Improved Upper Bounds on the ML Decoding Error Probability of Parallel and Serial Concatenated Turbo Codes via their Ensemble Distance Spectrum

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

August 1999

Abstract

The ensemble performance of parallel and serial concatenated turbo codes is considered, where the ensemble is generated by a uniform choice of the interleaver and of the component codes taken from the set of time varying recursive systematic convolutional codes. Following the derivation of the input-output weight enumeration functions of the ensembles of random parallel and serial concatenated turbo codes,the tangential sphere upper bound is employed to provide improved upper bounds on the block and bit error probabilities of these ensembles of codes for the binary-input additive white Gaussian noise channel, based on coherent detection of equi-energy antipodal signals and *maximum likelihood decoding*. The influence of the interleaver length and the memory length of the component codes are investigated. The improved bounding technique proposed here is compared to the conventional union bound and to a recent alternative bounding technique by Duman and Salehi which incorporates modified Gallager bounds. The advantage of the derived bounds is demonstrated for a variety of parallel and serial concatenated coding schemes with either fixed or random recursive systematic convolutional component codes, and it is especially pronounced in the region exceeding the cutoff rate, where the performance of turbo codes is most appealing. These upper bounds are also compared to simulation results of the iterative decoding algorithm.

Keywords: turbo codes, distance spectrum, ML decoding, iterative decoding, uniform interleaver, AWGN channel.

This work has been supported by the Neaman Institute, Consortium on Digital Communications.

I. Introduction

The discovery of turbo codes in 1993 [7] is one of the exciting recent developments in coding theory. The codes have demonstrated near Shannon limit performance on a Gaussian channel with relatively simple component codes and large interleavers. Intensive literature on this subject has appeared since the introduction of these codes, as is evidenced by [1]–[38] and references therein.

In addition to simulations, theoretical upper bounds on the bit error probability of turbo codes have been developed. Since it has not yet been tractable to obtain analytic bounds for a particular interleaver and particular component codes, the bounds have been developed as averages over certain ensembles, featuring *random coding* properties. However, since mostly these bounds are based on a union bounding technique, they give useless results for energy per bit to spectral noise density $\left(\frac{E_b}{N_0}\right)$ ratios below the value corresponding to the cutoff rate (R_0) of the channel, a region which is of particular interest for the turbo codes operation.

An upper bound on the bit error probability of a parallel concatenated coding scheme averaged over the interleavers of a given length was proposed in [2]. A probabilistic interleaver called the 'uniform interleaver' was introduced in [2], taking into consideration all the possible interleaving permutations, including the option of a non interleaved code as a particular case, where all interleaving permutations are uniformly weighted. That permits an easy derivation of the input-output weight enumeration function (IOWEF) of the parallel concatenated code relying on the IOWEF of its component codes. A similar union upper bound to the bit error probability of a serially concatenated coding scheme averaged over the interleavers of a given length was reported in [4].

Union bounds for serially concatenated codes with ML decoding for the binary-input additive white Gaussian noise (AWGN) channel were studied in [38] and compared to the performance of iterative soft output decoding algorithms. The component codes were explicitly chosen fixed while the interleaver was random and uniform. A set of recursion relations were developed, based on the chosen component codes, to facilitate the numerical computation of the union bound. These union bounds indicate that the interleaver gain, for long enough interleavers, was achieved above the value of $\frac{E_b}{N_0}$ that corresponds to the cutoff rate.

Indeed, the ensemble of codes considered in [38] was generated by all the interleaving permutations rather than all codes as is usually done in random coding applications, but the union bound is still the weak link as was demonstrated in [38] by computer simulations, using iterative MAP soft-output decoding. These simulations demonstrated an interleaver gain even for $\frac{E_b}{N_0}$ values corresponding to code rates above the cutoff rate but below the channel capacity.

The IOWEF of the ensembles of random parallel and serial concatenated turbo codes were derived in [35],[31] respectively. The ensemble of random codes is generated by a uniform choice of the interleaver from the set of interleavers of length N, and also a uniform choice of the component codes from the set of time varying recursive systematic convolutional (RSC) codes with a fixed memory length m. These derivations reduce the performance behavior of random turbo codes to a two parameter family, with the parameters: the interleaving length N and the memory length of the component codes m (the memory length of the RSC codes is assumed here to be the same). Following the derivations of the IOWEF of these ensembles of codes, the union bound was employed to provide upper bounds on their bit error probabilities for an AWGN channel and ML decoding [31],[35].

We focus in [31] on serially concatenated turbo codes with rate $\frac{1}{2}$ time-varying RSC codes as component codes and examine also parallel concatenated turbo codes with three component codes [14], which gives rise of an overall code of rate $\frac{1}{4}$ (a similar overall rate as for a serially concatenated code with two rate $\frac{1}{2}$ component codes).

An upper bound on the block and bit error probabilities of turbo codes with ML decoding is derived [17], using a modified version of Gallager's bound rather than the standard union bound. This result is a generalization of the transfer function bounds providing a tighter upper bound as compared to the union bound. The upper bound on the bit error probability derived in [17] requires the partition of the code to constant weight subcodes, such that each one of them includes codewords that have also the same information weight. Then, the improved upper bound in [17] is applied on each subcode and finally, the union bound is applied to get an upper bound on the bit error probability of the overall code. Indeed, the double constraints used to partition the code to subcodes, weaken the upper bound on the bit error probability in [17], as the union bound is applied on so many subcodes. The bound in [17] happens then to be useful for some range below the channel cutoff rate and it does not diverge at the cutoff rate like the union bound. Typically, the upper bound on the block error probability is a tight bound for $\frac{E_b}{N_0}$ values 0.5–0.7 dB below the $\frac{E_b}{N_0}$ value that corresponds to cutoff rate, and diverges at $\frac{E_b}{N_0}$ values 0.8–1.0 dB below that value. The gain with respect to the union bound achieved by the upper bound on the bit error probability is even lessened. These bounds on the bit and block error probabilities of turbo codes are not covering thus the full range of their usefulness. The upper bound is derived for turbo codes with fixed component codes and a random uniform interleaver. A generalization of these upper bounds for some other error-correction codes as for example: binary linear block codes, systematic convolutional codes (not necessarily recursive) and serially concatenated codes are also available.

In [37], an upper bound on the block error probability for an arbitrary binary-input symmetric channel is presented. This upper bound, based on Gallager's 1963 technique, is examined for the

binary-input AWGN channel and some parallel concatenated turbo codes. However, the upper bound in [17] is slightly better. An extended bounding technique based on Gallager's 1963 bound is reported in [34], where also comparisons to the bounds here for selected convolutional and block turbo codes are presented. The basic idea of the ensemble performance (averaged over the interleaver and in some cases also over the component codes) upper bounds on the bit error probability here [32] is based on applying a modified version of the tangential sphere bound [30], without any need to partition the code to subcodes, and hence there is no need to employ a union bound over subcodes as in [17].

The improved bounding technique described here has been utilized in [28] to analyze the serially interleaved concatenated codes, where the outer code is a standard convolutional code and the inner code is a recursive convolutional code of rate 1. Focus is put on the ubiquitous inner differential encoder (used in particular to resolve phase ambiguities), and it was analytically demonstrated that the error probabilities corresponding to a coherent detection of BPSK modulation over the AWGN channel, for this construction is advantageous as compared to the stand-alone convolutional code. This in spite of the fact that the inner code is of rate 1. Our bounding technique has also been used in a recent extensive investigation of block and turbo-block codes [33], demonstrating impressive tightness of the bounds.

A comparison between the bounding techniques here and in [17], demonstrates that our bounding technique is advantageous and it extends further the region of $\frac{E_b}{N_0}$ for which the bounds are useful. This is also the general conclusion when compared to Gallager bounds in the form investigated in [34], though particular examples of high-rate turbo-block codes were found for which the bounds in [34] yield marginally improved tightness. These upper bounds that refer to ML decoding are compared here with computer simulations of iterative soft-output decoding, based on the LOG-MAP decoding algorithm.

II. Preliminaries

In this section, we state the underlying assumptions on which our bounds are based, introduce notations and basic relations from [2, 4, 12, 13, 17, 30, 31, 32, 35, 38] which apply to parallel and serial concatenated turbo codes, and state further relations and comments useful to our analysis and conclusions.

A. Assumptions:

In our analysis we consider the case where the information bits are encoded by serial or parallel concatenated turbo codes and BPSK modulated. The equi-energy signals are transmitted through an AWGN channel, the received signals are coherently detected and then ML decoding is performed.

The component codes of the turbo encoder are assumed to be time-varying RSC codes with the same memory length m (see Fig. 1) or fixed RSC codes. A uniform interleaving of length N is incorporated in both structures (see Figs. 2a-c). A termination with m additional cycles of the shift register is assumed [13], though the results for large values of interleaver length ($N \gg m$), are insensitive to the specific termination method.

B. Notations and relations:

B.1 The distance spectra of parallel and serial concatenated codes:

A serial concatenated turbo code c_s with components c_{out} and c_{in} as outer and inner codes respectively, is the first concatenation structure being considered here (see Fig. 2b). The rate R of code c_s in units of bit/symbol, is the product of the rates of its component codes. The uniform interleaver situated between the component codes is operating on bits (and not on symbols) and has a length of N and the common memory length of the component codes is m.

The number of codewords of the code c_s that are encoded by information bits of Hamming weight w and have also a total Hamming weight of h is designated by $A_{w,h}^{c_s}$. Here, for serially concatenated codes, the number of information bits is the product of the interleaver length N and the rate of the outer code $R^{(\text{out})}$, since N is also the length of a codeword of the outer code c_{out}.

As the component codes are assumed here to be systematic, then also the serial concatenated code c_s is a systematic code, and therefore $A_{w,h}^{c_s} = 0$ if $w > h$. Similar definitions related to the component codes are derived for $A_{w,\ell}^{c_{\text{out}}}$ and $A_{\ell,h}^{c_{\text{in}}}$. As before, since the component codes are systematic, that implies that for $w > \ell$ or $\ell > h$: $A_{w,\ell}^{c_{\text{out}}} = 0$ or $A_{\ell,h}^{c_{\text{in}}} = 0$ respectively.

These notations are consistent with those used in papers [4],[31],[38] that deal with serial concatenated codes. However, unlike papers [2],[35] that address parallel concatenated turbo codes, the parameter h of $A_{w,h}^{c_s}$ is the Hamming weight of the entire codeword of c_s, not only of its parity bits.

For a serially concatenated code c_s with a uniform interleaver of length N, the following equation

holds [4]:

$$A_{w,h}^{c_s} = \sum_{\ell=0}^{N} \frac{A_{w,\ell}^{c_{\text{out}}} \, A_{\ell,h}^{c_{\text{in}}}}{\binom{N}{\ell}} \; . \tag{1}$$

Clearly, by linearity, a zero input results in a zero output and therefore,

$$A_{0,0}^{c_s} = 1 \; . \tag{2}$$

The following notations were adopted from [31],[35] for the derivation of the distance spectrum for the considered random ensemble of serially concatenated codes:

Let T be the random variable describing the number of cycles a time varying recursive shift register of memory length m is active, i.e. is in a non-zero state as a result of a random binary input sequence whose first bit is '1' Let p_k be the probability that the random variable T equals k, $p_k = \text{Prob}\,\{T = k\}$. Clearly, $p_k = 0$ for $k < m$, since the memory length of the shift register is m. Moreover, as long as the shift register is in a non-zero state, $\{s_1(n)\,,\; n \geq 1\}$ (see Fig. 1) will be a sequence of i.i.d. random variables, uniformly distributed on GF(2), and independent of the input process x [35].

As shown in [35], p_k satisfies the equation:

$$p_k = 2^{-k} \sum_{j=1}^{m} d_j \, \rho_j^k - \delta(k) \; , \tag{3}$$

where $\delta(k)$ equals 1 for $k = 0$ and 0 otherwise, where $\frac{1}{\rho_j}$ is the j^{th} zero of $1 - \sum_{i=1}^{m} z^i$ (all zeros of $1 - \sum_{i=1}^{m} z^i$ have multiplicity 1), and where the coefficients d_j are determined by the equation:

$$\sum_{j=1}^{m} \frac{d_j}{1 - \rho_j \, z} = \frac{1 - \sum_{i=1}^{m-1} z^i}{1 - \sum_{i=1}^{m} z^i} \; . \tag{4}$$

An alternative method for the computation of the probabilities $\{p_k\}$ is derived in [31], which is advantageous over the method above only for low values of k, i.e., $k \leq (m+1)^2$. We adhere therefore to equations (3),(4) for the determination of the probabilities $\{p_k\}$. Since we are interested in the output of the shift register within a finite interval, $p_{k,\ell}$ is defined as in [31],[35]:

$$p_{k,\ell} = \begin{cases} p_k & \text{if} \quad k < \ell \\ 1 - \sum_{j=0}^{\ell-1} p_j & \text{if} \quad k = \ell \\ 0 & \text{if} \quad k > \ell \end{cases} \; . \tag{5}$$

For a given binary linear systematic block code C of dimension L, let $A^c(W,Z) = \sum_{w=0}^{L} A_w^c(Z)\, W^w$ be its input-output weight enumeration function IOWEF, where $A_w^c(Z) = \sum_{\ell} A_{w,\ell}^c\, Z^\ell$ designates the conditional IOWEF assuming information weight w.

Based on the analysis in [31] for serial concatenation with component codes that are time-varying RCS codes of rates $\frac{1}{2}$ and memory length m, (where $\frac{N}{2}$ bits are encoded by the outer encoder, which in turn generates N bits that are permuted by a random interleaver and are encoded by the inner encoder which generates $2N$ bits), the following equation holds:

$$A_{1,1}^{c_s} = \frac{A_{1,1}^{c_{\text{out}}}\, A_{1,1}^{c_{\text{in}}}}{N} = \frac{1}{4N} \left(\sum_{i_1=0}^{\frac{N}{2}-1} \sum_{k_1=0}^{\frac{N}{2}-1-i_1} 2^{-k_1}\, p_{k_1,\, \frac{N}{2}-1-i_1} \right) \left(\sum_{i_2=0}^{N-1} \sum_{k_2=0}^{N-1-i_2} 2^{-k_2}\, p_{k_2,\, N-1-i_2} \right). \quad (6)$$

For a linear systematic block code C of dimension L, S_w is defined in [35],[31] as the set of binary L-tuples of Hamming weight w.

The dimension of the component codes of a parallel concatenation is equal to the interleaver length. On the other hand, related to the outer code of a serially concatenated code, $S_w^{(\text{out})}$ is defined as the set of binary $NR^{(\text{out})}$-tuples of Hamming weight w ($R^{(\text{out})} = \frac{1}{2}$ in our analysis, but the technique can be generalized). The set $S_w^{(\text{in})}$, for the inner code of the serial concatenation, is defined similar to S_w for parallel concatenation in [35]; the sets $S_w^{(\text{in})}$ and S_w in [35] are the same, since the input to the inner code is of length N as is the input length of parallel concatenation).

Following the explanation and notations in [31],[35], for $x \in S_w$, let i_1, i_2 ... i_w ($0 \le i_1 < i_2 < \cdots < i_w \le L-1$) be the positions of the non-zero inputs. After the first non-zero input enters the shift register at time i_1, the register stays active for a time T. If there exists an index j, $1 < j \le w$, such that $i_1 + T < i_j$, then the non-zero input at time i_j will activate the shift register again. As before, the shift register will stay active for a time T which is independent of the first activity time. The time span that the output is active is relevant (being the time span in which either the input is non-zero or the shift register is active) over the observation span of L (the length of binary tuples in S_w).

Let E_w be the random variable describing this time span, averaged over a uniform choice over S_w, and let Prob $\{E_w = k\} = q_k^w$. In a similar manner, based on the definitions of $S_w^{(in)}$ and $S_w^{(\text{out})}$ for the component codes of a serial concatenated code, the random variables $E_\ell^{(\text{in})}$ and $E_w^{(\text{out})}$ and the corresponding probabilities $q_{k_2}^{\ell}(c_{\text{in}})$ and $q_{k_1}^{w}(c_{\text{out}})$ are defined (where $1 \le k_2 \le N$ and $1 \le k_1 \le \frac{N}{2}$, related to the inner and outer codes of the serial concatenated code c_s, respectively).

The probabilities $\left\{q_{k_2}^{\ell}(c_{\rm in})\right\}_{\ell=1}^{N}$ and $\left\{q_{k_1}^{w}(c_{\rm out})\right\}_{w=1}^{\frac{N}{2}}$ related to the inner and outer codes respectively, were calculated by computer simulations with the aid of the statistical algorithm proposed in [35].

Based on the analysis of [31], for random serially concatenated codes, the following relations hold:

For integer values of h, such that $2 \leq h \leq \dfrac{3N}{2}+1$:

$$A_{1,h}^{c_s} = \sum_{\ell=1}^{\min\left(\frac{N}{2}+1,h\right)} \frac{A_{1,\ell}^{c_{\rm out}}\, A_{\ell,h}^{c_{\rm in}}}{\binom{N}{\ell}}$$

$$= \frac{1}{N}\left(\sum_{i_1=0}^{\frac{N}{2}-1}\sum_{k_1=0}^{\frac{N}{2}-1-i_1} p_{k_1,\,\frac{N}{2}-1-i_1}\, 2^{-(k_1+1)}\right)\left(\sum_{i_2=0}^{\max(0,N-h+1)}\sum_{k_2=h-2}^{N-1-i_2} p_{k_2,\,N-1-i_2}\, 2^{-(k_2+1)}\,\binom{k_2+1}{h-1}\right)$$

$$+ \sum_{\ell=2}^{\min\left(\frac{N}{2}+1,h\right)}\left\{\left(\sum_{i_1=0}^{\frac{N}{2}-\ell+1}\sum_{k_1=\ell-2}^{\frac{N}{2}-1-i_1} p_{k_1,\,\frac{N}{2}-1-i_1}\, 2^{-(k_1+1)}\,\binom{k_1+1}{\ell-1}\right)\sum_{k_2=\max(\ell,h-\ell)}^{N} 2^{-k_2}\, q_{k_2}^{\ell}(c_{\rm in})\,\binom{k_2}{h-\ell}\right\} \tag{7}$$

where for integer values of h exceeding $N+1$, only the second term affects $A_{1,h}^{c_s}$ (the first term is zero if $h > N+1$) and for integer values of h exceeding $\frac{3N}{2}+1$: $A_{1,h}^{c_s}=0$. Now

$$A_{w,h}^{c_s} = \binom{\frac{N}{2}}{w} \sum_{\ell=\max\,(w,h-N)}^{\min\left(\frac{N}{2}+w,h\right)}\left\{\sum_{k_1=\max(w,\ell-w)}^{\frac{N}{2}} q_{k_1}^{w}(c_{\rm out})\, 2^{-k_1}\,\binom{k_1}{\ell-w}\cdot\sum_{k_2=\max(\ell,h-\ell)}^{N} q_{k_2}^{\ell}(c_{\rm in})\, 2^{-k_2}\,\binom{k_2}{h-\ell}\right\}, \tag{8}$$

for integer values of w, h such that $2 \leq w \leq \frac{N}{2}$ and $w \leq h \leq \frac{3N}{2}+w$.

Finally, the IOWEF for the random ensemble of serially concatenated turbo codes takes the following form:

$$A^{c_s}(W,Z) = \sum_{w,h} A_{w,h}^{c_s}\, W^w\, Z^h = 1 + A_{1,1}^{c_s}\, WZ + W\sum_{h=2}^{\frac{3N}{2}+1} A_{1,h}^{c_s}\, Z^h + \sum_{w=2}^{\frac{N}{2}}\sum_{h=w}^{\frac{3N}{2}+w} A_{w,h}^{c_s}\, W^w\, Z^h \tag{9}$$

where the coefficients of the first, second, third and fourth terms above are based on equations (2),(6),(7),(9) respectively.

The conditional IOWEF for the random ensemble of the parallel concatenated convolutional codes c_p using K component codes and $K-1$ uniform interleavers of length N (see Figs. 2a,c as

examples for $K = 2, 3$ respectively) is related to the conditional IOWEF of its component codes by

$$A_w^{c_p}(Z) = \frac{\Big(A_w^c(Z)\Big)^K}{\binom{N}{w}^{K-1}} \ . \tag{10}$$

Here it is assumed that the Hamming weight of the information bits is w.

Based on the analysis in [35] for random ensemble of the parallel concatenated turbo codes, the following relations hold for the conditional IOWEF of the component codes (assumed here to be time-varying RSC codes):

$$\begin{aligned} A_0^c(Z) &= 1 \\ A_1^c(Z) &= \sum_{i=0}^{N-1} \sum_{k=0}^{N-1-i} p_{k,\,N-1-i}\, 2^{-(k+1)} \sum_{j=0}^{k+1} \binom{k+1}{j} Z^j \\ A_w^c(Z) &= \binom{N}{w} \sum_{k=0}^{N} q_k^w \, 2^{-k} \sum_{j=0}^{k} \binom{k}{j} Z^j \qquad w = 2, 3 \ \ldots \ N \ . \end{aligned} \tag{11}$$

Under our assumptions, the IOWEF for the random ensemble of parallel concatenated turbo codes (with K component codes and $K-1$ uniform interleavers of length N) is the following:

$$\begin{aligned} A^{c_p}(W, Z) &= \sum_{w=0}^{N} W^w \, A_w^{c_p}(Z) \\ &= 1 + \sum_{w=1}^{N} \frac{W^w \Big[A_w^c(Z)\Big]^K}{\binom{N}{w}^{K-1}} \ . \end{aligned} \tag{12}$$

For the cases examined here of parallel and serial concatenated turbo codes with fixed component codes and random interleavers, we calculated the IOWEF of the component codes by the method described in [27]. Then, the IOWEF of the serial or parallel concatenated turbo codes were evaluated based on the IOWEF of its components by Eqs. (1) or (10) respectively, as we assume throughout a *uniform* interleaving.

B.2 Craig's formula used for the union bound on the bit error probability:

By definition, $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{t^2}{2}}\, dt$ is the probability that a random Gaussian variable with zero mean and unit variance exceeds the value x. For the exponential form of the union bound,

the following inequality $Q(x) \leq \frac{1}{2}\ e^{-\frac{x^2}{2}}$ for $x \geq 0$, is customary applied. A tighter upper bound on the bit error probability is derived by using the identity in [9]:

$$Q(x) = \frac{1}{\pi} \int_0^{\frac{\pi}{2}} e^{-\frac{x^2}{2\sin^2\theta}}\, d\theta\ , \quad x \geq 0\ . \tag{13}$$

With the aid of equation (13), this yields the following upper bound on the bit error probability of a binary linear block code C,

$$P_b \leq \frac{1}{\pi N} \int_0^{\frac{\pi}{2}} W\ \frac{\partial A^c(W,Z)}{\partial W}\Big|_{W=Z=e^{-\frac{RE_b}{N_0\ \sin^2\theta}}}\ d\theta\ , \tag{14}$$

replacing the upper bound:

$$P_b \leq \frac{W}{2N}\ \frac{\partial A^c(W,Z)}{\partial W}\Big|_{W=Z=e^{-\frac{RE_b}{N_0}}}\ ,$$

which obviously is looser. Finally, the integration over θ in the upper bound (14) is performed numerically. The applicability of equation (13) is demonstrated in [6],[15].

B.3 The tangential sphere bound

The tangential sphere bound which is the essential ingredient of our bounding technique, is an upper bound on the message error probability, introduced in [20],[30] and shortly reviewed here. Suppose that the signals transmitted through an AWGN channel for each message (represented by a codeword of a linear block code C), are of the same energy E. The energy of each signal is $E = nE_s$, when n is the block code length and E_s is the energy transmitted per symbol.

It can be shown that the tangential sphere bound is always tighter than the tangential bound [6] and the union bound, especially for low and moderate values of $\frac{E_b}{N_0}$ [20]. The properties of the tangential-sphere bound (and also the upper bounds in [6],[21]) follow by the central inequality,

$$\text{Prob}\ (A) \leq \text{Prob}\ (\underline{z} \in B, A) + \text{Prob}\ (\underline{z} \notin B)\ . \tag{15}$$

In the case of the tangential sphere bound, A is an event that represents a message decoding error, B is an n-dimensional cone with a half angle θ and radius $r = \sqrt{nE_s}\ \tan\theta$, and $\underline{z}$ is the noise vector added to the transmitted signal.

The tangential sphere bound on the block error probability P_e is based only on the distance

spectrum $\{S_k\}$ of the binary linear block code C and it reads:

$$P_e \leq \int_{-\infty}^{+\infty} \frac{dz_1}{\sqrt{2\pi}\,\sigma}\, e^{-\frac{z_1^2}{2\sigma^2}} \left\{ \begin{array}{l} 1-\overline{\gamma}\left(\frac{n-1}{2}\,,\,\frac{r_{z_1}^2}{2\sigma^2}\right) \\ +\sum\limits_{k:\,\frac{\delta_k}{2}<\alpha_k} S_k \left[Q\left(\frac{\beta_k(z_1)}{\sigma}\right) - Q\left(\frac{r_{z_1}}{\sigma}\right)\right] \overline{\gamma}\left(\frac{n-2}{2}\,,\,\frac{r_{z_1}^2-\beta_k^2(z_1)}{2\sigma^2}\right) \end{array} \right\}. \tag{16}$$

The following parameters are used in (16):

$$\left\{ \begin{array}{lcl} \sigma^2 & = & \frac{N_0}{2} \quad \text{with } N_0 \text{ standing for the one-sided spectral density} \\ & & \text{of the additive white Gaussian noise} \\ r_{z_1} & = & \left(1-\frac{z_1}{\sqrt{nE_s}}\right) r \\ \beta_k(z_1) & = & \frac{r_{z_1}}{\sqrt{1-\frac{\delta_k^2}{4nE_s}}} \cdot \frac{\delta_k}{2r} \\ \alpha_k & = & r\sqrt{1-\frac{\delta_k^2}{4nE_s}}\,, \end{array} \right. \tag{17}$$

δ_k is defined to be the Euclidean distance between two signals that their corresponding codewords differ in k symbols ($k \leq n$). Thus, for the case of antipodal signals $\delta_k = 2\sqrt{kE_s}$.

Also,

$$\overline{\gamma}\,(a,x) = \frac{1}{\Gamma(a)} \int_0^x t^{a-1}\, e^{-t}\, dt\,, \text{ for positive values of } a, x \tag{18}$$

designates the normalized incomplete gamma function.

A geometric interpretation of the tangential sphere bound is presented in Fig. 2 of [20].

The upper bound (16) is valid for all positive values of r and thus the optimal radius r (in the sense of achieving the tightest upper bound) is determined by setting the derivative of the right side of the bound (16) to zero, yielding the following optimization equation:

$$\left\{ \begin{array}{l} \sum\limits_{k:\,\frac{\delta_k}{2}<\alpha_k} S_k \int_0^{\theta_k} \sin^{n-3}\,\phi\, d\phi = \frac{\sqrt{\pi}\,\Gamma\left(\frac{n-2}{2}\right)}{\Gamma\left(\frac{n-1}{2}\right)} \\ \theta_k = \cos^{-1}\left(\frac{\delta_k}{2r}\,\frac{1}{\sqrt{1-\frac{\delta_k^2}{4nE_s}}}\right). \end{array} \right. \tag{19}$$

It is evident that this upper bound does not exceed 1, (let $\theta \to 0$ implying $P_e \stackrel{\triangle}{=} \text{Prob}\,(A) \leq 1$), in contrast to the union bound, especially for moderate and low values of E_b/N_0. The validity of the tangential sphere bound for our work here is further discussed in Appendix A.

III. Analysis: A Derivation of An Improved Upper Bound on the Bit Error Probability of a Linear Binary Block Code

In this section we will derive an improved upper bound on the bit error probability of a linear binary block code C. It is applied in section IV as an analytic tool to get an upper bound on the *bit* error probability of parallel and serial concatenated turbo codes via their ensemble distance spectrum. In Appendix C, we show that there is no need to partition the overall code, as done in [17],[37] to find efficient upper bounds on bit and block error probabilities, and as expected partition degrades the tightness of the upper bound.

Based on the derivation of the tangential sphere bound, let z_1 be the radial component noise, then

$$\text{Prob}\left(E_k(z_1)\,,\ \underline{z} \in C_n(\theta)\right) \tag{20}$$

$$= \int_{\beta_k(z_1)}^{r_{z_1}} \frac{1}{\sqrt{2\pi}\,\sigma}\, e^{-\frac{z_2^2}{2\sigma^2}}\, \overline{\gamma}\left(\frac{n-2}{2}\,,\ \frac{r_{z_1}^2 - z_2^2}{2\sigma^2}\right) dz_2$$

where $\underline{z}$ is an n-dimensional Gaussian noise vector added by the AWGN channel to the transmitted signal, where $z_i \sim N\Big(0,\ \frac{N_0}{2}\Big)$ for $i = 1, 2 \ldots n$, $C_n(\theta)$ is an n-dimensional cone of half angle θ and $E_k(z_1)$ is the error event of a wrong ML decoding between a pair of two equi-energy signals, represented by two arbitrary codewords whose Hamming distance is k. Both parameters r_{z_1} and $\beta_k(z_1)$ are determined by Eq. (17) (see Fig. 2 of [20]).

Let S_k be the number of codewords of Hamming weight k ($k = 0, 1, 2, \ldots n$) in a binary linear block code C and let $A_{w,k}$ be the number of codewords of Hamming weight k encoded by information bits of Hamming weight w. Then clearly $\sum_{w=0}^{nR} A_{w,k} = S_k$, for $k = 0, 1, 2, \ldots n$.

By the union bound, the bit error probability of the subcode that includes the all-zero codeword and the S_k codewords of Hamming weight k, given that the all-zero codeword is transmitted, the radial component noise z_1, and also $\underline{z} \in C_n(\theta)$ is upper bounded by

$$\sum_{w=1}^{nR} \left\{\left(\frac{w}{nR}\right) A_{w,k} \cdot \text{Prob}\Big(E_k(z_1)\,,\ \underline{z} \in C_n(\theta)\Big)\right\}$$

$$= \int_{\beta_k(z_1)}^{r_{z_1}} \frac{1}{\sqrt{2\pi}\,\sigma}\, e^{-\frac{z_2^2}{2\sigma^2}} \cdot \sum_{w=1}^{nR} \left(\frac{w}{nR}\right) A_{w,k} \cdot \overline{\gamma}\left(\frac{n-2}{2}\,,\, \frac{r_{z_1}^2 - z_2^2}{2\sigma^2}\right) dz_2 \tag{21}$$

$$= \sum_{w=1}^{nR} \left(\frac{w}{nR}\right) A_{w,k} \cdot \int_{\beta_k(z_1)}^{r_{z_1}} \frac{1}{\sqrt{2\pi}\,\sigma}\, e^{-\frac{z_2^2}{2\sigma^2}} \cdot \overline{\gamma}\left(\frac{n-2}{2}\,,\, \frac{r_{z_1}^2 - z_2^2}{2\sigma^2}\right) dz_2\ .$$

Denote,

$$S'_k \stackrel{\triangle}{=} \sum_{w=1}^{nR} \left(\frac{w}{nR}\right) A_{w,k} \quad k = 1, 2, \ldots\ n\ . \tag{22}$$

Then we get the following conditional upper bound on the bit error probability of the considered subcode:

$$\text{Prob}\left(e_{b,k}(z_1)\,,\ \underline{z} \in C_n(\theta)\right) \leq S'_k \int_{\beta_k(z_1)}^{r_{z_1}} \frac{1}{\sqrt{2\pi}\,\sigma}\, e^{-\frac{z_2^2}{2\sigma^2}}\ \overline{\gamma}\left(\frac{n-2}{2}\,,\, \frac{r_{z_1}^2 - z_2^2}{2\sigma^2}\right)\ dz_2\ , \tag{23}$$

where $e_{b,k}(z_1)$ is an event that represents an error in one of the information bits of the decoded codeword (ML decoding is performed), given the all-zero codeword was transmitted, each one of the other codewords has a Hamming weight k and the radial component of the noise vector is z_1. By the union bound, we get (similarly to the concept of the analysis in [20]):

$$\text{Prob}\left(e_b(z_1)\,,\ \underline{z} \in C_n(\theta)\right) \leq \sum_{k:\,\beta_k(z_1) < r_{z_1}} \text{Prob}\left(e_{b,k}(z_1)\,,\ \underline{z} \in C_n(\theta)\right)\ , \tag{24}$$

where $e_b(z_1)$ is an event that represents an error in one of the information bits of the decoded codeword (that relates now to the overall block code C). Since the code C is linear, the assumption that the all-zero codeword was transmitted is immaterial (in contrast to the event $e_{b,k}(z_1)$ that corresponds to a subcode that includes the all-zero codeword and also the S_k codewords of Hamming weight k in the code C). If the radial component z_1 of the noise is given, then based on properties of the Chi-squared distribution, it is demonstrated in [20] that the conditional probability that the noise vector $\underline{z}$ causes the detected signal to lie outside the half cone $C_n(\theta)$, is of the form:

$$\text{Prob}\left(\underline{z} \notin C_n(\theta) | z_1\right) = 1 - \overline{\gamma}\left(\frac{n-1}{2}\,,\, \frac{r_{z_1}^2}{2\sigma^2}\right)\ , \tag{25}$$

where the corresponding notations are presented in Eq. (17). Applying now the union bound on the bit error probability of the ML decoded overall code C (conditioned on z_1) is upper bounded by

$$P_b(z_1) = \text{Prob}\left(e_b(z_1)\right)$$

$$\leq\ \ \text{Prob}\left(e_b(z_1)\,,\ \underline{z} \in C_n(\theta)\right) + \text{Prob}\left(\underline{z} \notin C_n(\theta)\right)$$

$$\leq \sum_{k:\,\beta_k(z_1)<r_{z_1}} \left\{\text{Prob}\left(e_{b,k}(z_1)\,,\ \underline{z}\in C_n(\theta)\right)\right\} + \text{Prob}\left(\underline{z}\notin C_n(\theta)\right)$$

$$= \sum_{k:\,\frac{\delta_k}{2}<\alpha_k} \left\{\text{Prob}\left(e_{b,k}(z_1)\,,\ \underline{z}\in C_n(\theta)\right)\right\} + \text{Prob}\left(\underline{z}\notin C_n(\theta)\right)$$

$$\leq \sum_{k:\,\frac{\delta_k}{2}<\alpha_k} \left\{ S'_k \int_{\beta_k(z_1)}^{r_{z_1}} \frac{1}{\sqrt{2\pi}\,\sigma}\, e^{-\frac{z_2^2}{2\sigma^2}}\ \overline{\gamma}\left(\frac{n-2}{2}\,,\ \frac{r_{z_1}^2-z_2^2}{2\sigma^2}\right) dz_2 \right\} + 1 - \overline{\gamma}\left(\frac{n-1}{2}\,,\ \frac{r_{z_1}^2}{2\sigma^2}\right)\,.$$

The upper bound on the bit error probability is derived by calculating the statistical expectation of $P_b(z_1)$ with respect to the random variable z_1, where $z_1 \sim N(0,\sigma^2)$ and $\sigma^2 = \frac{N_0}{2}$. This yields the following upper bounds on the bit error probability:

$$P_b = \int_{-\infty}^{+\infty} P_b(z_1)\cdot \frac{1}{\sqrt{2\pi}\,\sigma}\, e^{-\frac{z_1^2}{2\sigma^2}}\, dz_1 \tag{26}$$

$$\leq \int_{-\infty}^{+\infty} \frac{dz_1}{\sqrt{2\pi}\,\sigma}\, e^{-\frac{z_1^2}{2\sigma^2}} \left\{ \begin{array}{c} \displaystyle\sum_{k:\,\frac{\delta_k}{2}<\alpha_k} \left\{ S'_k \int_{\beta_k(z_1)}^{r_{z_1}} \frac{1}{\sqrt{2\pi}\,\sigma}\, e^{-\frac{z_2^2}{2\sigma^2}}\ \overline{\gamma}\left(\frac{n-2}{2}\,,\ \frac{r_{z_1}^2-z_2^2}{2\sigma^2}\right) dz_2 \right\} \\ +1 - \overline{\gamma}\left(\frac{n-1}{2}\,,\ \frac{r_{z_1}^2}{2\sigma^2}\right) \end{array} \right\}\,.$$

This upper bound features the same structure as the upper bound on the block error probability (16), but for the distance spectrum of the code, which is replaced by S'_k. Therefore, the optimization equation of the upper bound on the bit error probability is the same as the optimization equation of the upper bound on the block error probability (19), except for S_k, which is replaced by S'_k. The conclusion of appendix C as to the validity of the bounds applies also here. Since $S'_k = \sum_{w=1}^{nR}\left(\frac{w}{nR}\right) A_{w,k} \leq \sum_{w=0}^{nR} A_{w,k} = S_k$, then for every value of k, we get $S'_k \leq S_k$. This implies that the upper bound on the bit error probability does not exceed the upper bound on the block error probability. The conditions for the existence and uniqueness of a solution to the optimization Eq. (19) of the upper bound on the block error probability and of the optimization equation that correspond to the upper bound on bit error probability are discussed in Appendix B. It is proved there, that Eq. (19) has always a unique solution and also that the optimization equation, corresponding to the upper bound on the bit error proability, has always a unique solution unless the number of codewords is less than 8. Therefore, for the considered turbo codes, as they are interpreted as block codes consisting of many codewords (the number of which increases exponentially with the interleaver length N), the optimization equations of our two upper bounds (on the block and bit error probabilities) have always unique solutions.

IV. Results and Discussion

The outstanding ensemble performance of either parallel and serial concatenated turbo codes with large interleavers is attributed to the distance spectrum thinning observed for the concatenated schemes which shape the distance spectrum of the concatenated turbo codes to resemble more closely the binomial distance spectrum (see Figs. 3,4), [28],[29], where the later is advocated as a measure for good capacity approaching codes [1]. Fig. 5 demonstrates a comparison between the normalized distance spectrum of parallel concatenated turbo codes (two time-varying RSC component codes of rate $\frac{1}{2}$ and memory length $m = 5$ and a uniform interleaver of length $N = 200,400$) and the normalized binomial distribution, which is typical of a fully random binary block code of the same length $n = 3N$ and rate $R = \frac{1}{3}$. The match of the two curves is quite good for Hamming distances larger than twice the Gilbert-Varshamov (GV) bound, i.e. for normalized distances $\left(\frac{d}{n}\right)$ that are larger than $2h^{-1}(1-R) = 0.348$ @ $R = \frac{1}{3}$ bit/symbol, when $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ denotes the binary entropy function and h^{-1} denotes its inverse.

Fig. 6 demonstrates a comparison between the normalized average distance spectrum of serially concatenated codes (with inner and outer codes which are random time-varying RSC codes of rate $\frac{1}{2}$ and memory length $m = 5$ and a uniform interleaver of length $N = 200,400$ bits) and the normalized binomial distribution of a fully random block code of the same length $n = 2N$ and rate $R = \frac{1}{4}$. Similar to the normalized average distance spectrum of the ensemble of random parallel concatenated turbo codes, the match of the two curves is quite good for Hamming distances larger than twice the GV bound, i.e. for normalized distances that are larger than $2h^{-1}(1-R) = 0.429$ @ $R = \frac{1}{4}$ bit/symbol. For example, in Fig. 5a the block length is $n = 3N = 600$ bits and for Hamming distances larger than $0.348 \cdot 600 = 208.8$, indeed, there is a good match between the two curves. In Fig. 6a the block length is $n = 2N = 400$ bits (for the same length of the random interleaver, $N = 200$) and also here, for Hamming distances larger than $0.429 \cdot 400 = 171.6$, there is a good match between the curves.

It is demonstrated (see Figs. 5,6) that there is a good match between the normalized average distance spectrum of either random parallel and serial concatenated codes and the normalized binomial distribution of a fully random block code of the same length and rate, for Hamming distances that are adequately large. Yet, the normalized average distance spectrum of the random parallel or serial concatenated codes becomes significantly larger than the corresponding normalized binomial distribution especially for low Hamming weights (see Figs. 5,6), and this relative increase may explain an inherent degradation in performance as compared to optimal or even fully random codes [1],[26].

By comparing the ensemble performance of parallel and serial concatenated turbo codes for the AWGN channel with ML decoding and coherent detection of the BPSK modulated signals, it was demonstrated by our bounding technique that the longer the random and uniform interleaver is, the more advantageous the improved upper bound becomes as compared to the union bound. This is demonstrated in Figs. 7–13 and 17–19 for parallel and serial concatenated turbo codes.

Fig. 7 demonstrates a comparison between the union bound (in its standard Q-form) and the improved upper bounds derived in section III on the bit and block error probabilities of random serially concatenated turbo codes (see Fig. 2b). The ensemble is generated by a uniform choice over all possible interleavers of length N ($N = 50, 100, 200, 400$) and over the component codes taken from the set of time varying recursive systematic convolutional codes with memory length of $m = 5$. We focus on rate $\frac{1}{2}$ component codes here, so the overall code rate is $R = \frac{1}{4}$.

The value of $\frac{E_b}{N_0}$ that corresponds to the cutoff rate for an AWGN channel with bipolar inputs is related to the code rate R by

$$\frac{E_b}{N_0} = -\frac{\ln(2^{1-R} - 1)}{R} = 1.85 \text{ dB } @ \, R = \frac{1}{4} \text{ bit/symbol} \,, \tag{27}$$

while the value of $\frac{E_b}{N_0}$ that corresponds to the channel capacity is

$$\frac{E_b}{N_0} = -0.79 \, \text{dB } @ \, R = \frac{1}{4} \text{ bit/symbol} \,. \tag{28}$$

As expected for long codes, the standard union bound yields meaningful results only in the rate region below the cutoff rate, excluding the rate region where the performance of turbo codes is most appealing.

Fig. 7a presents a comparison between upper bounds on the block error probability for this considered ensemble with a uniform interleaver of length $N = 100, 200, 400$. No partitioning of the code to subcodes (as done in [17],[37]) is employed here. For an upper bound on the block error probability of 10^{-2}, the gain of $\frac{E_b}{N_0}$ achieved by the tangential sphere bound as compared to the union bound (in Q-form) is 0.10, 0.50, 0.95 dB for $N = 100, 200, 400$ respectively. For example, the tangential sphere upper bound on the block error probability for a random interleaver of length $N = 400$ equals 10^{-2} for $\frac{E_b}{N_0} = 1.10$ dB while the union bound yields 2.05 dB (a gain of 0.95 dB).

Fig. 7b presents a comparison between upper bounds on the bit error probability for the same ensemble of random serially concatenated codes. The improved upper bound is based on the tangential sphere bound and the analysis in section III and it is compared to the union bound. For an upper bound on the bit error probability of 10^{-3}, the gain of $\frac{E_b}{N_0}$ is 0.05, 0.30, 0.70, 1.05 dB for a uniform interleaver of length $N = 50, 100, 200, 400$ respectively.

Figs. 8 and 9 demonstrate a comparison between the union bound (in Q-form) and the improved upper bounds derived in section III on the block and the bit error probabilities of random parallel concatenated turbo codes with $K = 2$ and 3 component codes (see Figs. 2a,c) respectively. Again, the ensemble is generated by a uniform interleaver of length N ($N = 50, 100, 200, 400$) and the component codes taken from the set of time varying recursive systematic convolutional codes with memory length of $m = 5$ and rate $\frac{1}{2}$. The overall code rate of the turbo codes considered in Figs. 8 and 9 is therefore $R = \frac{1}{3}$ and $R = \frac{1}{4}$ respectively. The improved upper bounds on the block and bit error probabilities refer to Figs. 8a, 9a and Figs. 8b, 9b respectively.

For the random codes in Figs. 8 and 9, the values of $\frac{E_b}{N_0}$ that correspond to the channel cutoff rate of a binary-input AWGN channel are 2.03 dB and 1.85 dB respectively and the channel capacity corresponds to $\frac{E_b}{N_0} = -0.50$ dB and -0.79 dB respectively. As expected, the union bound is useful only at rates below the channel cutoff rate.

Fig. 8a depicts a comparison between upper bounds on the block error probability. The improved upper bound is based on the tangential sphere bound and is compared to the union bound (in Q-form). For an upper bound on the block error probability of 0.1, the gain of $\frac{E_b}{N_0}$ is 0.3, 0.4, 0.65 dB for $N = 50, 100, 400$ respectively. For example, if $N = 400$, the improved upper bound on the block error probability is 0.1 for $\frac{E_b}{N_0} = 1.55$ dB (0.3 dB below the $\frac{E_b}{N_0}$ value that corresponds to the cutoff rate), instead of $\frac{E_b}{N_0} = 2.2$ dB (based on the union bound in Q-form).

Fig. 8b presents a comparison between upper bounds on the bit error probability that are based on the tangential sphere bound and the analysis in section III. These improved bounds are compared to the union bound in Q-form. For an upper bound on the bit error probability of 10^{-3}, the gain of $\frac{E_b}{N_0}$ is 0, 0.15, 0.45 and 0.95 dB for an interleaver length of $N = 50, 100, 200, 400$ respectively. For example, if $N = 400$, the improved upper bound on the bit error probability is 10^{-3} for $\frac{E_b}{N_0} = 1.3$ dB, that is 0.55 dB below the $\frac{E_b}{N_0}$ value that corresponds to the cutoff rate for a binary-input AWGN channel (instead of 2.3 dB, based on the union bound in Q-form).

Fig. 9a presents a comparison between upper bounds on the block error probability of random parallel concatenated turbo codes with $K = 3$ component codes (see Fig. 2c). Again, a component code is assumed to be a random time-varying RSC code of memory length $m = 5$ and rate $\frac{1}{2}$. The two uniform interleavers of length N are i.i.d (independent and identically distributed). The increased number of component codes and interleavers of the turbo encoder, improves their performance [14] and this effect is demonstrated also by the improved upper bounds on the block and the bit error probabilities. The upper bounding technique is based on the tangential sphere bound with no partitioning of the turbo code and it is compared to the union bound (in Q-form).

For an upper bound on the block error probability of 10^{-2}, the improvement in $\frac{E_b}{N_0}$ (as compared to the union bounds) is 0.2, 0.6 and 0.9 dB for uniform interleavers of length $N = 50, 100, 200$ respectively. For example, the improved upper bound on the block error probability for the ensemble of codes and interleavers mentioned above (where $N = 200$), ensures ML decoding of blocks (of 200 binary information bits) transmitted through an AWGN channel with associated probability of at least 99%, provided the SNR per bit $\left(\frac{E_b}{N_0}\right)$ equals 1.2 dB (0.65 dB below the $\frac{E_b}{N_0}$ value that corresponds to the channel cutoff rate) instead of 2.1 dB (based on the union bound in Q-form), as is demonstrated by Fig. 9a.

Fig. 9b depicts a comparison between upper bounds on the bit error probability of the same ensemble of random multiple-turbo codes, where the improved upper bounds are based on the tangential sphere bound and our analysis. For an upper bound on the bit error probability of 10^{-3}, the gain of $\frac{E_b}{N_0}$ is 0.3, 0.65, 1.1 and 1.4 dB for random and uniform interleavers of length $N = 50, 100, 200, 400$ respectively. For example, the improved upper bound on the bit error probability is 10^{-3} for the case of $N = 400$ at $\frac{E_b}{N_0} = 0.65$ dB instead of 2.05 dB (based on the union bound in Q-form).

Parallel to results presented in [31],[35], it is also verified here that increasing the memory length of the random time-varying RSC component codes m above $\log_2 N$ affects negligibly the ensemble performance of either parallel and serial concatenated codes, while increasing the decoding complexity of the codes (see Figs. 10–12). This result is proved analytically in [31], by showing first that the average activity time of a time-varying recursive shift register (i.e. the average number of cycles that the shift register is not in the zero state) with a memory length of m is $2^{m+1} - 2$. Choosing $m = \lfloor \log_2 N \rfloor$, yields an average activity time that is approximately twice the interleaver length N. Therefore with high probability the shift register does not return to the zero state after being activated by the first '1' at its input. Thus, based the distance spectra of these ensembles of random turbo codes it is demonstrated that increasing the memory length m of the component codes above $\lfloor \log_2 N \rfloor$ is not effective, since it improves negligibly the ensemble performance of the concatenated turbo codes, while increasing considerably the decoding complexity of the codes.

Fig. 13 depicts a comparison between the improved upper bounds on the bit error probability of the ensembles of random serial and parallel concatenated turbo codes. The component codes of the two random concatenated codes are time-varying RSC codes of memory length $m = 4, 5, 7$ and rate $\frac{1}{2}$ (the component codes have the same memory length m). The serially concatenated codes are generated by a uniform interleaver of length $N_1 = 200$ time-varying RSC component codes of length m. On the other hand, the parallel concatenated turbo codes are generated by two uniform interleavers, which are independently chosen of length $N_2 = 100$ and $K = 3$ component codes (see

Fig. 2c). This comparison between serial and parallel concatenated turbo codes is done under equal rate and interleaving delay. This comparison yields that the improved upper bound on the bit error probability of the serial concatenated codes are advantageous for low and moderate values of $\frac{E_b}{N_0}$ (at rates below the channel cutoff rate). This conclusion is consistent with that reported in [31] on the grounds of the union bound (that usually diverges for rates below the cutoff rate in contrast to our improved upper bound, and therefore this conclusion based on the improved upper bounds is more reliable).

Our bounding technique is compared to a recent alternative bounding technique proposed by Duman and Salehi [17], where a modified version of Gallager bound replaces the standard union bound (see Figs. 16–17). The technique of [17] is used for specific component codes and a uniform interleaving. Though the Gallager bound as in [18] where applied to random codes achieves the channel capacity, there are a number of places in the derivation of the upper bound in [17], where it is loosened as compared to the actual value of the error probability. The weakening of the Gallager bound is more dominant in the derivation of the upper bound on the bit error probability than of the upper bound on the block error probability [17], since in the first case the code is partitioned to subcodes $c_{i,d}$ which include all the code words with the same information weight i and total Hamming weight d including also the all zero codeword. On the other hand, the upper bounds on the bit error probability presented here [32], are applied on the whole code and therefore based on Appendix C that an upper bound is advantageous over a similar upper bound that apply an arbitrary partitioning of the code to subcodes. The main difference between the two bounding techniques is a result of the fact that for the tangential sphere bound all the signals must only have the same energy (geometrically, all the codewords lie on the same sphere). Since all the codewords are of the same length and also the energy per bit is constant, all the signals possess the same energy, however the technique in [17], even for the derivation of the block error probability implies that the subcodes c_d, must have a constant Hamming weight d, for all their non zero codewords. This additional constraint results in a partition with an increased number of subcodes as compared with our bounds here, which when combined with the union bound applied on the subcodes yields a looser bound. In addition, the tangential sphere bound applied here once for the overall code, was demonstrated to be a tighter upper bound in most cases for block codes as compared to a variety of other upper bounds [6]–[20], giving thus another advantage to the bounding technique proposed here. The tightness of the upper bound for ML decoding can be assessed by comparing the simulation results of the soft-output iterative decoding algorithm with the upper bound here. It is considered to be tight as long as it is close enough to the simulation results based on the iterative decoding, pre-assuming that the iterative decoding technique performs close to ML decoding for moderate values of E_b/N_0. The upper bound on the block error probability for a parallel concatenated code with two fixed RSC component codes $G_1(D) = G_2(D) = \left[1, \frac{1+D^2}{1+D+D^2}\right]$

and a uniform interleaver of length $N = 500, 1000$ (see Fig. 14) seems to be tight for $\frac{E_b}{N_0} \geq 1$ dB (see Fig. 16,17). For rate $\frac{1}{3}$ transmission, the channel cutoff rate corresponds to $\frac{E_b}{N_0} = 2.03$ dB and the channel capacity with binary inputs corresponds to $\frac{E_b}{N_0} = -0.50$ dB. Therefore, the new upper bound on the block error probability seems to be reasonably tight for $\frac{E_b}{N_0}$ values 1.0 dB below the $\frac{E_b}{N_0}$ value that corresponds to the cutoff rate but 1.5 dB above the value that corresponds to the channel capacity. The upper bound on the block error probability by Duman and Salehi [17] is useful only for $\frac{E_b}{N_0} \geq 1.5$ dB, corresponding to $\frac{E_b}{N_0}$ values of 0.5 dB below the $\frac{E_b}{N_0}$ which represents the cutoff rate and diverges 0.8–1.0 dB below that value. This comparison demonstrates the extension of the region of $\frac{E_b}{N_0}$ for which our bounds are useful by about 0.5 dB over those of [17] in the examined case. Fig. 16b refers to an interleaver length of $N = 1000$, and the tangential sphere bound is a reasonably tight upper bound in this case for $\frac{E_b}{N_0} \geq 0.9$ dB.

For the turbo code in Fig. 14, the upper bounds on the bit error probability here are tight for $\frac{E_b}{N_0} \geq 1.3$ or 1.2 dB for $N = 500, 1000$ respectively (see Figs. 17a,b). The Duman and Salehi upper bound on the bit error probability in [17] is tight only for $\frac{E_b}{N_0} \geq 1.8$ dB (see Fig. 17a) where both upper bounds refer to the turbo code mentioned above of rate $R = \frac{1}{3}$ and a uniform interleaver of length $N = 500$ (see Fig. 14). Thus, the range of $\frac{E_b}{N_0}$ for which the bounds on the bit error probability are useful is extended in this case by 0.5 dB by the new upper bound derived here. As is observed from the comparisons of the upper bounds on the bit and the block error probabilities in [17],[32] for the considered turbo code, the upper bound on the block error probability (either in [17] and [32]) is useful in a wider range of $\frac{E_b}{N_0}$ values than the corresponding upper bound on the bit error probability. In certain cases, it is demonstrated in Figs. 8a and 10 that the upper bounds on the block and on the bit error probabilities of the maximum likelihood decoding fall below simulated performance of iterative decoding. This demonstrates the mild sub-optimality of the iterative decoding for moderate and low $\frac{E_b}{N_0}$ regions.

For the multiple-turbo code in Fig. 18, a comparison between upper bounds on the bit error probability is depicted in Fig. 19a (a random turbo code with fixed RSC component codes and a uniform interleaver of length $N = 192$) and simulation results based on the soft-output iterative decoding algorithm [14]. The fixed component codes are the same RSC codes and their generators are $G_1(D) = G_2(D) = G_3(D) = \left[1, \frac{1+D^2}{1+D+D^2}\right]$. An interleaver of length 192 bits corresponds to 20 ms frames at a bit rate of 9.6 Kbps, modelling typical speech coding systems and therefore of interest (see [21],[11, 29, 37] and references therein). The degradation in the performance of the iterative decoding as compared to maximum likelihood decoding seems to increase with the increased number of component codes as demonstrated by comparing the bounds in Figs. 17a and

19a (with $K = 2, 3$ component codes respectively). For example, the improved upper bound on the bit error probability based on our analysis is 10^{-3} or 10^{-4} for $\frac{E_b}{N_0} = 0.7$ or 1.0 dB respectively (instead of 1.3 and 1.6 dB respectively based on the computer simulations of the soft-output iterative LOG-MAP decoding algorithm with 20 iterations in [14]) (see Fig. 18,19a). In addition, for an upper bound on the bit error probability of 10^{-3} or 10^{-4}, the gain of $\frac{E_b}{N_0}$ achieved by the improved upper bound (as compared to the union bound) is 1.15 or 0.95 dB respectively. The case of $N = 800$ for the multiple turbo code presented in Fig. 18 is considered and impressive upper bound on the block and bit error probabilities are demonstrated in Fig. 19b (a bit error probability of 10^{-4} is achieved for $\frac{E_b}{N_0} = 0.3$ dB, while the channel capacity of a binary-input AWGN channel corresponds to $\frac{E_b}{N_0} = -0.8$ dB.

In Fig. 20, a rate-$\left(\frac{1}{3}\right)$ turbo code is presented with two RSC component codes whose generators in octal form are 21 and 37 forward and backward respectively. The interleaver is uniform and its length is $N = 1000$. A termination of $m = 4$ bits is performed after each frame for returning it to the all-zero state. A comparison between upper bounds on the bit error probability of ML decoding and simulation results of the LOG-MAP iterative decoding algorithm demonstrates a good match between the improved upper bound based on the tangential sphere bound and the simulation results of the iterative decoding (see Fig. 21). Therefore, as is demonstrated in several examples here, the improved bounding technique for ML decoding which is based on the tangential sphere bound also approximates the performance of iteratively decoded turbo codes with an efficient iterative decoding algorithm.

V. Summary and Conclusions

Unlike random binary block codes that have a binomial distance spectrum and are known to achieve capacity, based on the exponential deviation of the distance spectrum of turbo codes from the binomial distribution at low Hamming weights, it is not obvious that there exists any decoding method (including the optimal ML decoding), which achieves the theoretical Shannon capacity for turbo codes. We derive here upper bounds on the ensemble performance of parallel and serial concatenated turbo codes for the AWGN channel and ML decoding (given in terms of bit and block error probabilities). The ensemble is generated here by a uniform choice of the interleaver of length N and of component codes taken from the set of time varying RSC codes of memory length m. In addition, we investigate also the ensemble performance, where the ensemble of codes is generated by a uniform interleaver of length N and the component codes are fixed RSC codes.

We devise a general upper bounding technique on the bit and block error probabilities, based

on the tangential sphere upper bound [20],[30] without any partitioning of the code to subcodes. The bounding technique is applied on parallel and serial concatenated turbo codes with rate $\frac{1}{2}$ component codes and is also examined for parallel concatenated turbo codes with three component codes of rate $\frac{1}{2}$ (yielding an overall code of rate $\frac{1}{4}$, i.e., the same overall rate as of serial concatenated codes with two rate $\frac{1}{2}$ component codes).

In parallel to results reported in [31],[35], the performance behavior of randomly concatenated and interleaved codes is reduced to a three parameter family: the interleaver length N, the memory length m of the component codes (all the component codes are assumed to have the same memory length) and the number K of component codes employed in a parallel concatenation (for serial concatenation two ($K = 2$) component codes are assumed: the inner and outer codes).

It is also verified here that increasing the memory length of the component codes m above $\log_2 N$ affects negligibly the ensemble performance of either parallel or serial concatenated codes, while evidently increasing the decoding complexity of the codes.

The technique for calculating the IOWEF of fixed convolutional codes [27], is used to apply our improved bounding technique on fixed component codes. Comparing the results with a recent alternative bounding technique [17] by Duman and Salehi, which incorporates a modified Gallager bound, demonstrates a significant advantage of our bounding technique. For example, with an interleaver length of $N = 500$, the upper bound on the block error probability is a reasonably tight bound for $\frac{E_b}{N_0}$ values, approximately 1 dB below the value of $\frac{E_b}{N_0}$ corresponding to the cutoff rate, extending thus the region of $\frac{E_b}{N_0}$ for which the upper bounds derived in [17] are useful by about 0.6 dB.

In certain cases it was demonstrated that the upper bounds on the block and the bit error probabilities of the ML decoding fall below simulated performance of soft-output iterative decoding algorithms. This demonstrates the mild sub-optimality of the iterative decoding for moderate and low values of $\frac{E_b}{N_0}$. Moreover, the degradation of the iterative decoding as compared to ML decoding seems to increase with the increased number of the component codes.

A comparison between serial and parallel concatenated turbo codes is done under equal rate and interleaving delay. This comparison shows that the improved upper bounds on the bit error probability of the serially concatenated codes are advantageous for low and moderate values of $\frac{E_b}{N_0}$ (i.e. at rates below the cutoff rate). This conclusion is consistent with that reported in [31] on the grounds of the union bound (that usually diverges for long codes at rates above the cutoff rate), but the conclusion here is more reliable as the improved upper bounds are useful for an extended range of $\frac{E_b}{N_0}$.

The bounding technique derived here was used to substantiate theoretically the surprisingly

good performance demonstrated in [28] for serially interleaved concatenated codes, where the outer code is a standard non-recursive convolutional code, the inner code is a recursive convolutional code of rate 1 (a differential encoder in particular) and the ensemble is generated by all random and uniform interleavers of length $N = 1000$.

Based on our bounds, we conjecture that the performance of turbo codes with short RSC component codes and relatively large interleavers is dominated by the lower part of the distance spectrum, which exhibits marked deviation when compared to the binomial distribution of random codes. The higher distances, say above twice the Gilbert-Varshamov distance resemble well the binomial distribution. It should be emphasized though that it is not the minimum distance which governs performance [1], but rather a whole region of low-weight distances. That is in contrast to ensembles of random codes, where typical weights (associated with typical sequences [10]) dominate.

As is demonstrated in several examples here, the improved bounding technique for ML decoding which is based on the tangential sphere bound, also approximates the performance of iteratively decoded turbo codes with the LOG-MAP based iterative decoding algorithm.

Appendix A: A discussion on the validity of the tangential sphere upper bound

In [20], the tangential sphere bound is derived where only the upper half cone is taken into account (see Fig. 2 in [20]), not accounting for the impact of the lower half cone. The purpose of this appendix is to justify the use here of the relevant version of the tangential sphere bound, and to demonstrate by some examples that the second half cone has an absolutely marginal impact on the upper bound.

As can be realized from Eq. (17), if $z_1 > \sqrt{nE_s}$, then $r_{z_1} < 0$ and $\beta_k(z_1) < 0$. Therefore, the tangential sphere bound (16) should read,

$$P_e \leq \int_{-\infty}^{+\infty} \frac{dz_1}{\sqrt{2\pi}\,\sigma}\, e^{-\frac{z_1^2}{2\sigma^2}} \left[1 - \overline{\gamma}\left(\frac{n-1}{2}\,,\,\frac{r_{z_1}^2}{2\sigma^2}\right) + A(z_1)\right]\,, \tag{A.1}$$

where

$$A(z_1) = \begin{cases} \displaystyle\sum_{k:\,\frac{\delta_k}{2}<\alpha_k} S_k \left[Q\left(\frac{\beta_k(z_1)}{\sigma}\right) - Q\left(\frac{r_{z_1}}{\sigma}\right)\right] \cdot \overline{\gamma}\left(\frac{n-2}{2}\,,\,\frac{r_{z_1}^2 - \beta_k^2(z_1)}{2\sigma^2}\right) & \text{if} \quad z_1 \leq \sqrt{nE_s} \\ \displaystyle\sum_{k=1}^{n} S_k \left[Q\left(\frac{\beta_k(z_1)}{\sigma}\right) - Q\left(\frac{r_{z_1}}{\sigma}\right)\right] \cdot \overline{\gamma}\left(\frac{n-2}{2}\,,\,\frac{r_{z_1}^2 - \beta_k^2(z_1)}{2\sigma^2}\right) & \text{if} \quad z_1 > \sqrt{nE_s}\,. \end{cases} \tag{A.2}$$

The reason is that if $z_1 \leq \sqrt{nE_s}$, the inequality $\beta_k(z_1) < r_{z_1}$ holds only for values of k, such that $\frac{\delta_k}{2} < \alpha_k$. On the other hand, if $z_1 > \sqrt{nE_s}$, the range of integration of the component noise z_2 is $\beta_k(z_1) \leq z_2 \leq -r_{z_1}$ (see [20]). All values of k satisfy in this case the inequality: $\beta_k(z_1) < 0 < -r_{z_1}$ and therefore the summation is over $k = 1, 2, \ldots, n$ in this case.

From the derivation of the tangential sphere bound, the optimization of the radius r of the cone (the upper half cone for the case that $z_1 \geq \sqrt{nE_s}$ or the lower half cone for the case that $z_1 \leq \sqrt{nE_s}$), results in an upper bound that does not exceed unity. Therefore, for any value of z_1, we get after optimization:

$$A(z_1) + 1 - \overline{\gamma}\left(\frac{n-1}{2}\,,\,\frac{r_{z_1}^2}{2\sigma^2}\right) \leq 1\,. \tag{A.3}$$

Since $z_1 \sim N(0, \sigma^2)$ where $\sigma^2 = \frac{N_0}{2}$, then the probability that z_1 exceeds $\sqrt{nE_s}$ is $Q\left(\frac{\sqrt{nE_s}}{\sigma}\right) = Q\left(\sqrt{2nR \cdot \frac{E_b}{N_0}}\right)$, where n is the length of the block code and R is its rate.

For the case of a parallel concatenated turbo code, the relation $N = nR$ holds, where N is the

interleaver length. Therefore, if for example: $\frac{E_b}{N_0} = 0$ dB and $N = 500$, then we find that:

$$\text{Prob}\,(z_1 \geq \sqrt{nE_s}) = Q\left(\sqrt{2N\,\frac{E_b}{N_0}}\right) = Q(\sqrt{1000}) \approx 8 \cdot 10^{-220} \ll 1\ . \tag{A.4}$$

This probability is by all means negligible, so the lower half cone (that corresponds to the case that $z_1 > \sqrt{nE_s}$) has an absolutely marginal influence on the block error probability.

Even for short and moderate block codes, the probability that corresponds to the lower half cone is negligible. As an example, examine (24,12) Golay code, whose block length is $n = 24$ and its rate is $R = \frac{1}{2}$. For $\frac{E_b}{N_0}$ =0.19 dB (that corresponds to the capacity of a binary input AWGN channel for a code rate of $\frac{1}{2}\,\frac{\text{bit}}{\text{symbol}}$), it follows that

$$\text{Prob}\,(z_1 \geq \sqrt{nE_s}) = Q\left(\sqrt{2nR \cdot \frac{E_b}{N_0}}\right) = 2.8 \cdot 10^{-7}\ . \tag{A.5}$$

The tangential sphere (upper) bound on the block error probability for the Golay code at $\frac{E_b}{N_0} =$ 0.19 dB is 0.285. Therefore, even in this case (of a short block code), the probability Prob $(z_1 \geq \sqrt{nE_s})$ is absolutely negligible as compared to the upper bound on the block error probability. We conclude therefore that for all practical purposes in our work, the term connected with the lower half cone of the tangential sphere bound is negligible, when compared to the upper bound on the block error probability. This observation justifies the use of the tangential sphere bound, as is presented in Eq. (16).

Appendix B: A proof of the existence and uniqueness of a solution to the optimization equation of the tangential sphere bound and an algorithm to solve this equation

It will be proved here that there always exists a unique solution to the optimization Eq. (19) of the tangential sphere bound. This statement holds for every distance spectrum of a linear block code C and Euclidean distances between any pair of the signals. This result is also independent of the block length n, the rate R and the signal energy E_s.

To this end, define a function:

$$g(r) = \sum_{k:\,\frac{\delta_k}{2} < \alpha_k} S_k \int_0^{\theta_k} \sin^{n-3}\,\phi\; d\phi\ , \tag{B.1}$$

where θ_k, δ_k and α_k are determined by Eqs. (17) and (19) and $\{S_k\}_{k=0}^{n}$ is the distance spectrum of the code C. If the value of r is increased ($r > 0$), then by Eq. (17) the angles θ_k ($k = 1, 2, \ldots, n$)

also increase ($0 \leq \theta_k \leq \frac{\pi}{2}$), and therefore for every value of k, such that $\frac{\delta_k}{2} < \alpha_k$, the value of the integral $\int_0^{\theta_k} \sin^{n-3} \phi \, d\phi$ is increased. Moreover, α_k grows linearly with r (for all values of k), and therefore the number of values of k that satisfy the inequality $\frac{\delta_k}{2} < \alpha_k$ is increased by 1 while r is increased as to satisfy the equation, $\frac{\delta_k}{2} = \alpha_k$ (for some value of $0 \leq k \leq n$). Therefore, $g(r)$ is an increasing function of $r\,(r > 0)$.

If $r \to 0^+$, for no k $(k = 0, 1, 2, \ldots, n)$, $\frac{\delta_k}{2} < \alpha_k$ (since $\alpha_k = 0$ and δ_k is non-negative), which yields that $\lim_{r \to 0^+} g(r) = 0$. For $r \to +\infty$, then for every value $1 \leq k \leq n$, the inequality $\frac{\delta_k}{2} < \alpha_k$ holds (since $\alpha_k \to +\infty$ but δ_k is finite and is independent of r). From the relation $\theta_k = \cos^{-1}\left(\frac{\delta_k}{2r} \frac{1}{\sqrt{1 - \frac{\delta_k^2}{4nE_s}}}\right)$ in Eq. (17), we get $\lim_{r \to \infty} \theta_k = \frac{\pi}{2}\,(0 \leq k \leq n)$. If $r \to \infty$ the summation in the function $g(r)$ is over all values of k between 0 and n, yielding

$$\lim_{r \to \infty} g(r) = \sum_{k=0}^{n} S_k \int_0^{\frac{\pi}{2}} \sin^{n-3} \phi \, d\phi = 2^{nR} \int_0^{\frac{\pi}{2}} \sin^{n-3} \phi \, d\phi \,. \tag{B.2}$$

By Eq. 3.621.1 in [19],

$$\int_0^{\frac{\pi}{2}} \sin^{\mu-1} x \, dx = 2^{\mu-2} B\left(\frac{\mu}{2}, \frac{\mu}{2}\right) = \frac{2^{\mu-2} \left[\Gamma\left(\frac{\mu}{2}\right)\right]^2}{\Gamma(\mu)} = \frac{\sqrt{\pi}}{2} \frac{\Gamma\left(\frac{\mu}{2}\right)}{\Gamma\left(\frac{\mu+1}{2}\right)} \quad \text{for } \mu \geq 1 \,, \tag{B.3}$$

where the last equality in (B.2) results in $\Gamma(2x) = \frac{2^{2x-1}}{\sqrt{\pi}} \cdot \Gamma(x)\,\Gamma\left(x + \frac{1}{2}\right)$ for $x > 0$.
Therefore, if $n = 3, 4, 5 \cdots$,

$$\lim_{r \to \infty} g(r) = 2^{nR-1} \cdot \left(\frac{\sqrt{\pi}\,\Gamma\left(\frac{n-2}{2}\right)}{\Gamma\left(\frac{n-1}{2}\right)}\right) \,. \tag{B.4}$$

Since for a block code C of length n, $R \geq \frac{1}{n}$, then

$$\lim_{r \to \infty} g(r) \geq \frac{\sqrt{\pi}\,\Gamma\left(\frac{n-2}{2}\right)}{\Gamma\left(\frac{n-1}{2}\right)} \,.$$

Since $g(r)$ is an increasing function of $r \in (0, \infty)$ and also

$$\lim_{r \to 0^+} g(r) = 0 \,, \; \lim_{r \to \infty} g(r) \geq \frac{\sqrt{\pi}\,\Gamma\left(\frac{n-2}{2}\right)}{\Gamma\left(\frac{n-1}{2}\right)} \,, \tag{B.5}$$

then, to complete the proof that a solution of Eq. (19) exists and is unique, it is sufficient to show that the function $g(r)$ is continuous on the interval $r \in (0, \infty)$. This implies that $g(r)$ achieves any value between $\lim_{r \to 0^+} g(r)$ and $\lim_{r \to \infty} g(r)$ and hence Eq. (19) should have a unique solution.

The function $g(r)$ is continuous on the interval $r \in (0, \infty)$, because each of the involved integrals $\int_0^{\theta_k} \sin^{n-3} \phi \, d\phi$ is a continuous function of r (as θ_k is a continuous function of r, if $\frac{\delta_k}{2} < \alpha_k$). Moreover, when r assumes a value, such that for some k : $\frac{\delta_k}{2} = \alpha_k$ $(1 \leq k \leq n)$, the term $S_k \int_0^{\theta_k} \sin^{n-3} \phi \, d\phi$ that is added to the summation in the function $g(r)$ is zero:

$$\frac{\delta_k}{2} = \alpha_k \implies \theta_k = \cos^{-1}\left(\frac{\delta_k}{2\alpha_k}\right) = 0 \Rightarrow S_k \int_0^{\theta_k} \sin^{n-3} \phi \, d\phi = 0 \, . \tag{B.6}$$

The additional term in the summation cannot cause any discontinuity in the function $g(r)$. Thus the function $g(r)$ is continuous on the interval $(0, \infty)$, which implies, as said before, the uniqueness of the solution of Eq. (19).

The continuous function $g(r)$ is increasing in the interval $r \in (0, \infty)$, facilitating to solve Eq. (19) by the following algorithm:

Step 1: Calculate

$$r_k = \frac{\delta_k}{2} \frac{1}{\sqrt{1 - \frac{\delta_k^2}{4nE_s}}} \text{ for } \quad k = 1, 2, \ldots, n \, .$$

* If we assume that $\delta_1 < \delta_2 < \cdots < \delta_n$ (meaning that, the more symbols the two codewords differ, the larger the distance between the corresponding signals is), then $r_1 < r_2 < \cdots < r_n$.

Step 2: Calculate

$$g(r_j) = \sum_{k=0}^{j-1} S_k \int_0^{\theta_k} \sin^{n-3} \phi \, d\phi \quad \text{for} \quad j = 1, 2, \ldots, n \, .$$

Step 3: If $\dfrac{\sqrt{\pi}\, \Gamma\left(\frac{n-2}{2}\right)}{\Gamma\left(\frac{n-1}{2}\right)} < g(r_1)$, then the solution of (19) falls into the interval $(0, r_1)$. If for some $1 \leq j \leq n-1$: $g(r_j) < \dfrac{\sqrt{\pi}\, \Gamma\left(\frac{n-2}{2}\right)}{\Gamma\left(\frac{n-1}{2}\right)} < g(r_{j+1})$, then the solution of Eq. (19) is in the interval (r_j, r_{j+1}). Otherwise, the solution of Eq. (19) is in the interval (r_n, ∞).

Step 4: Use the bisection method in the interval from step 3, to find a sufficiently accurate solution of Eq. (19).

For the upper bound on the bit error probability, the relevant optimization equation is the same as Eq. (19), replacing the distance spectrum (S_k) by (S'_k). It follows that

$$\lim_{r\to\infty} g(r) = \sum_{k=1}^{n} S'_k \cdot \frac{\sqrt{\pi}}{2} \frac{\Gamma\left(\frac{n-2}{2}\right)}{\Gamma\left(\frac{n-1}{2}\right)} \quad \text{and} \quad \lim_{r\to 0^+} g(r) = 0\,. \tag{B.7}$$

By our discussion, referred to the block error probability, we demand the following inequality:

$$\lim_{r\to\infty} g(r) \geq \frac{\sqrt{\pi}}{2} \frac{\Gamma\left(\frac{n-2}{2}\right)}{\Gamma\left(\frac{n-1}{2}\right)}\,, \tag{B.8}$$

which is satisfied, if and only if, $\sum_{k=1}^{n} S'_k \geq 2$. Since $S'_k = \sum_{w=1}^{nR} \left(\frac{w}{nR}\right) A_{w,k}$ $(k = 1, 2, \ldots, n)$, it follows

$$\begin{aligned}
\sum_{k=1}^{n} S'_k &= \sum_{k=1}^{n} \sum_{w=1}^{nR} \left(\frac{w}{nR}\right) A_{w,k} \\
&\geq \sum_{k=1}^{n} \left(\frac{w}{nR}\right) \sum_{w=1}^{nR} A_{w,k} \\
&= \frac{1}{nR} \sum_{k=1}^{n} S_k \\
&= \frac{2^{nR}-1}{nR}\,.
\end{aligned}$$

(Since the binary block code is linear, it includes the all-zero codeword, so $\sum_{k=1}^{n} S_k = 2^{nR} - 1$).

Therefore, it is sufficient for a unique solution of the optimization equation in the bit-error probability case that the $\frac{2^{nR}-1}{nR} \geq 2$ holds (otherwise, a solution may not exist). Noticing that $f(x) = \frac{2^x-1}{x}$ is an increasing function in the interval $(0, \infty)$, it follows that the inequality above is equivalent to $R \geq \frac{2.660}{n}$. Since $R = \frac{k}{n}$ is the code rate, then the existence and uniqueness of a solution to the optimization equation is guaranteed for $k \geq 3$, which holds in all interesting cases for adequately long codes.

Appendix C: Some observations on the application of the tangential sphere bound

We prove that it is advantageous to apply the tangential sphere bound (as an upper bound on the block error probability or the bit error probability) on the whole code. Any partition of the code to subcodes for which the tangential sphere bound is used individually and finally all these upper bounds are added (based on the union bound concept) yields a looser result.

To this end, assume without loss of generality that the binary linear block code C is partitioned to arbitrary two subcodes, C_1 and C_2, such that $C = C_1 \bigcup C_2$ and $C_1 \bigcap C_2$ is the all-zero codeword. Then we compare the upper bound on the block (bit) error probability of the code C with the sum of the upper bounds on the block (bit) error probabilities of the subcodes C_1 and C_2. Let $\{S_k^{(1)}\}_{k=0}^n$ and $\{S_k^{(2)}\}_{k=0}^n$ be the distance spectrum of each of the subcodes C_1 and C_2 respectively and let $\{S_k\}_{k=0}^n$ be the distance spectrum of the code C. In case the upper bound on the bit error probability is considered (instead of the upper bound on the block error probability), we replace S_k by S_k'. Let $P_e^u(C_1)$, $P_e^u(C_2)$ and $P_e^u(C)$ be the conditional upper bounds of the subcodes C_1, C_2 and C respectively, given the all-zero codeword is transmitted. Based on our notations, we get by the tangential sphere bound applied separately on each of the subcodes C_1 and C_2:

$$P_e^u(C_1) = \sum_{k:\, \frac{\delta_k}{2} < \alpha_{k,1}} \left\{ S_k^{(1)} \cdot E_{z_1} \left[\text{Prob}\left(E_k(z_1),\, \underline{z} \in C_n(\theta_1) \right) \right] \right\} + \text{Prob}\left(\underline{z} \notin C_n(\theta_1) \right)$$

$$P_e^u(C_2) = \sum_{k:\, \frac{\delta_k}{2} < \alpha_{k,2}} \left\{ S_k^{(2)} \cdot E_{z_1} \left[\text{Prob}\left(E_k(z_1),\, \underline{z} \in C_n(\theta_2) \right) \right] \right\} + \text{Prob}\left(\underline{z} \notin C_n(\theta_2) \right)$$

where $C_n(\theta)$ is an n-dimensional cone of half angle θ and the angles θ_1, θ_2 are derived for each one of the subcodes C_1 and C_2 respectively by the optimization Eq. (19) of the tangential sphere bound. The vector $\underline{z}$ and the error event $E_k(z_1)$ were defined in B.3 of section II. $E_{z_1}(\cdot)$ denotes the statistical expectation over the Gaussian random variable z_1 and also α_{k_1}, α_{k_2} are determined via Eq. (17) following the values of the radius r_1 and r_2 respectively. Therefore, the sum of the upper bounds that corresponds to the subcodes C_1 and C_2 is

$$\begin{aligned} &P_e^u(C_1) + P_e^u(C_2) \\ &= \sum_{k:\, \frac{\delta_k}{2} < \alpha_{k,1}} \left\{ S_k^{(1)} \cdot E_{z_1} \left[\text{Prob}\left(e_k(z_1),\, \underline{z} \in C_n(\theta_1) \right) \right] \right\} + \text{Prob}\left(\underline{z} \notin C_n(\theta_1) \right) \\ &+ \sum_{k:\, \frac{\delta_k}{2} < \alpha_{k,2}} \left\{ S_k^{(2)} \cdot E_{z_1} \left[\text{Prob}\left(e_k(z_1),\, \underline{z} \in C_n(\theta_2) \right) \right] \right\} + \text{Prob}\left(\underline{z} \notin C_n(\theta_2) \right). \end{aligned}$$

Using the relation $r = \sqrt{nE_s}\,\tan\theta$ (see Fig. 1 in [20]), we see that if the value of θ is decreased, then $\alpha_k = r\sqrt{1-\frac{\delta_k^2}{4nE_s}}$ is also decreased for each value of $k\,(k = 1, 2, \ldots, n)$. Since δ_k (the Euclidean distance between two signals that correspond to a pair of codewords of Hamming distance k) is independent of the angle θ, then the set of integers k, such that $\frac{\delta_k}{2} < \alpha_k$ is not increased. Let θ_3 be the minimal value between θ_1 and θ_2, i.e. $\theta_3 = \min(\theta_1, \theta_2)$. Therefore, by Eq. (17) where $\alpha_{k,j} = \sqrt{nE_s}\,\tan\theta_j\,\sqrt{1-\frac{\delta_k^2}{4nE_s}}$ $(k = 1, 2, \ldots, n$ and $j = 1, 2, 3)$, it follows that $\alpha_{k,3} \le \min(\alpha_{k,1}, \alpha_{k,2})$ for $k = 1, 2, \ldots, n$. The following inequality (where $\alpha_{k,3}$ replaces $\alpha_{k,1}$ and $\alpha_{k,2}$) then results,

$$
\begin{aligned}
&P_e^u(c_1) + P_e^u(c_2) \\
&\quad \ge \sum_{k:\,\frac{\delta_k}{2}<\alpha_{k,3}} \left\{ S_k^{(1)} \cdot E_{z_1}\left[\text{Prob}\left(e_k(z_1),\, \underline{z} \in C_n(\theta_3)\right)\right]\right\} + \text{Prob}\left(\underline{z} \notin C_n(\theta_1)\right) \\
&\quad + \sum_{k:\,\frac{\delta_k}{2}<\alpha_{k,3}} \left\{ S_k^{(2)} \cdot E_{z_1}\left[\text{Prob}\left(e_k(z_1),\, \underline{z} \in C_n(\theta_3)\right)\right]\right\} + \text{Prob}\left(\underline{z} \notin C_n(\theta_2)\right).
\end{aligned}
$$

$\alpha_{k,3}$ is the value of α_k that corresponds to the half angle θ_3 of the n-dimensional cone $C_n(\theta_3)$. Since $C = C_1 \bigcup C_2$ and $C_1 \bigcap C_2$ includes only the all-zero codeword, then evidently,

$$
\begin{aligned}
S_k &= S_k^{(1)} + S_k^{(2)} \quad k = 1, 2, \ldots, n \\
S'_k &= S'^{(1)}_k + S'^{(2)}_k \quad k = 1, 2, \ldots, n\,.
\end{aligned}
$$

By the union bound, since $C_n(\theta_3) = C_n(\theta_1) \bigcap C_n(\theta_2)$ (as θ_3 was determined as the minimal angle between θ_1 and θ_2) it follows,

$$
\text{Prob}\left(\underline{z} \notin C_n(\theta_1)\right) + \text{Prob}\left(\underline{z} \notin C_n(\theta_2)\right) \ge \text{Prob}\left(\underline{z} \notin C_n(\theta_3)\right).
$$

Hence the final inequality

$$
\begin{aligned}
&P_e^u(C_1) + P_e^u(C_2) \\
&\quad \ge \sum_{k:\,\frac{\delta_k}{2}<\alpha_{k,3}} \left\{ S_k \cdot E_{z_1}\left[\text{Prob}\left(e_k(z_1),\, \underline{z} \in C_n(\theta_3)\right)\right]\right\} + \text{Prob}\left(\underline{z} \notin C_n(\theta_3)\right) \\
&\quad \ge \min_{\theta}\left\{ \sum_{k:\,\frac{\delta_k}{2}<\alpha_k} \left\{ S_k \cdot E_{z_1}\left[\text{Prob}\left(e_k(z_1),\, \underline{z} \in C_n(\theta)\right)\right]\right\} + \text{Prob}\left(\underline{z} \notin C_n(\theta)\right)\right\} \\
&\quad = P_e^u(C)\,,
\end{aligned}
$$

which then yields that code partitioning cannot be beneficial when used in conjunction with the tangential sphere bounding techniques.

References

[1] G. Battail, "A conceptual framework for understanding turbo codes", *IEEE Journal on Selected Areas in Communications*, Vol. 16, No. 2, pp. 245–254, February 1998.

[2] S. Benedetto and G. Montorsi, "Unveiling turbo codes: some results on parallel concatenated coding schemes", *IEEE Trans. Information Theory*, Vol. 42, No. 2, pp. 409–428, March 1996.

[3] S. Benedetto, G. Montorsi, D. Divsalar and F. Pollara, "A soft-input soft-output maximum aposteriori (MAP) module to decode parallel and serial concatenated codes", JPL TDA Progress Report 42–127, pp. 1–20, November 15, 1996.

[4] S. Benedetto, G. Montorsi, D. Divsalar and F. Pollara, "Serial concatenation of interleaved codes: performance analysis, design, and iterative decoding, JPL TDA Progress Report, 42–126, August 15, 1996. See also: *Proceedings 1997 IEEE Int. Symp. Information Theory (ISIT'97)*, p. 106, Ulm, Germany, June 29–July 4, 1997.

[5] S. Benedetto, G. Montorsi, D. Divsalar and F. Pollara, "Iterative decoding of serially concatenated codes with interleavers and comparison with turbo codes", *Proceedings of 1997 Global Communications Conference (GLOBECOM'97)*, pp. 654–658, USA, Phoenix, Arizona, November 4–8, 1997.

[6] E.R. Berlekamp, "The technology of error correction codes", *Proc. of the IEEE*, Vol. 68, No. 5, pp. 564–593, May 1980.

[7] C. Berrou, A. Glavieux and P. Thitimajshima, "Near Shannon limit error correcting coding and decoding: turbo–codes", *Proc. of International Conference on Communications*, pp. 1064–1070, Geneva, Switzerland, May 23–26, 1993. See also: C. Berrou and A. Glavieux, "Near optimum error correcting coding and decoding: turbo–codes", *IEEE Trans. Commun.*, Vol. **44**, No. 10, pp. 1261–1271, October 1996.

[8] R.E. Blahut, Principles and Practice of Information Theory, Addison-Wesley Publishing Company, Reading, Massachusetts 1987.

[9] 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)*. See also M.K. Simon and D. Divsalar, "Some new twists to problems involving the Gaussian probability integral", *IEEE Trans. Communications*, Vol. 46, No. 2, pp. 200–210, February 1998.

[10] Csiszàr and J. Körner, "Information Theory: Coding Theorems for Discrete Memoryless Systems", Academic press, New York, 1981.

[11] F. Daneshgaran and M. Mondin, "An efficient algorithm for obtaining the distance spectrum of turbo codes", *Proceedings of the International Symposium on Turbo Codes and Related Topics*, pp. 251–254, Brest, France, 3–5 September, 1997.

[12] D. Divsalar, S. Dolinar, R.J. McEliece and F. Pollara, "Performance analysis of turbo codes", *Proceedings of IEEE ICC'95*, pp. 91–96, Seattle, Washington, June 1995. See also S. Benedetto and G. Montorsi, "Performance evaluation of turbo codes", *Electronic Letters*, vol. 31, no. 3, pp. 163–165, February 1995.

[13] D. Divsalar and F. Pollara, "Turbo codes for PCS applications", *Proceedings of IEEE ICC'95*, pp. 54–59, Seattle, Washington, June 1995.

[14] D. Divsalar and F. Pollara, "Multiple turbo codes", *Proceedings 1995 IEEE Military Communications Conference*, pp. 279–285, San Diego, USA, 5–8 November 1995.

[15] D. Divsalar and F. Pollara, "Hybrid concatenated codes and iterative decoding", JPL TDA Progress Report 42–130, pp. 1–23, August 15, 1997. See also: D. Divsalar and F. Pollara, "Serial and hybrid concatenated codes with applications", *Proceedings on the International Symposium on Turbo Codes and Related Topics*, pp. 80–87, Brest, France, 3–5 September, 1997.

[16] S. Dolinar, L. Ekroot and F. Pollara, "Improvements on the probability of error bounds for block codes on the Gaussian channel", *Proceedings 1994, IEEE Int. Symp. Information Theory (ISIT'94)*, p. 243, Trondheim, Norway, June 27–July 1, 1994.

[17] 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. See also: T.M. Duman, "Turbo codes and turbo coded modulation systems: Analysis and performance bounds", Ph.D. dissertation, Electr. Comput. Eng. Dept., Northeastern University, Boston, MA, May 1998.

[18] R.G. Gallager, Information Theory and Reliable Communications, Wiley, N.Y. 1968.

[19] I.S. Gradshteyn and I.M. Ryzhik, "Tables of Integrals, Series and Products", Academic press, Fifth Edition, 1994.

[20] H. Herzberg and G. Poltyrev, "The error probability of M-ary PSK block coded modulation schemes", *IEEE Trans. on Communications*, vol. 44, no. 4, pp. 427–433, April 1996.

[21] B. Hughes, "On the error probability of signals in additive white Gaussian noise", *IEEE Trans. on Information Theory*, Vol. 37, No. 1, pp. 151–155, January 1991.

[22] P. Jung, "Comparison of turbo-code decoders applied to short frame transmission systems", *IEEE Journal on Selected Areas in Communications*, vol. 14, no. 3, pp. 530–537, 1996.

[23] P. Jung and M. Nabhan, "Performance evaluation of turbo codes for short frame transmission systems", *IEE Electronics Letters*, vol. 30, no. 2, pp. 111–113, 1994.

[24] P. Jung and M. Nabhan, "Dependence of the error performance of turbo codes on the interleaver structure in short frame transmission systems", *IEE Electronics Letters*, vol. 30, no. 4, pp. 287–288, 1994.

[25] H. Koorapaty, Y.P.E. Wang and K. Balachandran, "Performance of turbo codes with short frame sizes", *Proceedings of IEEE 97th Vehicular Technology Conference (VTC'97)*, pp. 329–333, Phoenix, Arizona, USA, May 4–7, 1997.

[26] D.L. Lazic, T. Beth and M. Calic, "How close are turbo codes to optimal codes", *Proc. Int. Symp. Turbo Codes and Related Topics*, pp. 192–195, Brest, France, 3–5 September 1997.

[27] R.J. McEliece, "How to compute weight enumerators for convolutional codes", pp. 121–141 in *Communications and Coding*, M. Darnell and B. Honary, eds. Taunton and Somerset, England Research Studies Press Ltd. 1998. See also: http://www.systems.caltech.edu/EE/faculty/rjm.

[28] M. Peleg, I. Sason, S. Shamai (Shitz) and A. Elia, "On interleaved differentially encoded convolutional codes", Technion CC Pub #235, March 1998. To appear in the *IEEE Trans. on Information Theory*.

[29] 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.

[30] G. Poltyrev, "Bounds on the decoding error probability of binary linear codes via their spectra", *IEEE Trans. on Information Theory*, Vol. 40, No. 10, pp. 1261–1271, October 1996.

[31] I. Sason and S. Shamai (Shitz), "On union bounds for random serially concatenated codes with maximum likelihood decoding", Technical Report EE–110, Technion, September 1997, *Proc. French-Israel Workshop in Coding and Information Integrity*, Ein-Boqeq, Dead-Sea, Israel, 27–29, October 1997. To appear in the *European Transactions on Telecommunications*.

[32] I. Sason and S. Shamai (Shitz), "Improved upper bounds on the performance of parallel and serial concatenated turbo codes", *Proceedings of the 1998 IEEE International Symposium of Information Theory*, p. 30, MIT, Cambridge, MA, USA, 16–21 August, 1998.

[33] I. Sason and S. Shamai (Shitz), "Bounds on the error probability of ML decoding for block and turbo-block codes", *Annales des Telecommunications*, Vol. 54, No. 3–4, pp. 183–200, March-April 1999.

[34] I. Sason, S. Shamai (Shitz), E. Telatar and R. Urbanke, "The Gallager bounding technique for serial and parallel concatenated turbo like codes", Technical Report, CC Pub. No. 258, Technion, Israel, December 1998.

[35] E. Telatar and R. Urbanke, "On the ensemble performance of turbo codes", *Proceedings 1997 IEEE Int. Symp. Information Theory (ISIT'97)*, pp. 105, Ulm Germany, June 29–July 4, 1997. See also: http://cm.bell-labs.com/who/ruediger/pub.html.

[36] A.J. Viterbi, Principles of coherent communication, Chapter 8, pp. 242–244, McGraw-Hill, 1966.

[37] A.M. Viterbi and A.J. Viterbi, "Improved union bound on linear codes for the input-binary AWGN channel, with applications to turbo codes", *Proceedings of the 1998 IEEE International Symposium on Information Theory*, p. 29, MIT, Cambridge, MA, USA, 16–21 August 1998.

[38] A.J. Viterbi, A.M. Viterbi, J. Nicolas and N.T. Sindushyana, "Perspectives on interleaved concatenated codes with iterative soft-output decoding", *Proceedings of the International Symposium on Turbo Codes & Related Topics*, pp. 47–54, Brest, France, 3–5 September, 1997.

Figure Captions

Figure 1: a time-varying recursive shift register of length m.

The state equations of the shift register at time n:

$$s_1(n+1) = \sum_{k=1}^{m} s_k(n)\, c_k(n) + x(n)$$

$$s_k(n+1) = s_{k-1}(n) \quad k = 2, 3, \ldots, m$$

$$y(n) = s_m(n)$$

where $c_k(n)$ $(k = 1, 2, \ldots, m)$ are i.i.d random symmetric binary taking on the values '0' or '1' with equal probability for every moment of time n.

Figure 2: Parallel and serial concatenated turbo codes.

a. Parallel concatenation of two components of rate $\frac{1}{2}$ time-varying RSC codes ([35]), giving an overall code rate of $\frac{1}{3}$ (without puncturing).

b. Serial concatenation of rate $\frac{1}{2}$ time-varying RSC codes and overall rate $\frac{1}{4}$ [31].

c. Parallel concatenation of three components of rate $\frac{1}{2}$ time-varying RSC codes, giving an overall rate of $\frac{1}{4}$ (without puncturing).

Figure 3: The normalized average distance spectrum of random parallel concatenated turbo code with two component codes of rate $\frac{1}{2}$ and of memory length $m = 5$ (see Fig. 2a). The overall rate is $R = \frac{1}{3}$ and the length of the random interleaver is $N = 50, 100, 200, 400$ bits.

Figure 4: The normalized average distance spectrum of random serially concatenated code with inner and outer codes that are time varying recursive systematic convolution codes of rate $\frac{1}{2}$ and of memory length $m = 5$ (see Fig. 2b). The overall rate is $R = \frac{1}{4}$ and a random interleaver between the component codes is of length $N = 50, 100, 200, 400$ bits.

Figure 5: a. A comparison between the normalized average distance spectrum of the ensemble of a random parallel concatenated code (memory length of its components: $m = 5$, overall rate: $R = \frac{1}{3}$ and a random interleaver of length $N = 200$, see Fig. 2a) and the normalized binomial distribution of a fully random block code of the same code length $n = 600$ bits and of the same rate.

b. A comparison between the normalized average distance spectrum of the ensemble of a random parallel concatenated code (memory length of its components: $m = 5$, overall rate: $R = \frac{1}{3}$ and a random interleaver of length $N = 400$, see Fig. 2a) and the normalized binomial distribution of a fully random block code of the same code length $n = 1200$ bits and of the same rate.

Figure 6: a. A comparison between the normalized average distance spectrum of the ensemble of random serially concatenated code (memory length of its components: $m = 5$,

overall rate: $R = \frac{1}{4}$ and a random interleaver of length $N = 200$, see Fig. 2b) and the normalized binomial distribution of a fully random block code of the same code length $n = 400$ bits and of the same rate.

b. A comparison between the normalized average distance spectrum of the ensemble of random serially concatenated code (memory length of its components: $m = 5$, overall rate: $R = \frac{1}{4}$ and a random interleaver of length $N = 400$, see Fig. 2b) and the normalized binomial distribution of a fully random block code of the same code length $n = 800$ bits and of the same rate.

Figure 7: A comparison between upper bounds on the ensemble performance of serially concatenated random codes (see Fig. 2b) in a binary-input AWGN channel with ML decoding. The memory length of the two component codes is $m = 5$, the overall rate is $R = \frac{1}{4}$ and the uniform interleaver is of length $N = 50, 100, 200, 400$ bits.

a. Upper bounds on the block error probability. The improved bounds are based on the tangential sphere bound and are compared to the union bounds.

b. Upper bounds on the bit error probability. The improved bounds are based on the tangential sphere bound and are compared to the union bound.

Figure 8: A comparison between upper bounds on the ensemble performance of parallel concatenated random (turbo) codes (see Fig. 2a) in a binary-input AWGN channel with ML decoding. The memory length of the two component codes is $m = 5$, the overall rate is $R = \frac{1}{3}$ and the interleaver is of length $N = 50, 100, 200, 400$ bits.

a. Upper bounds on the block error probability. The improved bounds are based on the tangential sphere bound and are compared to the union bound.

b. Upper bounds on the bit error probability. The improved bounds are based on the tangential sphere bound. Corresponding union bounds are also shown.

Figure 9: A comparison between upper bounds on the ensemble performance of parallel concatenated random (turbo) codes with $K = 3$ component codes (see Fig. 2c) in a binary-input AWGN channel with ML decoding. The memory length of the three component codes is $m = 5$, the overall rate is $R = \frac{1}{4}$ and the two random interleavers are of length $N = 50, 100, 200$ bits.

a. Upper bounds on the block error probability. The improved bounds are based on the tangential sphere bound and are compared to the union bound (in Q-form).

b. Upper bounds on the bit error probability. The improved bounds are based on the tangential sphere bound and are compared to the union bound (in Q-form).

Figure 10: Upper bounds on the bit error probability of serially concatenated random codes with two component codes of rate $\frac{1}{2}$ (overall rate $\frac{1}{4}$) and a random uniform interleaver of length $N = 200$, as a function of $m = 3, 4, 5, 6, 7, 8$ - the memory length of its

components (see Fig. 2b).

a. Upper bounds based on the union bound (Q-form).

b. Upper bounds based on the tangential sphere bound.

Figure 11: Upper bounds on the bit error probability of parallel concatenated random turbo codes with two component codes of rate $\frac{1}{2}$ (overall rate $\frac{1}{3}$) and two random uniform interleavers of length $N = 100$, as a function of $m = 3, 4, 5, 6, 7$ - the memory length of its components (see Fig. 2a).

a. Upper bounds based on the union bound (Q-form).

b. Upper bounds based on the tangential sphere bound.

Figure 12: Upper bounds on the bit error probability of parallel concatenated random turbo codes with three component codes of rate $\frac{1}{2}$ (overall rate $\frac{1}{4}$) and two random uniform interleavers of length $N = 100$, as a function of $m = 3, 4, 5, 6, 7$ - the memory length of its components (see Fig. 2c).

a. Upper bounds based on the union bound (Q-form).

b. Upper bounds based on the tangential sphere bound.

Figure 13: A comparison between the improved upper bounds on the bit error probabilities of serially concatenated random codes with inner and outer codes of rate $\frac{1}{2}$ (an overall rate of $\frac{1}{4}$) and a random uniform interleaver of length $N = 200$ and of parallel concatenated random (turbo) codes with three component codes of rate $\frac{1}{2}$ (the same overall rate $R = \frac{1}{4}$) and two random uniform interleavers of length $N = 100$ (the same interleaving delay), as a function of $m = 4, 5, 7$ - the memory length of its components (see Figs. 2b,c).

Figure 14: A parallel concatenated turbo code with generators are $G_1(D) = G_2(D) = \left[1, \frac{1+D^2}{1+D+D^2}\right]$ (RSC codes of memory length $m = 2$ and N is the length of the uniform interleaver. The rate of the overall code is $R = \frac{1}{4}$.

Figure 15: The distance spectrum of the parallel concatenated turbo code in Fig. 14:

$G_1(D) = G_2(D) = \left[1, \dfrac{1+D^2}{1+D+D^2}\right]$, $R = \frac{1}{3}$ (see Fig. 14).

(a) $N = 500$.

(b) $N = 1000$.

Figure 16: A comparison of upper bounds on the block error probability of parallel concatenated codes in a binary-input AWGN channel with ML decoding and simulation results of the iterative decoding. The fixed two component codes are RSC codes of rate $\frac{1}{2}$ and their generators are the same, $G_1(D) = G_2(D) = \left[1, \frac{1+D^2}{1+D+D^2}\right]$. The random interleaver is of

length N and the overall rate of the turbo code is $\frac{1}{3}$ (see Fig. 14). The upper bounds for ML decoding are based on the tangential sphere bound, Duman and Salehi bound [17] and the union bound (in Q-form). The simulation results of the iterative decoding are based on the LOG-MAP decoding algorithm with 3,5,7 and 10 iterations.

a. $N = 500$.

b. $N = 1000$.

Figure 17: A comparison of upper bounds on the bit error probability of parallel concatenated (turbo) codes in a binary-input AWGN channel with ML decoding versus simulation results of iterative decoding. The fixed two component codes are RSC codes of rate $\frac{1}{2}$ (an overall rate of $\frac{1}{3}$) and a memory length of $m = 2$. The generators of the two component codes are the same, $G_1(D) = G_2(D) = \left[1, \frac{1+D^2}{1+D+D^2}\right]$ and the random interleaver is of length N (see Fig. 14). The simulation results of the iterative decoding are based on the LOG-MAP decoding algorithm with 3,5,7 and 10 iterations. The upper bounds on the bit error probability are based on the tangential sphere bound, Duman and Salehi bound [17] and the union bound (in Q-form).

a. $N = 500$.

b. $N = 1000$.

Figure 18: A parallel concatenated multiple turbo code, whose generators are $G_1(D) = G_2(D) = G_3(D) = \left[1, \frac{1+D^2}{1+D+D^2}\right]$ (RSC codes of memory length $m = 2$) and N is the length of the two uniform interleavers (independently chosen). The overall rate of the code is $R = \frac{1}{4}$.

Figure 19: A comparison of upper bounds on the block and bit error probabilities of multiple turbo codes in a Gaussian channel with ML decoding with simulation results of iterative decoding. The fixed three component codes are RSC codes of rate $\frac{1}{2}$ (an overall rate of $\frac{1}{4}$) and a memory length of $m = 2$. The generators of the three component codes are the same, $G_1(D) = G_2(D) = G_3(D) = \left[1, \frac{1+D^2}{1+D+D^2}\right]$ and the two random interleavers have length N (see Fig. 18).

a. $N = 192$. The simulation results of the iterative decoding are based on [14] (with 20 iterations for each value of $\frac{E_b}{N_0}$). The performance of the iterative decoding is compared to the union bound (in Q-form) and to the tangential sphere bound.

b. $N = 800$. Improved upper bounds on the block and bit error probabilities and the corresponding union bounds in Q-form.

Figure 20: A rate $\frac{1}{3}$ parallel concatenated turbo code with two RSC component codes whose generators are in octal form 21 and 37 forward and backward respectively $\left(G_1(D) = G_2(D) = \left[1, \frac{1+D^4}{1+D+D^2+D^3+D^4}\right]\right)$ with a uniform interleaver of length $N = 1000$. A termination of $m = 4$ bits is used at the end of each block.

Figure 21: A comparison of upper bounds on the bit error probability of ML decoding and simulation results of the LOG-MAP iterative decoding algorithm (10 iterations are performed). The compared upper bounds of ML decoding are:

1 – union bound in Q-form (tight version).

2 – Duman and Salehi bound [17].

3 – the improved bound based on the tangential sphere bound.

Simulation results of the LOG-MAP iterative decoding after 1,3,5,7 and 10 iterations are also presented.

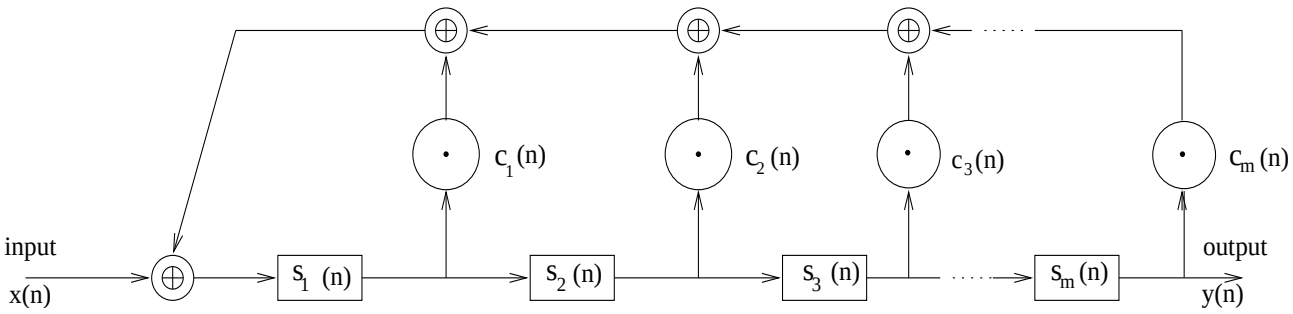


Figure 1.

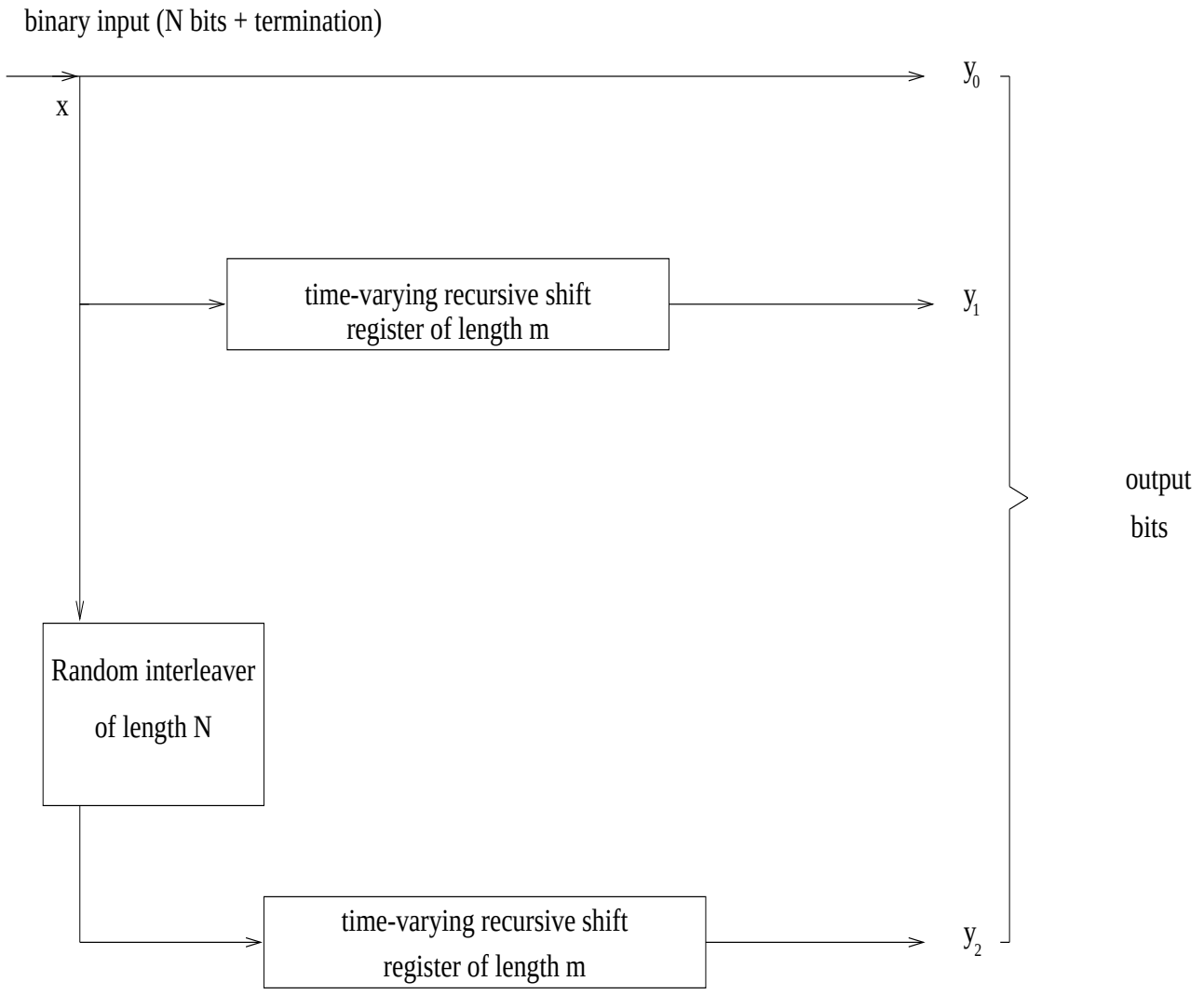


Figure 2(a).

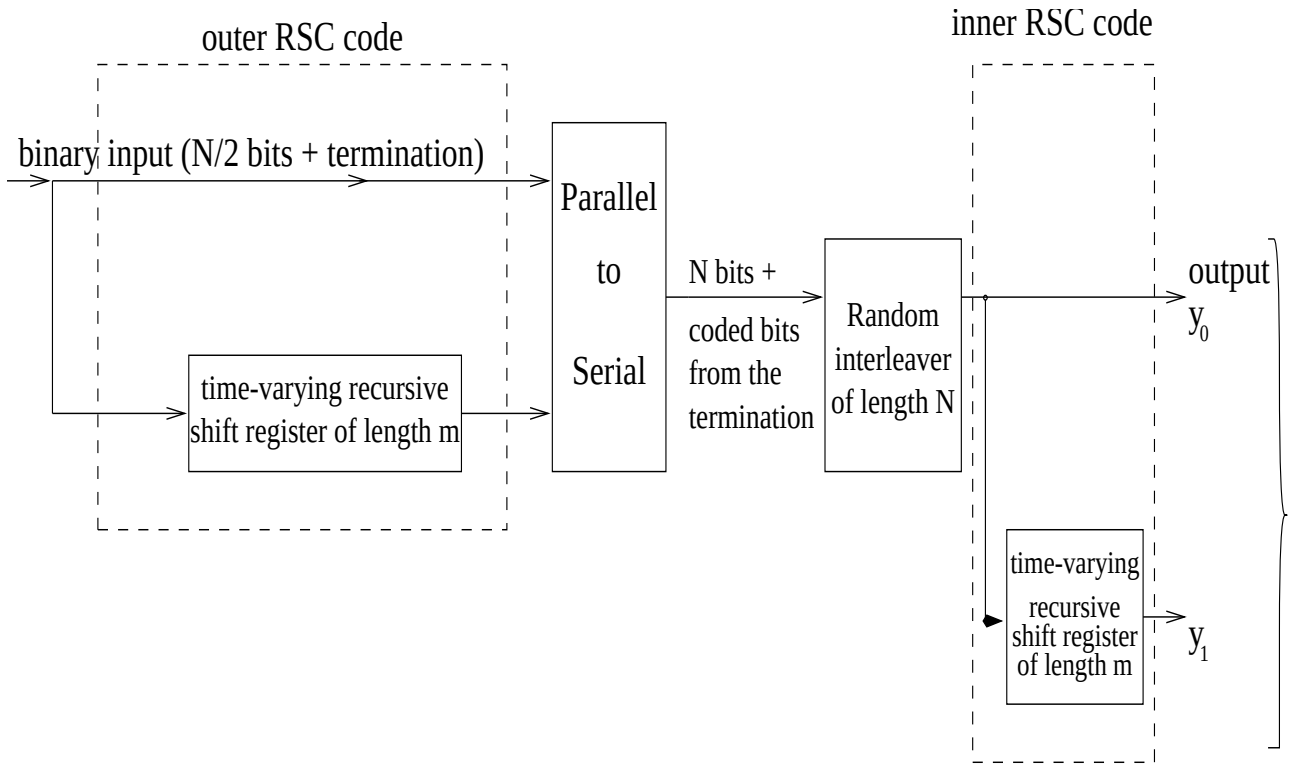


Figure 2(b).

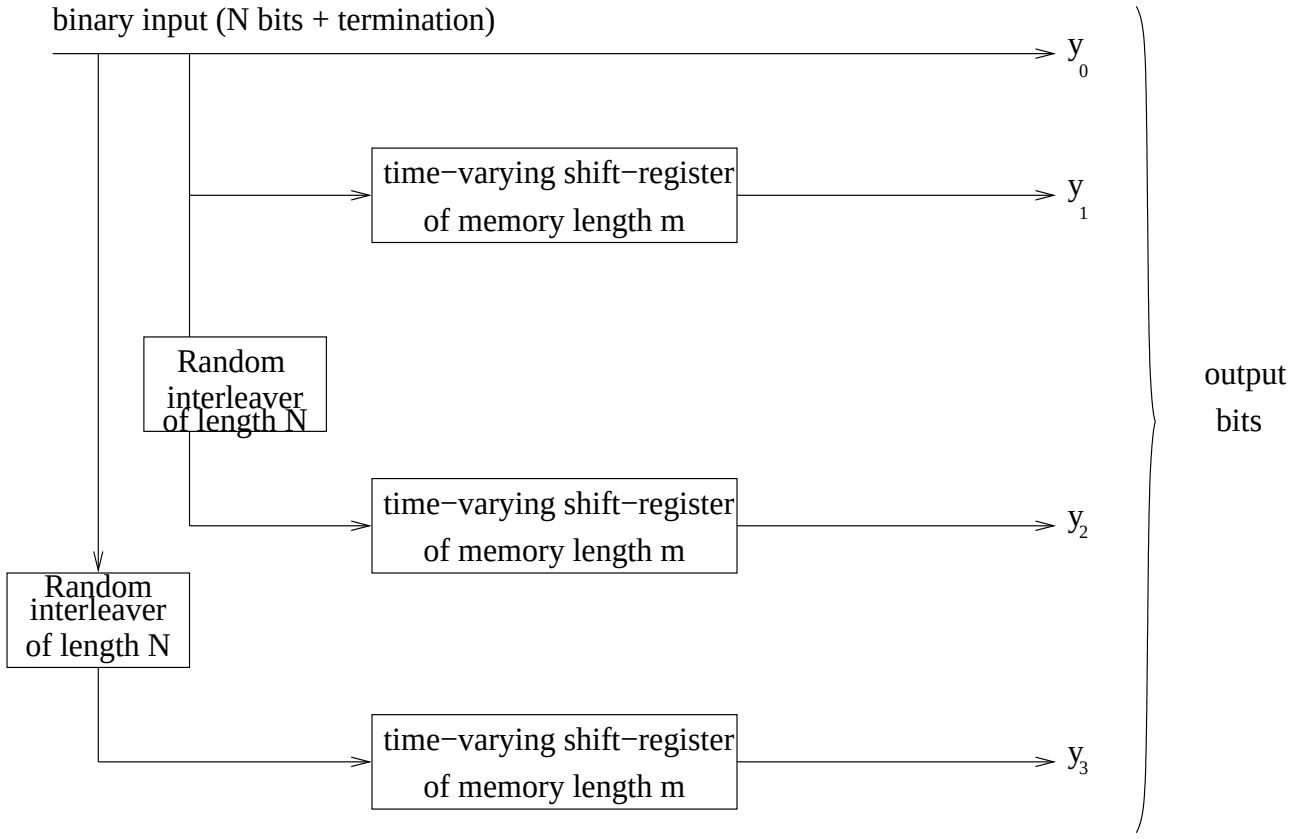


Figure 2(c).

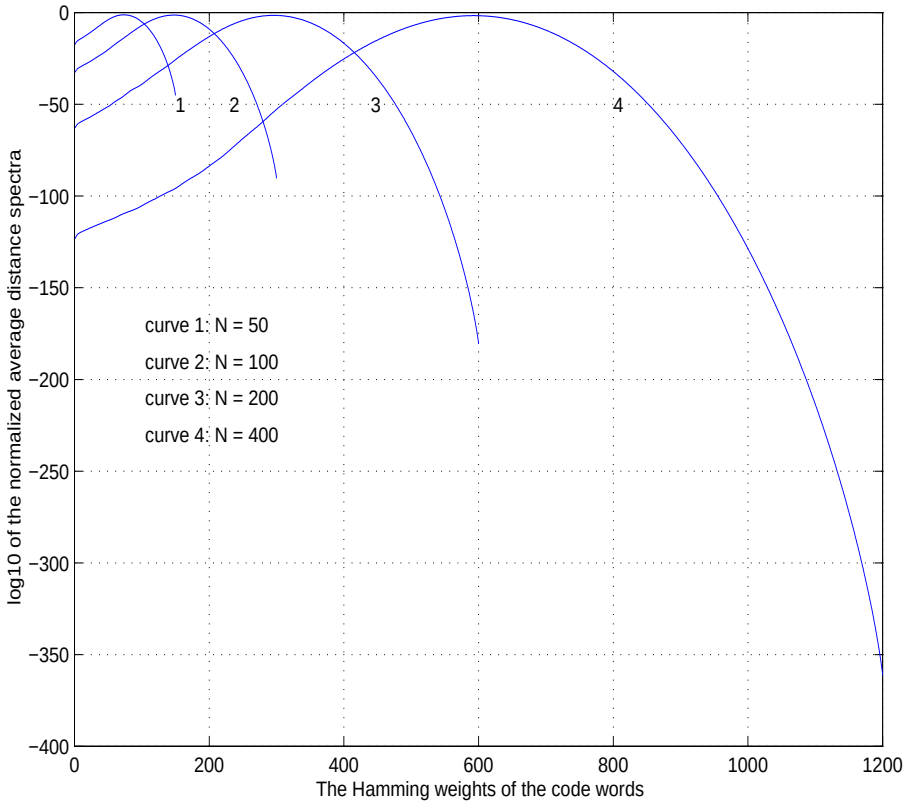


Figure 3.

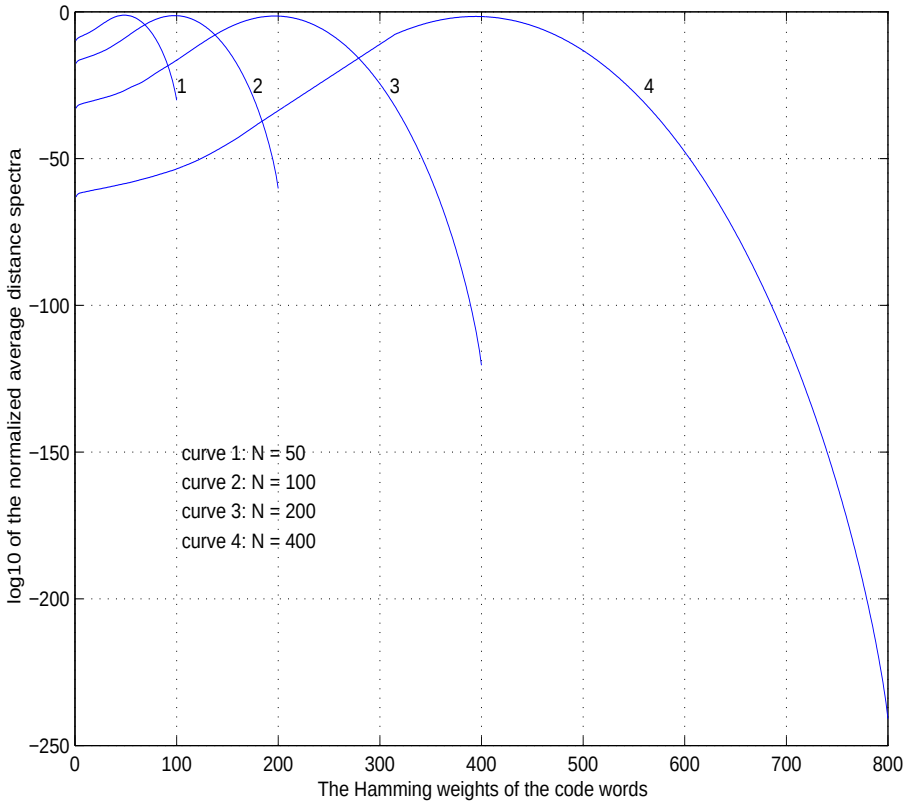


Figure 4.

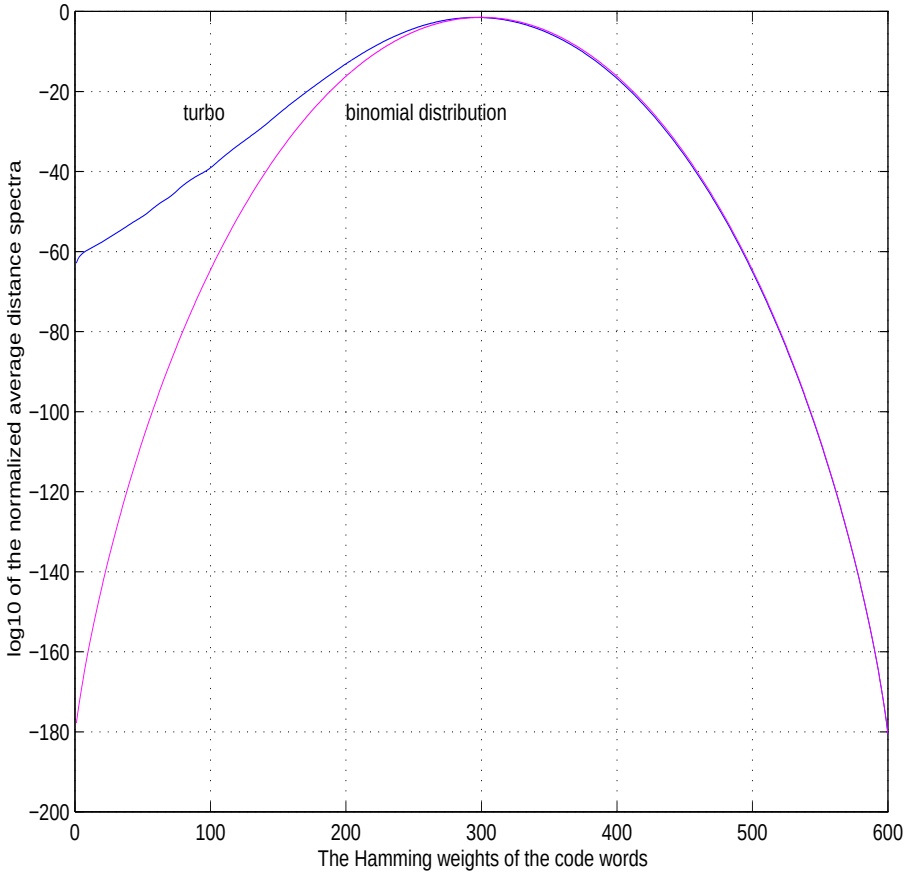
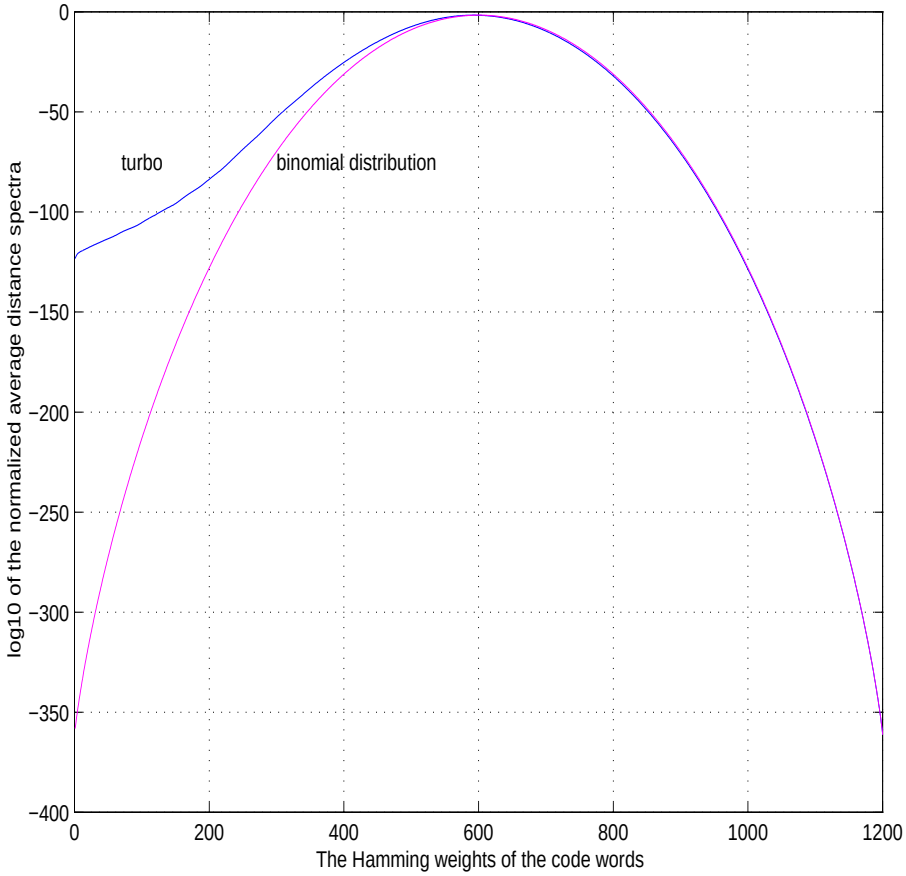

turbo
binomial distribution
log10 of the normalized average distance spectra
The Hamming weights of the code words
0
−20
−40
−60
−80
−100
−120
−140
−160
−180
−200
0
100
200
300
400
500
600

Figure 5(a).


turbo
binomial distribution
log10 of the normalized average distance spectra
The Hamming weights of the code words
0
−50
−100
−150
−200
−250
−300
−350
−400
0
200
400
600
800
1000
1200

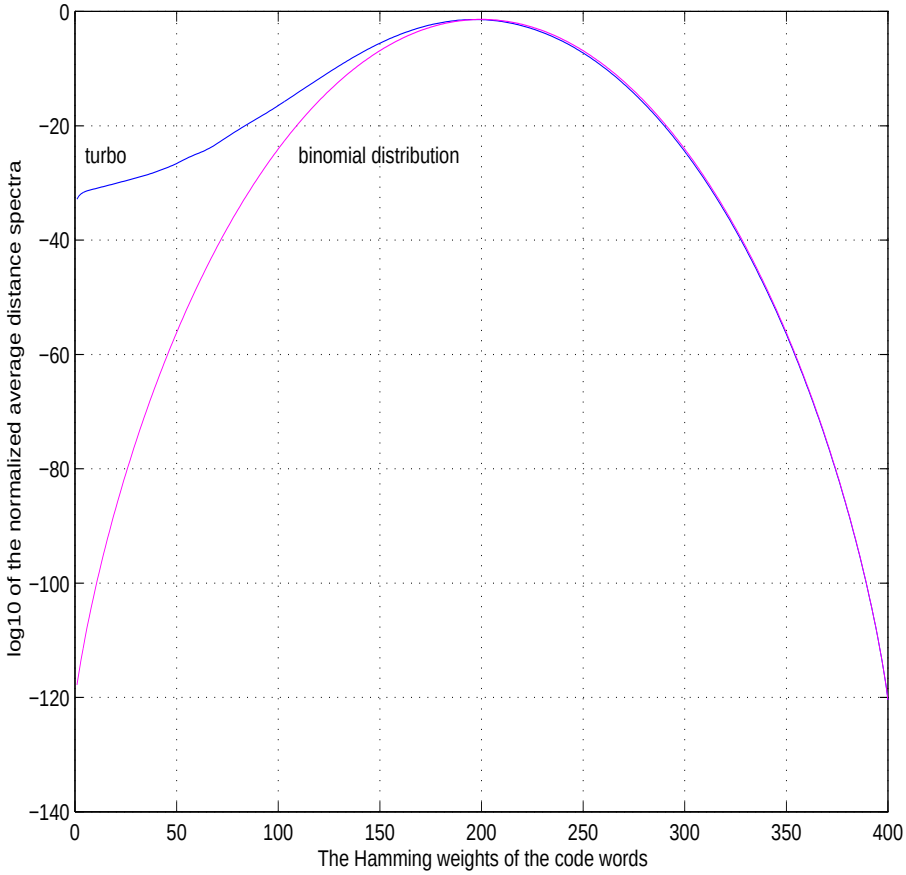
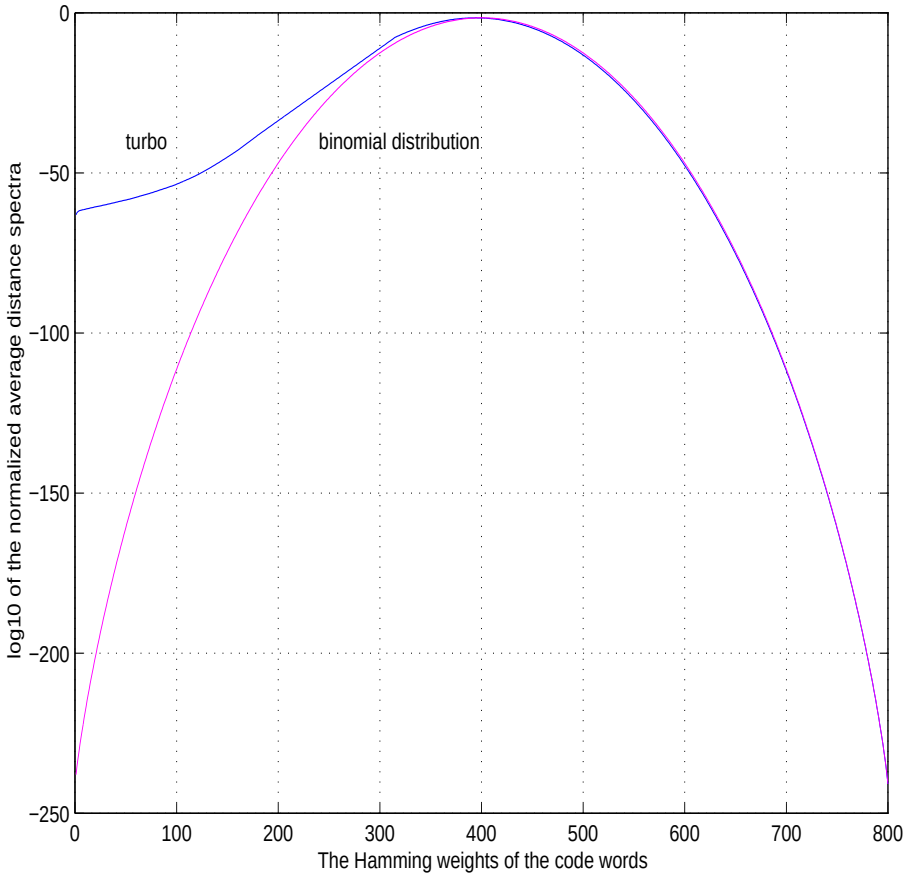

0
−20
−40
−60
−80
−100
−120
−140
0
50
100
150
200
250
300
350
400
turbo
binomial distribution
log10 of the normalized average distance spectra
The Hamming weights of the code words

Figure 6(a).


0
−50
−100
−150
−200
−250
0
100
200
300
400
500
600
700
800
turbo
binomial distribution
log10 of the normalized average distance spectra
The Hamming weights of the code words

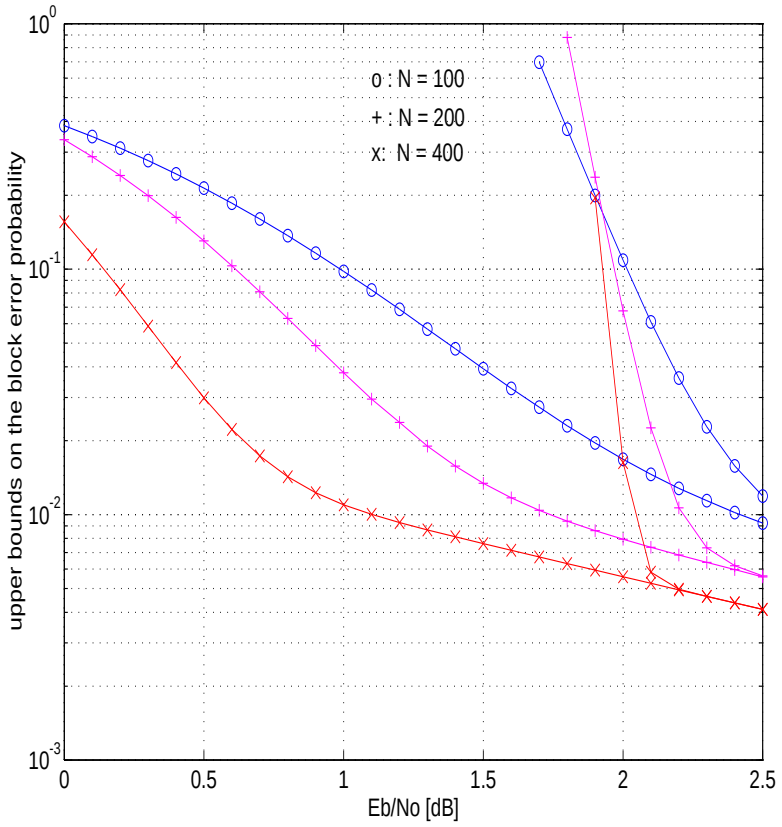
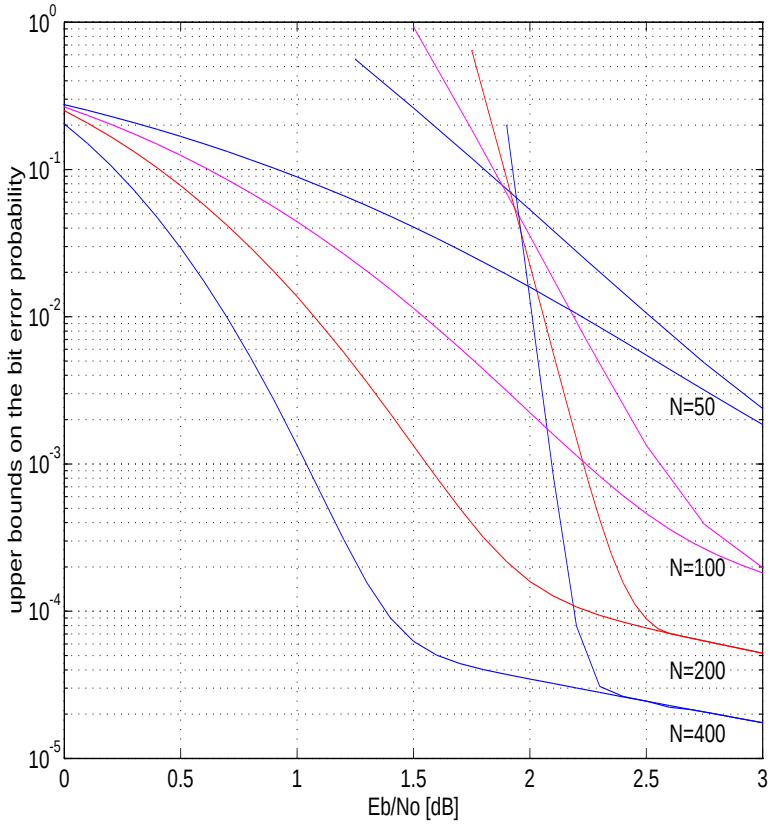

o : N = 100
+ : N = 200
x: N = 400
upper bounds on the block error probability
Eb/No [dB]

Figure 7(a).


N=50
N=100
N=200
N=400
upper bounds on the bit error probability
Eb/No [dB]

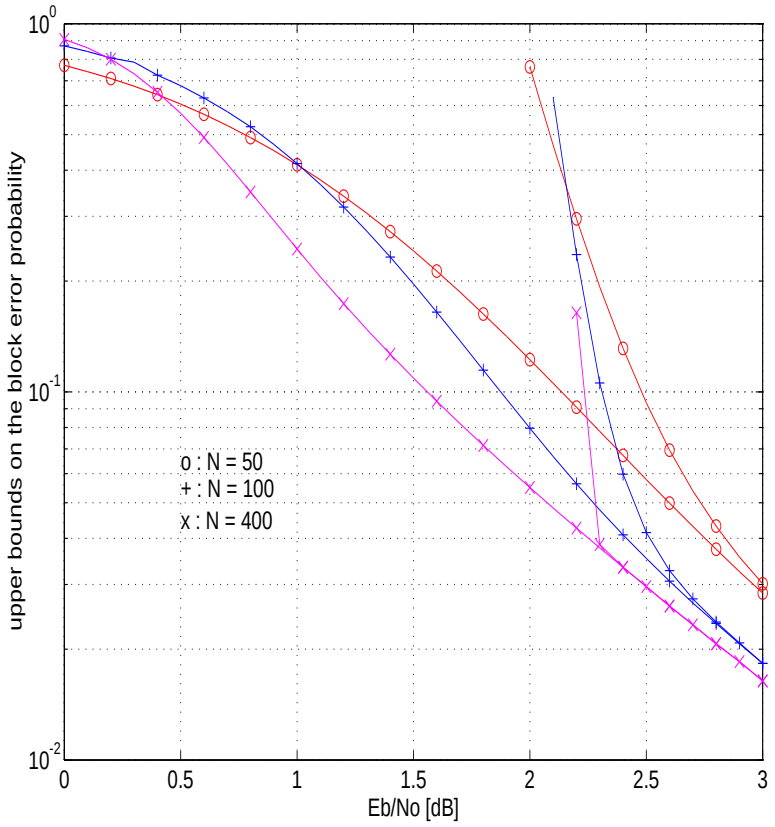
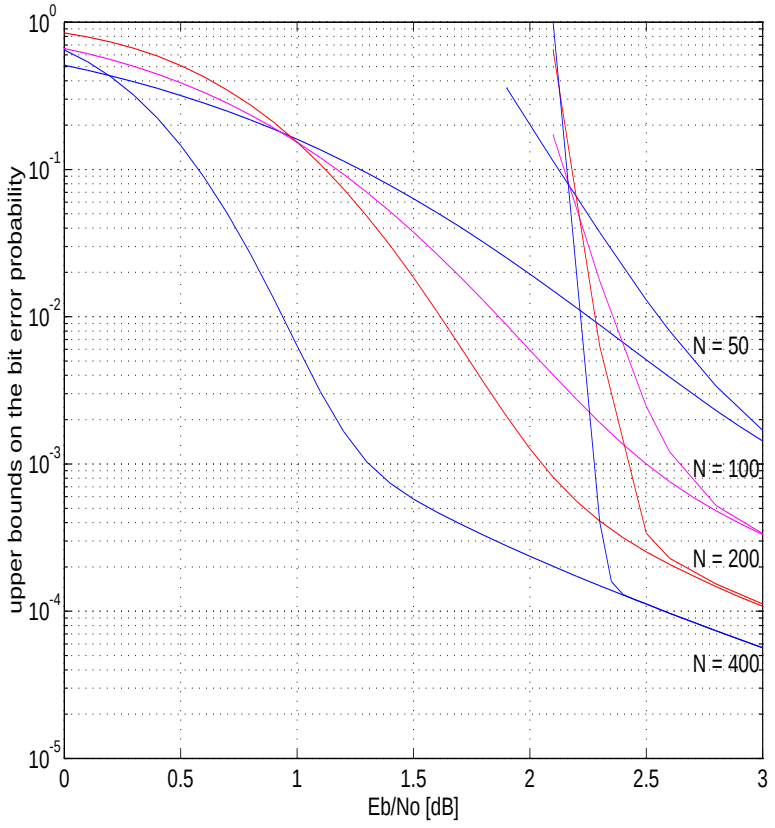

upper bounds on the block error probability
Eb/No [dB]
o : N = 50
+ : N = 100
x : N = 400

Figure 8(a).


upper bounds on the bit error probability
Eb/No [dB]
N = 50
N = 100
N = 200
N = 400

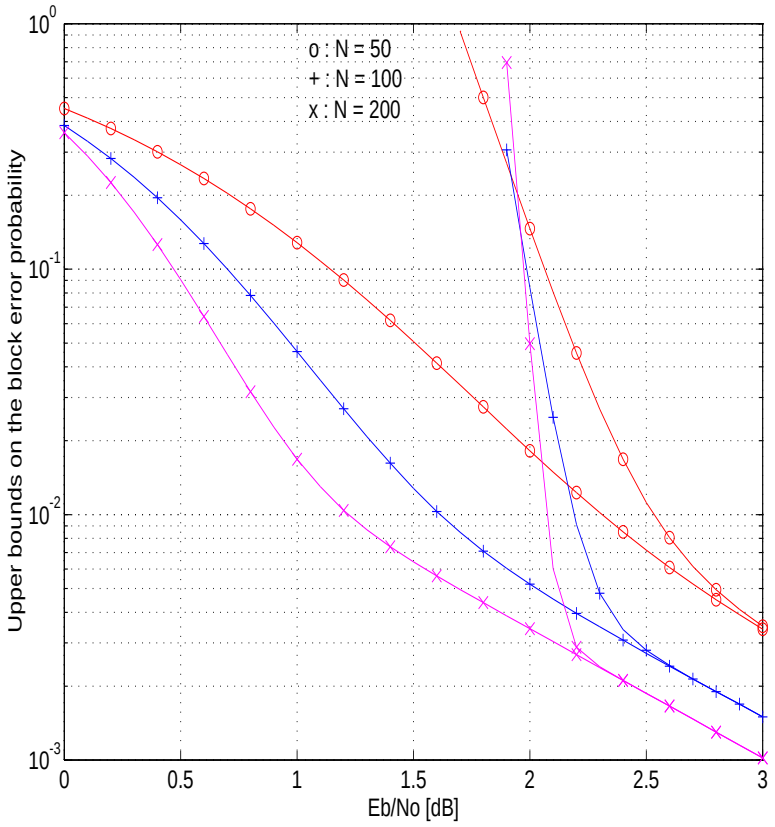
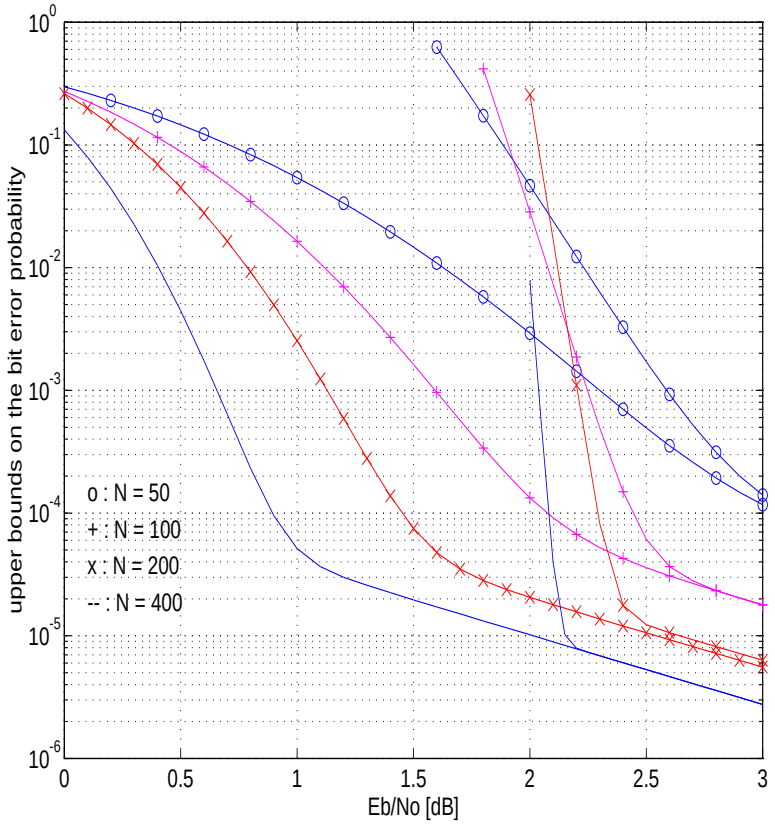

o : N = 50
+ : N = 100
x : N = 200
Upper bounds on the block error probability
Eb/No [dB]
10^0
10^-1
10^-2
10^-3
0
0.5
1
1.5
2
2.5
3

Figure 9(a).


o : N = 50
+ : N = 100
x : N = 200
-- : N = 400
upper bounds on the bit error probability
Eb/No [dB]
10^0
10^-1
10^-2
10^-3
10^-4
10^-5
10^-6
0
0.5
1
1.5
2
2.5
3

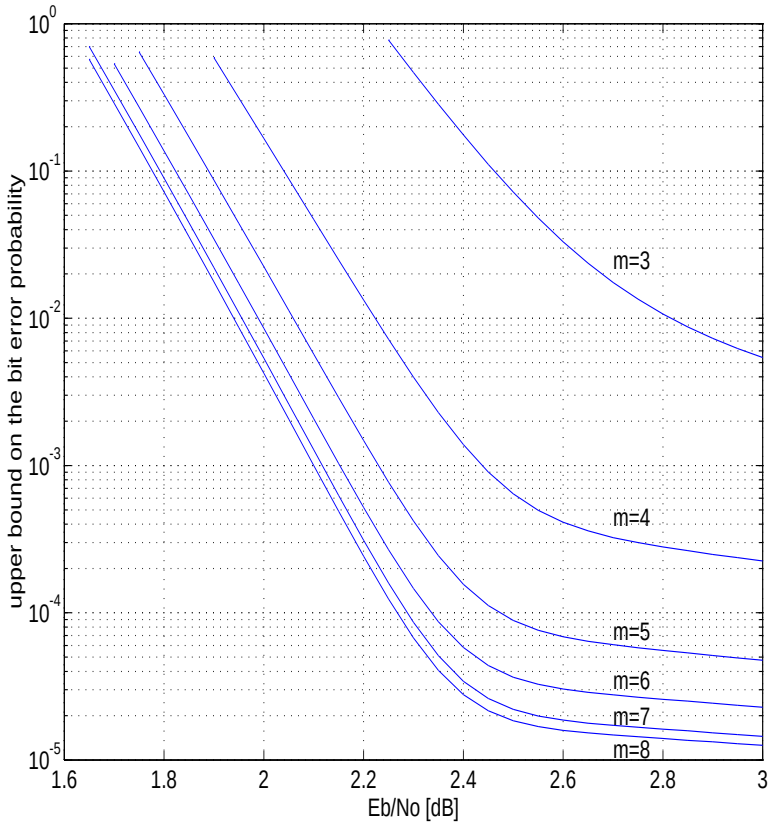
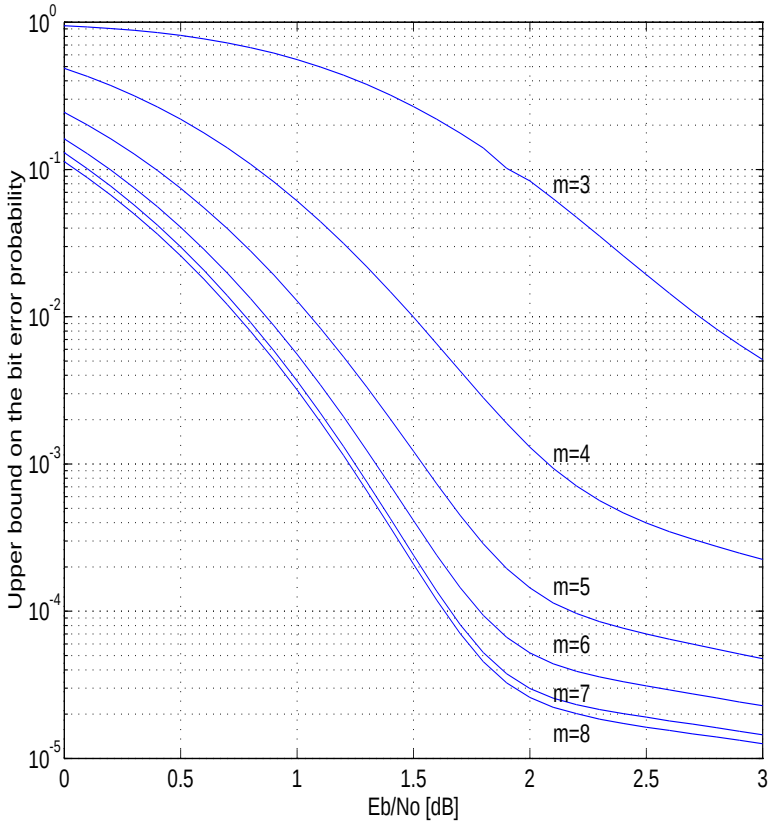

upper bound on the bit error probability
Eb/No [dB]
m=3
m=4
m=5
m=6
m=7
m=8

Figure 10(a).


Upper bound on the bit error probability
Eb/No [dB]
m=3
m=4
m=5
m=6
m=7
m=8

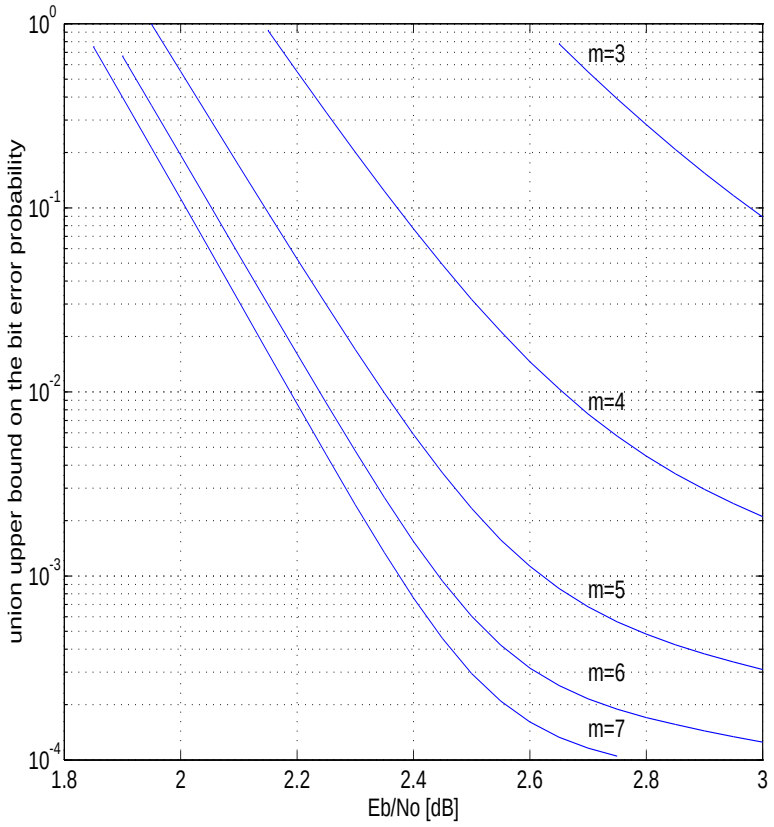
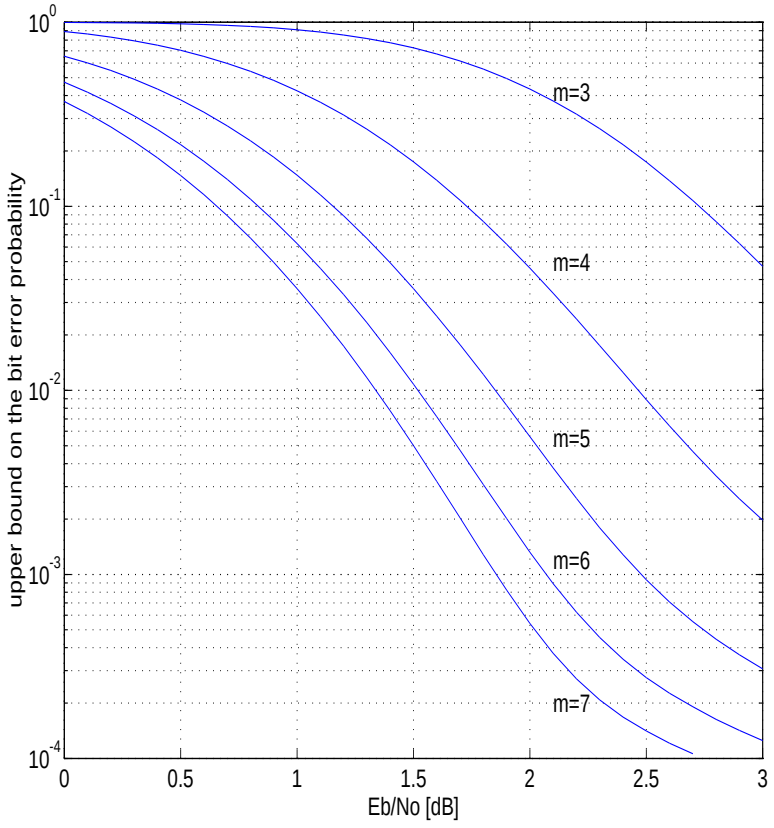

union upper bound on the bit error probability
Eb/No [dB]
m=3
m=4
m=5
m=6
m=7

Figure 11(a).


upper bound on the bit error probability
Eb/No [dB]
m=3
m=4
m=5
m=6
m=7

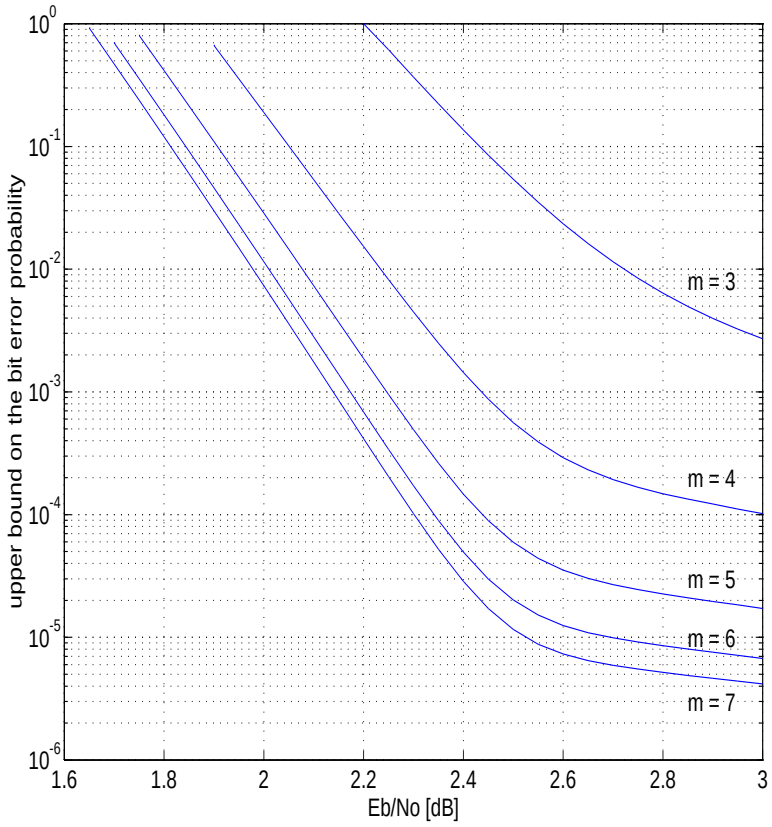
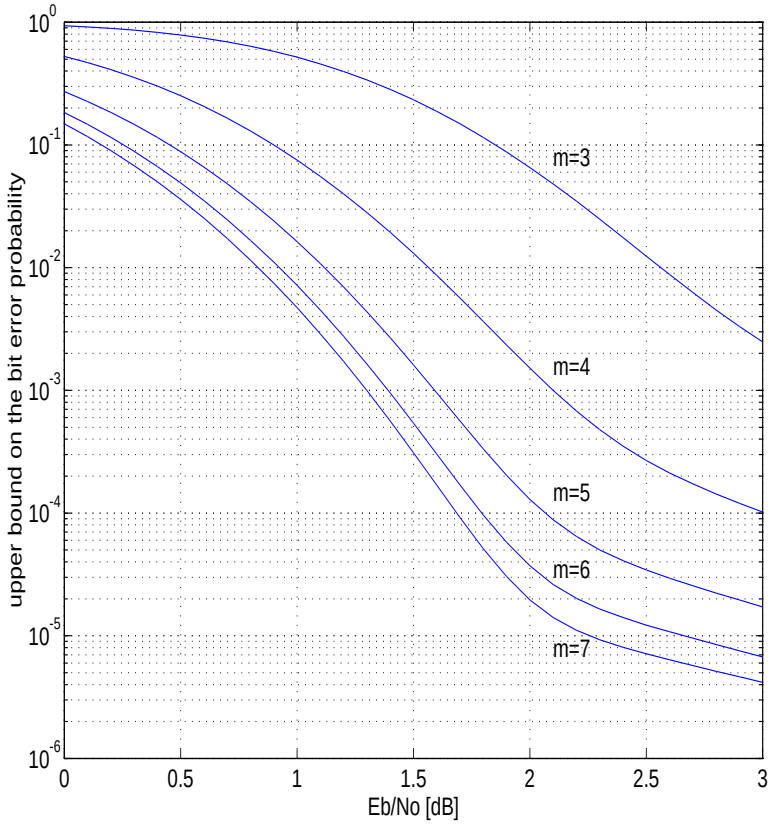

upper bound on the bit error probability
Eb/No [dB]
m = 3
m = 4
m = 5
m = 6
m = 7

Figure 12(a).


upper bound on the bit error probability
Eb/No [dB]
m=3
m=4
m=5
m=6
m=7

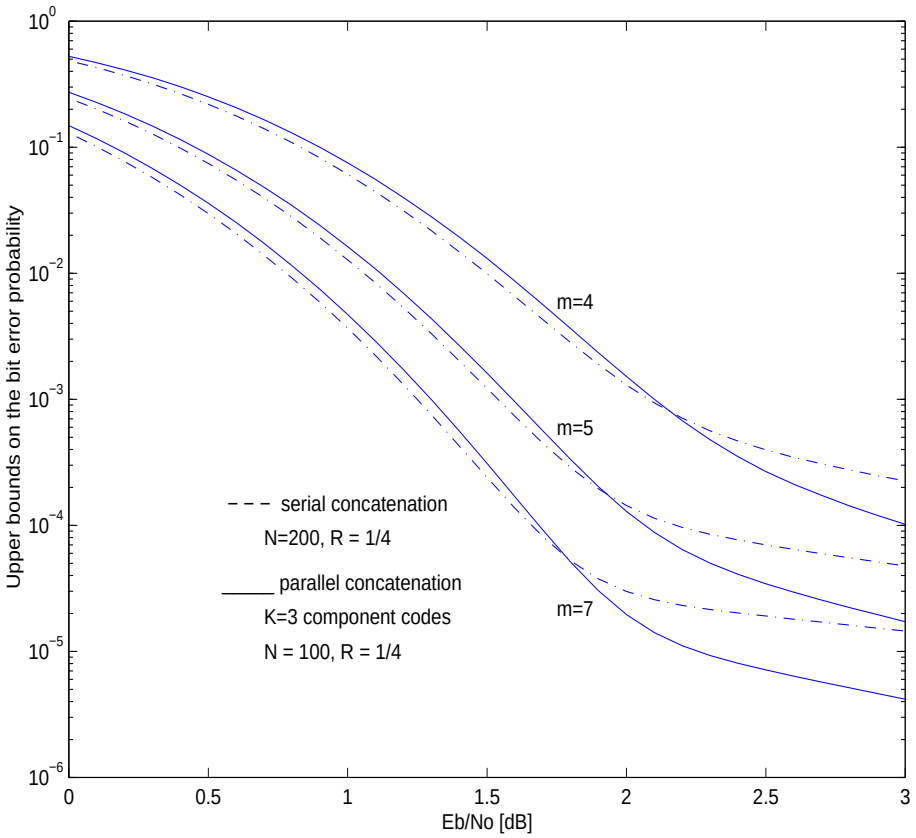


Figure 13.

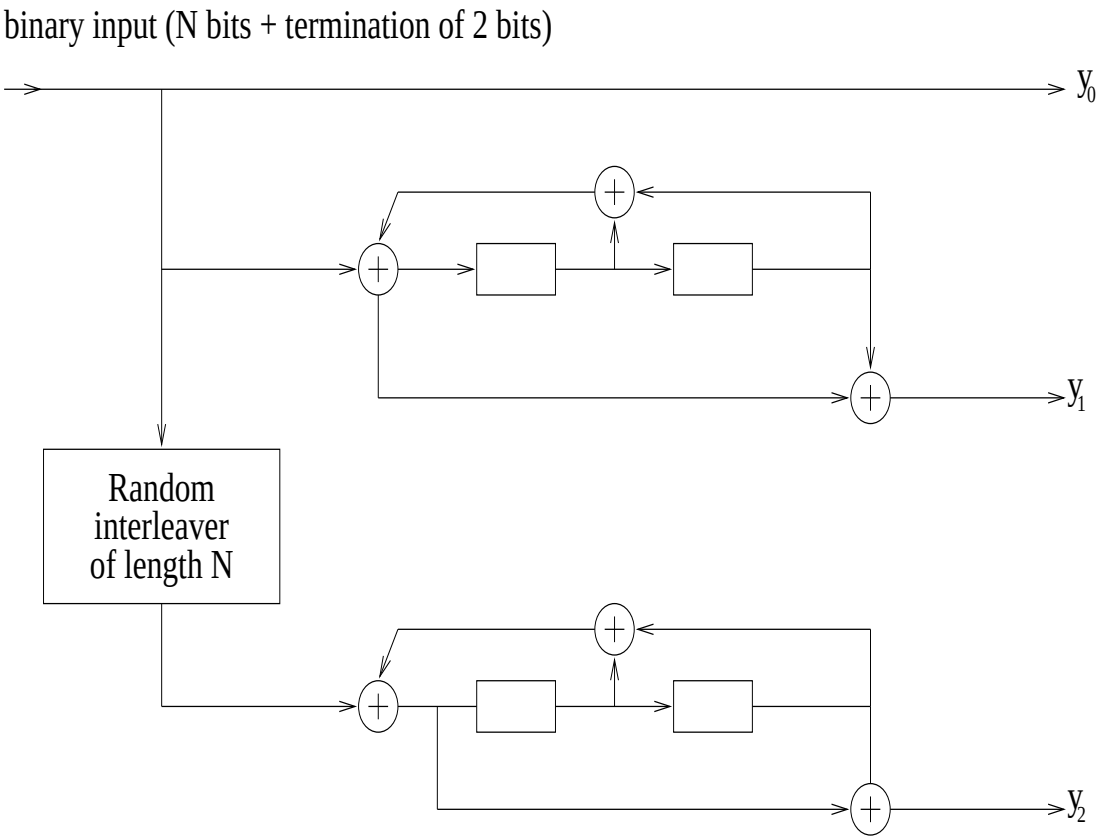


Figure 14.

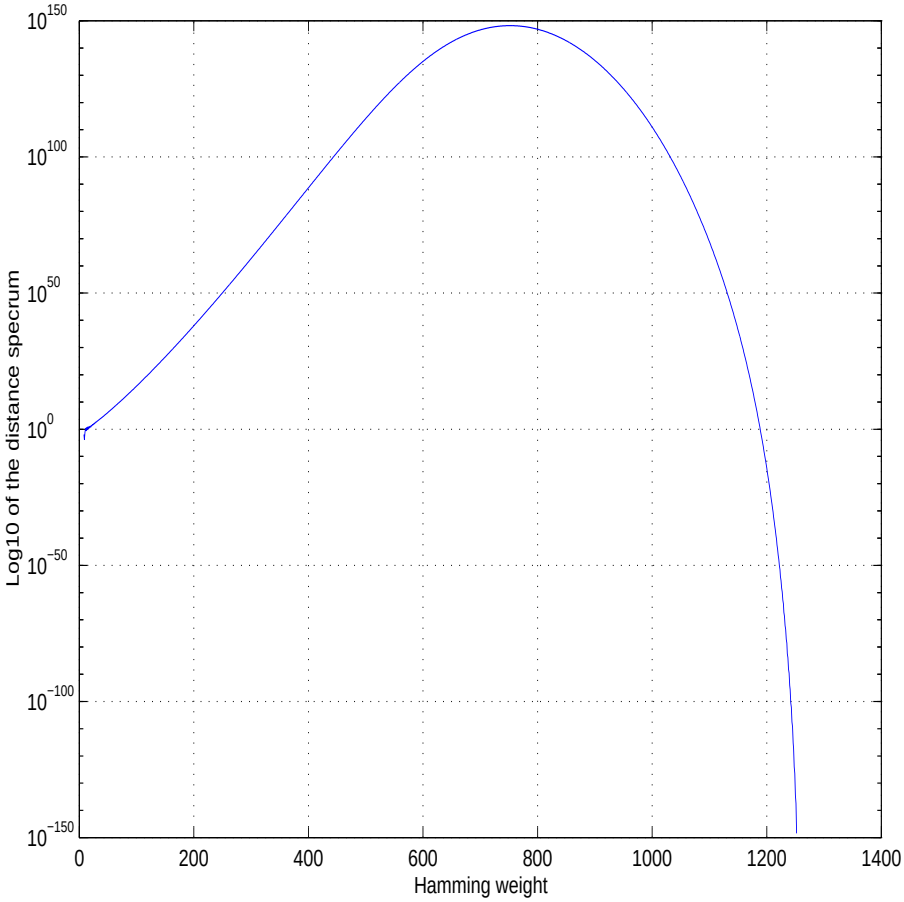
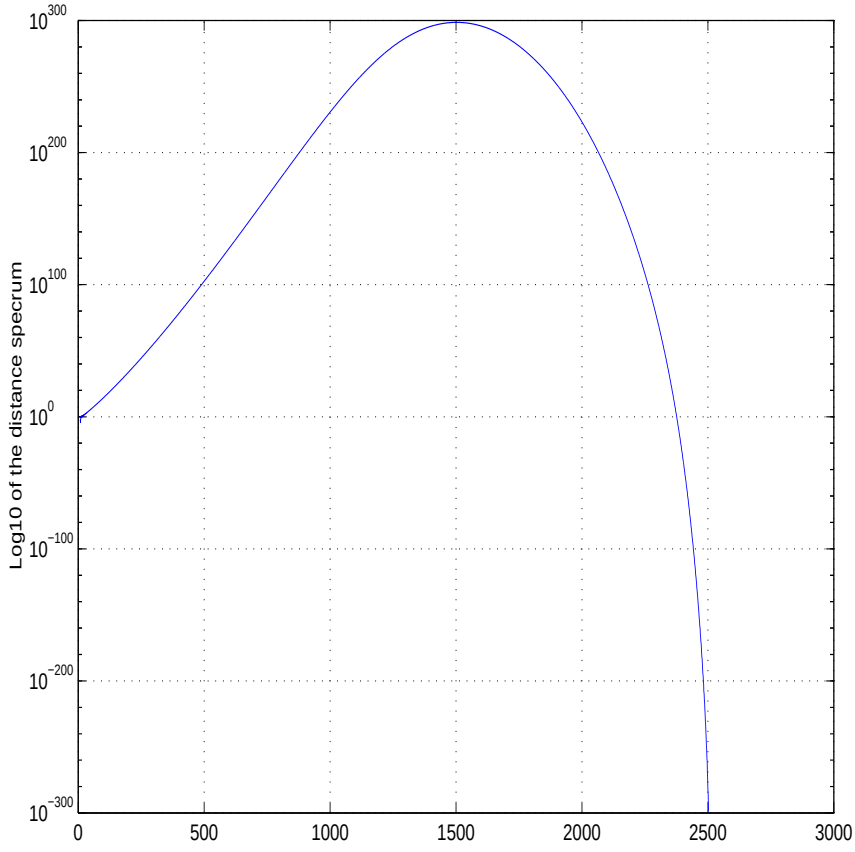

Log10 of the distance specrum
Hamming weight
10^{150}
10^{100}
10^{50}
10^{0}
10^{-50}
10^{-100}
10^{-150}
0
200
400
600
800
1000
1200
1400

Figure 15(a).


Log10 of the distance specrum
10^{300}
10^{200}
10^{100}
10^{0}
10^{-100}
10^{-200}
10^{-300}
0
500
1000
1500
2000
2500
3000

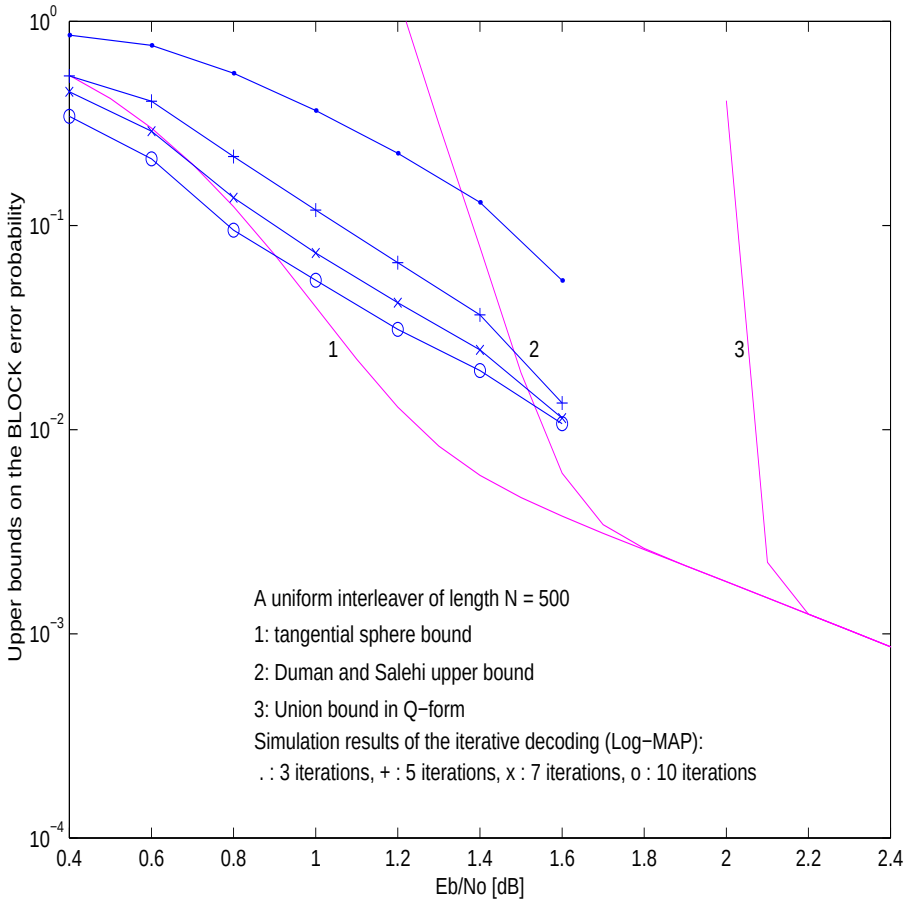
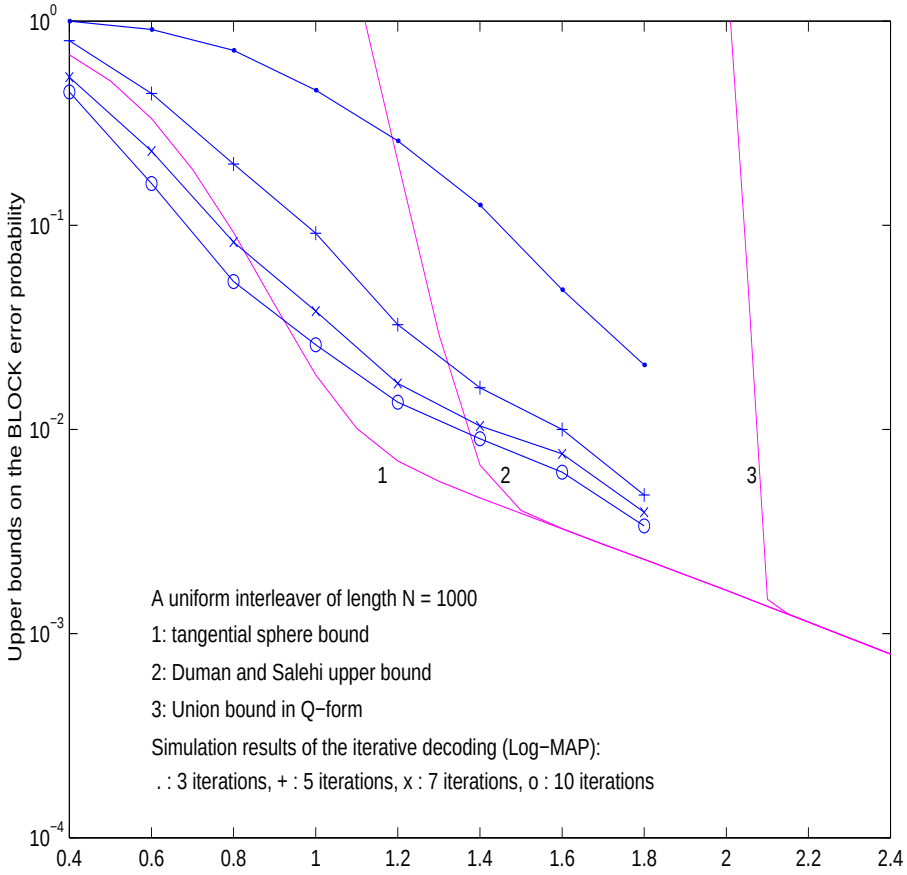

Upper bounds on the BLOCK error probability
Eb/No [dB]
A uniform interleaver of length N = 500
1: tangential sphere bound
2: Duman and Salehi upper bound
3: Union bound in Q−form
Simulation results of the iterative decoding (Log−MAP):
. : 3 iterations, + : 5 iterations, x : 7 iterations, o : 10 iterations
1
2
3

Figure 16(a).


Upper bounds on the BLOCK error probability
Eb/No [dB]
A uniform interleaver of length N = 1000
1: tangential sphere bound
2: Duman and Salehi upper bound
3: Union bound in Q−form
Simulation results of the iterative decoding (Log−MAP):
. : 3 iterations, + : 5 iterations, x : 7 iterations, o : 10 iterations
1
2
3

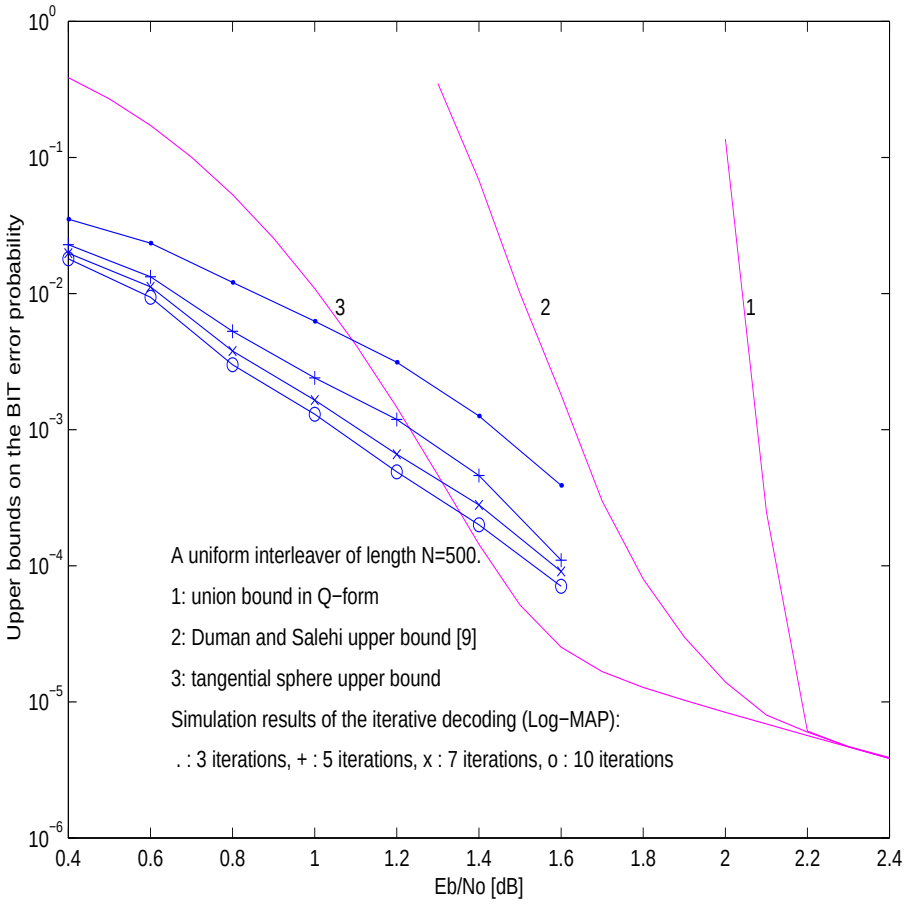
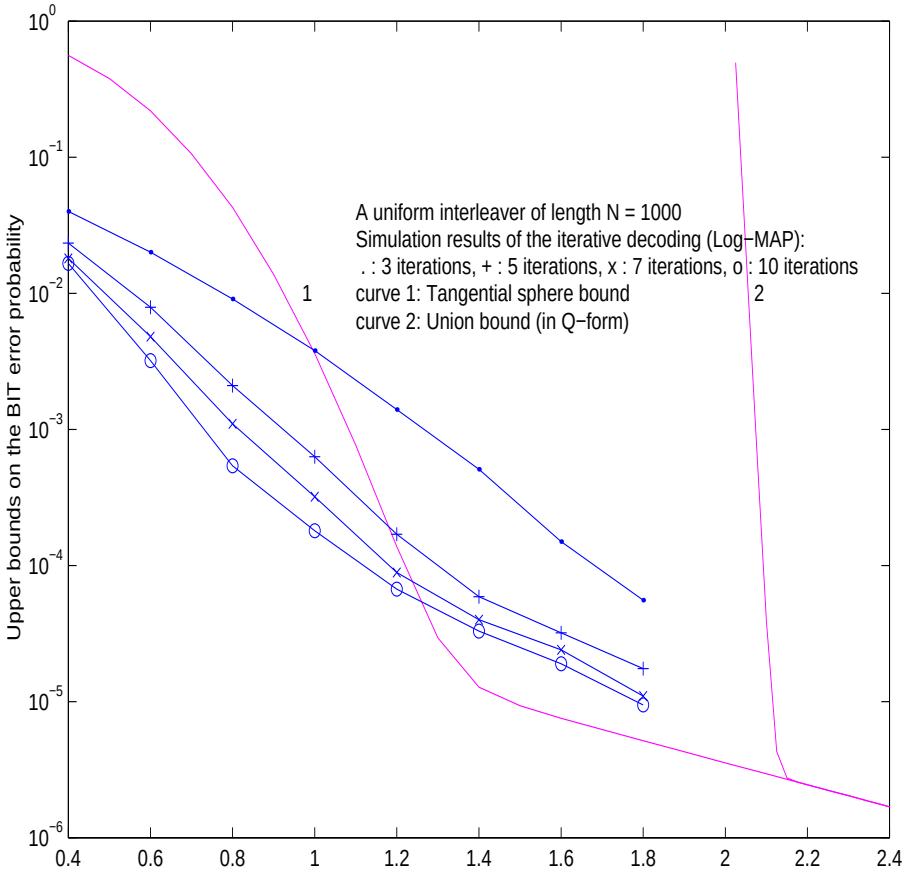

Upper bounds on the BIT error probability
Eb/No [dB]
A uniform interleaver of length N=500.
1: union bound in Q−form
2: Duman and Salehi upper bound [9]
3: tangential sphere upper bound
Simulation results of the iterative decoding (Log−MAP):
. : 3 iterations, + : 5 iterations, x : 7 iterations, o : 10 iterations
1
2
3

Figure 17(a).


Upper bounds on the BIT error probability
A uniform interleaver of length N = 1000
Simulation results of the iterative decoding (Log−MAP):
. : 3 iterations, + : 5 iterations, x : 7 iterations, o : 10 iterations
curve 1: Tangential sphere bound
curve 2: Union bound (in Q−form)
1
2

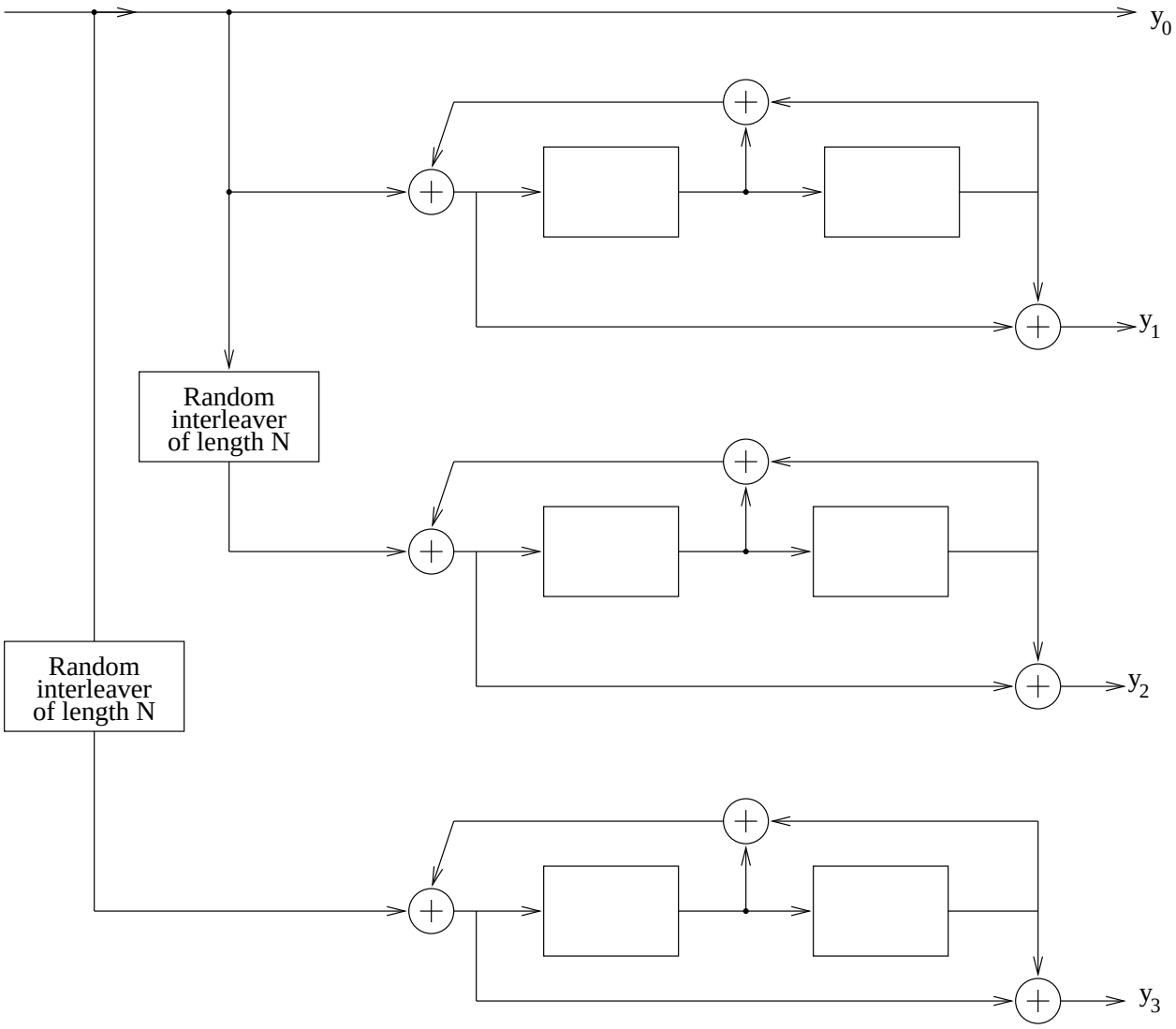

binary input (N bits + termination of 2 bits)
y_0
y_1
Random interleaver of length N
y_2
Random interleaver of length N
y_3

Figure 18.

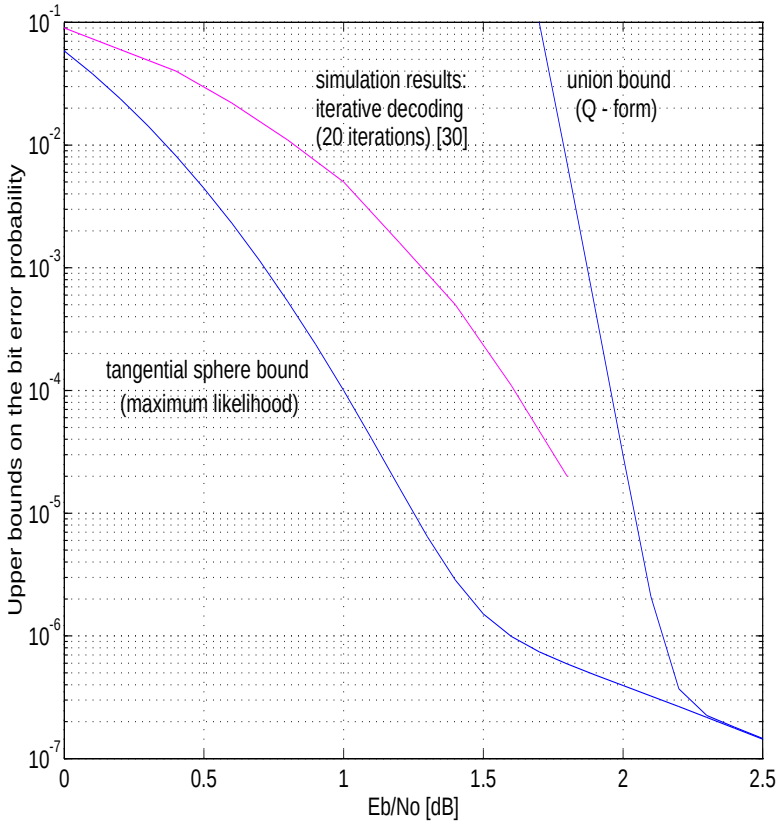
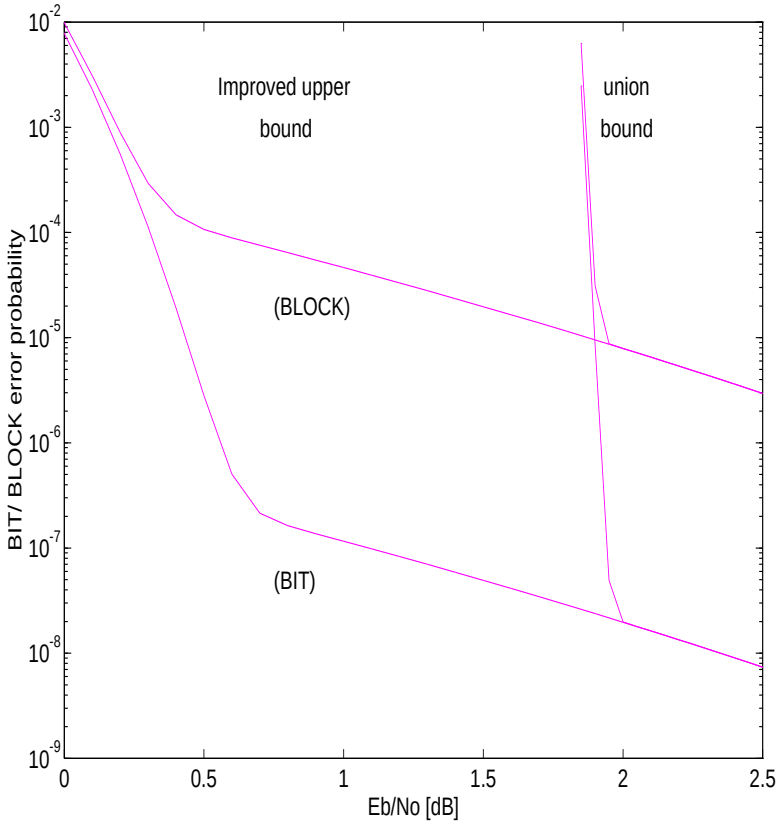

simulation results:
iterative decoding
(20 iterations) [30]
union bound
(Q - form)
tangential sphere bound
(maximum likelihood)
Upper bounds on the bit error probability
Eb/No [dB]

Figure 19(a).


Improved upper
bound
union
bound
(BLOCK)
(BIT)
BIT/ BLOCK error probability
Eb/No [dB]

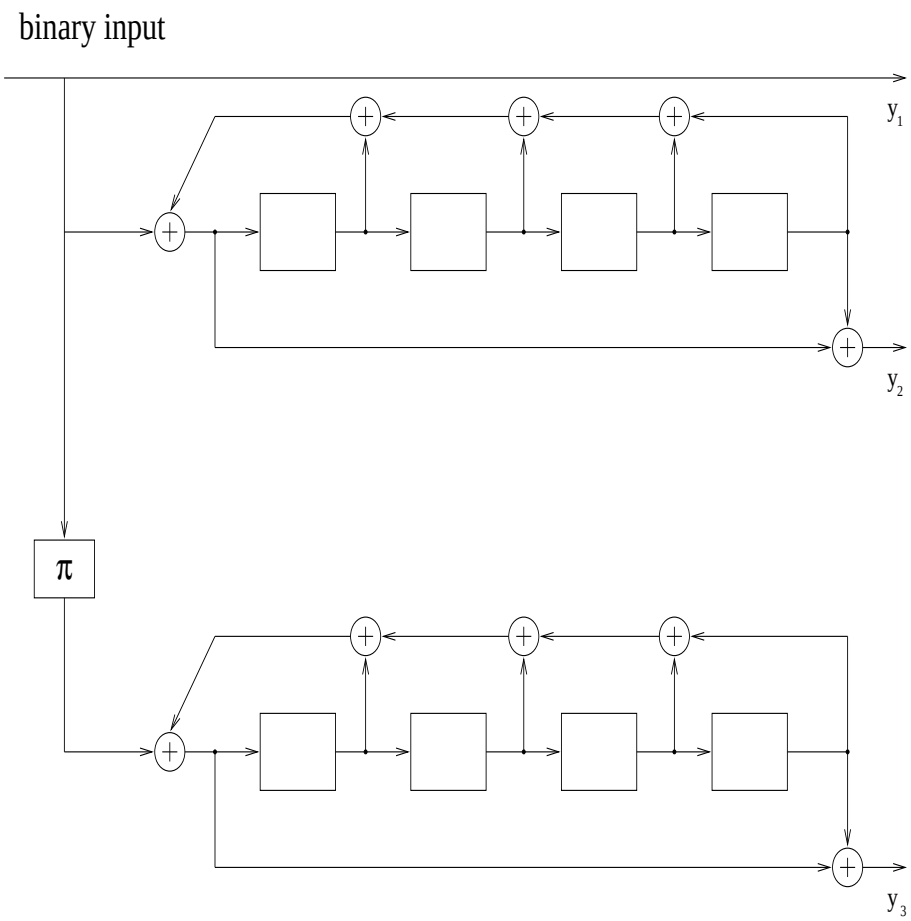
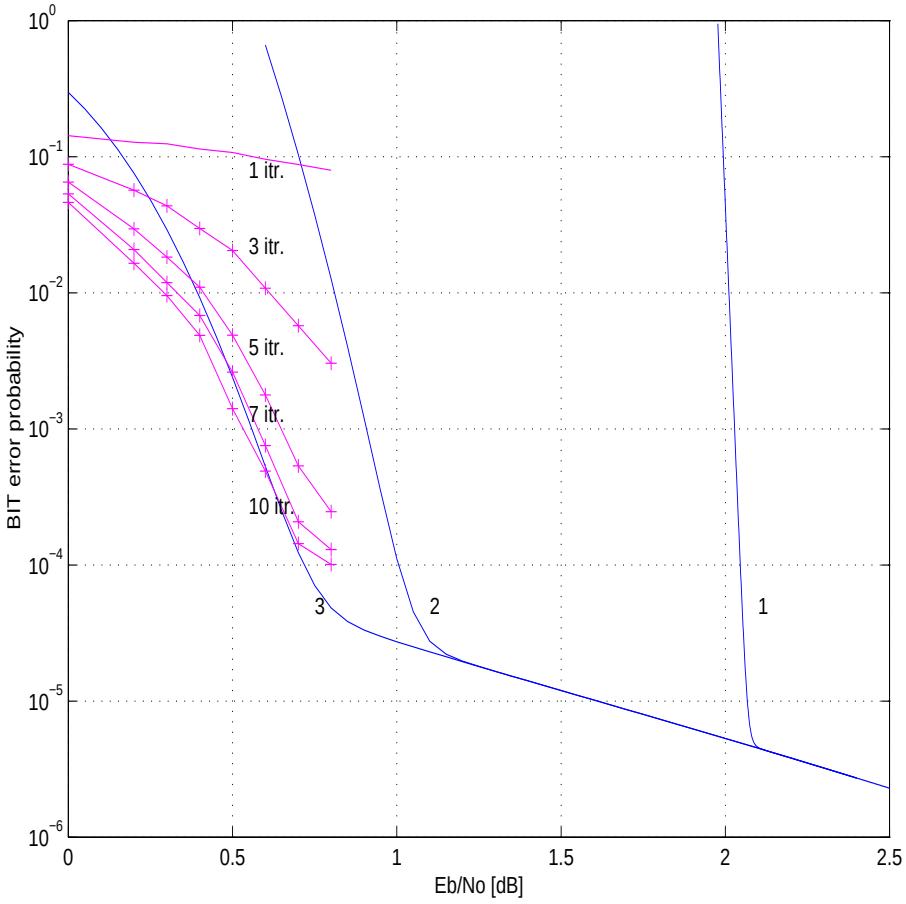

binary input
y1
y2
π
y3

Figure 20.


BIT error probability
Eb/No [dB]
1 itr.
3 itr.
5 itr.
7 itr.
10 itr.
1
2
3