Columbia, Canada, 6–10 June, 1999.
- [2] S. Benedetto and G. Montorsi, “Unveiling turbo codes: some results of parallel concatenated coding schemes”, *IEEE Trans. on Information Theory*, vol. 42, no. 2, pp. 409–429, March 1996.
- [3] C. Berrou, A. Glavieux and P. Thitimajshima, “Near Shannon limit error-correcting coding and decoding”, *Proceedings 1993 IEEE International Conference on Communications (ICC’93)*, pp. 1064–1070, Geneva, Switzerland, May 1993.
- [4] E. Biglieri, J. Proakis and S. Shamai (Shitz), “Fading channels: Information-theoretic and communications aspects”, *IEEE Trans. on Information Theory*, vol. 44, no. 6, pp. 2619–2692, October 1998.
- [5] J. Craig, “A new, simple and exact result for calculating error probability for two-dimensional signal constellation”, *Proceedings of 1991 Mil. Commun. Conf. (MILCOM’91)*, Boston, MA, USA, 1991, pp. 25.5.1–25.5.5.
- [6] D. Divsalar, H. Jin and R.J. McEliece, “Coding theorems for ‘turbo-like’ codes”, *Proceedings 1998 Allerton Conference*, Allerton House, Monticello, Illinois, September 23–25, 1998, pp. 201–210.
- [7] D. Divsalar, “A simple tight bound on error probability of block codes with application to turbo codes”, TMO Progress Report 42–139, JPL, pp. 1–35, November 1999.
- [8] D. Divsalar and E. Biglieri, “Upper bounds to error probabilities of coded systems over AWGN and fading channels”, *Proceedings 2000 IEEE Global Telecommunications Conference (GLOBECOM’00)*, pp. 1605–1610, San Francisco, California, November 2000.
- [9] T. M. Duman and M. Salehi, “New performance bounds for turbo codes”, *IEEE Trans. on Communications*, vol. 46, no. 6, pp. 717–723, June 1998.
- [10] T. M. Duman and M. Salehi, “The union bound for turbo coded modulation systems over fading channels”, *IEEE Trans. on Communications*, vol. 47, no. 10, pp. 1495–1502, October 1999.
- [11] T.M. Duman, “Turbo codes and turbo coded modulation systems: Analysis and performance bounds”, Ph.D. dissertation, Elect. Comput. Eng. Dep., Northeastern University, Boston, MA USA, May 1998.
- [12] K. Engdahl and K. Sh. Zigangirov, “Tighter bounds on the error probability of fixed convolutional codes”, *IEEE Trans. on Information Theory*, vol. 47, no. 4, pp. 1625–1630, May 2001.
- [13] R. G. Gallager, *Low density parity check codes*, Cambridge, MA, MIT Press, 1963. Available at <http://justice.mit.edu/people/gallager.html>.
- [14] R. G. Gallager, “A simple derivation of the coding theorem and some applications”, *IEEE Trans. on Information Theory*, pp. 3–18, January 1965.
- [15] E. K. Hall and S. G. Wilson, “Design and analysis of turbo codes on Rayleigh fading channels”, *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 2, pp. 160–174, February 1998.

- [16] H. Herzberg and G. Poltyrev, “Techniques for bounding the probability of decoding error for block coded modulations structures”, *IEEE Trans. on Information Theory*, vol. 40, pp. 903–911, May 1994.
- [17] H. Jin and R.J. McEliece, “RA codes achieve AWGN channel capacity”, *Proceedings 1999 Applied Algebra, Algebraic Algorithms and Error Correcting Codes (AAECC-13)*, Honolulu, Hawaii, USA, November 15–19, 1999, pp. 10–18.
- [18] A. Lapidoth and S. Shamai (Shitz), “Fading channels: How perfect need “perfect side information” be ? ”, *Proc. 1999 IEEE Information Theory Workshop (ITW’99)*, pp. 36–38, Kruger National Park, South Africa, June 20–25, 1999.
- [19] D.J.C Mackay and R.M. Neal, “Near Shannon limit performance of low density parity check codes”, *IEEE Electronic Letters*, vol. 33, no. 6, pp. 457–458, March 1997.
- [20] R.J. McEliece, “How to compute weight enumerators for convolutional codes”, in *Communications and Coding*, M. Darnel and B. Honary, eds., Tauton, Research Studies, 1998, chapter 6, pp. 121–141.
- [21] L.C. Perez, J. Seghers and D. J. Costello, “A distance spectrum interpretation of turbo codes”, *IEEE Trans. on Information Theory*, vol. 42, no. 6, pp. 1698–1709, November 1996.
- [22] G. Poltyrev, “Bounds on the decoding error probability of binary linear codes via their spectra”, *IEEE Trans. on Information Theory*, vol. 40, no. 4, pp. 1284–1292, July 1994.
- [23] I. Sason and S. Shamai (Shitz), “Improved upper bounds on the decoding error probability of parallel and serial concatenated turbo codes via their ensemble distance spectrum”, *IEEE Trans. on Information Theory*, vol. 46, no. 1, pp. 1–23, January 2000.
- [24] I. Sason and S. Shamai (Shitz), “Improved upper bounds on the ensemble performance of ML decoded low density parity check codes”, *IEEE Communications Letters*, vol. 4, no. 3, pp. 89–91, March 2000.
- [25] I. Sason and S. Shamai (Shitz), “Improved upper bounds on the ML performance of turbo codes for interleaved Rician fading channels, with comparison to iterative decoding”, *Proceedings 2000 IEEE International Conference on Communications (ICC 2000)*, pp. 591–596, New Orleans, LA, June 2000.
- [26] I. Sason and S. Shamai, “On Gallager-type bounds for the mismatched decoding regime with applications to turbo codes”, *Proceedings IEEE 2001 International Symposium on Information Theory*, p. 134, Washington, D.C, USA, June 2001.
- [27] I. Sason, S. Shamai and D. Divsalar, “On simple and tight upper bounds on the ML decoding error probability for block codes operating over interleaved fading channels”, *Proceedings Sixth International Symposium on Communication Theory and Applications (ISCTA’01)*, pp. 236–241, 15-20 July, 2001, Ambleside, UK.
- [28] S. Shamai and I. Sason, “Variations on the Gallager bounds, connections and applications”, *IEEE Trans. on Information Theory*, vol. 48, no. 12, pp. 3029–3051, December 2002.
- [29] S. Shamai and I. Sason, “On Gallager’s bounding technique: performance bounds for turbo codes in Gaussian and fading channels”, *Proceedings of the 2nd International Symposium on Turbo Codes & Related Topics*, pp. 27-34, Brest, France, September 2000.
- [30] M. K. Simon and D. Divsalar, “Some new twists to problems involving the Gaussian probability integral”, *IEEE Trans. on Communications*, vol. 46, no. 2, pp. 200–210, February 1998.

Figure Captions

- Figure 1: (a) Block diagram of a uniformly interleaved rate-1/4 RA code. The block is composed of $N = 1024$ information bits, the number of repetitions is $q = 4$, and the interleaver length is $qN = 4096$.
 (b) The sequence $\{S'_d\}_{d=1}^{qN}$ defined in (13), which is calculated for the rate 1/4 RA code depicted in Fig. 1(a).
- Figure 2: A comparison between some upper bounds on the bit error probability (referring to the ML decoding) for the ensemble of rate-1/4 RA codes depicted in Fig. 1(a), where the codes are operating over a fully interleaved Rayleigh fading channel with perfect CSI.
 1. The generalization of the Duman & Salehi bound.
 2. The Divsalar & Biglieri bound [8].
 3. The generalized Engdahl & Zigangirov bound.
 4. The generalized Viterbi & Viterbi bound [27].
 5. The union bound.
 These bounds are also compared with computer simulation results of the sum-product iterative decoding algorithm (with 20 iterations).
- Figure 3: Plots of the theoretical rate-distortion curves (with respect to the bit error probability) for rate-1/3 block codes which operate over fully interleaved Rayleigh fading channels with perfect CSI and MRC diversity of orders $L = 1, 2, 3, 4$ or $L \rightarrow \infty$ (where the latter corresponds to a binary-input AWGN channel).
- Figure 4: (a) Block diagram of the ensemble of uniformly interleaved rate- $\frac{1}{3}$ turbo codes, where the components of the turbo codes are fixed RSC codes with identical generators: $G_1(D) = G_2(D) = \left[1, \frac{1+D^4}{1+D+D^2+D^3+D^4}\right]$, and the interleaver is of length $N = 1000$. Termination of the trellis of both component codes to the all-zero state is assumed after N information bits.
 (b) The sequence $\{S'_d\}_{d=1}^n$ defined in (13), which is calculated for the ensemble of uniformly interleaved turbo codes depicted in Fig. 4(a).
- Figure 5: Comparison between improved upper bounds on the bit error probability (section III) and the union bound, for the ensemble of the rate-1/3 uniformly interleaved turbo codes (Fig. 4(a)). The codes operate over fully interleaved Rayleigh fading channels with various orders (L) of MRC diversity and perfect CSI. These bounds are depicted for: (a) $L = 1$, (b) $L = 4$, (c) $L = 6$, and are compared with computer simulation results of the Log-MAP based iterative decoding algorithm (with up to 10 iterations).
- Figure 6: Comparison between the generalization of the second version of Duman and Salehi bounds (see section III) and the union bound. These bounds on the bit error probability are applied to the ensemble of the rate-1/3 uniformly interleaved turbo codes depicted in Fig. 4(a). The codes operate over fully interleaved Rayleigh fading channels with perfect CSI and MRC space diversity of orders $L = 1, 2, 3, 4$.
- Figure 7: Comparison between the generalization of the second version of Duman and Salehi bounds (see section III) and the union bound on the ML decoded bit error probability. These bounds are applied to the ensemble of the rate-1/3 uniformly interleaved turbo codes depicted in Fig. 4(a), operating over a fully interleaved Rician fading channel (with $K = 2.33$ dB) and perfect CSI. Computer simulation results of the Log-MAP based iterative decoding algorithm (with up to 10 iterations) are also shown.

Figure 8: Comparison between the normalized logarithms (on base 2) of the distance spectrum of some rate- $\frac{1}{3}$ ensembles of codes, plotted versus the normalized Hamming weights of their codewords. The normalization is with respect to the common block length (3000) of these codes.

1. The ensemble of uniformly interleaved turbo codes depicted in Fig. 4(a).
2. Gallager's ensemble of (3000, 4, 6) LDPC codes, (rate $\sim \frac{1}{3}$).
3. Gallager's ensemble of (3000, 6, 9) LDPC codes, (rate $\sim \frac{1}{3}$).
4. The ensemble of fully random block codes of length $n = 3000$ and rate $R = \frac{1}{3}$.

The Gallager's upper bounds on the distance spectra of the ensembles of the regular LDPC codes [13] are depicted in curves 2,3.

Figure 9: Comparison between the generalization of Duman and Salehi bounds (section III) and the union bounds on the block error probability with ML decoding. These bounds are applied to some code ensembles operating over fully interleaved Rayleigh fading channels with or without MRC space diversity: $L = 1, 4$ in Figures 9(a) and 9(b), respectively.

1. The ensemble of uniformly interleaved turbo codes depicted in Fig. 4(a), (rate $\frac{1}{3}$).
2. Gallager's ensemble of (3000, 4, 6) LDPC codes, (rate $\sim \frac{1}{3}$).
3. Gallager's ensemble of (3000, 6, 9) LDPC codes, (rate $\sim \frac{1}{3}$).

Figure 10: Generalized Duman and Salehi upper bounds on the ML decoding error probability of some ensembles of Gallager's $(n, 6, 9)$ LDPC codes with block lengths $n = 3K, 5K, 10K, 20K$ and $40K$. The code rates of these ensembles of regular LDPC codes approach $\frac{1}{3}$. Fully interleaved Rayleigh fading channels with and without space diversity are examined.

Fig. 10(a) – no space diversity, Fig. 10(b) – MRC space diversity of order $L = 4$.

The upper bounds on the asymptotic thresholds (where $n \rightarrow +\infty$) referring to the ML decoding are compared in terms of $\frac{E_b}{N_0}$ with the channel capacity.

Figure 11: Comparison between generalized Duman and Salehi upper bounds on the $\frac{E_b}{N_0}$ thresholds (where $n \rightarrow +\infty$) for ML decoded ensembles of Gallager's LDPC codes and uniformly interleaved RA codes. The ensembles of codes operate over fully interleaved Rayleigh fading channels with perfect CSI.

Fig. 11(a) – no space diversity, Fig. 11(b) - MRC space diversity of order $L = 4$.

Rate- $\frac{2}{3}$: 1a - ($j = 3, k = 9$), 1b - ($j = 4, k = 12$), 1c - ($j = 6, k = 18$) LDPC codes.

Rate- $\frac{3}{5}$: 2a - ($j = 4, k = 10$), 2b - ($j = 6, k = 15$) LDPC codes.

Rate- $\frac{1}{2}$: 3a - ($j = 3, k = 6$), 3b - ($j = 4, k = 8$), 3c - ($j = 8, k = 16$) LDPC codes.

Rate- $\frac{2}{5}$: 4a - ($j = 3, k = 5$), 4b - ($j = 6, k = 10$) LDPC codes.

Rate- $\frac{1}{3}$: 5a - RA codes ($q = 3$), 5b - ($j = 4, k = 6$), 5c - ($j = 8, k = 12$) LDPC codes.

Rate- $\frac{1}{4}$: 6a - RA codes ($q = 4$), 6b - ($j = 3, k = 4$), 6c - ($j = 6, k = 8$) LDPC codes.

Rate- $\frac{1}{5}$: 7a - RA codes ($q = 5$), 7b - ($j = 4, k = 5$) LDPC codes.

Rate- $\frac{1}{6}$: 8 - RA codes ($q = 6$).

Rate- $\frac{1}{7}$: 9 - RA codes ($q = 7$).

Rate- $\frac{1}{8}$: 10a - RA codes ($q = 8$), 10b - ($j = 7, k = 8$) LDPC codes.

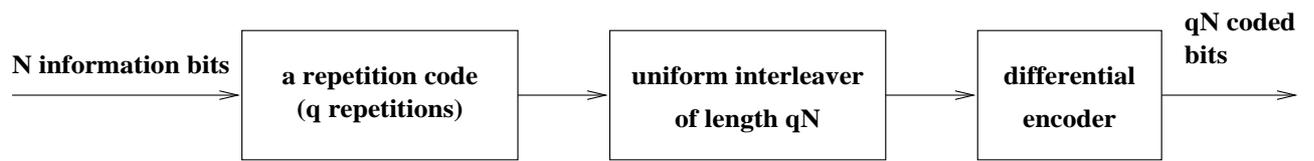


Figure 1a.

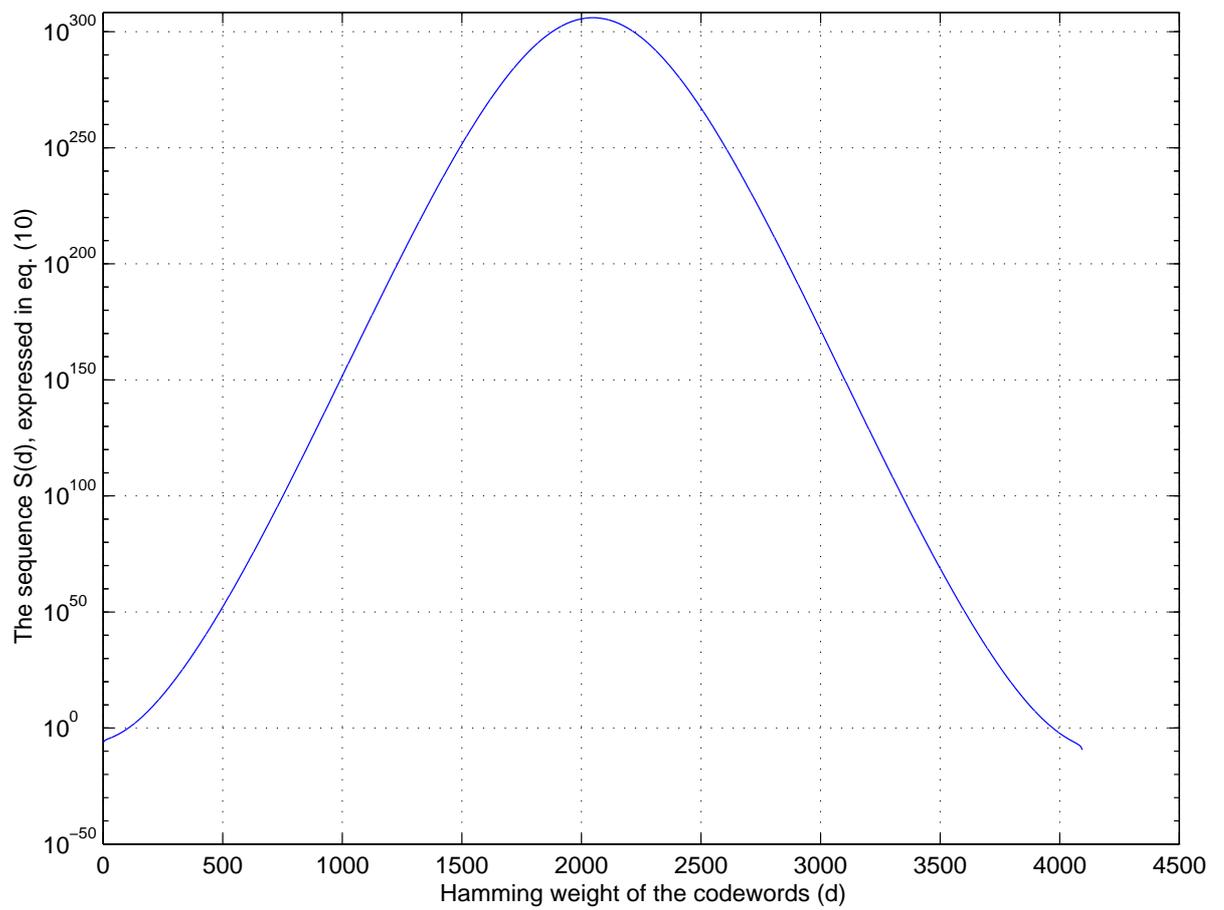


Figure 1b.

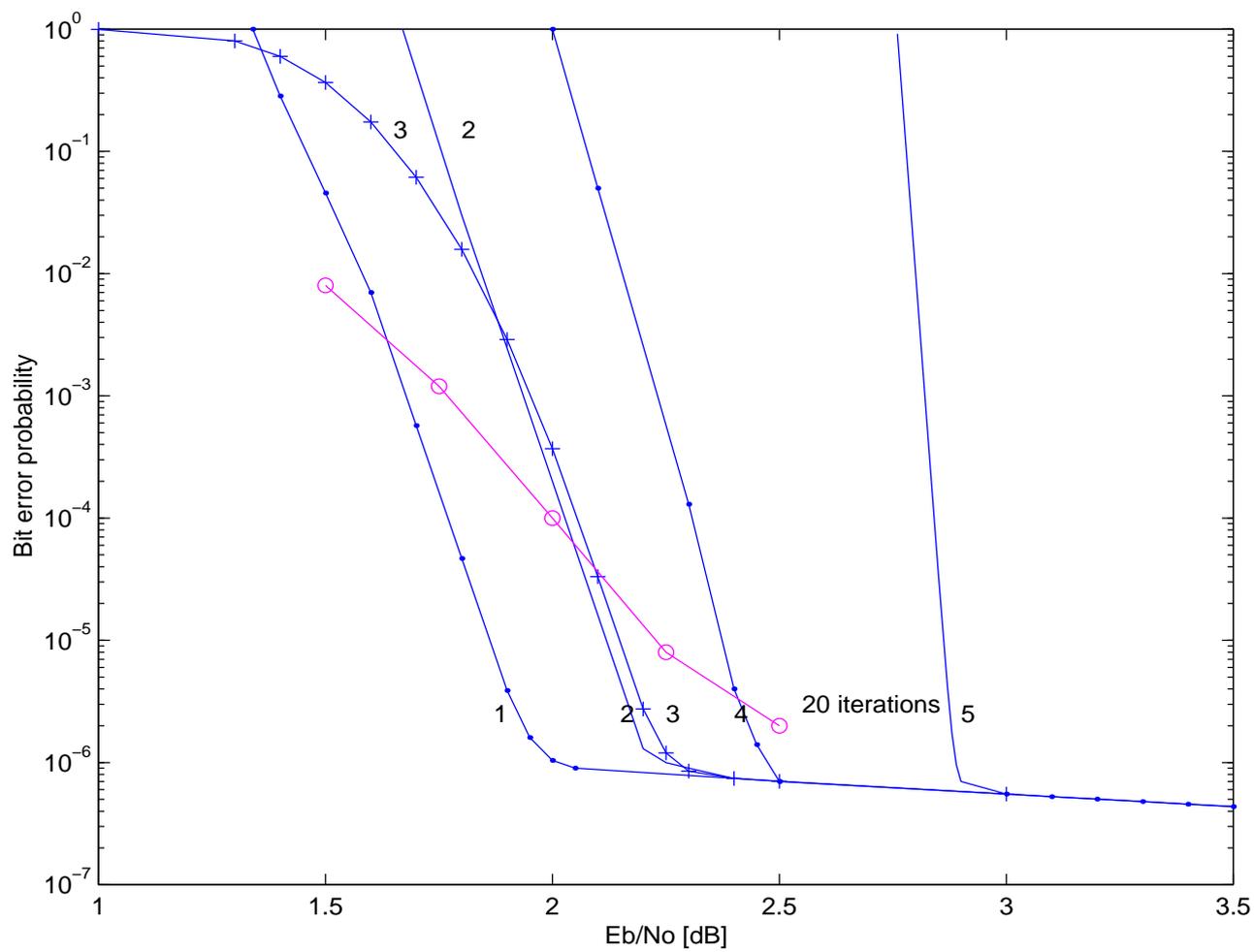


Figure 2.

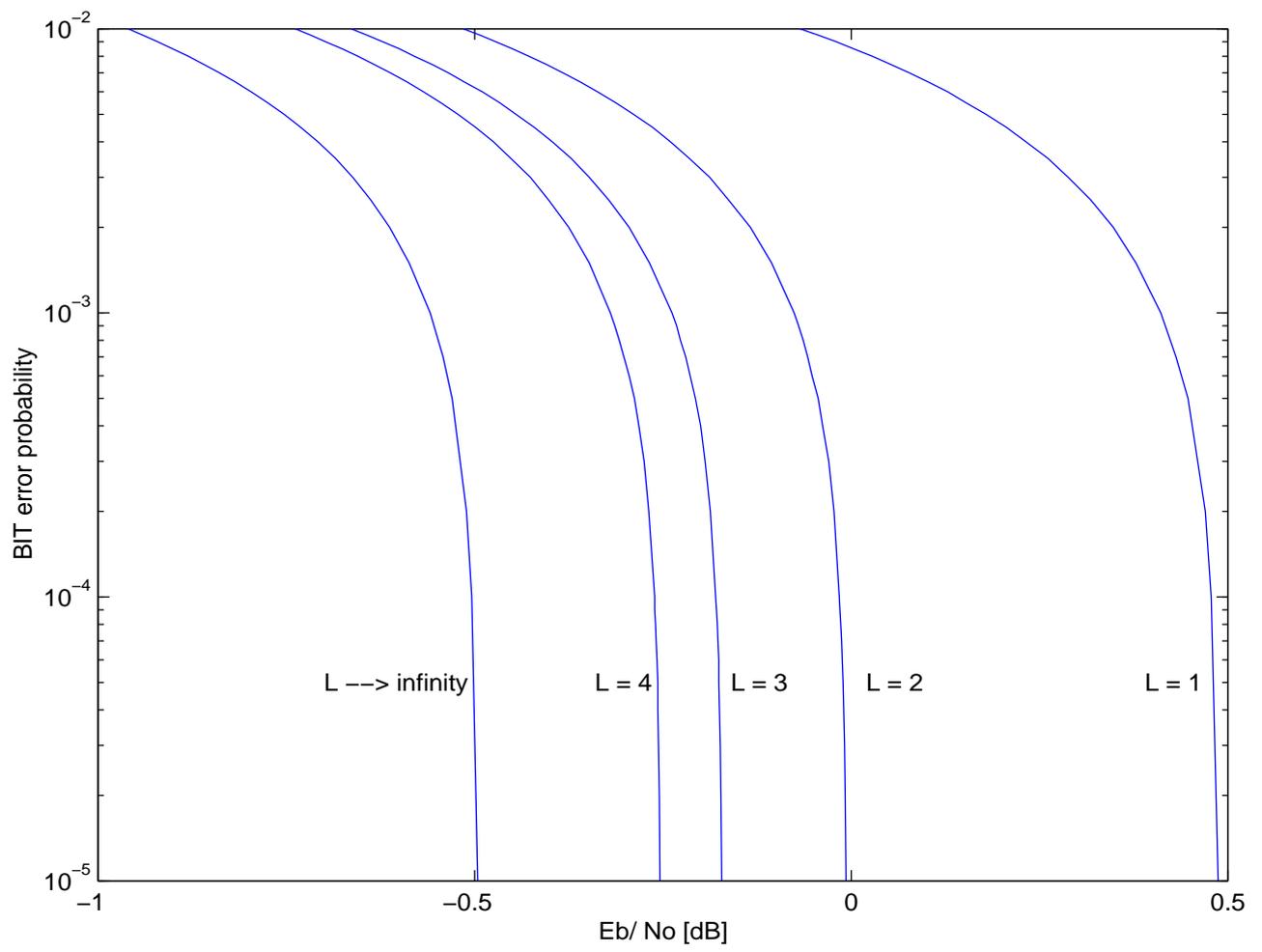


Figure 3.

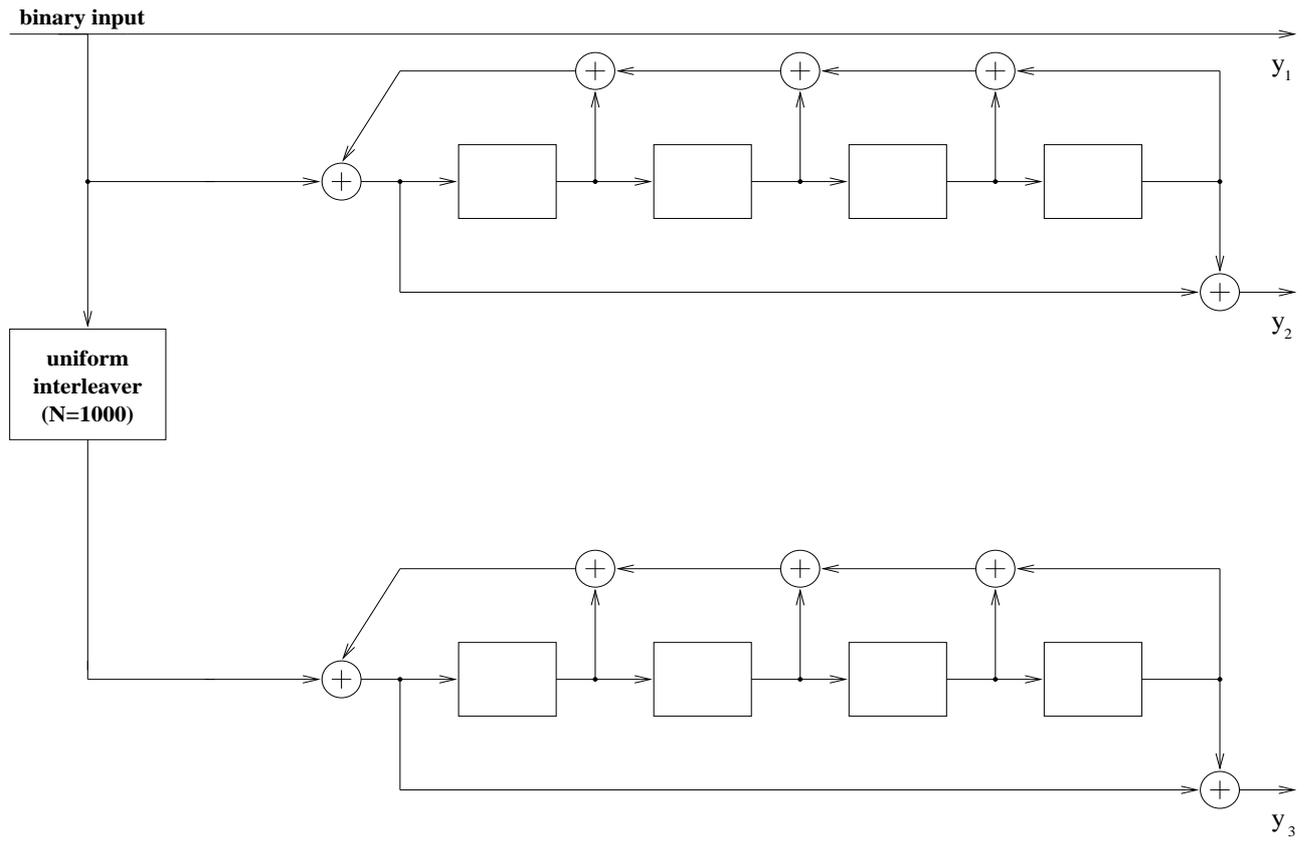


Figure 4a.

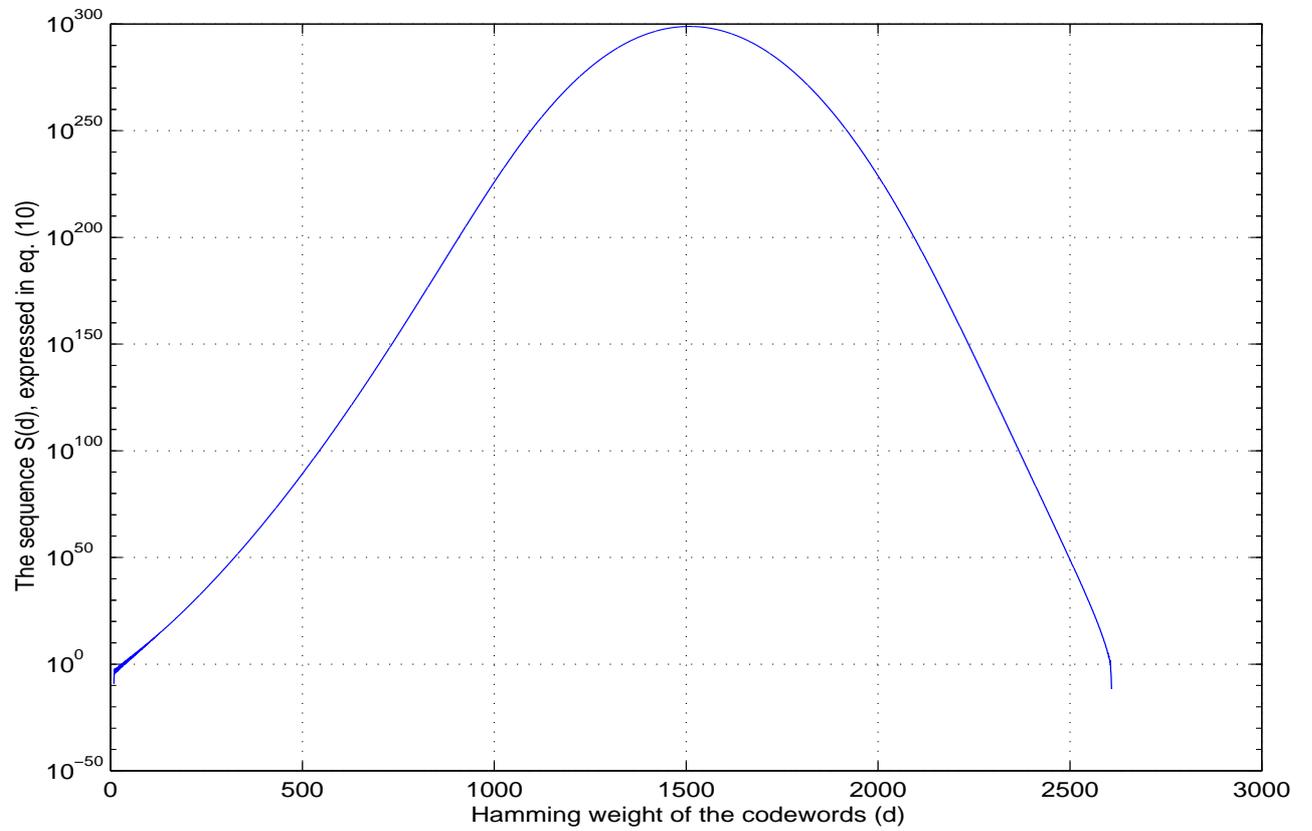


Figure 4b.

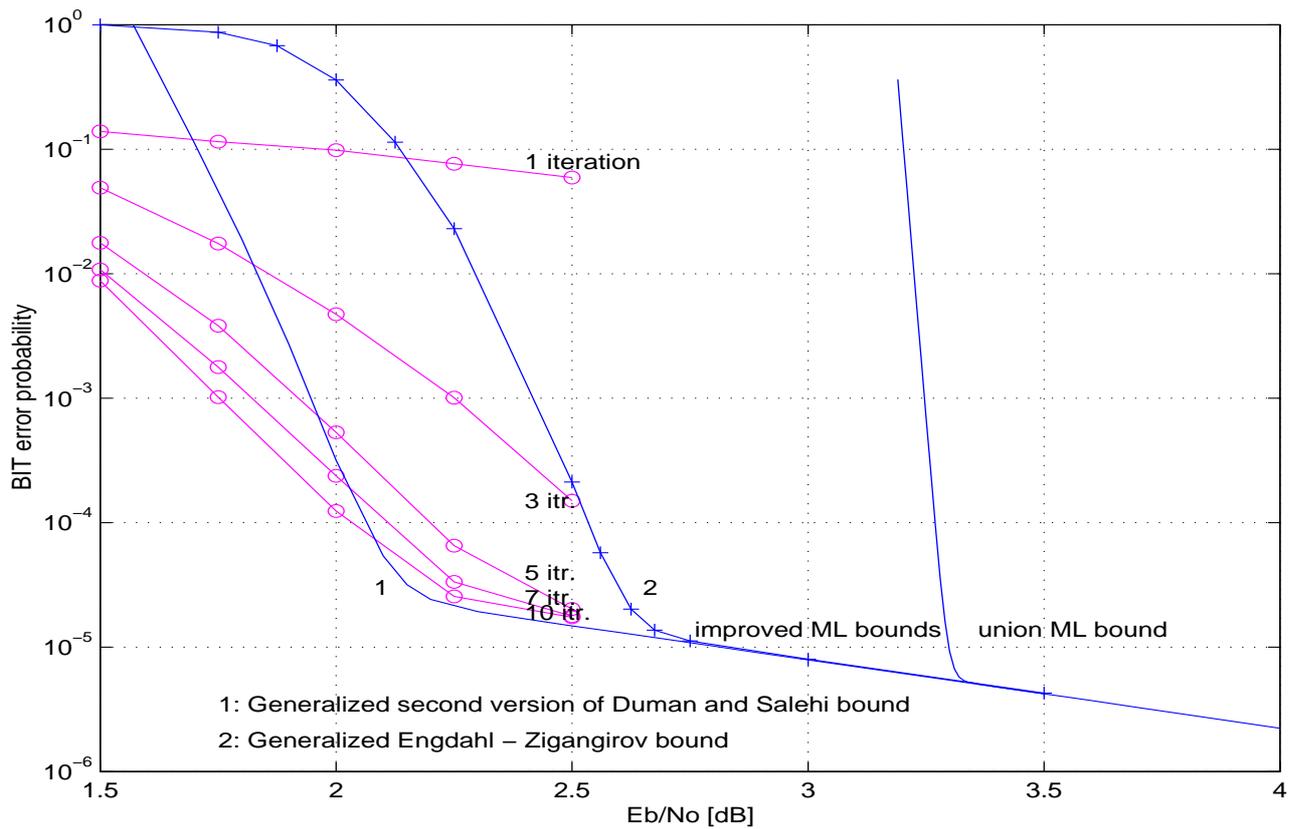


Figure 5a.

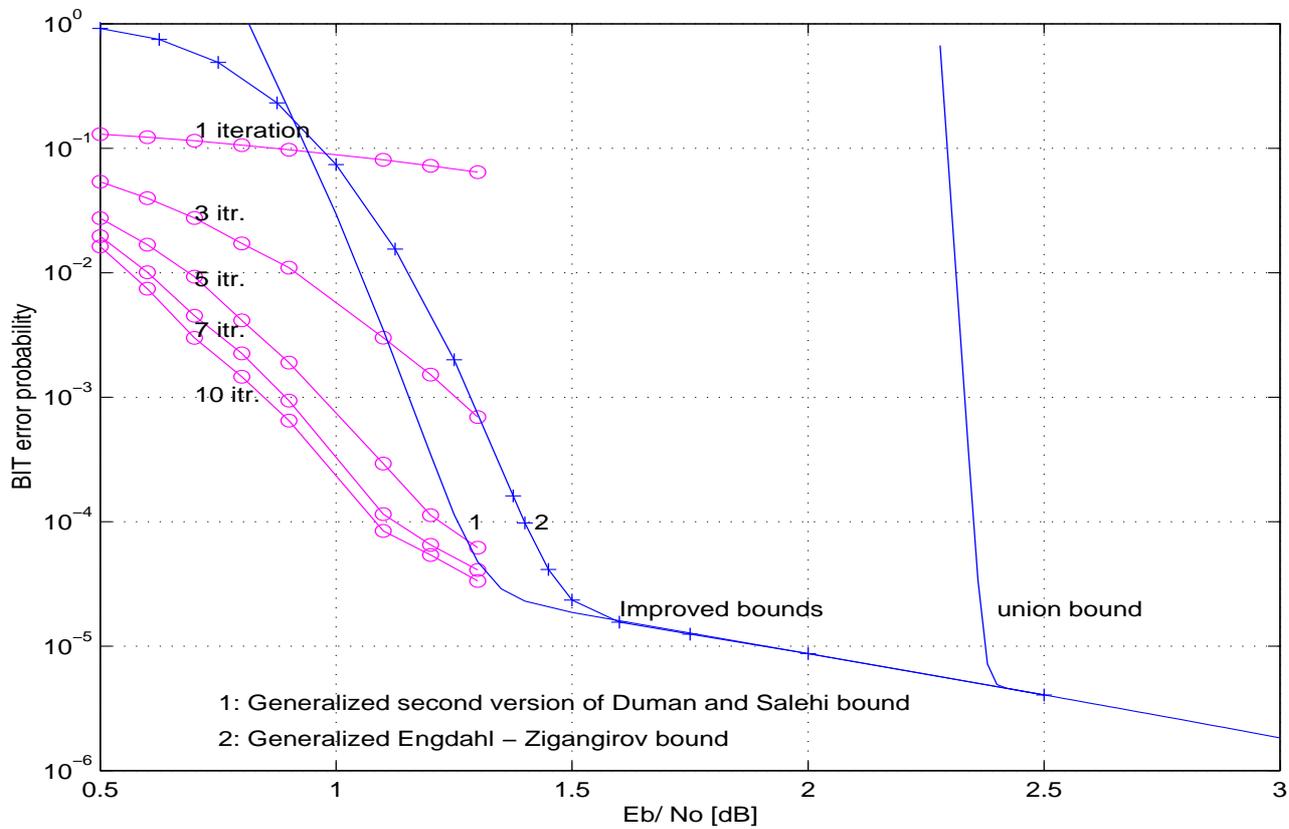


Figure 5b.

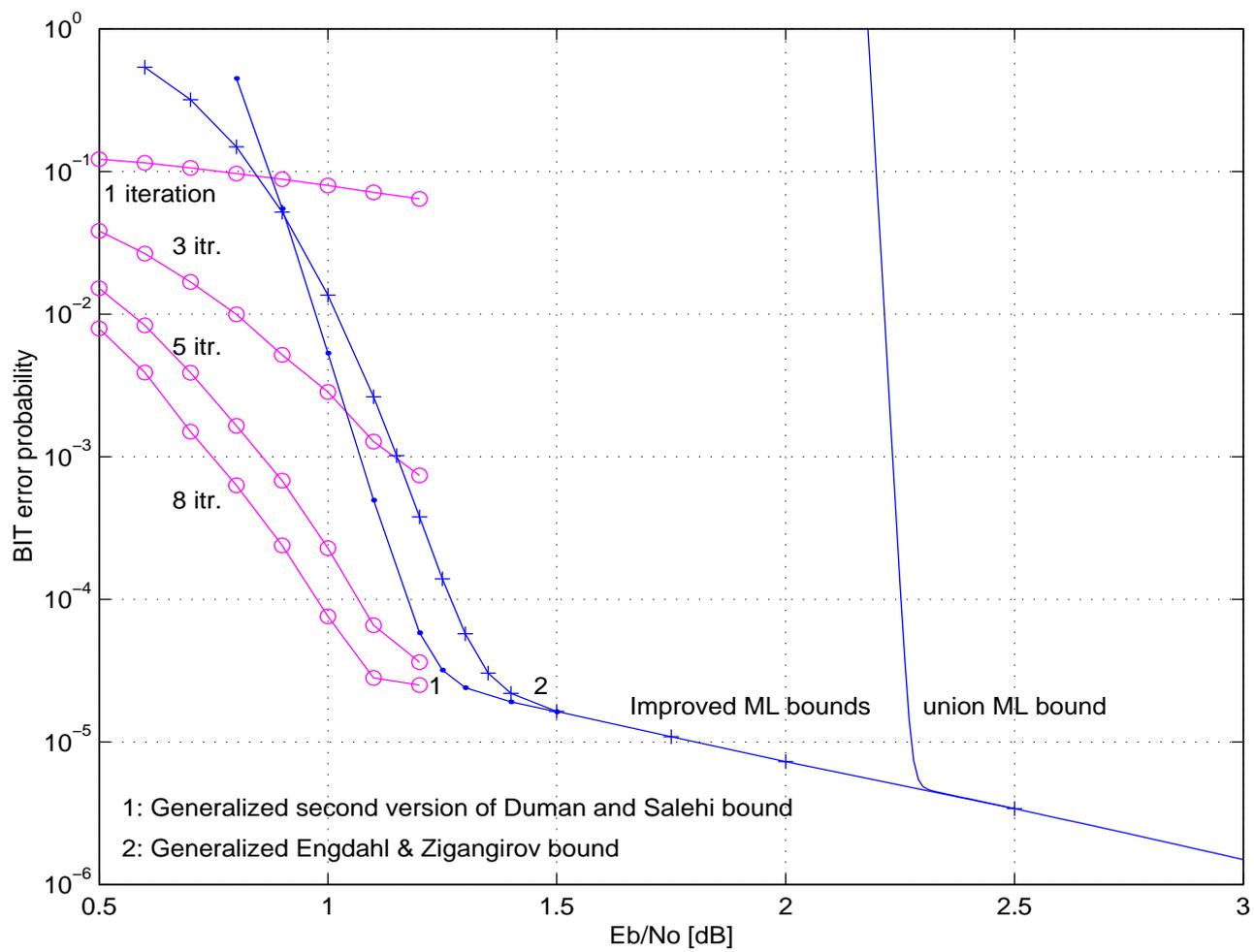


Figure 5c.

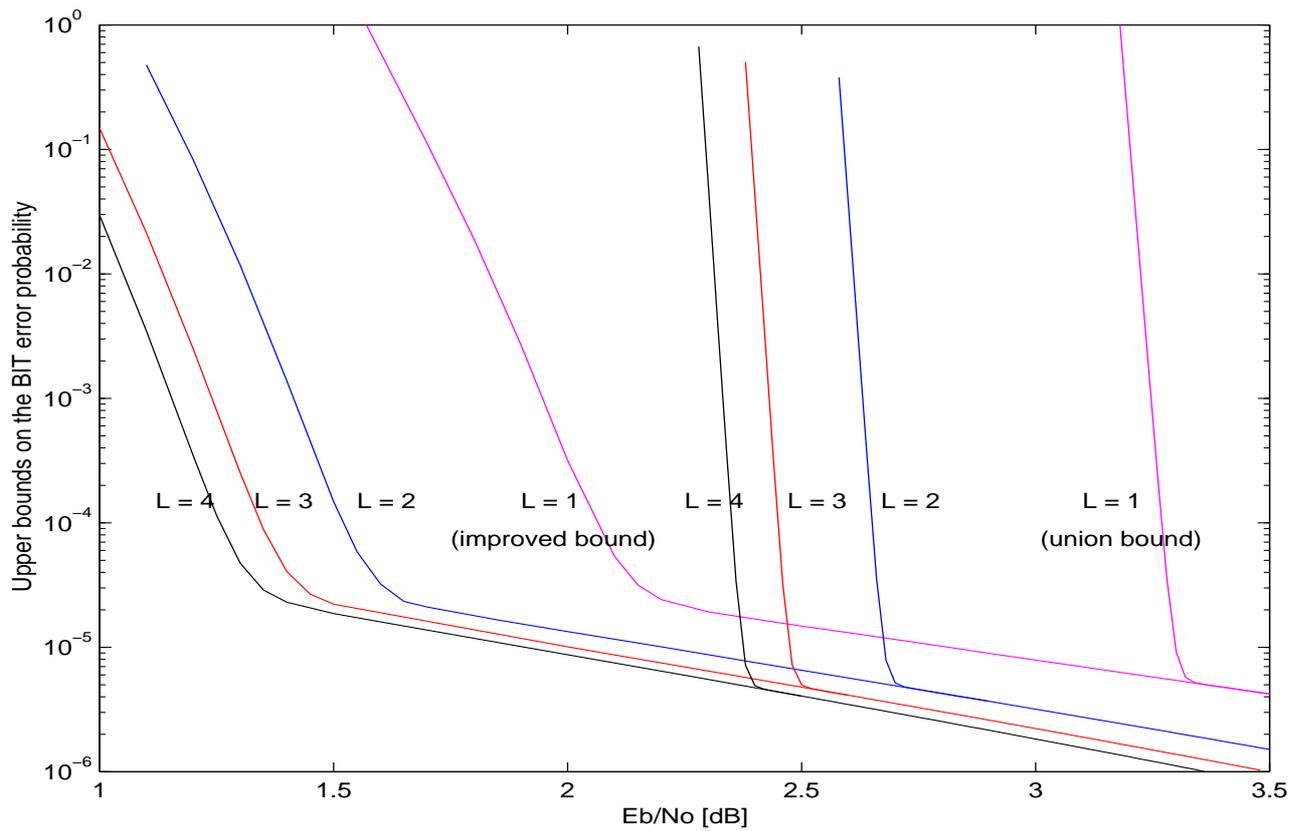


Figure 6.

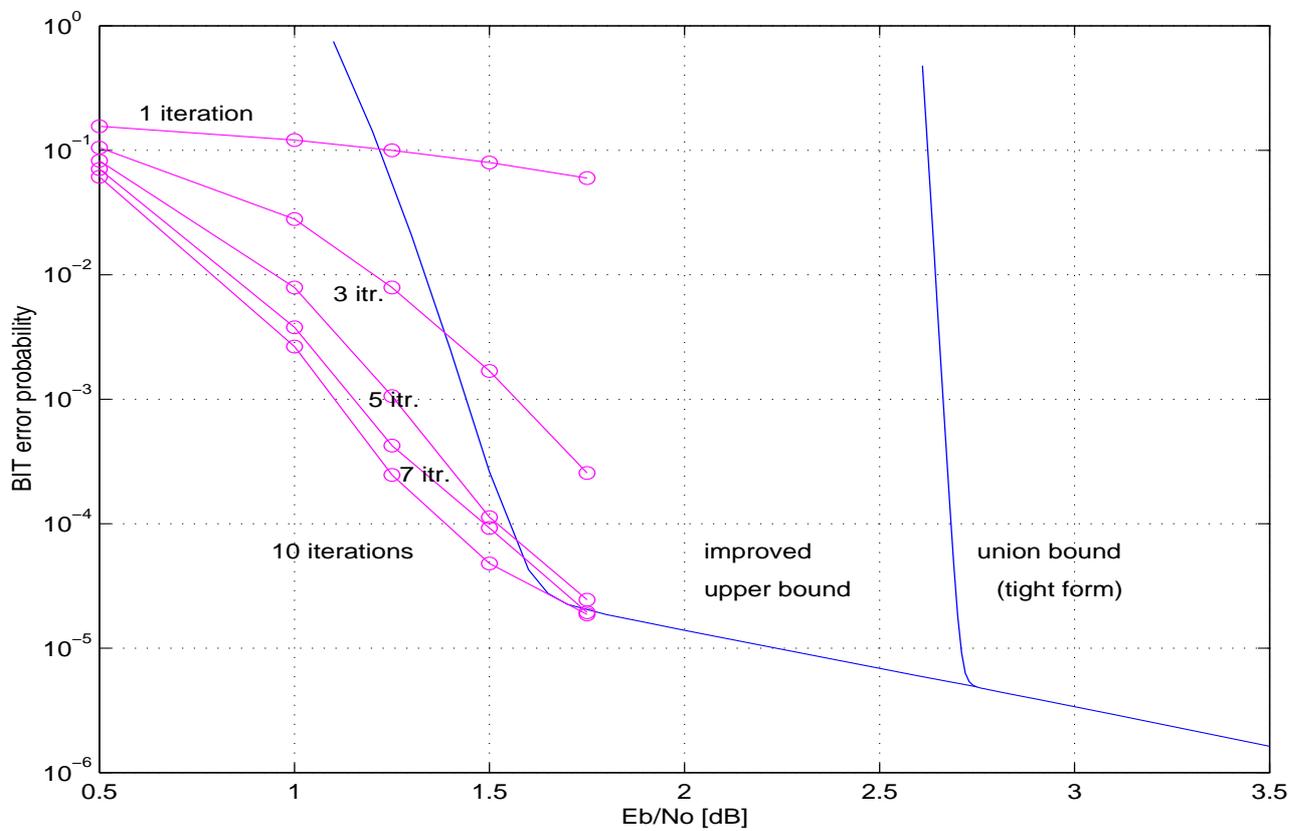


Figure 7.

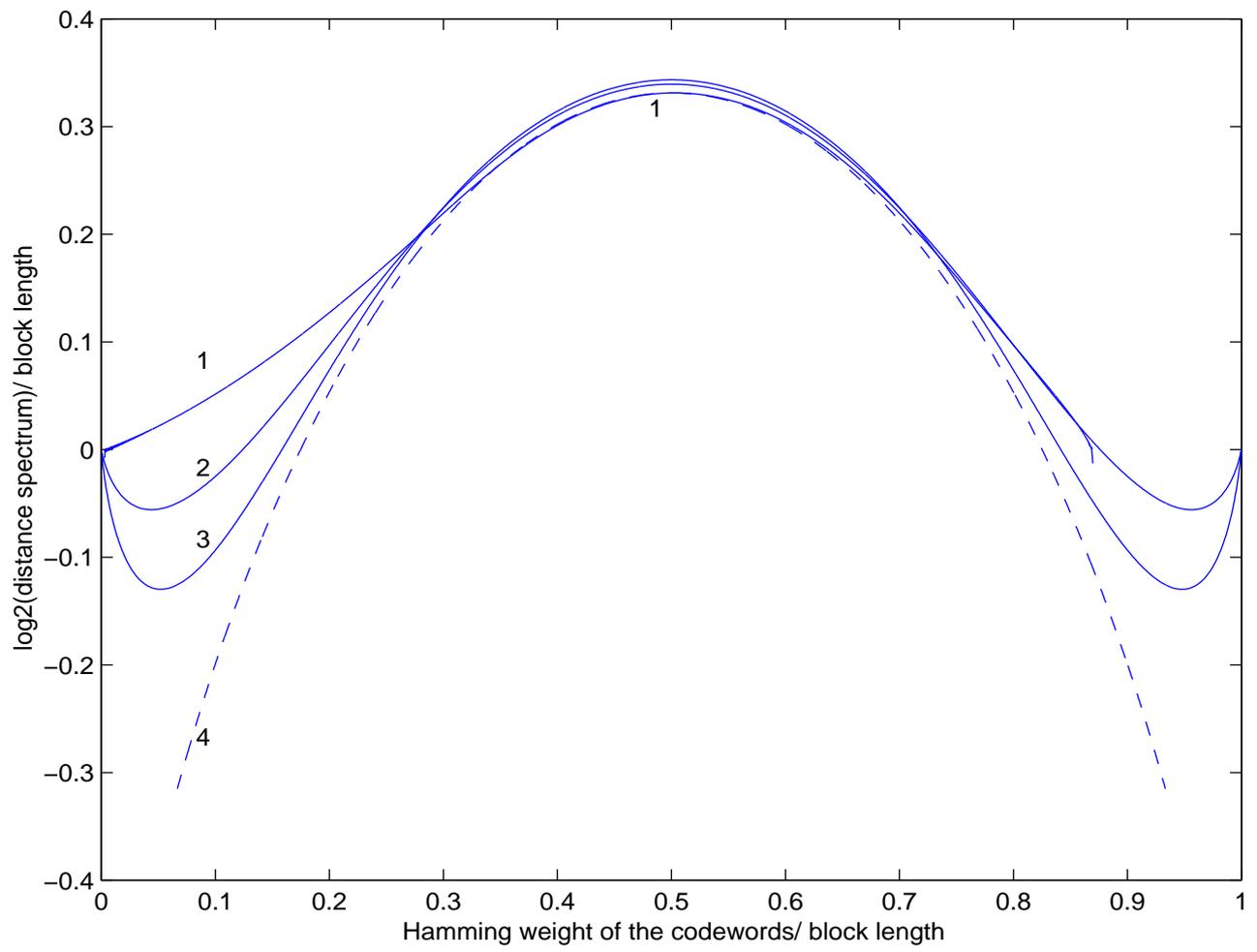


Figure 8.

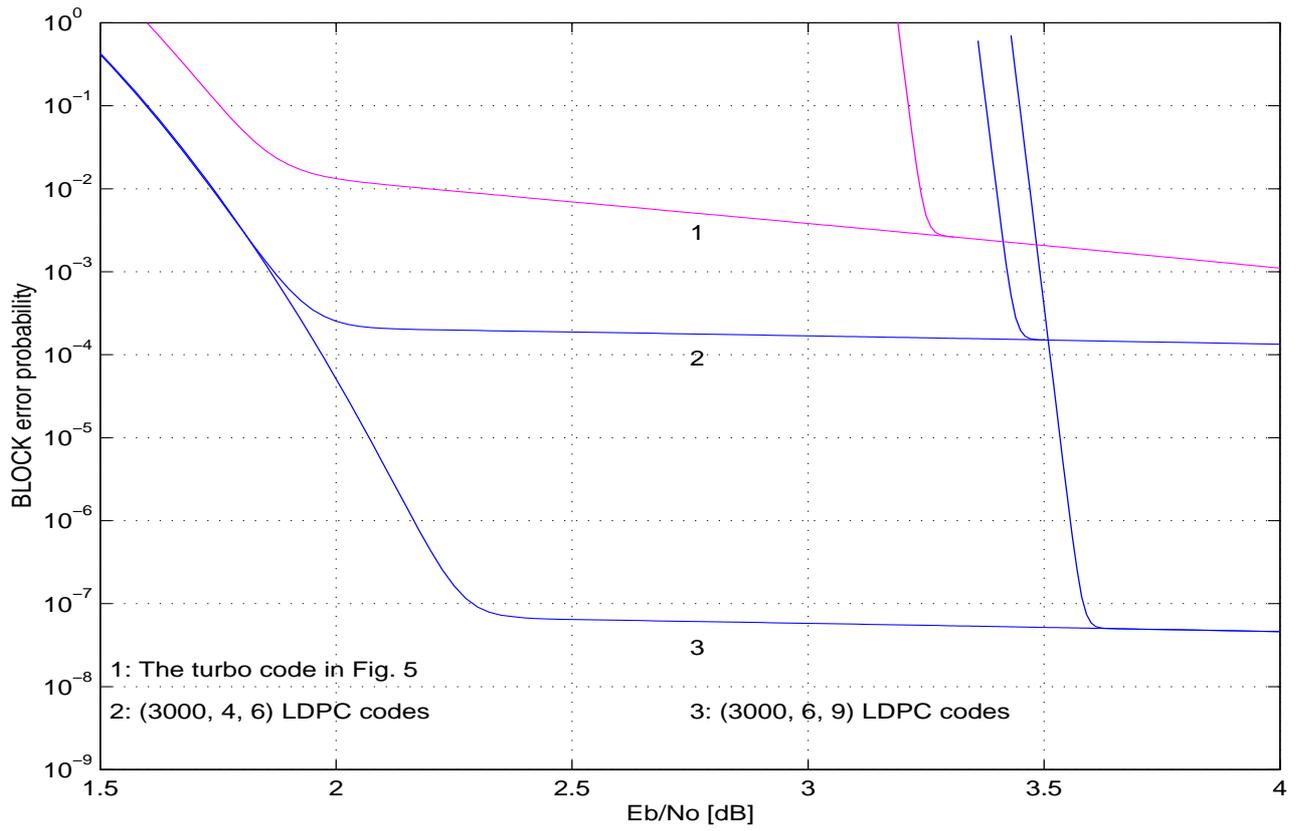


Figure 9a.

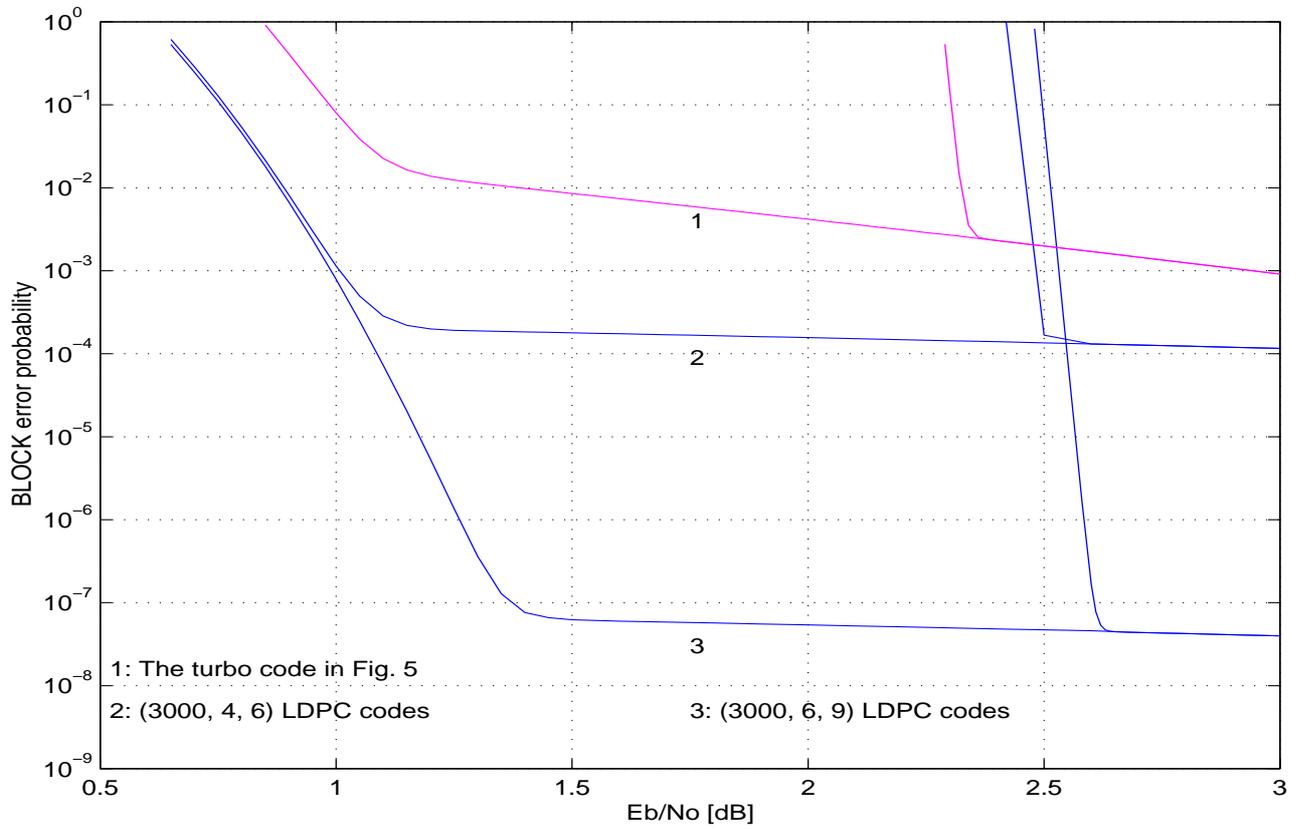


Figure 9b.

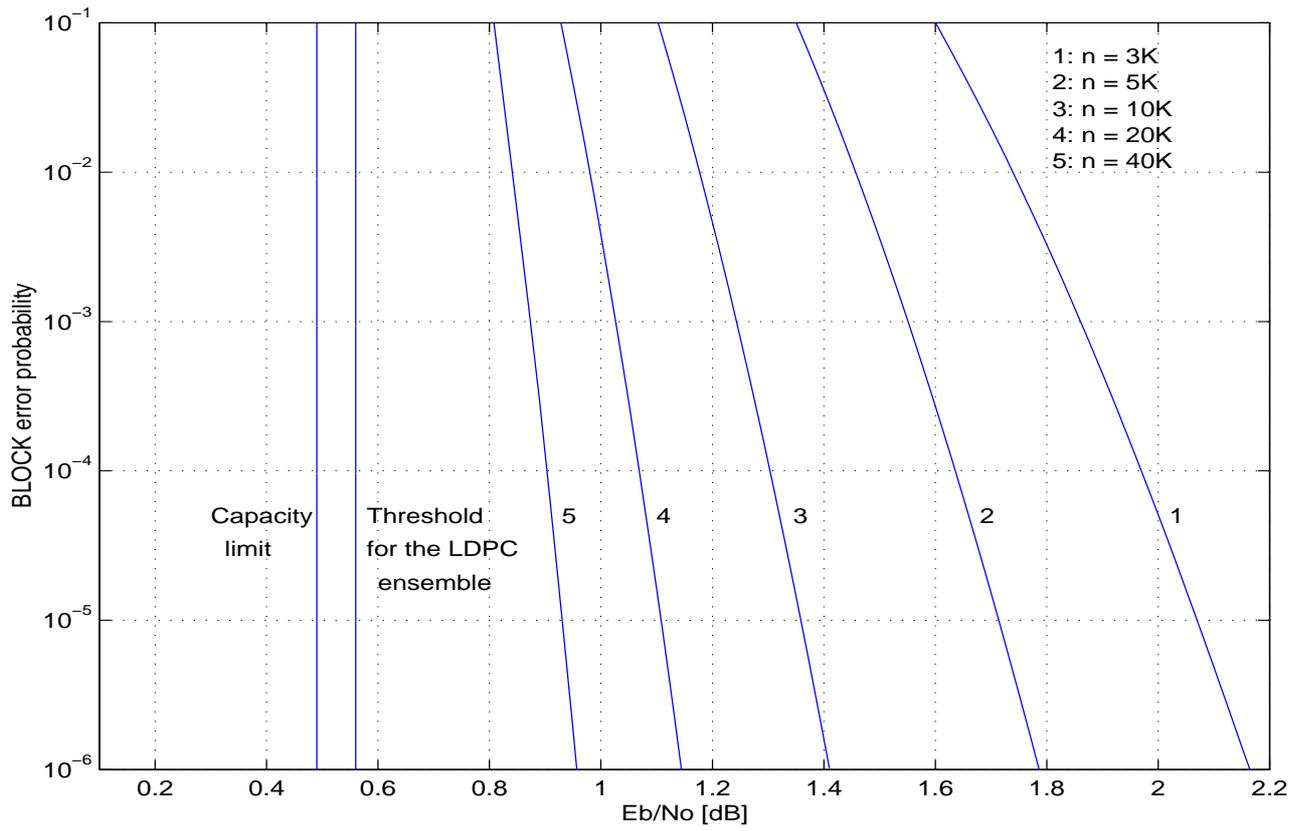


Figure 10a.

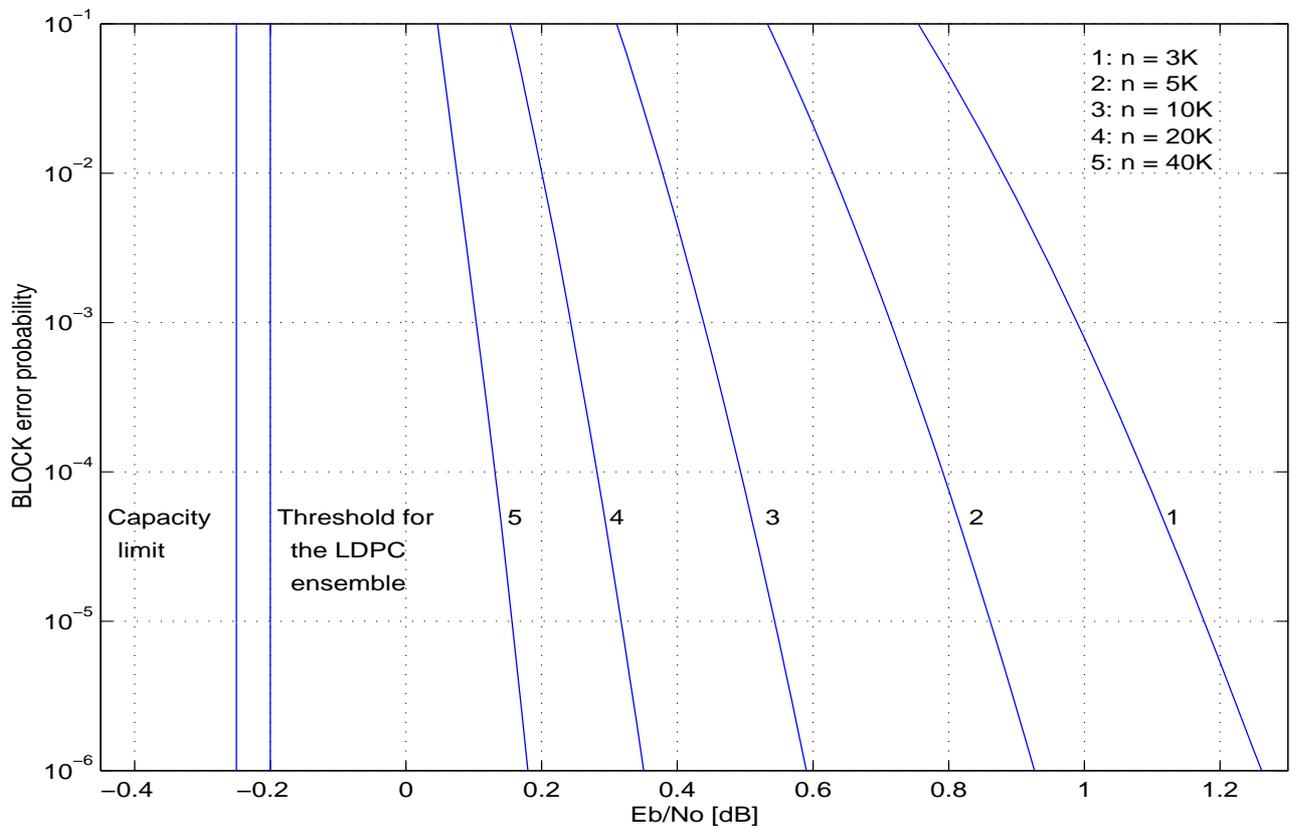


Figure 10b.

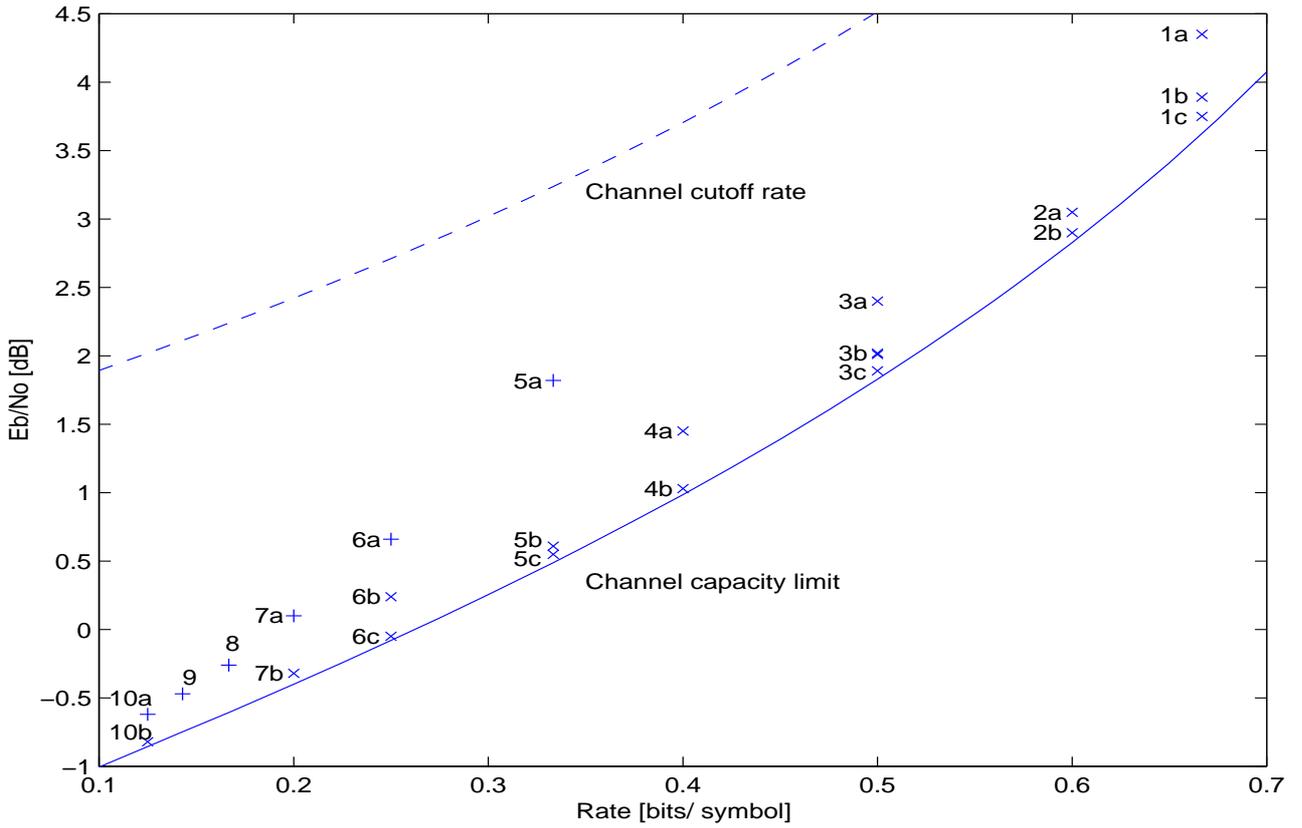


Figure 11a.

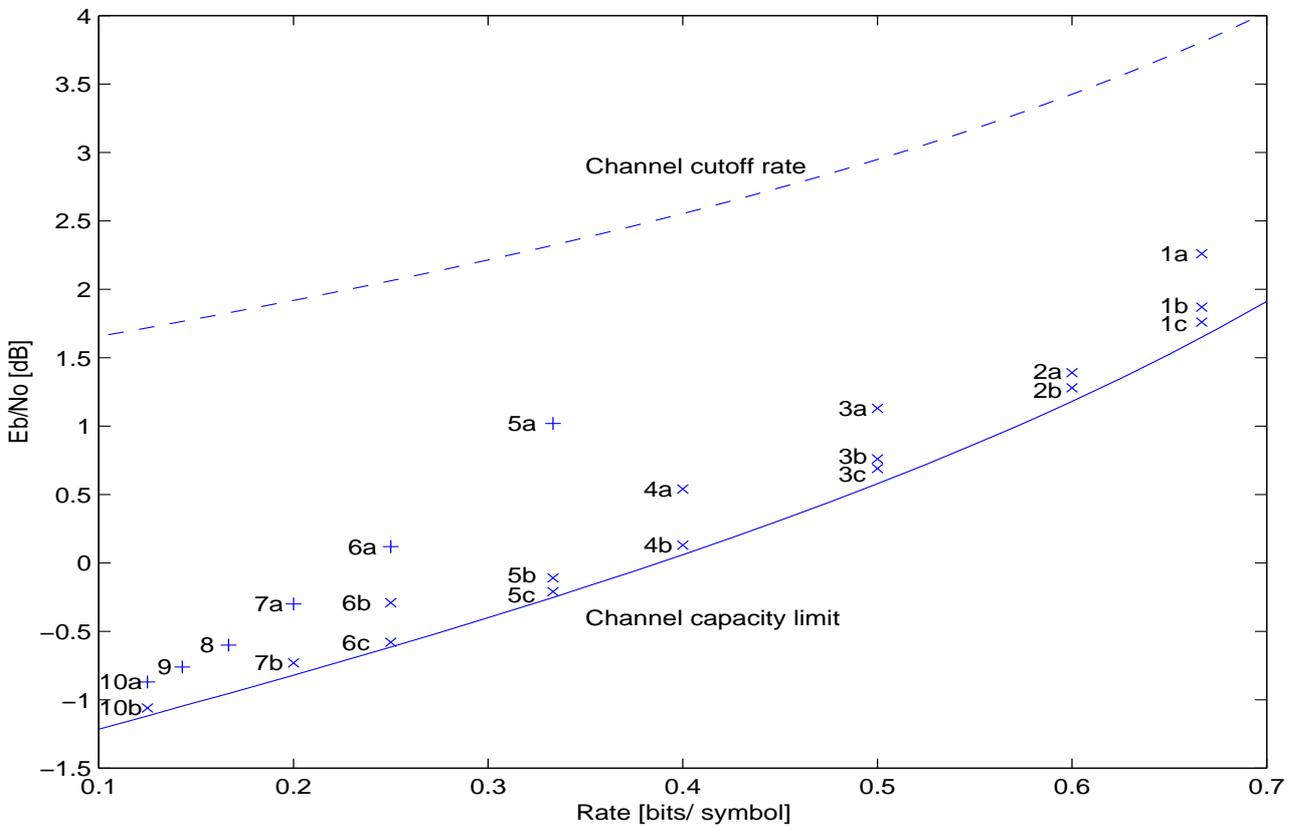


Figure 11b.