Tightened Upper Bounds on the ML Decoding Error Probability of Binary Linear Block Codes

Moshe Twitto Igal Sason Shlomo Shamai
Department of Electrical Enginnering
Technion, Haifa 32000, Israel
{tmoshe@tx, sason@ee, sshlomo@ee}.technion.ac.il

Abstract — **The performance of maximum-likelihood (ML) decoded binary linear block codes is addressed via the derivation of tightened upper bounds on their decoding error probability. The upper bounds on the block and bit error probabilities are valid for any memoryless, binary-input and output-symmetric communication channel. The effectiveness of these bounds is exemplified for ensembles of turbo-like codes.**

I. Introduction

Since the advent of information theory, the search for efficient coding systems has motivated the introduction of efficient bounding techniques tailored to specific codes or some carefully chosen ensembles of codes. The incentive for introducing and applying such bounds has strengthened with the introduction of various families of codes defined on graphs which closely approach the channel capacity with feasible complexity (e.g., turbo codes, repeat-accumulate codes, and low-density parity-check (LDPC) codes). Clearly, the desired bounds must not be subject to the union bound limitation, since for long blocks these ensembles of turbo-like codes perform reliably at rates which are considerably above the cutoff rate (R_0) of the channel (recalling that union bounds for long codes are not informative at the portion of the rate region above R_0, where the performance of these capacity-approaching codes is most appealing). Although maximum-likelihood (ML) decoding is in general prohibitively complex for long codes, the derivation of bounds on the ML decoding error probability is of interest, providing an ultimate indication of the system performance. Further, the structure of efficient codes is usually not available, necessitating efficient bounds on performance to rely only on basic features, such as the distance spectrum and the input-output weight enumeration function (IOWEF) of the examined code (for the evaluation of the block and bit error probabilities, respectively, of a specific code or ensemble).

A basic inequality which serves for the derivation of many previously reported upper bounds is the following:

$$\Pr(\text{word error}) \leq \Pr(\text{word error},\ \mathbf{y} \in \mathcal{R}) + \Pr(\mathbf{y} \notin \mathcal{R}) \quad (1)$$

where $\mathbf{y}$ denotes the received vector at the output of the receiver, and $\mathcal{R}$ is an arbitrary geometrical region which can be interpreted as a subset of the observation space. This category includes the tangential bound of Berlekamp where the volume $\mathcal{R}$ is a half-space separated by a plane, the sphere bound by Herzberg and Poltyrev [6] where $\mathcal{R}$ is a hyper-sphere, Poltyrev's tangential-sphere bound [8] (TSB) where $\mathcal{R}$ is a circular cone, and Divsalar's bound [1] where $\mathcal{R}$ is a hyper-sphere with an additional degree of freedom with respect to the center of the sphere.

Another approach is the Gallager bounding technique which provides a conditional upper bound on the ML decoding error probability given an arbitrary transmitted (length-N) codeword $\mathbf{c}_m$ ($P_{\mathrm{e}|m}$). The conditional decoding error probability is upper bounded by (see [3])

$$P_{\mathrm{e}|m} \leq \left(\sum_{m' \neq m} \sum_{\mathbf{y}} p_N(\mathbf{y}|\mathbf{c}_m)^{\frac{1}{\rho}} \ \psi_N^m(\mathbf{y})^{1-\frac{1}{\rho}} \ \left(\frac{p_N(\mathbf{y}|\mathbf{c}_{m'})}{p_N(\mathbf{y}|\mathbf{c}_m)} \right)^{\lambda} \right)^{\rho} \quad (2)$$

where $0 \leq \rho \leq 1$ and $\lambda \geq 0$. Here, $\psi_N^m(\mathbf{y})$ is an arbitrary probability tilting measure (which may depend on the transmitted codeword $\mathbf{c}_m$), and $p_N(\mathbf{y}|\mathbf{c})$ designates the transition probability measure of the channel. Connections between these two seemingly different bounding techniques in (1) and (2) were demonstrated in [14], showing that many previously reported bounds (or their Chernoff versions) whose derivation originally relied on the concept shown in inequality (1) can in fact be re-produced as particular cases of the bounding technique used in (2); to this end, one simply needs to choose the suitable probability tilting measure ψ_N^m which serves as the "kernel" for reproducing various previously reported bounds. The observations in [14] relied on some fundamental results which were reported by Divsalar [1].

The tangential-sphere bound (TSB) of Poltyrev often happens to be the tightest upper bound on the ML decoding error probability of block codes whose transmission takes place over a binary-input AWGN channel. However, in the random coding setting, it fails to reproduce the random coding exponent [5] while the second version of the Duman and Salehi (DS2) bound does (see [14]). The Shulman-Feder bound (SFB) can be derived as a particular case of the DS2 bound (see [14]), and it achieves the random coding error exponent. Though the SFB is informative for some structured linear block codes with good Hamming properties, it appears to be a loose bound, for example, when considering sequences of linear block codes whose minimum distance grows sub-linearly with the block length. However, the tightness of this bounding technique is significantly improved by combining the SFB with the union bound; this approach was exemplified for some structured ensembles of LDPC codes (see e.g., [7] and the proof of [12, Theorem 2.2]).

In this paper, we introduce improved upper bounds on both the bit and block error probabilities. Section II presents some preliminary material. In Section III, we introduce an upper bound on the block error probability which is in general tighter than the SFB, and combine the resulting bound with the union bound. Similarly, an appropriate upper bound on the bit error probability is introduced. By applying the new bounds to ensembles of turbo-like codes over the binary-input AWGN channel, we demonstrate in Section IV the usefulness of the new bounds, especially for some coding structures of high rates.

For a tutorial paper on performance bounds of linear codes, the reader is referred to [11]. Due to space limitations, the proofs of the new bounds in this paper and further discussion are provided in [15]. Moreover, the effect of expurgating the distance spectrum is exemplified in [15], showing that for some ensembles, this expurgation further tightens the bounds.

II. Preliminaries

It is well known that at rates below the channel capacity, the block error probability of the ensemble of fully random block codes vanishes exponentially with the block length. In the following, the Shulman and Feder bound is introduced, as a preparatory step to the continuation of our discussion.

We consider here the transmission of a binary linear block code $\mathcal{C}$ where the communication takes place over a memoryless binary-input output-symmetric (MBIOS) channel. The analysis refers to the decoding error probability under soft-decision ML decoding.

The Shulman and Feder bound (SFB) [13] on the block error probability of an (N, K) binary linear block code $\mathcal{C}$, transmitted over a memoryless channel is given by

$$P_{\mathrm{e}} \leq 2^{-NE_{\mathrm{r}}(R+\frac{\log \alpha(\mathcal{C})}{N})} \tag{3}$$

where

$$E_{\mathrm{r}}(R) = \max_{0\leq\rho\leq 1} \left(E_0(\rho) - \rho R\right) \tag{4}$$

$$E_0(\rho) \triangleq -\log_2 \left\{ \sum_y \left[\frac{1}{2} p(y|0)^{\frac{1}{1+\rho}} + \frac{1}{2} p(y|1)^{\frac{1}{1+\rho}} \right]^{1+\rho} \right\}. \tag{5}$$

E_{r} is the random coding error exponent [5], $R \triangleq \frac{K}{N}$ designates the code rate in bits per channel use, and

$$\alpha(\mathcal{C}) \triangleq \max_{1\leq l\leq N} \frac{A_l}{2^{-N(1-R)} \binom{N}{l}}. \tag{6}$$

In the RHS of (6), $\{A_l\}$ denotes the distance spectrum of the code. Hence, for fully random block codes, $\alpha(\mathcal{C})$ is equal to 1, and the Shulman-Feder bound (SFB) particularizes to the random coding bound [5]. In general, the parameter $\alpha(\mathcal{C})$ in the SFB (3) measures the maximal ratio of the distance spectrum of a code (or ensemble) and the average distance spectrum which corresponds to fully random block codes of the same block length and rate.

The original proof of the SFB is quite involved. In [14], a simpler proof of the SFB is derived, and by doing so, the simplified proof reproduces the SFB as a particular case of the DS2 bound (see Eq. (2)). To this end, we choose a suitable tilting measure ψ_N^m in (2) which provides an elegant proof of the SFB (see [14, Section 4A]); this proof also shows that the SFB forms as a particular case of the DS2 bound in (2) [3, 14].

In order to tighten the SFB bound for linear block codes, Miller and Burshtein [7] suggested to partition the original linear code $\mathcal{C}$ into two subcodes, namely $\mathcal{C}'$ and $\mathcal{C}''$; the subcode $\mathcal{C}'$ contains the all-zero codeword and all the codewords with Hamming weights of $l \in \mathcal{U} \subseteq \{1, 2, ..., N\}$, while $\mathcal{C}''$ contains the other codewords which have Hamming weights of $l \in \mathcal{U}^{\mathrm{c}} = \{1, 2, ..., N\} \setminus \mathcal{U}$ and the all-zero codeword. From the symmetry of the channel, the union bound provides the following upper bound on the ML decoding error probability:

$$P_{\mathrm{e}} = P_{\mathrm{e}|0} \leq P_{\mathrm{e}|0}(\mathcal{C}') + P_{\mathrm{e}|0}(\mathcal{C}'') \tag{7}$$

where $P_{\mathrm{e}|0}(\mathcal{C}')$ and $P_{\mathrm{e}|0}(\mathcal{C}'')$ designate the conditional ML decoding error probabilities of $\mathcal{C}'$ and $\mathcal{C}''$, respectively, given that the all zero codeword is transmitted. We note that although the code $\mathcal{C}$ is linear, its two subcodes $\mathcal{C}'$ and $\mathcal{C}''$ are in general *non-linear.*

III. Improved Upper Bounds

As a continuation of Section II, one can rely on different upper bounds on the conditional error probabilities $P_{\mathrm{e}|0}(\mathcal{C}')$ and $P_{\mathrm{e}|0}(\mathcal{C}'')$, i.e., we may bound $P_{\mathrm{e}|0}(\mathcal{C}')$ by the SFB, and rely on an alternative approach to obtain an upper bound on $P_{\mathrm{e}|0}(\mathcal{C}'')$. For example, if we consider the binary-input AWGN channel, then the TSB (or even union bounds) may be used in order to obtain an upper bound on the conditional error probability $P_{\mathrm{e}|0}(\mathcal{C}'')$ which corresponds to the subcode $\mathcal{C}''$. In order to obtain the tightest bound in this approach, one should look for an optimal partitioning of the original code $\mathcal{C}$ into two subcodes, based on the distance spectrum of $\mathcal{C}$. The solution of the problem is quite tedious, because in general, if the subset $\mathcal{U}$ can be an arbitrary subset of the set of integers $\{1, \ldots, N\}$, then one has to compare $\sum_{i=0}^{N} \binom{N}{i} = 2^N$ different possibilities for $\mathcal{U}$. However, we may use practical optimization schemes to obtain good results which may improve the tightness of both the SFB and TSB. By relying on the SFB in order to obtain an upper bound on the conditional decoding error probability of the subcode $\mathcal{C}'$ (i.e., an upper bound on $P_{\mathrm{e}|0}(\mathcal{C}')$), one can see from (6) that the parameter α in this case is equal to the maximal ratio of the distance spectrum of the original code $\mathcal{C}$ (or ensemble) and the corresponding binomial distribution which represents the average distance spectrum of fully random block codes; this maximal value is taken w.r.t. the Hamming weights referred to the set $\mathcal{U}$.

An easy way to make an efficient partitioning of a linear code $\mathcal{C}$ is to compare its distance spectrum (or the average distance spectrum for an ensemble of linear codes) with the average distance spectrum of the ensemble of fully random block codes of the same rate and block length. Let us designate the latter distance spectrum by

$$B_l \triangleq 2^{-N(1-R)} \binom{N}{l} \qquad l = 0, 1, \quad N. \tag{8}$$

Then, it is suggested to partition the set of codewords of $\mathcal{C}$ in a way so that all the codewords with Hamming weight l for which $\frac{A_l}{B_l}$ is smaller than some threshold (which should be larger than 1 but close to it) are associated with a subcode $\mathcal{C}'$, and the other codewords are associated with $\mathcal{C}''$ which is the complementary subcode of $\mathcal{C}'$ w.r.t. $\mathcal{C}$. The following algorithm is proposed for the calculation of the upper bound on the block error probability under ML decoding:

<u>**Algorithm 1**</u>

1. Set

$$\mathcal{U} = \Phi, \quad \mathcal{U}^{\mathrm{c}} = \{1, 2, ...N\}, \quad l = 1$$

where Φ designates an empty set, and set the initial value of the upper bound to be equal to 1.

2. Compute the ratio $\frac{A_l}{B_l}$ where $\{A_l\}$ is the distance spectrum of the binary linear block code (or the average distance of an ensemble of such codes), and $\{B_l\}$ is the binomial distribution introduced in (8).

3. If this ratio is smaller than some threshold (where the value of the threshold is typically set to be slightly larger than 1), then the element l is added to the set $\mathcal{U}$, i.e.,

$$\mathcal{U} := \mathcal{U} + \{l\}, \quad \mathcal{U}^{\mathrm{c}} := \mathcal{U}^{\mathrm{c}} \setminus \{l\}.$$

4. Update correspondingly the upper bound in the RHS of (7) (we will derive later the appropriate upper bounds on $P_{\mathrm{e}|0}(\mathcal{C}')$ and $P_{\mathrm{e}|0}(\mathcal{C}'')$.

5. Set the bound to be the minimum between the RHS from Step 4 and its previous value.

6. Set $l = l + 1$ and go to Step 2.

7. The algorithm terminates when l gets the value N (i.e., the block length of the code) or actually, the maximal value of l for which A_l does not vanish.[1]

From the discussion above, it is clear that the combination of the SFB with another upper bound has the potential to tighten the overall upper bound on the ML decoding probability. This improvement is expected to be especially pronounced for ensembles whose average distance spectrum resembles the binomial distribution over a relatively large range of Hamming weights, but whose average distance spectrum deviates significantly from the binomial distribution for relatively low and large Hamming weights (e.g., ensembles of uniformly interleaved turbo codes possess this property, as indicated in [9, Section 4]). This bounding technique was successfully applied by Miller and Burshtein [7] and also by Sason and Urbanke [12] to ensembles of regular low-density parity-check (LDPC) codes where the SFB was combined with union bounds. If the range of Hamming weights where the average distance spectrum of an ensemble resembles the binomial distribution is relatively large, then according to the above algorithm, one would expect that $\mathcal{C}'$ typically contains a very large fraction of the overall number of the codewords of a code from this ensemble. Hence, in order to obtain an upper bound on $P_{\mathrm{e}|0}(\mathcal{C}'')$, where $\mathcal{C}''$ is expected to contain a rather small fraction of the codewords in $\mathcal{C}$, we may use a simple bound such as the union bound while expecting not to pay a significant penalty in the tightness of the overall bound on the decoding error probability (P_{e}).

The following bound introduced in Theorem III.1 is derived as a particular case of the DS2 bound [3]. The beginning of its derivation is similar to the steps in [14, Section 4A], but we later deviate from the analysis there in order to modify the SFB. We finally obtain a tighter version of the SFB.

Theorem III.1 (Modified Shulman and Feder Bound) Let $\mathcal{C}$ be a binary linear block code of length N and rate R, and let $\{A_l\}$ designate its distance spectrum. Let this code be partitioned into two subcodes, $\mathcal{C}'$ and $\mathcal{C}''$, where $\mathcal{C}'$ contains the all-zero codeword and all the other codewords of $\mathcal{C}$ whose Hamming weights are in an arbitrary set $\mathcal{U} \subseteq \{1, 2, \ldots, N\}$; the second subcode $\mathcal{C}''$ contains the all-zero codeword and the other codewords of $\mathcal{C}$ which are not included in $\mathcal{C}'$. Assume that the communication takes place over a memoryless binary-input output-symmetric (MBIOS) channel with transition probability measure $p(y|x)$, $x \in \{0, 1\}$. Then, the block error probability of $\mathcal{C}$ under ML decoding is upper bounded by

$$P_{\mathrm{e}} \leq P_{\mathrm{e}|0}(\mathcal{C}') + P_{\mathrm{e}|0}(\mathcal{C}'')$$

where for $0 \leq \rho \leq 1$

$$\begin{aligned} P_{\mathrm{e}|0}(\mathcal{C}') \leq \mathrm{SFB}(\rho) \, \cdot & \\ \cdot \left[\sum_{l \in \mathcal{U}} \binom{N}{l} \left(\frac{A(\rho)}{A(\rho)+B(\rho)} \right)^{l} \left(\frac{B(\rho)}{A(\rho)+B(\rho)} \right)^{N-l} \right]^{\rho} & \qquad (9) \\ A(\rho) \triangleq \sum_{y} \left\{ [p(y|0)p(y|1)]^{\frac{1}{1+\rho}} \left[\frac{1}{2} p(y|0)^{\frac{1}{1+\rho}} + \frac{1}{2} p(y|1)^{\frac{1}{1+\rho}} \right]^{\rho-1} \right\} & \\ B(\rho) \triangleq \sum_{y} \left\{ p(y|0)^{\frac{2}{1+\rho}} \left[\frac{1}{2} p(y|0)^{\frac{1}{1+\rho}} + \frac{1}{2} p(y|1)^{\frac{1}{1+\rho}} \right]^{\rho-1} \right\}. & \end{aligned}$$

The multiplicative term, $\mathrm{SFB}(\rho)$, in the RHS of (9) designates the conditional Shulman-Feder upper bound of the subcode $\mathcal{C}'$ given the transmission of the all-zero codeword, i.e.,

$$\mathrm{SFB}(\rho) = 2^{-N\left(E_0(\rho) - \rho\left(R + \frac{\log(\alpha(\mathcal{C}'))}{N}\right)\right)}, \quad 0 \leq \rho \leq 1 \qquad (10)$$

and E_0 is introduced in (5). An upper bound on the conditional block error probability for the subcode $\mathcal{C}''$, $P_{\mathrm{e}|0}(\mathcal{C}'')$, can be either a standard union bound or any other bound.

Discussion: In [7, Theorem 1], Miller and Burshtein introduced an upper bound which combines the Shulman and Feder bound with the union bound, and applied it to two ensembles of LDPC codes. In [12, Theorem 2], Sason and Urbanke applied the same bounding technique to obtain an upper bound on the average ML decoding error probability of Gallager's ensemble of regular LDPC codes. Based on this bound which applies to *optimal ML decoding* over MBIOS channels, it was proved in [7, 12] that for suitable constructions of these ensembles, the average block error probability vanishes asymptotically (as the block length tends to infinity) at rates which can be made arbitrarily close to the channel capacity.

The improvement of the bound introduced in Theorem III.1 stems from the introduction of the ρ-dependent factor which multiplies $\mathrm{SFB}(\rho)$ in the RHS (9); this multiplicative term cannot exceed 1 since

$$\begin{aligned} & \sum_{l \in \mathcal{U}} \binom{N}{l} \left(\frac{A(\rho)}{A(\rho)+B(\rho)} \right)^{l} \left(\frac{B(\rho)}{A(\rho)+B(\rho)} \right)^{N-l} \\ & \leq \sum_{l=0}^{N} \binom{N}{l} \left(\frac{A(\rho)}{A(\rho)+B(\rho)} \right)^{l} \left(\frac{B(\rho)}{A(\rho)+B(\rho)} \right)^{N-l} = 1. \end{aligned}$$

This multiplicative factor which appears in the new bound (9) is useful for finite-length codes with small to moderate block lengths. The upper bound (9) on $P_{\mathrm{e}|0}(\mathcal{C}')$ is clearly at least as tight as the corresponding conditional SFB. We refer to the upper bound (9) as the modified SFB (MSFB). The conditional block error probability of the subcode $\mathcal{C}''$, given that the all-zero codeword is transmitted, can be bounded by a union bound or any improved upper bound conditioned on the transmission of the all-zero codeword. In general, one is looking for an appropriate balance between the two upper bounds on $P^{(1)}_{\mathrm{e}|0}$ and $P^{(2)}_{\mathrm{e}|0}$ (see Algorithm 1). The improvement that is achieved by using the MSFB instead of the corresponding SFB is exemplified later (see Section IV) for ensembles of uniformly interleaved turbo codes.

An Upper Bound on Bit Error Probability: Let $\mathcal{C}$ be a binary linear block code whose transmission takes place over an arbitrary MBIOS channel, and let P_{b} designate the bit error probability of $\mathcal{C}$ under ML decoding. In [10, Appendix A],

[1] The number of steps can be reduced by factor of 2 for binary linear codes which contain the all-ones codeword (hence maintain the property $A_l = A_{N-l}$). For such codes, the update equation in Step 3 becomes: $\mathcal{U} := \mathcal{U} + \{l, N-l\}$, $\mathcal{U}^{\mathrm{c}} := \mathcal{U}^{\mathrm{c}} - \{l, N-l\}$ and the algorithm terminates when l gets the value $\lceil \frac{N}{2} \rceil$.

Sason and Shamai derived an upper bound on the bit error probability of systematic, binary linear block codes which are transmitted over fully interleaved fading channels with perfect channel state information at the receiver. Here we generalize the result of [10] for arbitrary MBIOS channels.

Theorem III.2 (The SFB version on the BER) Let $\mathcal{C}$ be a binary linear block code of length N and dimension K, and assume that the transmission of the code takes place over an MBIOS channel. Let $A_{w,l}$ designate the number of codewords in $\mathcal{C}$ which are encoded by information bits whose Hamming weight is w and their Hamming weight after encoding is l. Then, the bit error probability of $\mathcal{C}$ under ML decoding is upper bounded by

$$P_{\mathrm{b}} \leq 2^{-NE_{\mathrm{r}}\left(R+\frac{\log \alpha_{\mathrm{b}}(\mathcal{C})}{N}\right)} \tag{11}$$

where E_{r} denotes the ransom coding error exponent (see (4)), $R=\frac{K}{N}$ is the code rate of $\mathcal{C}$, and

$$\alpha_{\mathrm{b}}(\mathcal{C}) \triangleq \max_{0\leq l\leq N} \frac{A'_l}{2^{-N(1-R)}\binom{N}{l}}, \qquad A'_l \triangleq \sum_{w=1}^{K}\left(\frac{w}{K}\right)A_{w,l}.$$

Similarly to the derivation of the combined upper bound on the block error probability in Theorem III.1, we suggest to partition the code into two subcodes in order to get improved upper bounds on the bit error probability. Since the code is linear and the channel is MBIOS, the conditional decoding error probability is independent of the transmitted codeword (so, we assume again that the all-zero codeword is transmitted). By the union bound

$$P_{\mathrm{b}} = P_{\mathrm{b}|0} \leq P_{\mathrm{b}|0}(\mathcal{C}') + P_{\mathrm{b}|0}(\mathcal{C}'') \tag{12}$$

where $P_{\mathrm{b}|0}(\mathcal{C}')$ and $P_{\mathrm{b}|0}(\mathcal{C}'')$ denote the conditional ML decoding bit error probabilities of two disjoint subcodes $\mathcal{C}'$ and $\mathcal{C}''$ which partition the block code $\mathcal{C}$ (except that these two subcodes have the all-zero vector in common), given that the all-zero codeword is transmitted. The construction of the subcodes $\mathcal{C}'$ and $\mathcal{C}''$ is aimed to minimize the overall upper bound on the bit error probability in (12).

Upper bound on $P_{\mathrm{b}|0}(\mathcal{C}')$: Let $A_{w,l}$ designate the number of codewords of Hamming weight l which are encoded by a sequence of information bits of Hamming weight w. Similarly to the discussion on the block error probability, we use the bit-error version of the SFB (see Eq. (11)) as an upper bound on $P_{\mathrm{b}|0}(\mathcal{C}')$. From Theorem III.2, it follows that the conditional bit error probability of the subcode $\mathcal{C}'$, given that the all-zero codeword is transmitted is upper bounded by

$$P_{\mathrm{b}|0}(\mathcal{C}') \leq 2^{-NE_{\mathrm{r}}\left(R+\frac{\log \alpha_{\mathrm{b}}(\mathcal{C}')}{N}\right)} \tag{13}$$

where

$$\alpha_{\mathrm{b}}(\mathcal{C}') \triangleq \max_{l\in\mathcal{U}} \frac{A'_l(\mathcal{C}')}{B_l}\ ,$$
$$A_l{}'(\mathcal{C}') \triangleq \begin{cases} \sum_{w=1}^{NR}\left(\frac{w}{NR}\right)A_{w,l} & \text{if } l\in\mathcal{U} \\ 0 & \text{otherwise}\end{cases} \tag{14}$$

and the set $\mathcal{U}$ in (14) stands for an arbitrary subset of $\{1,\ldots,N\}$.

Upper bound on $P_{\mathrm{b}|0}(\mathcal{C}'')$: We may bound the conditional bit error probability of the subcode $\mathcal{C}''$, $P_{\mathrm{b}|0}(\mathcal{C}'')$, by an improved upper bound. For the binary-input AWGN, the modified version of the TSB, as shown in [9] is an appropriate bound. This bound is the same as the original TSB in [8], except that the distance spectrum $\{A_l\}$ is replaced by $\{A_l{}'(\mathcal{C}'')\}$ where

$$A_l{}'(\mathcal{C}'') \triangleq \begin{cases} \displaystyle\sum_{w=1}^{NR}\left(\frac{w}{NR}\right)A_{w,l} & \text{if } l\in\mathcal{U}^{\mathrm{c}} \\ 0 & \text{otherwise}\end{cases} \tag{15}$$

and $\mathcal{U}^{\mathrm{c}}$ stands for an complementary set of $\mathcal{U}$ in (14), i.e., $\mathcal{U}^{\mathrm{c}} \triangleq \{1,\ldots,N\}\setminus\mathcal{U}$. For the binary-input AWGN channel, the TSB on the conditional bit error probability admits the final form in [9]. As the simplest alternative to obtain an upper bound on the conditional bit error probability of the subcode $\mathcal{C}'$ given that the all-zero codeword is transmitted, one may use the union bound (UB) for the binary-input AWGN channel

$$\begin{aligned} P_{\mathrm{b}|0}(\mathcal{C}'') &\leq \sum_{w=1}^{NR}\left(\frac{w}{NR}\right)\sum_{l\in\mathcal{U}^{\mathrm{c}}} A_{w,l}\, Q\left(\sqrt{\frac{2lRE_{\mathrm{b}}}{N_0}}\right) \\ &= \sum_{l=1}^{N} A'_l(\mathcal{C}'')\, Q\left(\sqrt{\frac{2lRE_{\mathrm{b}}}{N_0}}\right)\end{aligned}$$

where E_{b} is the energy per information bit and $\frac{N_0}{2}$ is the two-sided spectral power density of the additive noise.

In order to tighten the upper bound (13), we obtain the bit-error version of the MSFB (see Eq. (9)), by following the steps of the derivation of Theorem III.1. A further tightening of the bound on the bit error probability leads to the following theorem:

Theorem III.3 (Simplified DS2 Bound) Let $\mathcal{C}$ be a binary linear block code of length N and rate R, and let $A_{w,l}$ designate the number of codewords which are encoded by information bits whose Hamming weight is w and their Hamming weight after encoding is l (where $0\leq w\leq NR$ and $0\leq l\leq N$). Let the code $\mathcal{C}$ be partitioned into two subcodes, $\mathcal{C}'$ and $\mathcal{C}''$, where $\mathcal{C}'$ contains all the codewords in $\mathcal{C}$ with Hamming weight $l\in\mathcal{U}\subseteq\{1,2,\ldots,N\}$ and the all-zero codeword, and $\mathcal{C}''$ contains all the other codewords of $\mathcal{C}$ and the all-zero codeword. Let

$$A_l{}'(\mathcal{C}') \triangleq \begin{cases} \sum_{w=1}^{NR}\left(\frac{w}{RN}\right)A_{w,l} & \text{if } l\in\mathcal{U} \\ 0 & \text{otherwise}\end{cases}\ . \tag{16}$$

Assume that the communication takes place over an MBIOS channel. Then, under ML decoding, the bit error probability of $\mathcal{C}$, is upper bounded by

$$P_{\mathrm{b}} \leq P_{\mathrm{b}|0}(\mathcal{C}') + P_{\mathrm{b}|0}(\mathcal{C}'')$$

where

$$P_{\mathrm{b}|0}(\mathcal{C}') \quad\leq\quad 2^{-N\left(E_0(\rho)-\rho\left(R+\frac{\log\bar{\alpha}_\rho(\mathcal{C}')}{N}\right)\right)},\ \ 0\leq\rho\leq 1 \tag{17}$$

$$\bar{\alpha}_\rho(\mathcal{C}') \triangleq \sum_{l=0}^{N}\left\{\frac{A'_l(\mathcal{C}')}{2^{-N(1-R)}\binom{N}{l}}\cdot\binom{N}{l}\left(\frac{A(\rho)}{A(\rho)+B(\rho)}\right)^{l}\left(\frac{B(\rho)}{A(\rho)+B(\rho)}\right)^{N-l}\right\}. \tag{18}$$

$A(\rho), B(\rho)$ and E_0 are introduced in Theorem III.1. As before, an upper bound on the conditional bit error probability for the subcode $\mathcal{C}''$, $P_{\mathrm{b}|0}(\mathcal{C}'')$, can be either a union bound or any other improved bound.

Evidently, the upper bound (17) is tighter than the bit-error version of the SFB in (13), because $\bar{\alpha}_\rho(\mathcal{C}')$ which is the expected value of $\frac{A_l'(\mathcal{C}')}{B_l}$ is not larger than $\alpha_{\rm b}(\mathcal{C}')$ which is the maximal value of $\frac{A_l'(\mathcal{C}')}{B_l}$.

IV. Numerical Results

This section presents numerical results regarding improved upper bounds on the ML decoding error probability of linear block codes. We apply the bounds introduced in Sections III to ensembles of turbo codes with components which are linear binary block codes. It is assumed here that the encoded bits are BPSK modulated, transmitted over an AWGN channel, and coherently detected.

Figures 1 presents improved upper bound for the ensemble of uniformly interleaved turbo (parallel concatenated) codes, having two identical component codes chosen uniformly at random and independently from the ensemble of systematic binary linear block codes. We assume that the parameters of the overall code are (N, K), so the parameters of its component codes are $(\frac{N+K}{2}, K)$. In addition, the length of the interleaver is K. The input-output weight enumeration of the considered ensemble is given in closed form in [15, Appendix] (this result was originally derived by Soljanin and Urbanke, but was not reported in the literature). We apply the improved bounds on the performance bounds to this ensemble, where we choose the parameters to be $(N, K) = (1144, 1000)$ (hence, the rate of the parallel concatenated ensemble is $R = 0.8741$ bits per channel use). The plots of various upper bounds on the block and bit error probabilities are shown in Fig. 1. The new bounds provide in this case the tightest reported upper bounds on the block and bit error probabilities. For the block error probability, the upper bound which combines the MSFB with the union bound (see Theorem III.1) achieves a gain of 0.10 dB over the TSB, referring to a block error probability of 10^{-4}. Referring to bounds on the bit error probability, a gain of 0.11 dB is obtained for a BER of 10^{-4}; this gain over the TSB is obtained by the bound which combines the union bound with the simplified DS2 bound (see Theorem III.3).

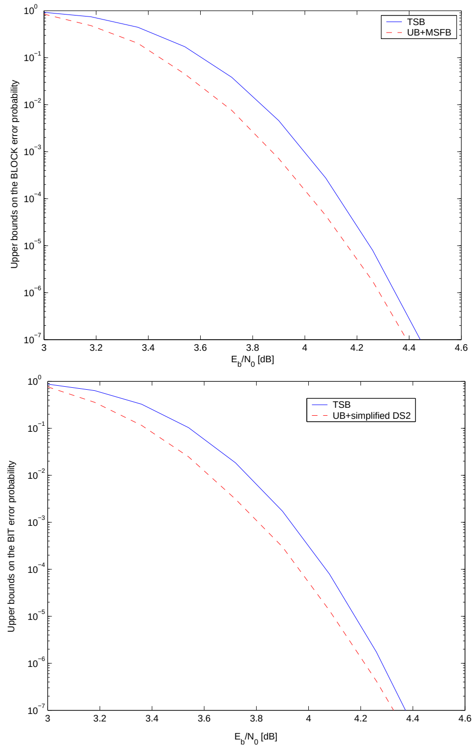

Figure 1: Comparison between upper bounds on the block and bit error probabilities of an ensemble of turbo codes whose two components are chosen uniformly at random from the ensemble of (1072, 1000) binary systematic linear block codes; its overall code rate is 0.8741 bits per channel use. The compared bounds under ML decoding are the tangential-sphere bound (TSB), and the upper bounds of Theorem III.1 and Theorem III.3 (for the upper and lower plots, referring to bounds on the block and bit error probabilities, respectively).

References

[1] D. Divsalar, "A simple tight bound on error probablity of block codes with applications to turbo codes," *TMO progress report*, 42–139 NASA, JPL, Pasadena, CA, USA, November 1999

[2] 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.

[3] T. M. Duman,"Turbo codes and turbo coded modulation systems: Analysis and performance bounds," Ph.D. dissertation, Elect. Comput. End. Dep., Northeastern University, Boston, MA, USA, May 1998.

[4] R. G. Gallager,"*Low-Density Parity-Check Codes*," Cambridge, MA, USA, MIT press, 1963.

[5] R. G. Gallager, "A simple derivation of the coding theorem and some applications,"*IEEE Trans. on Information Theory*, vol. 11, no. 1, pp. 3–18, January 1965

[6] H. Herzberg and G. Poltyrev, "Techniques of bounding the probability of decoding error for block modulation structures", *IEEE trans. on Information Theory,* vol. 40, no. 3, pp. 903–911, May 1994.

[7] G. Miller and D. Burshtein, "Bounds on the ML decoding error probability of LDPC codes," *IEEE Trans.on Information Theory*, vol. 47, no. 7, pp. 2696–2710, November 2001.

[8] G. Poltyrev, "Bounds on the decoding error probability of linear binary codes via their spectra," *IEEE Trans. on Information Theory*, vol. 40, pp. 1284–1292, July 1994.

[9] I. Sason and S. Shamai, "Improved upper bounds on the ML decoding error probability of parallel and serial concatenated Turbo codes via their ensemble distance spectrum," *IEEE Trans. on Information Theory*, vol. 46, no. 1, pp. 24–47, January 2000.

[10] —, "On Improved bounds on decoding error probability of block codes over interleaved fading channels, with applications to Turbo-like codes," *IEEE Trans. on Information Theory*, vol. 47, no. 6, pp. 2275–2299, September 2001.

[11] —, "Performance analysis of linear codes under maximum-likelihood decoding: a tutorial," submitted to *Foundations and Trends in Communications and Information Theory*, NOW Publishers, Delft, the Netherlands, December 2005.

[12] I. Sason and R. Urbanke, "Parity-check density versus performance of binary linear block codes over memoryless symmetric channels," *IEEE Trans. on Information Theory*, vol. 49, no. 7, pp. 1611–1635, July 2003.

[13] N. Shulman and M. Feder, "Random coding techniques for nonrandom codes,"*IEEE Trans. on Information Theory*, vol. 45, no. 6, pp. 2101–2104, September 1999.

[14] S. Shamai and I. Sason, "Variations on the Gallager bounds, connections, and applications, " *IEEE Trans. on Information Theory*, vol. 48, no. 12, pp. 3029–3051, December 2002.

[15] M. Twitto, I. Sason and S. Shamai, "Tightened upper bounds on the ML decoding error probability of binary linear codes," submitted to *IEEE Trans. on Information Theory.*