ELSEVIER

Physica A 302 (2001) 22–34

PHYSICA A

www.elsevier.com/locate/physa

Variations on the Gallager bounds with some applications

S. Shamai*, I. Sason

Department of Electrical Engineering, Technion, Haifa 32000, Israel

Abstract

By generalizing the framework of the second version of the Duman–Salehi bound encompassing also deterministic and random codes, we demonstrate its rather broad features and show that this variation provides the natural bridge between the 1961 and 1965 Gallager bounds. This approach entails a natural geometric interpretation, encompassing also a large class of efficient recent bounds (or their Chernoff versions), which are demonstrated to be special cases of the generalized second version of the Duman–Salehi bound. Implications and applications of these observations are pointed out, referring to known bounds as well as a novel extended version of the Shulman–Feder bound. © 2001 Elsevier Science B.V. All rights reserved.

1. Introduction

Since the error performance of efficiently coded communication systems rarely admits exact expressions, tight analytical bounds emerge as a useful theoretical and engineering tool for assessing performance and for acquiring insight into the effect of the main system parameters. Specific good codes are not easily identified, giving rise to ensembles of codes over which performance should be accurately assessed. The motivation for introducing and applying such bounds has strengthened with the recent introduction of turbo codes and the rediscovery of the low density parity check (LDPC) codes. Clearly, the useful bounds must not be subjected to the union bound limitations such as the cutoff rate limit for long enough codes, as these families of codes perform considerably beyond the cutoff rate and approach the capacity limit. Useful bounds should also be applicable to either deterministic codes or ensembles of codes relying on basic features such as the distance spectrum or input–output weight enumeration functions (IOWEF)

* Corresponding author.
E-mail addresses: sshlomo@ee.technion.ac.il (S. Shamai), eeigal@tiger.technion.ac.il (I. Sason).

PII: S0378-4371(01)00437-X

of the examined codes. Among the classical techniques is the Fano–Gallager [1,2] (referred to as the 1961 Fano–Gallager and the 1965 Gallager [3] bounds. Several such bounds have recently been introduced (see Refs. [1,2,4–19] and references in Ref. [16]).

In our work, we focus on the second version of the recently introduced bounds by Duman–Salehi [5,9,14], whose derivation is based on the 1965 Gallager bounding technique [3]. Although originally derived for binary signaling over an additive white Gaussian noise (AWGN) channel, we demonstrate here its rather broad features in a variety of aspects. In our setting, we shall use and build on some of the interesting results in Ref. [5], where insightful observations on the Duman–Salehi bounding technique are provided and some efficient and easily applicable bounds are introduced.

2. The Gallager bounds and the Duman and Salehi variation

2.1. The 1965 Gallager bound

The maximum likelihood (ML) decoding error probability conditioned on an arbitrary transmitted (length — N) codeword $\underline{x}^m$ ($P_{e|m}$), is upper bounded by the 1965 Gallager bound [3]:

$$P_{e|m} \leqslant \sum_{\underline{y}} p_N(\underline{y}|\underline{x}^m) \left(\sum_{m' \neq m} \left(\frac{p_N(\underline{y}|\underline{x}^{m'})}{p_N(\underline{y}|\underline{x}^m)} \right)^{\lambda} \right)^{\rho} , \tag{1}$$

where $\lambda, \rho \geqslant 0$. Here, $\underline{y}$ designates the observation vector (with N components) and $p_N(\underline{y}|\underline{x})$ is the channel's transition probability measure. The upper bound (1) is usually not easily evaluated in terms of basic features of particular codes, but for example, orthogonal codes and the special case, where $\rho = 1$ and $\lambda = \frac{1}{2}$ (yielding the Bhattacharyya-union bound). For ensembles of random codes, with M independent codewords selected with the distribution $q_N(\underline{x})$, the classical Gallager bound on the average error probability of ML decoding results:

$$P_e \leqslant (M-1)^{\rho} \sum_{\underline{y}} \left(\sum_{\underline{x}} q_N(\underline{x}) p_N(\underline{y}|\underline{x})^{1/(1+\rho)} \right)^{1+\rho} , \tag{2}$$

where $0 \leqslant \rho \leqslant 1$ and where P_e designates the average decoding error probability (where the average is taken over the randomly and independently selected codewords). For the case of memoryless channel ($p_N(\underline{y}|\underline{x}) = \prod_{i=1}^{N} p(y_i|x_i)$) and input distribution ($q_N(\underline{x}) = \prod_{i=1}^{N} q(x_i)$), the random coding Gallager bound (2) admits the form [3]:

$$P_e \leqslant e^{-NE_{RC}(R,q)}$$

$$E_{RC}(R,q) = \max_{0 \leqslant \rho \leqslant 1} (E_0(\rho,q) - \rho R) ,$$

$$E_0(\rho,q) = -\ln \sum_{y} \left(\sum_{x} q(x) p(y|x)^{1/(1+\rho)} \right)^{1+\rho} , \tag{3}$$

where $R = \ln M/N$ is the code rate and $E_{RC}(R,q)$ is the random coding error exponent [3].

2.2. The 1961 Fano–Gallager bound

The 1961 Gallager bound on ML decoding [2] relies on the distance spectrum of the N-length block code (or ensemble of codes), and therefore can be also applied to fixed codes or restricted ensembles of codes (differing from the ensemble of the fully random block codes, as in the 1965 Gallager bound). The derivation of this bound is based on the 1961 Fano bounding technique [1]. The concept of this bounding is as follows:

Let $\underline{x}^m$ be the transmitted codeword and define the tilted ML metric: $D(\underline{x}^{m'}, \underline{y}) = \ln(f_N^m(\underline{y})/p_N(\underline{y}|\underline{x}^{m'}))$, where $\underline{x}^{m'}$ is an arbitrary codeword and $f_N^m(\underline{y})$ (may depend on $\underline{x}^m$) is an arbitrary function which is positive if $p_N(\underline{y}|\underline{x}^{m'})$ is positive. If the ML decoding is applied, an error occurs if for some $m' \neq m$:

$$D(\underline{x}^{m'}, \underline{y}) \leqslant D(\underline{x}^m, \underline{y}) . \tag{4}$$

The received space Y^N is divided into two *disjoint* subspaces:

$$Y^N = Y_g^N \bigcup Y_b^N ,$$

$$Y_g^N = \{\underline{y} : D(\underline{x}^m, \underline{y}) \leqslant Nd\} ,$$

$$Y_b^N = \{\underline{y} : D(\underline{x}^m, \underline{y}) > Nd\} , \tag{5}$$

where d is an arbitrary real number.

The conditional ML decoding error probability is upper bounded by a sum of two terms:

$$P_{e|m} \leqslant \text{Prob}\,(\underline{y} \in Y_b^N) + \text{Prob}\,(\text{error}, \underline{y} \in Y_g^N) , \tag{6}$$

which is the starting point of many efficient bounds [4–6,11,12,16] and references therein. We restrict now our consideration to the case, where $f_N^m(\underline{y})$ can be expressed in the product form $f_N^m(\underline{y}) = \prod_{i=1}^N f(y_i)$, where f is an even function ($f(y) = f(-y)$).

For the special case of binary linear block codes and a symmetric memoryless channel, it is demonstrated in Ref. [13] by invoking the Chernoff bounds that

$$P_e \leqslant 2^{h_2(\rho)} g(s)^{N(1-\rho)} \left(\sum_{l=0}^{N} S_l h(r)^l g(r)^{N-l} \right)^{\rho} , \tag{7}$$

where $0 \leqslant \rho \leqslant 1$ and $h_2(\rho)$ is the binary entropy function. $\{S_l\}_{l=0}^N$ designates the distance spectrum of the considered block code. Based on the symmetry of the channel and the function f:

$$g(s)=\frac{1}{2}\sum_{y}([p(y|0)]^{1-s}+[p(y|1)]^{1-s})f(y)^{s}\,,$$

$$h(r)=\sum_{y}[p(y|0)p(y|1)]^{(1-r)/2}f(y)^{r}\,, \tag{8}$$

with $s \geqslant 0$, $r \leqslant 0$, $-\infty < d < +\infty$, $0 \leqslant \rho \leqslant 1$, and where f is optimized to get the tightest upper bound (7).

2.3. The Duman–Salehi bound (version II)

The Duman–Salehi bounding technique [9,10], originates from the 1965 Gallager bound [3] and it yields

$$P_{e|m} \leqslant \left(\sum_{m'\neq m}\sum_{\underline{y}} p_N(\underline{y}|\underline{x}^m)^{1/\rho}\,\psi_N^m(\underline{y})^{1-1/\rho}\left(\frac{p_N(\underline{y}|\underline{x}^{m'})}{p_N(\underline{y}|\underline{x}^m)}\right)^{\lambda}\right)^{\rho}, \tag{9}$$

where $0 \leqslant \rho \leqslant 1$ and $\lambda \geqslant 0$, and where $\psi_N^m(\underline{y})$ is an arbitrary probability measure (which may also depend on $\underline{x}^m$).

An alternative form is given by

$$P_{e|m} \leqslant \left(\sum_{\underline{y}} G_N^m(\underline{y})p_N(\underline{y}|\underline{x}^m)\right)^{1-\rho}$$

$$\times\left\{\sum_{m'\neq m}\sum_{\underline{y}} p_N(\underline{y}|\underline{x}^m)G_N^m(\underline{y})^{1-1/\rho}\left(\frac{p_N(\underline{y}|\underline{x}^{m'})}{p_N(\underline{y}|\underline{x}^m)}\right)^{\lambda}\right\}^{\rho}, \tag{10}$$

where $0 \leqslant \rho \leqslant 1$, $\lambda \geqslant 0$ and the unnormalized tilting measure $G_N^m(\underline{y})$ satisfies

$$\psi_N^m(\underline{y})=\frac{G_N^m(\underline{y})p_N(\underline{y}|\underline{x}^m)}{\sum_{\underline{y}} G_N^m(\underline{y})p_N(\underline{y}|\underline{x}^m)}\,. \tag{11}$$

3. Interconnections and observations

3.1. The Duman–Salehi bound: random coding version

For the ensemble of random codes, where the N-length codewords are randomly and independently selected with respect to the input distribution $q_N(\underline{x})$, the generalized Duman–Salehi bound yields the following upper bound:

$$P_e \leqslant (M-1)^{\rho}\sum_{\underline{y}}\left\{\left(\sum_{\underline{x}} q_N(\underline{x})p_N(\underline{y}|\underline{x})^{1-\lambda\rho}\right)\left(\sum_{\underline{x}'} q_N(\underline{x}')p_N(\underline{y}|\underline{x}')^{\lambda}\right)^{\rho}\right\}. \tag{12}$$

with $0 \leqslant \rho \leqslant 1$, $\lambda \geqslant 0$ and where the optimal selection for the unnormalized tilting measure in (10) is

$$G_N^m(\underline{y}) = \left(\sum_{\underline{x}'} q_N(\underline{x}') \left(\frac{p_N(\underline{y}|\underline{x}')}{p_N(\underline{y}|\underline{x}^m)} \right)^{\lambda} \right)^{\rho} . \tag{13}$$

For $\lambda = 1/(1+\rho)$, one obtains the standard random coding Gallager bound (2). It is hence demonstrated that in the standard random coding setting, no penalty is incurred for invoking the Jensen inequality in the Duman–Salehi (version II) bounding technique, as long as the optimization in (12) and (13) is done.

3.2. The connection between the 1961 Fano–Gallager bound with the Duman–Salehi bounds

Aided by the Chernoff inequality, the optimization over the parameter d yields [5]

$$P_{e|m} \leqslant 2^{h_2(\rho)} \left(\sum_{\underline{y}} p_N(\underline{y}|\underline{x}^m) \left(\frac{f_N^m(\underline{y})}{p_N(\underline{y}|\underline{x}^m)} \right)^{s} \right)^{1-\rho} \left(\sum_{m' \neq m} \sum_{\underline{y}} p_N(\underline{y}|\underline{x}^m) \right.$$

$$\left. \times \left(\frac{p_N(\underline{y}|\underline{x}^{m'})}{p_N(\underline{y}|\underline{x}^m)} \right)^{t} \left(\frac{f_N^m(\underline{y})}{p_N^m(\underline{y}|\underline{x}^m)} \right)^{s(1-1/\rho)} \right)^{\rho}, \quad \begin{array}{l} 0 \leqslant \rho \leqslant 1, \\ t, s \geqslant 0 . \end{array} \tag{14}$$

Divsalar [5] renames t by λ (where t is a non-negative parameter) and also sets

$$G_N^m(\underline{y}) = \left(\frac{f_N^m(\underline{y})}{p_N(\underline{y}|\underline{x}^m)} \right)^{s} , \tag{15}$$

reproducing then the Duman–Salehi upper bound (10) with an additional multiplying factor of $2^{h_2(\rho)}$ (where $1 \leqslant 2^{h_2(\rho)} \leqslant 2$). This demonstrates the superiority of the Duman–Salehi second version bound over the 1961 Fano–Gallager technique when applied for a particular code or ensemble of codes. It has been demonstrated in Ref. [13] that the Fano–Gallager technique equals the 1965 standard random coding Gallager bound (12) up to the $2^{h_2(\rho)}$ coefficient, where the latter as shown before, agrees with the optimized Duman–Salehi bound.

3.3. A geometric interpretation of the Gallager-type bounds

The connections between the Fano–Gallager tilting measure and the Duman–Salehi normalized and unnormalized tilting measures (which are designated here by $f_N^m(\underline{y})$, $\psi_N^m(\underline{y})$ and $G_N^m(\underline{y})$, respectively) are indicated in Eqs. (11) and (15), and they also provide some geometric interpretations of various reported bounds. The measure $f_N^m(\underline{y})$ in the 1961 Fano–Gallager bound, which, in general, does not imply a product form, yields a geometric interpretation associated with the conditions in inequalities (5), which specify the disjoint regions $Y_g^N, Y_b^N \subseteq Y^N$. The geometric interpretation of the 1961 Fano–Gallager bound is not necessarily unique.

The non-uniqueness emerges due to the shifting and factoring invariance of the inequality

$$\ln\left(\frac{f_N^m(\underline{y})}{p_N(\underline{y}|\underline{x}^m)}\right) \leqslant Nd\,, \tag{16}$$

and due to fact that the parameter d is also subjected to optimization. We demonstrate this non-uniqueness in Ref. [16] focusing on the Divsalar bound [5], which is associated with the decision region (N-dimensional sphere with a shifted center)

$$Y_g^N = \left\{\underline{y}\,|\sum_{l=1}^{N}(y_l - \eta\gamma x_l^m)^2 \leqslant Nr^2\right\}\,, \tag{17}$$

where $\gamma = \sqrt{2RE_b/N_0}$ is the square root of the signal-to-noise ratio and η, r are parameters subjected to optimization. It is verified [16] that the 1961 Fano–Gallager tilting measures:

$$f_N^m(\underline{y}) = \prod_{l=1}^{N}\left\{\exp\left(\frac{1}{2}\left(\frac{1}{\eta}-1\right)(y_l)^2\right)\right\}\,, \tag{18}$$

$$f_N^m(\underline{y}) = \prod_{l=1}^{N}\left\{\exp\left(\frac{\gamma}{2}(1-\eta)x_l^m y_l\right)\right\}\,, \tag{19}$$

$$f_N^m(\underline{y}) = \prod_{l=1}^{N}\{\exp(-\theta(y_l - \phi x_l^m)^2)\}\,, \tag{20}$$

where $\phi = \gamma(\eta + (1-\eta)/2\theta)$ and $\theta \neq 0$ in Eq. (20), yield in fact all equivalent regions to (17).

4. Generalizations and special cases

In this section, we demonstrate that many reported bounds can be considered as special cases of the generalized (second version) of the Duman–Salehi bound, and we also propose generalizations of the Shulman–Feder bound [17]. Some of these observations have been reported in detail in Ref. [16].

4.1. A generalization of the Shulman–Feder bound

In Ref. [16] the generalized version of the Shulman–Feder bound [17] is derived as a particular case of the generalized Duman–Salehi bound. Let C be a fixed binary linear block code, where its distance spectrum is designated by $\{S_l\}_{l=0}^{N}$. We get in Ref. [16]:

$$P_{e|0} \leqslant \exp - NE\left(\rho', PR + \frac{1}{N}\frac{P}{Q}\ln\left(\sum_{l=0}^{N} b_l\left(\frac{v_l}{b_l}\right)^{Q}\right), q = \frac{1}{2}\right),\quad 0 \leqslant \rho' \leqslant \frac{1}{P}\,, \tag{21}$$

where $E(\rho,R,q)$ is introduced in Eq. (3), $v_l = S_l/(M-1)$, $b_l = 2^{-N}\binom{N}{l}$, $(l=0,1,2,\dots,N)$, $P \geqslant 1$ and $1/P + 1/Q = 1$. The Shulman–Feder bound [17] is recognized as a special case, where $P=1$, $Q \to \infty$. The improvement in the tightness of generalized bound (21) (as compared to the Shulman–Feder bound) is expected to take place for codes whose distance spectrum exponentially deviates from the binomial distribution of the ensemble of fully random block codes, especially at low Hamming weights (e.g., turbo and LDPC codes). For a pure binomial distance spectrum operating over a binary-input and symmetric-output channel, $P=1$ is optimal and the Shulman–Feder bound matches the Gallager random coding bound. Consider the inequality for the term in the error exponent of (21):

$$\frac{1}{N}\frac{P}{Q}\ln\left(\sum_{l=0}^{N} b_l\left(\frac{v_l}{b_l}\right)^{Q}\right) \geqslant \frac{1}{N}D(\underline{v}\|\underline{b})\,.$$

The divergence $D(\underline{v}\|\underline{b})$ then constitutes a lower bound on the rate loss as compared to pure random codes (with binomial distance spectra) and hence it provides some operative meaning to Battail's proposition [20] for the design of weakly random-like turbo codes.

4.2. *The Duman–Salehi bound (first version)*

The first version of the Duman–Salehi bound [10] for a binary-input AWGN channel is a particular case of their second version [9], where the normalized tilting measure in Eq. (9) is

$$\psi_N^m(\underline{y}) = \prod_{l=1}^{N}\psi(y_l) = \prod_{l=1}^{N}\left\{\sqrt{\frac{\alpha}{2\pi}}\exp\left[-\frac{\alpha}{2}\left(y_l - \frac{\beta}{\alpha}\sqrt{\frac{2E_s}{N_0}}x_l^m\right)^2\right]\right\} \tag{22}$$

with α,β parameters being subjected to optimization.

The overall Duman–Salehi bound results by partitioning the code to constant Hamming subcodes and invoking the union bound

$$P_e = P_{e|0} \leqslant \sum_{d=d_{\min}}^{N} P_{e|0}(d)\,, \tag{23}$$

where $d_{\min}$ is the minimum Hamming distance of the N-length block code and $P_{e|0}(d)$ is the conditioned decoding error probability with respect to the subcode with a constant Hamming weight d. The Duman–Salehi [10] first version bound then equals

$$P_{e|0}(d) \leqslant (S_d)^{\rho}\alpha^{N(1-\rho)/2}\left(\alpha - \frac{\alpha-1}{\rho}\right)^{-N\rho/2}\exp\left\{N\left(\frac{RE_b}{N_0}\right)\left[-1+\frac{(\beta^*)^2(1-\rho)}{\alpha} + \frac{\rho(1-d/N)(\beta^*+(1-\beta^*)/\rho)^2}{\alpha-(\alpha-1)/\rho}\right]\right\}\,, \tag{24}$$

$$\beta^* = 1-(d/N)/(1/\alpha) - d/N(1-\rho),$$

and where $0 \leqslant \alpha \leqslant 1/(1-\rho)$, $0 \leqslant \rho \leqslant 1$, are subjected to further optimization.

4.3. The Viterbi–Viterbi bound (first version)

The Viterbi–Viterbi bound [18] on the ML decoding error probability for BPSK modulated block codes operating over a binary-input AWGN channel is given by (23) with

$$P_e \leqslant (S_d)^\rho \exp\left(\frac{-NRE_b}{N_0}\,\frac{(d/N)\rho}{1-d/N(1-\rho)}\right), \tag{25}$$

where $0 \leqslant \rho \leqslant 1$. The optimization over the parameter ρ gives then the Viterbi–Viterbi upper bound [19] which reads

$$P_e \leqslant \exp(-NE_{v_1}(r_d)), \tag{26}$$

where

$$E_{v_1}(r_d) = \begin{cases} (\frac{d}{N})c - r_d, & 0 \leqslant \frac{r_d}{c} \leqslant \frac{d}{N}(1-\frac{d}{N}), \\ \left(\sqrt{c} - \sqrt{\frac{r_d(1-\frac{d}{N})}{\frac{d}{N}}}\right)^2, & \frac{d}{N}(1-\frac{d}{N}) \leqslant \frac{r_d}{c} < \frac{d/N}{1-d/N}, \end{cases} \tag{27}$$

$$r_d = \frac{\ln(S_d)}{N}, \qquad c = \frac{\gamma^2}{2} = \frac{RE_b}{N_0}. \tag{28}$$

This bound turns to be a special case of the Duman–Salehi first version bound, where $\alpha = 1$ is substituted in Eq. (24) (see Ref. [16]).

4.4. The Viterbi–Viterbi bound (second version)

The second version of the Viterbi–Viterbi bounds [19] is based on the 1961 Gallager–Fano bound and it reads

$$P_{e|0}(l) \leqslant \exp(-NE_{v_2}(r_l)),$$

$$E_{v_2}(r_l) = \max_{0\leqslant\rho\leqslant 1}\left\{-\rho r_l + \frac{l}{N}\ln(\tilde{h}(\rho)) + \left(1-\frac{l}{N}\right)\ln(\tilde{g}(\rho)) - (1-\rho)\ln(\tilde{h}(\rho)+\tilde{g}(\rho))\right\}, \tag{29}$$

where $r_l = \ln(S_l)/N$. Based on the symmetry of the binary-input and memoryless channel:

$$\tilde{h}(\rho) = \sum_y [p(y|0)^{1/(1+\rho)} + p(-y|0)^{1/(1+\rho)}]^{-(1-\rho)}[p(y|0)p(-y|0)]^{1/(1+\rho)},$$

$$\tilde{g}(\rho) = \sum_y [p(y|0)^{1/(1+\rho)} + p(-y|0)^{1/(1+\rho)}]^{-(1-\rho)} p(y|0)^{2/(1+\rho)}. \tag{30}$$

This bound is again a special case of the Duman–Salehi bound (second version) using the unnormalized tilting measure:

$$G_N^m(\underline{y}) = \prod_{l=1}^{N} \{(p(y_l|0)^{1/(1+\rho)} + p(y_l|1)^{1/(1+\rho)})^\rho \, p(y_l|0)^{-\rho/(1+\rho)}\} . \tag{31}$$

4.5. The Divsalar bound

The Divsalar bound [5] results also as a particular case of the 1961 Fano–Gallager bounding technique for a binary-input AWGN channel, as demonstrated in Section 3.3. It has also been indicated there that several alternative geometrical interpretations can be used. This bound given in Ref. [5] in closed form reads

$$P_e \leqslant \sum_{d=d_{\min}}^{N} \min\left(\exp(-NE_D(c,d,\beta^*)), S_d Q(\sqrt{2dc})\right) , \tag{32}$$

where

$$E_D(c,d,\beta) = -r_d + \frac{1}{2}\ln[\beta + (1-\beta)\exp(2r_d)] + \frac{(d/N)\beta}{1-(d/N)(1-\beta)} , \tag{33}$$

$$\beta^* = \left[c\left(\frac{1-(d/N)}{(d/N)}\right)\frac{2}{1-\exp(-2r_d)} + \left(\frac{1-(d/N)}{(d/N)}\right)^2 [(1+c)^2 - 1]\right]^{1/2} - \left(\frac{1-(d/N)}{d/N}\right)(1+c) , \tag{34}$$

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{+\infty} \exp\left(-\frac{t^2}{2}\right) \mathrm{d}t \tag{35}$$

and the parameters $c = E_s/N_0$, $r_d = \ln(S_d)/N$. In fact, it is verified in Ref. [16] that the Divsalar bound coincides with the corresponding tilting measure of the first version of the Duman–Salehi bound (22), where $\alpha = (2\theta - 1)s + 1$, $\beta = (2\theta - 1)\eta s + 1$ and where α and s are properly selected parameters [16]. This is the ground for the observation in Ref. [5] that the Divsalar bound is a closed form version of the Duman–Salehi bound (first version) [8].

4.6. The fully ideally interleaved fading channels with perfect channel side information (CSI)

The model here is: $y = ax + n$, where y stands for the received signal, x stands for the BPSK modulated input signal (it is $\pm\sqrt{2E_s}$) and n designates the additive zero mean and $N_0/2$ variance Gaussian component. The fading a is assumed to be ideally interleaved and perfectly known at the receiver and hence is considered to be real valued as the receiver compensates for any phase rotation. The bounds are based on first decomposing the code to subcodes over which a union bound is applied as in Eq. (23).

4.6.1. Optimized Duman–Salehi bound

In Ref. [14], the measure

$$\Psi(\underline{y},\underline{a}) = \prod_{l=1}^{N} \psi(y_l, a_l)\,, \tag{36}$$

is optimized as to yield the best possible Duman–Salehi (second version) bound (9), where (y, a) are interpreted as the available measurements at the receiver.

4.6.2. Exponential tilting measure

In Ref. [15], a sub-optimal selection for ψ in (36) is suggested which in fact is motivated by the first version of the Duman–Salehi bound [10], where an exponential tilting is also applied to the fading sample a (treated as a measurement). This gives rise to the following exponential tilting measure:

$$\psi(y,a) = \frac{\sqrt{(\alpha/2\pi)}\exp\left[-\alpha/2(y - au\sqrt{2E_s/N_0})^2 - (\alpha v^2 a^2 E_s/N_0)\right]p(a)}{\int_0^{+\infty} p(a)\exp(-(\alpha v^2 a^2 E_s/N_0))\,\mathrm{d}a}\,, \tag{37}$$

where $\alpha \geqslant 0$, $-\infty < u < +\infty$, $-\infty < v < +\infty$, $\alpha u < 1/(1-\rho)$, and where $p(a)$ designates the probability density function of the independent fading samples. This yields a closed form bound which reads [15]

$$P_{e|0}(d) \leqslant (S_d)^{\rho} \alpha^{(-N(1-\rho)/2)} \left(\alpha - \frac{\alpha-1}{\rho}\right)^{-N\rho/2} \left(\frac{1}{1+t}\right)^{N(1-\rho)} \times \left(\frac{1}{1+\varepsilon}\right)^{d\rho} \left(\frac{1}{1+v}\right)^{(N-d)\rho}\,, \tag{38}$$

with

$$t = \frac{\alpha v^2 E_s}{N_0}\,, \tag{39}$$

$$v = \frac{E_s}{N_0}\left[\alpha(u^2+v^2)\left(1-\frac{1}{\rho}\right) + \frac{1}{\rho} - \frac{(\alpha u - (\alpha u - 1)/\rho)^2}{\alpha - (\alpha-1)/\rho}\right]\,,$$

$$\varepsilon = \frac{E_s}{N_0}\left[\alpha(u^2+v^2)\left(1-\frac{1}{\rho}\right) + \frac{1}{\rho} - \frac{(\alpha u - (\alpha u - 1)/\rho - 2\lambda)^2}{\alpha - (\alpha-1)/\rho}\right]\,.$$

This bound is in fact equivalent to the Divsalar–Biglieri bound [6] which has been derived via a geometric extension of the associated decision region in the Divsalar bound [5] (by rotating the displaced sphere region). The bound in Ref. [15] also

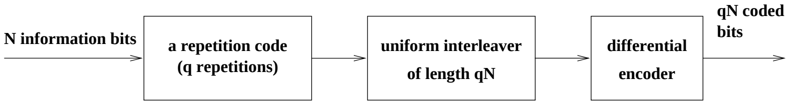

Fig. 1. Block diagram of the ensemble of rate-$\frac{1}{4}$ and uniformly interleaved RA (repeat and accumulate) codes.

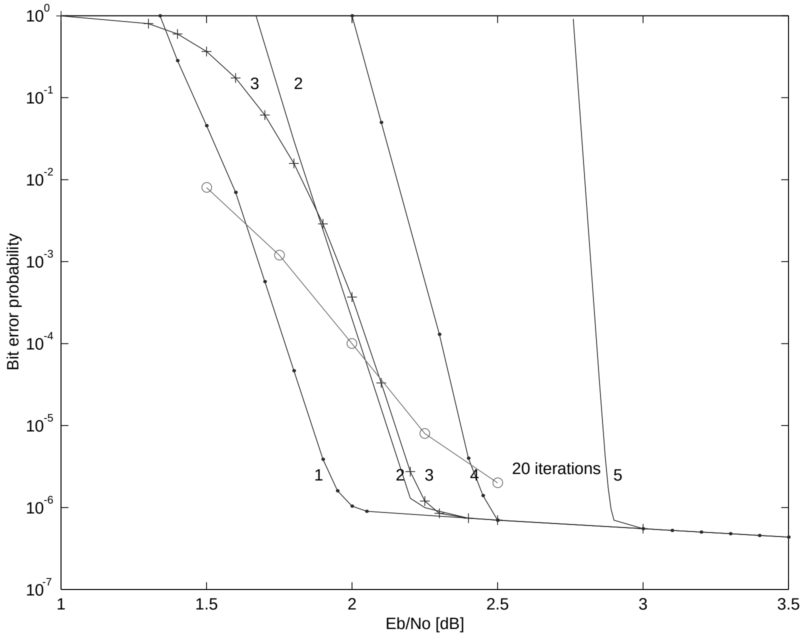

Fig. 2. A comparison between bounds of RA codes for a Rayleigh channel: (1) Generalized Duman–Salehi [14]; (2) Divsalar–Biglieri [6,5]; (3) Engdahl–Zigangirov [11]; (4) Generalized Viterbi–Viterbi [15]; (5) Union bound. These bounds are compared with simulation results of the LOG-Map iterative decoding algorithm (20 iterations).

particularizes to the Viterbi–Viterbi (first version) extended bound to the fading channel [15], which results by setting in (39):

$$\alpha = 1, \quad u = 1 - \xi\rho, \quad v = \sqrt{1-(1-\xi\rho)^2}, \quad \lambda = \frac{1+\xi(1-\rho)}{2}\,. \tag{40}$$

We demonstrate the comparative tightness of several bounds when applied to the repeat-accumulate codes [7] of rate $\frac{1}{4}$, operating over the ideally interleaved Rayleigh channel. The system is depicted in Fig. 1. A block of 1024 information bits is encoded in each block, repeated $q = 4$ times, interleaved by a uniform interleaver of length $N = 4096$ and finally differentially encoded.

A comparison between upper bounds on the bit error probability, associated with the ML decoding of the RA coding scheme of Fig. 1, operating over a fully interleaved Rayleigh fading channel with perfect side information on the i.i.d fading samples is shown in Fig. 2. The following upper bounds are shown: The generalized

Duman–Salehi second version bound [14]; the Divsalar–Biglieri bound [6] equivalent also to the bound in Ref. [15]; the generalized Engdahl–Zigangirov bound [14]; the generalized Viterbi–Viterbi (first version) bound [15]; and the union bound. The upper bounds on the ML decoding are compared with the computer simulation results of the log-MAP iterative decoding algorithm with 20 iterations. The relative tightness of the investigated bounds as well as a marked advantage over the union bound of the optimized Duman–Salehi bound [14] is clearly demonstrated.

4.7. The Chernoff version of some reported bounds

In his paper [5], Divsalar derived simplified Chernoff versions of some upper bounds, which result as particular cases of the 1961 Fano–Gallager bounding technique, and therefore are also special cases of the Duman–Salehi setting. These simplified Chernoff versions include: the Chernoff version of the sphere bound [5,8], the Chernoff version of the tangential bound [4,5], the Chernoff version of the tangential sphere bound [5,12]. In Ref. [16] it is also shown that the Chernoff version of the Engdahl and Zigangirov bound [11] derived for a binary-input AWGN channel, is a particular case of the generalized Duman–Salehi bound. The decision region Y_g^N associated with the transmitted codeword $\underline{x}^m$ for the Engdahl–Zigangirov bound is an N-dimensional plane:

$$Y_g^N = \left\{ \underline{y} \,|\, \sum_{l=1}^{N} y_l x_l^m \geqslant Nd \right\} , \tag{41}$$

where the associated tilting measure is identified to be

$$f_N^m(\underline{y}) = \prod_{l=1}^{N} \left\{ \exp\left(-\frac{1}{2} y_l^2 + \beta y_l x_l^m \right) \right\}, \quad \beta \neq \sqrt{\frac{2E_s}{N_0}} . \tag{42}$$

5. Summary and conclusions

In addressing the Gallager bounding techniques and their variations, we focus here on the Duman–Salehi variation, which originates from the standard 1965 Gallager classical bound [3]. The considered bounds on the block and bit error probabilities rely on the calculable distance spectrum and the input–output weight enumerator functions of the codes. By generalizing the framework of the second version of the Duman–Salehi bound (see Section 2), we demonstrate its rather broad features and indeed this variation provides the natural bridge between the 1961 and 1965 Gallager bounds ([2,3], respectively). It is suitable for both random and specific codes, as well as for either bit or block error analysis. Some observations and interconnections among the Gallager and Duman–Salehi bounds for random and deterministic codes are presented in Section 3, which partially rely on the most insightful observations by Divsalar [5]. Focus is on geometric interpretations of the 1961 Gallager-type bounds as motivated by the Duman–Salehi setting, reflecting the non-uniqueness of their associated tilting measures. We use this unifying framework to generalize the Shulman–Feder bound as well as to demonstrate that this setting accounts for a large class of recently proposed bounds. The basic bounding framework can be also applied to the mismatched decoding setting [16].

References

[1] R.M. Fano, Transmission of Information, MIT Press and Wiley, New York, 1961.
[2] R.G. Gallager, Low Density Parity Check Codes, MIT Press, Cambridge, MA, USA, 1963.
[3] R.G. Gallager, A simple derivation of the coding theorem and some applications, IEEE Trans. Inf. Theory 11 (1) (1965) 3–18.
[4] E.R. Berlekamp, The technology of error correction codes, Proc. IEEE 68 (5) (1980) 564–593.
[5] D. Divsalar, A simple tight bound on error probability of block codes with application to turbo codes, TMO Progress Report 42–139, JPL, November 1999, pp. 1–35.
[6] D. Divsalar, E. Biglieri, Upper bounds to error probabilities of coded systems beyond the cutoff rate, IEEE International Symposium on Information Theory 2000 (ISIT 2000), Sorrento, Italy, June 2000, pp. 25–30.
[7] D. Divsalar, H. Jin, R.J. McEliece, Coding theorems for 'turbo-like' codes, Proceedings of the 1998 Allerton Conference, Monticello, Illinois, September 1998, pp. 201–210.
[8] S. Dolinar, L. Ekroot, F. Pollara, Improved error probability bounds for block codes on the Gaussian channel, Proceedings of the 1994 IEEE International Symposium on Information Theory, Trondheim, Norway, June 24–July 1, 1994.
[9] T.M. Duman, Turbo codes and turbo coded modulation systems: Analysis and performance bounds, Ph.D. Dissertation, Electrical & Computer Engineering Department, Northeastern University, Boston, MA, USA, May 1998.
[10] T.M. Duman, M. Salehi, New performance bounds for turbo codes, IEEE Trans. Commun. 46 (6) (1998) 717–723.
[11] K. Engdahl, K.Sh. Zigangirov, Tighter bounds on the error probability of fixed convolutional codes, IEEE Trans. Inf. Theory 47 (2001) 1625–1630.
[12] G. Poltyrev, Bounds on the decoding error probability of binary linear codes via their spectra, IEEE Trans. Inf. Theory 40 (4) (1994) 1284–1292.
[13] I. Sason, S. Shamai, Gallager's 1961 bound: extensions and observations, Technical Report, CC No. 258, Technion, Israel, October 1998.
[14] I. Sason, S. Shamai, On improved bounds on the decoding error probability of block codes over interleaved fading channels, with application to turbo-like codes, IEEE Trans. Inf. Theory 47(6) (2001) 2275–2299.
[15] I. Sason, S. Shamai, D. Divsalar, On simple and tight upper bounds on the ML decoding error probability for block codes over fully interleaved fading channels, Proc. 6th Int. Symposium on Communication Theory and Applications, 2001, pp. 236–241.
[16] I. Sason, Upper bounds on the maximum likelihood decoding error probability for block codes and turbo-block codes, Ph.D. dissertation, Technion – Israel Institute of Technology, Haifa, Israel, September 2001.
[17] N. Shulman, M. Feder, Random coding techniques for nonrandom codes, IEEE Trans. Inf. Theory 45 (6) (1999) 2101–2104.
[18] A.M. Viterbi, A.J. Viterbi, An improved union bound for binary linear codes on the AWGN channel, with application to turbo decoding, Proceedings of IEEE Information Theory Workshop, San Diego, California, February 1998, p. 72.
[19] A.M. Viterbi, A.J. Viterbi, Improved union bound on linear codes for the binary-input AWGN channel, with application to turbo codes, Proceedings of the IEEE International Symposium on Information Theory (ISIT 1998), Cambridge, MA, August 16–21, 1998, p. 29.
[20] G. Battail, A conceptual framework for understanding turbo codes, Proceedings of the International Symposium on Turbo Codes and Related Topics, Brest, September 1997, pp. 55–62.