

# Lower Bounds on the Error Probability of Turbo Codes

Ayça Özçelikkale and Tolga M. Duman

**Abstract**—We present lower bounds on the error probability of turbo codes under maximum likelihood (ML) decoding. We focus on additive white Gaussian noise (AWGN) channels, and consider both ensembles of codes with uniform interleaving and specific turbo codes with fixed interleavers. To calculate the lower bounds, instead of using the traditional approach that only makes use of the distance spectrum, we propose to utilize the exact second order distance spectrum. This approach together with a proper restriction of the error events results in promising lower bounds.

## I. INTRODUCTION

Bounds on the error probability of error correction coding is useful for assessing the performance of different coding solutions since the exact error expressions are often difficult to find, and performing simulations is not always a viable approach. Motivated by this observation, we investigate lower bounds on the error probability of turbo codes under maximum likelihood decoding. We consider both uniform and fixed interleaving cases.

One of the main approaches for obtaining lower bounds on the error probability of coded systems is using sphere packing arguments [1–3]. Another approach is to use methods based on Bonferroni type inequalities or the de Caen’s inequality. To use these inequalities directly in the framework of error correction coding, one not only requires the distance spectrum of the code, but a generalized second order distance spectrum that gives the “correlation” between the codewords [4]. Nevertheless, Seguin has proposed a relaxation for AWGN channels under binary phase shift keying (BPSK) through which it is possible to find bounds that are calculable solely in terms of the distance spectrum. This approach has been used successfully for calculating different variants of lower bounds on the error probability [4–6].

Although Seguin’s relaxation technique is attractive from a computational point of view, it introduces a possible looseness in the bounds. In this paper, we illustrate that significant performance improvements can be obtained by calculating the second order distance spectrum exactly, and compute tight lower bounds on the error probability of turbo codes based on this observation. We consider both code ensembles with uniform interleaving and specific turbo codes with fixed interleavers. To accomplish this, we develop a technique for calculating the average second order distance spectrum for ensembles of turbo codes. To further tighten the bounds, we propose a number of approaches to restrict our attention to a properly chosen set of error events in the calculations. Our

results show that these two approaches, using the exact second order distance spectrum and proper restriction of the error events, result in promising lower bounds. In both uniform and fixed interleaving cases, our approach is shown to offer tighter bounds than the ones obtained by sphere packing bounds for moderate to high signal-to-noise ratios (SNRs) for the block lengths considered. Moreover, for the ensemble of turbo codes, the derived bounds tightly agree with the union bound in the high SNR region for the codes considered in this paper.

In the context of turbo codes, it is often desirable to assess the performance of ensemble of codes rather than specific codes. However, although the approaches based on the de Caen’s bound are shown to be very successful for specific codes, they are not directly applicable to ensembles of codes [7]. On the other hand, the bounds that use sphere packing arguments typically show loose performance as SNR increases. Our approach here offers a promising solution to this issue in the case of turbo code ensembles.

The article is organized as follows: In Sec. II, the system model is described, and different lower bounding techniques are explained. The improvements that make them tight and calculable for the error correction coding scenarios considered here are discussed in Sec. III. We develop techniques for calculation of the second order distance spectrum for turbo code ensembles in Sec. IV. In Sec. V, examples of the proposed lower bounds are reported. Finally, the paper is concluded in Sec. VI.

## II. SYSTEM MODEL

### A. The AWGN Channel

We consider transmission over an AWGN channel using an  $(L, N)$  linear block code. The received signal  $\mathbf{y}$  when the length  $L$  codeword  $\mathbf{c}_i$  is transmitted can be expressed as follows

$$\mathbf{y} = \mathbf{x}_i + \mathbf{n}, \quad (1)$$

where  $\mathbf{n}$  denotes the length  $L$  Gaussian noise vector with independently and identically distributed (i.i.d.) components with variance  $N_0/2$ . The channel input  $\mathbf{x}_i$  is obtained by mapping the codeword  $\mathbf{c}_i$  to  $\mathbf{x}_i$  with BPSK modulation where the bit 0/1 is mapped to  $\sqrt{E}/\sqrt{E}$ . Energy per bit is given as  $E_b = E/R$ , where  $R$  is the rate of the code.

Since we are focusing on geometrically uniform codes, the average frame error probability can be expressed as follows

$$P_e = P(\varepsilon|\mathbf{c}_0) = P\left(\bigcup_{i \neq 0} \varepsilon_i\right), \quad (2)$$

where  $\mathbf{c}_0$  denotes the all zero codeword. Here  $\varepsilon$  represents the error event and  $\varepsilon_i$  represents the pairwise error event

A. Özçelikkale and T. M. Duman are with the Dep. of Elect. Eng., Bilkent University, TR-06800, Ankara, Turkey e-mail: ayca, duman@ee.bilkent.edu.tr. T. M. Duman is on leave from Arizona State University. This publication was supported by the EC Marie Curie Career Integration Grant, PCIG12-GA-2012-334213, and TUBITAK 1001 Project, 113E223.

that the decoder decides on the codeword  $\mathbf{c}_i$  while  $\mathbf{c}_0$  has been actually sent. For ML decoder,  $\varepsilon_i$  may be expressed as  $\varepsilon_i = \{\|\mathbf{y} - \mathbf{x}_i\| \leq \|\mathbf{y} - \mathbf{x}_0\|\}$ , where  $\|\cdot\|$  represents the Euclidean norm.

### B. Lower Bounds on the Error Probability

We consider Kounias bound, a Bonferroni type bound which lower bounds the probability of union of a given set of events [8]. Using the Kounias bound, the probability of error over an AWGN channel can be lower bounded as follows

$$P(\varepsilon|\mathbf{c}_0) \geq \max_{\mathcal{J}} \left( \sum_{i \in \mathcal{J}} P(\varepsilon_i) - \sum_{i,j \in \mathcal{J}, i < j} P(\varepsilon_i \cap \varepsilon_j) \right), \quad (3)$$

where  $\mathcal{J} \subseteq \mathcal{I} = \{1, 2, \dots, M-1\}$  with  $M = 2^N$  for an  $(L, N)$  linear code. The individual probabilities in this bound can be expressed as  $P(\varepsilon_i) = Q(\sqrt{s}w(\mathbf{c}_i))$  and  $P(\varepsilon_i \cap \varepsilon_j) = \Psi(\rho_{ij}, \sqrt{s}w(\mathbf{c}_i), \sqrt{s}w(\mathbf{c}_j))$  where  $s = 2E/N_0$ ,  $w(\mathbf{c}_i)$  denotes the weight of the codeword  $\mathbf{c}_i$  [4], [5], [9].<sup>1</sup> We have

$$\begin{aligned} & \Psi(\rho, u', v') \\ &= \frac{1}{2\pi\sqrt{1-\rho^2}} \int_{u'}^{\infty} \int_{v'}^{\infty} \exp\left\{-\frac{u^2 - 2\rho uv + v^2}{2(1-\rho^2)}\right\} du dv, \\ & \rho_{ij} = \frac{w(\mathbf{c}_i \circ \mathbf{c}_j)}{\sqrt{w(\mathbf{c}_i)w(\mathbf{c}_j)}}, \end{aligned} \quad (4)$$

where  $\mathbf{c}_i \circ \mathbf{c}_j$  denotes the elementwise product of the two vectors  $\mathbf{c}_i$  and  $\mathbf{c}_j$ . Hence  $w(\mathbf{c}_i \circ \mathbf{c}_j)$  gives the number of indices that both of the codewords are 1. In this respect,  $\rho_{ij}$  can be interpreted as a measure of correlation between the codewords  $\mathbf{c}_i$  and  $\mathbf{c}_j$ . Thus, enumeration of the number of pairs of codewords with a given  $\rho_{ij}$  can be interpreted as a second order distance spectrum.

We note that lower bounds based on the Kounias bound can be calculated for ensembles of codes, since it is possible to take averages in this case. This is in contrast with the bounds that are based on the de Caen's inequality [10]

$$P(\varepsilon|\mathbf{c}_0) \geq \sum_{i \in \mathcal{I}} \left( \frac{P(\varepsilon_i)^2}{\sum_{j \in \mathcal{I}} P(\varepsilon_i \cap \varepsilon_j)} \right) \quad (5)$$

such as [4], [5]. We recall that it is not straightforward to apply these bounds to turbo code ensembles, since it is not clear how to process these terms under the expectation operation imposed by the ensemble average [7].

## III. COMPUTATION OF THE LOWER BOUND

### A. Second Order Distance Spectrum

Direct calculation of the bounds presented in Sec. II-B requires calculation of  $\Psi(\rho_{ij}, u', v')$ , hence calculation of  $\rho_{ij}$  for all codeword pairs of interest. To overcome this difficulty, Seguin has proposed a bounding technique that only uses the distance spectrum of the code. In particular, it is shown that  $\Psi(\rho_{ij}, u', v')$  is a monotonically increasing function of  $\rho_{ij}$ , and  $\rho_{ij}$  can be upper bounded by using the weights of

<sup>1</sup> $Q(u') = \frac{1}{\sqrt{2\pi}} \int_{u'}^{\infty} \exp(-u^2/2) du$ .

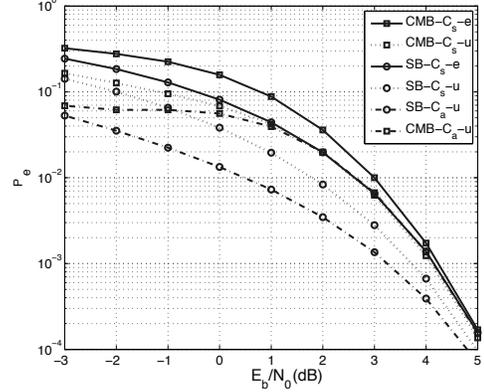


Fig. 1: Effect of using exact  $\rho$  values and subset selection on the tightness of the bounds for a Golay code ( $L = 23$ ,  $N = 12$ ). CMB: norm bound in [5], SB: bound in [4].  $C_s/C_a$ : Set of codewords used for calculating the bounds. e/u: strategy adopted regarding  $\rho$  values: *exact* or *upper-bounded*.

the codewords  $\mathbf{c}_i$  and  $\mathbf{c}_j$  [4]. Hence it is possible to find an expression that is still a valid lower bound by only using the distance spectrum of the code. This approach is adopted in a number of works to find promising lower bounds [4–6] that only use the distance spectrum.

Although this technique is attractive from a computational perspective, our investigations suggest that by calculating  $\rho_{ij}$  one can significantly improve the lower bounds. Fig. 1 illustrates this point for a Golay code ( $L = 23$ ,  $N = 12$ ). Similar observations can be made for other codes, including turbo codes. In the figure, the norm bound of [5] (CMB) and the bound in [4] (SB) are presented; both of which are based on (5). Bounds are calculated over the set of codewords with the minimum weight ( $C_s$ ). We note that due to the following

$$P\left(\bigcup_{i \in \mathcal{I}} \varepsilon_i\right) \geq P\left(\bigcup_{i \in \mathcal{I}_r, \subseteq \mathcal{I}} \varepsilon_i\right) \quad (6)$$

the bounds calculated over  $C_s$  are true lower bounds. For further comparison, bounds over the whole code ( $C_a$ ) with upper bounded  $\rho$  values are also presented. Comparing CMB- $C_s$ -e with CMB- $C_s$ -u and SB- $C_s$ -e with SB- $C_s$ -u, we observe that performances of both of these bounds significantly improve by using exact correlation values.

Hence it is of interest to keep track of  $\rho_{ij}$  values in order to calculate tight lower bounds despite the computational difficulty. In Sec. III-B, we propose a number of methods to reduce the number of codewords for which  $\rho_{ij}$  values will be calculated. In Sec. IV, we give details on how to systematically calculate  $\rho_{ij}$  values for convolutional codes, and turbo code ensembles with uniform interleaving.

### B. Subset Restriction

Direct calculation of the bound in (3) constitutes a computational challenge. It requires the complete second order distance spectrum of the code over all codewords, that is, the enumeration of  $\rho_{ij}$  for all possible codeword pairs  $\mathbf{c}_i$  and  $\mathbf{c}_j$ . Moreover, in order to tighten the bound, one has to perform an optimization over all subsets of  $\mathcal{I}$ , where the total number of subsets is  $2^{M-1} = 2^{2^N-1}$ . We observe that the optimization

can be done only over a restricted family of subsets of  $\mathcal{I}$ , and the result will still be a valid lower bound. By this restriction, one may also ease the computational burden related to the calculation of the second order weight enumeration by only calculating  $\rho_{ij}$  for the codewords in these subsets. Hence it is of interest to restrict ourselves *a priori* to properly chosen certain subsets of  $\mathcal{I}$ , and only optimize over these. For this purpose, we consider two approaches. In the first one, we directly restrict  $\mathcal{I}$  to a subset  $\mathcal{I}_r$  as shown in (6). We then apply the Kounias bound to the right hand side with  $\mathcal{J} \subseteq \mathcal{I}_r$ . In the second approach, we impose a certain structure on the subsets allowed. In the remainder of this section, we present details for these two approaches.

To choose a proper  $\mathcal{I}_r$ , we propose to restrict our analysis only to the codewords with low input and/or output weights. It is expected that the error events that account for most of the errors are the ones with the codewords that are close to the codeword sent (especially in the high SNR region). The codewords that are close to  $c_0$  will be the ones with low overall weight. In fact, it is possible to tighten the bounds by only using codewords with low output weights instead of calculating the bounds on the whole code. This property is illustrated in Fig. 1 for a Golay code ( $L=23$ ,  $N=12$ ). Comparing CMB- $C_s$ -u with CMB- $C_a$ -u and SB- $C_s$ -u with SB- $C_a$ -u, we observe that performances of both of these bounds significantly improve by using the set of codewords with minimum weight ( $C_s$ ) instead of all the codewords ( $C_a$ ).

In the case of turbo codes, using codewords with low input weights (in particular weight-two input sequences) and specific input patterns is a method successfully adopted in a number of scenarios, including assessing code performance and design of turbo codes [11], [12]. We note that due to the nature of the lower bounds we consider (and the property in (6)), we can directly consider subsets of the codewords, and the bounds calculated with these thresholding methods are true lower bounds. This is in contrast with the scenarios where similar approaches used for calculation of upper bounds result in only approximate bounds (although they show satisfactory performance for proper threshold values.) We present further details on this method in Sec. V.

For the uniform interleaving case, we also consider the following restriction: the set  $\mathcal{J}$  is chosen such that if a codeword with a given weight is in the set, then all the other codewords of that weight are also in the set. Under this restriction, the probability of error for a given interleaver can be lower bounded as

$$\begin{aligned} P(\varepsilon|c_0) &\geq \sum_{k \in \mathcal{J}} m_k Q(\sqrt{sk}) \\ &- \sum_{k, t \in \mathcal{J}, k < t} \sum_{\bar{\rho}: \bar{\rho} \neq 1} n_{\bar{\rho}, k, t} \Psi(\bar{\rho}, \sqrt{sk}, \sqrt{st}) \\ &- \frac{1}{2} \sum_{\bar{\rho}: \bar{\rho} \neq 1} n_{\bar{\rho}, k, k} \Psi(\bar{\rho}, \sqrt{sk}, \sqrt{sk}), \end{aligned} \quad (7)$$

where  $\mathcal{J}$  is a subset of the set of possible nonzero codeword weights, i.e.  $\{1, \dots, L\}$ . Here  $m_k$  is the number of codewords with weight  $k$ , and  $n_{\bar{\rho}, k, t}$  is the number of codeword pairs with correlation coefficient  $\bar{\rho}$ , 1<sup>st</sup> codeword weight  $k$ , and the

2<sup>nd</sup> codeword weight  $t$ . Therefore, the bound for the uniform interleaving case is found by taking the expectation of both sides with respect to the interleaver, and maximizing over  $\bar{\mathcal{J}}$ .

### C. Subset Optimization with Other Bounds

The property depicted in (6) can be also used for improving the computational efficiency and tightness of some of the other lower bounds for error probability, namely Seguin's bound in [4] and Cohen-Merhav bounds in [5]. In particular, Seguin's bound can be tightened as follows:

$$P(\varepsilon|c_0) \geq \max_{\mathcal{J} \in \mathcal{I}_r} \sum_{i \in \mathcal{J}} \left( \frac{P(\varepsilon_i)^2}{\sum_{j \in \mathcal{J}} P(\varepsilon_i \cap \varepsilon_j)} \right), \quad (8)$$

where the related probabilities can be calculated as before.

## IV. SECOND ORDER DISTANCE SPECTRUM FOR ENSEMBLES OF TURBO CODES

As discussed in Sec. III in order to calculate tight lower bounds on error probability, one needs to find the second order distance spectrum of the code. We now propose a technique to this end for turbo code ensembles. We first discuss how this calculation can be done for convolutional codes, and then show how these results can be used to find average second order distance spectrum for turbo code ensembles with uniform interleaving.

### A. Convolutional Codes

Let  $N$  be the length of the input bit sequence. Let us denote the state transition matrix of the code with  $S$ . Using  $S$ , one can calculate the number of paths with input weight  $i$ , and output weight  $o$ . Let us denote this number with  $t(i, o)$ . We now consider a pair of information bit sequences and the resulting codeword pair. For a pair of information bit sequences, let  $i_{b_1 b_2}$  denote the number of places where the first information sequence's bits are  $b_1$  and the second information sequence's bits are  $b_2$ , with  $b_j \in \{0, 1\}$ . Clearly,  $i_{00} + i_{01} + i_{10} + i_{11} = N$ . For output sequences, we define  $o_{b_1 b_2}$  similarly. Let  $\bar{i} = [i_{00} \ i_{01} \ i_{10} \ i_{11}]$  denote the cross information weight vector, and  $\bar{o} = [o_{00} \ o_{01} \ o_{10} \ o_{11}]$  denote the cross output weight vector. We note that  $\bar{o}$  is defined like this for the sake of completeness. For finding the second order distance spectrum of a convolutional code, it is enough to include  $o_{11}$ ,  $d_1$ ,  $d_2$  in  $\bar{o}$ , where  $d_1/d_2$  is the weight of the first/second codeword in the pair in the output sequence.

Associated with  $S$ , one can find a joint state transition matrix  $\bar{S}$  that governs the evaluation of two codewords together.  $\bar{S}$  is the state transition matrix corresponding to the product of two independent trellises associated with  $S$ . The states in this product trellis are in the form  $(s^1, s^2)$ , where  $s^1/s^2$  denotes the state of the path for the first/second codeword. The entries of  $\bar{S}$  are either zero corresponding to the case where transition is not allowed or in the form  $I_{00}^{p_{00}} I_{01}^{p_{01}} I_{10}^{p_{10}} I_{11}^{p_{11}} O_{00}^{q_{00}} O_{01}^{q_{01}} O_{10}^{q_{10}} O_{11}^{q_{11}}$ . Here  $p_{ij}$  or  $q_{ij}$  values are either 0 or 1 depending on whether the corresponding quantities are 0 or 1. For instance, when both of the input bits are 0,  $p_{00} = 1$ . To illustrate the idea, the code trellis for the two-state code with the polynomial description  $1 + D$  and the corresponding product trellis for codeword pairs are shown in Fig. 2 and Fig. 3, respectively. We note that elimination in some of the terms included in the

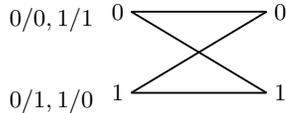


Fig. 2: Trellis of the rate  $R = 1$  code with the polynomial description  $1 + D$ .

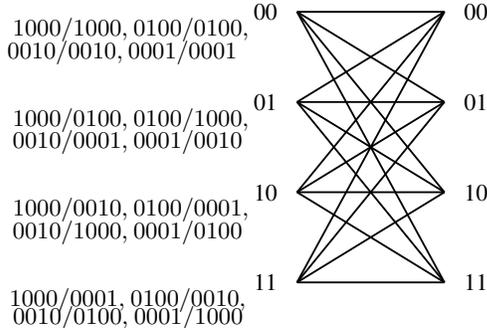


Fig. 3: Product trellis of the rate  $R = 1$  code with the polynomial description  $1 + D$ . Branch labels are in the form  $\bar{i}/\bar{o}$ .

entries of  $\bar{S}$  (and also the branch labels) in order to carry only the relevant information is possible.

By calculating the  $N^{\text{th}}$  power of  $\bar{S}$ , (and by accounting for trellis termination) one can associate the input cross information weight vector  $\bar{i}$  with the cross output weight vector  $\bar{o}$ . Hence one can find  $\bar{t}(\bar{i}, \bar{o})$ , the number of codeword pairs with cross information weights given by  $\bar{i}$ , and cross output weights given by  $\bar{o}$ . We note that using  $\bar{o}$ , one can calculate the correlation between the two codewords.

### B. Turbo Code Ensembles

We now present a technique to calculate the second-order distance spectrum for turbo codes with uniform interleaving. We illustrate the technique for  $R = 1/3$  parallel-concatenated codes. We assume that the information bit sequence goes through the first encoder without alteration, and is interleaved before it goes through the second encoder. We discuss the case of serially-concatenated codes at the end of the section.

Distance spectrum of uniformly interleaved turbo codes can be calculated by using the method proposed in [13]. To calculate the second order distance spectrum, we adopt the idea used for calculating the distance spectrum, but instead of considering a single codeword at a time, we propose to consider a codeword pair and make use of the calculations for convolutional codes above.

Let us consider a pair of information bit sequences with cross information weight vector  $\bar{i}$  entering the turbo encoder. This pair goes to the first encoder without any alteration, whereas both of the bit sequences are interleaved by the same interleaver before going through the second encoder. We note that despite the interleaving operation, for a given interleaver,  $\bar{i}$  does not change for the information bit sequence pairs entering the first encoder or the second encoder. Let  $\bar{t}_j(\bar{i}, \bar{o})$  denote the number of codewords with cross information weights given by  $\bar{i}$ , and cross parity weights given by  $\bar{o}$  for the encoder  $j$ . Let  $\bar{m}_p(\bar{i}, \bar{o}_1, \bar{o}_2)$  denote the average number of codeword pairs with information weight vector  $\bar{i}$ , first parity cross output weight vector  $\bar{o}_1$ , and second parity cross output weight vector

$\bar{o}_2$ , where entries of  $\bar{o}_j = [o_{00}^j o_{01}^j o_{10}^j o_{11}^j]$ ,  $j = 1, 2$ . Similar to the scenario where the average distance spectrum under uniform interleaving is determined by considering only one codeword,  $\bar{m}_p(\bar{i}, \bar{o}_1, \bar{o}_2)$  can be computed as follows

$$\bar{m}_p(\bar{i}, \bar{o}_1, \bar{o}_2) = \frac{\bar{t}_1(\bar{i}, \bar{o}_1) \bar{t}_2(\bar{i}, \bar{o}_2)}{\binom{N}{\bar{i}}}, \quad (9)$$

where  $\binom{N}{\bar{i}}$  denotes the multinomial coefficient  $\binom{N}{i_{00} i_{01} i_{10} i_{11}}$ . By using  $\bar{i}$ ,  $\bar{o}_1$ ,  $\bar{o}_2$ , one can calculate the correlation coefficient values associated with code pairs. To obtain the average number of codeword pairs with a given correlation coefficient  $\bar{\rho}$ , and the output weights  $w_1$  and  $w_2$ , we iterate over  $\bar{m}_p(\bar{i}, \bar{o}_1, \bar{o}_2)$  as follows

$$E[n_{\bar{\rho}, w_1, w_2}] = \sum_{\substack{[\bar{i}, \bar{o}_1, \bar{o}_2]: \\ d_1(\bar{i}, \bar{o}_1, \bar{o}_2) = w_1 \\ d_2(\bar{i}, \bar{o}_1, \bar{o}_2) = w_2 \\ f_\rho(\bar{i}, \bar{o}_1, \bar{o}_2) = \bar{\rho}}} \bar{m}_p(\bar{i}, \bar{o}_1, \bar{o}_2),$$

where  $d_j(\cdot)$  is the function that gives the weight of the  $j^{\text{th}}$  codeword in the pair

$$d_1(\bar{i}, \bar{o}_1, \bar{o}_2) \doteq i_{10} + i_{11} + o_{10}^1 + o_{11}^1 + o_{10}^2 + o_{11}^2 \quad (10)$$

$$d_2(\bar{i}, \bar{o}_1, \bar{o}_2) \doteq i_{01} + i_{11} + o_{01}^1 + o_{11}^1 + o_{01}^2 + o_{11}^2 \quad (11)$$

and  $f_\rho(\cdot)$  gives the correlation coefficient value

$$f_\rho(\bar{i}, \bar{o}_1, \bar{o}_2) \doteq \frac{i_{11} + o_{11}^1 + o_{11}^2}{d_1(i_{11}, \bar{o}_1, \bar{o}_2) d_2(i_{11}, \bar{o}_1, \bar{o}_2)}. \quad (12)$$

We now discuss how the second order distance spectrum can be found for the case of serially-concatenated convolutional codes. Here the information sequence first goes through first encoder, then the output of this encoder is interleaved, and the interleaved sequence is fed into the second encoder. To find the second order distance spectrum, once again we consider two codewords at a time, and cross weights of the sequences entering the interleaver. In particular, let  $\bar{m}_s(\bar{i}, \bar{w})$  the average number of codeword pairs with cross information weights  $\bar{i}$ , and cross output weights  $\bar{w}$ . Then for a serially-concatenated code with interleaver length  $N$ ,  $\bar{m}_s(\bar{i}, \bar{w})$  can be found as

$$\bar{m}_s(\bar{i}, \bar{w}) = \sum_{\bar{o}} \frac{\bar{t}_1(\bar{i}, \bar{o}) \bar{t}_2(\bar{o}, \bar{w})}{\binom{N}{\bar{o}}}. \quad (13)$$

The average number of output sequence pairs with given  $\bar{w}$  and  $\rho$  values can be found by summing over the other variables of interest as before.

## V. NUMERICAL RESULTS

We now present the bounds obtained by the proposed approach and compare them with the available bounds in the literature. One of the bounds we consider is the sphere packing bound in [1], which we refer as SP59. For calculation of the SP59 bound, we use the log domain approach proposed in [2]. The spherical bound proposed in [2] is not presented, since this bound is shown to be inferior to SP59 in the block lengths and rates considered here for target error probabilities in the order of  $10^{-4}$  [2]. To calculate the proposed bound, we choose the restricted set  $\mathcal{I}_r$  according to the discussion in Sec. III. After fixing the set  $\mathcal{I}_r$ , a proper subset  $\mathcal{J}$  is determined using the algorithms proposed in [6], [9].

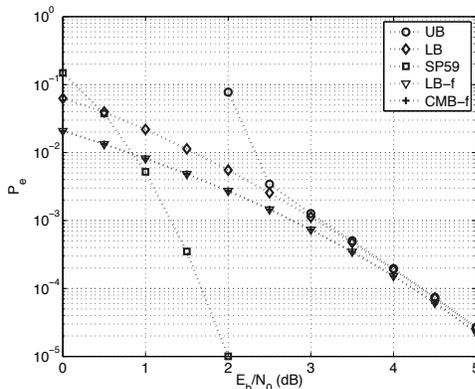


Fig. 4: Comparison of the proposed bounds with other bounds on the error probability,  $N = 100$ . UB: union bound, uniform interleaving. LB: Proposed lower bound, uniform interleaving. SP59: Shannon's sphere packing bound in [1]. LB-f: Proposed lower bound, fixed interleaver. CMB-f: Norm bound in [5] improved with exact  $\rho$  values and the subset selection approach, fixed interleaver.

In our numerical results, we consider the  $R = 1/3$  parallel turbo code with  $(5/7)_{\text{octal}}$  convolutional code as the component code at both encoders. The calculated bounds are presented in Fig. 4 for  $N = 100$ . We note that SP59 is calculated for a code with  $R = 1/3$  without accounting for the change in rate due to terminating zeros. If we had accounted for termination, the SP59 bound would have been even worse.

For the uniform interleaving case, the set  $\mathcal{I}_r$  consists of codewords with input weights  $\leq 3$ , and parity weights  $\leq 20$ . We observe that the proposed approach (LB) provides a significantly better performance than SP59 for moderate to high SNRs. Furthermore, the proposed bound shows a tight agreement with the union bound in the high SNR region for the codes considered here. We recall that bounds in [4], [5] are not directly applicable to the case of *ensemble* of codes [7], hence these comparisons cannot be made.

We now consider the fixed interleaver case. The interleaver is chosen arbitrarily. The set  $\mathcal{I}_r$  consists of codewords with input weight 2 with the pattern 1001 or the pattern 11. For the codewords with the pattern 11, we have only included the sequences where nonzero bits appear at the end of the input data sequence. Here first 1 appears as the  $(N-t)^{\text{th}}$  bit where  $t$  is chosen as 5, which is the minimum distance of the component code. Both of these input sequences are chosen because they are low weight and generate low weight parity sequences at the output of the 1<sup>st</sup> encoder. Hence both patterns are likely to create low weight codewords if the interleaver does not properly permute these sequences. In particular, the first input sequence pattern, in general, will create a long sequence of 1's, which continues until trellis termination. Here, due to placement of the pattern at the end of the sequence, these sequences of ones will be short. The pattern 1001 is chosen due to its self-termination property. Since the feedback polynomial of the component code is a divisor of  $1+D^3$ , any input sequence of the form  $10\dots 01$  where the number of 0's are  $3 \times k - 1$ ,  $k \geq 1 \in \mathbb{Z}_+$  generates an output with  $3 \times k + 1$  ones. Hence such an input sequence creates a low weight parity

sequence at the output of the first encoder.

We observe that the lower bounds for the fixed interleaver case (LB-f and CMB-f) provide significantly tighter performance than SP59 for moderate to high SNRs. The union (upper) bound is calculated for the case of uniform interleaving, hence it is not a true upper bound for the case with a fixed interleaver. Nevertheless, lower bounds are consistent with the union bound in terms of their high SNR behavior. We also observe that lower bounds give very close values. There is no known strict ordering between these bounds that holds in general (see for instance [10]), and this close performance is consistent with the fact that calculations are done over a very low number of codewords: the set  $\mathcal{I}_r$  has small cardinality, and some of these codewords are further eliminated from the set through optimization. Hence the error term with respect to the set  $\mathcal{I}_r$  that could be associated with each bound gets smaller.

## VI. CONCLUSIONS

We have investigated lower bounds on the error probability of turbo codes under ML decoding. To improve the existing bounds, we have proposed to use the exact second order distance spectrum and identification of a proper subset of error events. We have calculated lower bounds for turbo code ensembles with uniform interleaving, and specific turbo codes. The presented bounds show promising performance in both cases, and are illustrated to be significantly tighter than the sphere packing bounds for moderate to high SNRs for the block lengths considered.

## REFERENCES

- [1] C. Shannon, "Probability of error for optimal codes in a Gaussian channel," *Bell Syst. Tech. J.*, vol. 38, pp. 611–656, May 1959.
- [2] G. Wiechman and I. Sason, "An improved sphere-packing bound for finite-length codes over symmetric memoryless channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 5, pp. 1962–1990, 2008.
- [3] A. Valembois and M. Fossorier, "Sphere-packing bounds revisited for moderate block lengths," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 2998–3014, 2004.
- [4] G. Seguin, "A lower bound on the error probability for signals in white Gaussian noise," *IEEE Trans. Inf. Theory*, vol. 44, no. 7, pp. 3168–3175, 1998.
- [5] A. Cohen and N. Merhav, "Lower bounds on the error probability of block codes based on improvements on de Caen's inequality," *IEEE Trans. Inf. Theory*, vol. 50, no. 2, pp. 290–310, 2004.
- [6] F. Behnamfar, F. Alajaji, and T. Linder, "An efficient algorithmic lower bound for the error rate of linear block codes," *IEEE Trans. Commun.*, vol. 55, no. 6, pp. 1093–1098, 2007.
- [7] I. Sason and S. Shamai, "Performance analysis of linear codes under maximum-likelihood decoding: A tutorial," *Foundations and Trends in Communications and Information Theory*, vol. 3, no. 1-2, pp. 1–222, 2006.
- [8] E. G. Kounias, "Bounds for the probability of a union, with applications," *Ann. Math. Statist.*, vol. 39, no. 6, pp. 2154–2158, 1968.
- [9] H. Kuai, F. Alajaji, and G. Takahara, "Tight error bounds for nonuniform signaling over AWGN channels," *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2712–2718, 2000.
- [10] D. de Caen, "A lower bound on the probability of a union," *Discrete Mathematics*, vol. 169, no. 13, pp. 217 – 220, 1997.
- [11] O. Acikel and W. Ryan, "Punctured turbo-codes for BPSK/QPSK channels," *IEEE Trans. Commun.*, vol. 47, no. 9, pp. 1315–1323, 1999.
- [12] A. Reid, T. Gulliver, and D. Taylor, "Rate-1/2 component codes for nonbinary turbo codes," *IEEE Trans. Commun.*, vol. 53, no. 9, pp. 1417–1422, 2005.
- [13] D. Divsalar, S. Dolinar, J. McEliece, and F. Pollara, "Transfer function bounds on the performance of turbo codes," *TDA Progress Report 42-122*, pp. 44–55, Aug. 1995.