Gallager-Type Bounds for Non-Binary Linear Block Codes over Memoryless Symmetric Channels

Eran Hof  Igal Sason  Shlomo Shamai

Department of Electrical Engineering
Technion – Israel Institute of Technology
Haifa 32000, Israel
E-mails: {hof@tx, sason@ee, sshlomo@ee}.technion.ac.il

Abstract—The performance analysis of non-binary linear block codes is studied under ML decoding where it is assumed that the transmission takes place over memoryless symmetric channels. Gallager-type bounds are derived, and the proposed bounds are exemplified for expurgated regular ensembles of non-binary low-density parity-check (LDPC) codes. These bounds are also compared with classical and recent improved sphere-packing bounds, indicating that these bounding techniques are informative for the performance evaluation of coded communication systems which incorporate non-binary coding techniques.

I. INTRODUCTION

The performance analysis of coded communication systems is usually done via the derivation of tight upper and lower bounds on the decoding error probability. For a comprehensive tutorial on the performance analysis of binary linear block codes under ML decoding, see [1] and the references therein. The 1965 Gallager bound [2] is one of the well-known upper bounds on the decoding error probability of ensembles of fully random block codes, and it is informative at all rates below the channel capacity limit. Emerging from the 1965 Gallager bound, the bounds of Duman and Salehi [3], [4] hold for specific codes or structured ensembles and they are expressed in terms of the (average) distance spectrum of the codes (or ensembles). The Shulman and Feder bound (SFB) [5] is another Gallager-type bound which coincides with the 1965 Gallager bound for fully random block codes and can also be applied to structured codes or ensembles. An adaptation of the SFB to non-binary linear block codes was studied in [6] for the case of coding with a random coset mechanism.

This paper is focused on the derivation of Gallager-type upper bounds on the ML decoding error probability of ensembles of non-binary linear block codes whose transmission takes place over a memoryless symmetric channel. In this respect, we show the necessity in replacing the union bound by improved upper bounds on the decoding error probability. The upper bounds provided in this paper are compared to the sphere-packing 1959 (SP59) lower bound of Shannon [7], and the improved sphere-packing (ISP) lower bound provided in [8] (which improves the bounds in [9] and [10]).

This structure of the paper is as follows: The symmetry requirements and the message independence proposition are provided in Section II. The proposed bounding approach is introduced in Section III, and these bounds are exemplified in Section IV to Gallager’s ensembles of non-binary regular LDPC codes. Section V concludes the discussion. The reader is referred to the full paper version [11] for proofs, and for further discussions and applications.

II. SYMMETRY AND MESSAGE INDEPENDENCE

Let $\mathcal{X} = \{x_0, x_1, \ldots, x_{q-1}\}$ be a given alphabet with a cardinality $q$. We assume an addition operation, designated by $+$, over the alphabet $\mathcal{X}$ s.t. $\{\mathcal{X}, +\}$ is an abelian group and designate $x_0 = 0$ as the additive identity. In addition, let $\mathcal{Y}$ be a given discrete (or continuous) alphabet. We assume a memoryless channel, and denote the channel transition probability (or probability density, respectively) function by $p(y|x)$, where $x \in \mathcal{X}$ and $y \in \mathcal{Y}$.

Definition 1. [8, Section 3] A memoryless channel which is characterized by a transition probability $p$, an input-alphabet $\mathcal{X}$ and a discrete output alphabet $\mathcal{Y}$ is symmetric if and only if there exists a function $T : \mathcal{Y} \times \mathcal{X} \rightarrow \mathcal{Y}$ such that

1) For any $x \in \mathcal{X}$, the function $T(\cdot, x) : \mathcal{Y} \rightarrow \mathcal{Y}$ is bijective,

2) For any $x_1, x_2 \in \mathcal{X}$, the following two relations hold:

$$p(y|x_1) = p(T(y, x_2 - x_1)|x_2)$$

(1)

and

$$T(T(y, x_1), x_2) = T(y, x_1 + x_2).$$

(2)

When dealing with channels whose output alphabet is continuous, an additional requirement for $T$ is that its Jacobian equals to one. In this case, the condition in (1) implies that

$$\int p(y|x_1) \, dy = \int p(T(y, x_2 - x_1)|x_2) \, dy.$$

For binary linear block codes operating over MBIOS channels, their average error probability under ML decoding is independent of the actual transmitted codeword. The following proposition forms a generalization of this result for linear block codes communicated over memoryless and symmetric channels whose input alphabet is discrete. The proof of this

$^1$It is possible to use a generalized definition for both discrete and continuous output alphabets using the notion of unitary functions as done for example in [8].
proposition, as given in [11], follows in a similar way to the one provided in [13] for MBIOS channels.

**Proposition 1.** Let $C$ be a linear block code whose transmission takes place over a memoryless and symmetric channel. Then, the block error probability under ML decoding is independent of the transmitted codeword.

III. GALLAGER-TYPE BOUNDS FOR MEMORYLESS, SYMMETRIC CHANNELS

A. The second version of the Duman and Salehi (DS2) bound

Let $C = \{ x_m \}_{m=1}^{q^n}$ where $x_m = (x_{m,1}, \ldots, x_{m,n})$ be an $(n,k)$ linear block code defined over the input-alphabet $X$ with a cardinality $q$. Consider the conditional error probability under ML decoding given that the $m^{th}$ message is transmitted, denoted by $P_{e|m}$. The DS2 bound [3], [4] on this conditional error probability gets the form

$$P_{e|m} \leq \left\{ \frac{\sum_{y \in Y^n} G_n^m(y) p_n(y|x_m)}{\sum_{m \neq m} \left( \sum_{y \in Y^n} G_n^m(y) \right)^{1-\rho} \frac{p_n(y|x_m)}{p_n(y|x_m)}}^\lambda \rho \right\}^{1-\rho}$$

where $Y$ is a discrete output-characteristic, $G_n^m(y)$ is an arbitrary non-negative function of $y \in Y^n$, and $0 \leq \rho \leq 1$ and $\lambda \geq 0$ are arbitrary real-valued parameters (see, e.g., [1], [14], [15] and references therein). Here $p_n(y|x)$ designates the transition probability of the channel. Let $x \in C$ be a transmitted codeword and $y \in Y^n$ is the received vector. Notice that this bound holds for any channel regardless of its input alphabet (binary or non-binary).

Consider now the class of memoryless symmetric channels with an input-alphabet $X$. According to Proposition 1, $P_{e|n}$ is independent of the transmitted message $m$. We further assume that $G_n^0(y) = \prod_{i=1}^{n} g(y_i)$ is expressed in the following product form: $G_n^0(y) = \prod_{i=1}^{n} g(y_i)$. This provides the following single-letter upper bound on the ML decoding error probability:

**Proposition 2.** Consider an $(n,k)$ linear block code $C$ whose transmission takes place over a memoryless symmetric channel. Assume that the channel input and output alphabets are $X$ and $Y$, respectively, and let $p_n(y|x) = \prod_{i=1}^{n} p(y_i|x_i)$ be the transition probability of the channel. Then the block error probability of the code $C$ under ML decoding, $P_e$, satisfies

$$P_e \leq \left( \frac{\sum_{y \in Y^n} g(y)p(y|0)}{\sum_{m \neq 0} \left( \sum_{y \in Y^n} g(y) \right)^{1-\rho} \frac{p(y|0)}{p(y|0)}}^\lambda \rho \right)^{1-\rho}$$

where $g : Y \rightarrow \mathbb{R}$ is an arbitrary non-negative real function, $\lambda \geq 0$, and $0 \leq \rho \leq 1$ are arbitrary real-valued parameters.

B. Performance evaluation of ensembles of linear block codes

The following technical lemma considers the error probability under ML decoding of an ensemble of linear block codes:

**Lemma 1.** Let $C$ be an ensemble of linear block codes with a block length $n$, and let $d_{\min}$ be the minimum Hamming distance of a randomly selected codebook from this ensemble. Assume that there exist non-negative numbers $D_n$ and $\epsilon_n$, s.t.

$$\sum_{\{t \in T^*: n-t_0 \leq D_n\}} E[|C_t|] < \epsilon_n$$

where $E[|C_t|]$ denotes the expected number of codewords with a composition $t = (t_0, \ldots, t_{q-1})$, and $T^*$ denotes the entire set of compositions except for the one of the all-zero codeword. Then, the block error probability under ML decoding satisfies

$$P_e \leq \frac{P_e}{p(t_0)} \sum_{t \neq t_0} \frac{1}{|C_t|} + \epsilon_n.$$
where $n$ and $R$ are the block length and code rate (measured in $q$-ary symbols per channel use), respectively, and
\[ E_r(R) \triangleq \max_{0 \leq \rho \leq 1} \left( E_0(\rho) - \rho R \right) \]
\[ E_0(\rho) \triangleq -\log_q \left\{ \sum_{y \in \mathcal{Y}} \left( \frac{1}{q} \sum_{x \in \mathcal{X}} p(y|x) \frac{1}{1+\rho} \right)^\rho \right\} \]
\[ \alpha(\mathcal{C}, D_n) \triangleq \max_{\{ t \in \mathcal{T} : n-t_0 > D_n \}} \left\{ E \left[ \mathcal{C}_t \mid d_{\min} > D_n \right] \right\} \]

Proof outline: The proof follows from the bound in (5) with the setting
\[ g(y) = \left( \frac{1}{q} \sum_{x \in \mathcal{X}} p(y|x) \frac{1}{1+\rho} \right)^\rho p(y|0) - \frac{g_y}{\lambda}, \quad \lambda = \frac{1}{1+\rho} \]
where we rely on the symmetry of the memoryless channel. For a full proof, the reader is referred to [11].

Note that the SFB in [6] follows as a particular case of Theorem 2. A similar theorem can be stated for memoryless symmetric channels with continuous-output alphabets, where sums are replaced by integrals.

In general, the conditional expectation of the composition spectrum given that the minimum Hamming distance exceeds a certain positive threshold $D_n$ (i.e., $E \left[ |\mathcal{C}_t| \mid d_{\min} > D_n \right]$) is not available. Nevertheless, it is possible to use the inequality
\[ E \left[ |\mathcal{C}_t| \right] \geq E \left[ |\mathcal{C}_t| \mid d_{\min} > D_n \right] \left( 1 - \epsilon_n \right) \]
where the RHS of this inequality requires the knowledge of the expectation of the complete composition spectrum $E [ |\mathcal{C}_t| ]$.

Applying this to the RHS of the bound in Theorem 1, gives a looser version of this bound but is more amenable for analysis. The same inequality is valid when expurgation of codebooks is considered. The expurgated ensemble is constructed by removing from the original ensemble, all codebooks whose minimum Hamming distance is not above $D_n$. Since all codebooks in the expurgated ensemble have a minimum distance greater than $D_n$, the additive term $\epsilon_n$ on the RHS of (5) vanishes.

Consider an ensemble of linear block codes, and pick a codebook from this ensemble uniformly at random. We consider code ensembles which have the property that the probability that a vector is a codeword only depends on its Hamming weight (so all vectors of a fixed composition are codewords with equal probability). As a result, the expected complete composition spectrum $E \left[ |\mathcal{C}_t| \right]$ satisfies
\[ E \left[ |\mathcal{C}_t| \right] = P(t_0) \binom{n}{t} \]

where $P(l)$ denotes the probability that a word whose Hamming weight is $l$, forms a codeword in a randomly selected codebook from the ensemble. Assuming (8), the evaluation of $\alpha(\mathcal{C})$ in Theorem 2 is considerably reduced. In addition, it is possible to provide a refinement of the analysis used for the derivation of Theorem 2. Specifically, we tighten the bound by circumventing the need to take the maximization involved in the evaluation of $\alpha(\mathcal{C})$ in (7), and still obtain a bound which is computationally feasible due to the assumption in (8). This results in the following theorem:

Theorem 3. Under the assumption in (8), the block error probability satisfies
\[ P_e \leq A(\rho)^{n(1-\rho)} \sum_{D_n < l \leq n} \frac{P(l)}{1-\epsilon_n} B(\rho)^{n-l} C(\rho)^l \] + $\epsilon_n$
where $0 \leq \rho \leq 1$, $\epsilon_n$ is defined in (3), and
\[ A(\rho) \triangleq \sum_{y \in \mathcal{Y}} \left( \frac{1}{q} \sum_{x \in \mathcal{X}} p(y|x) \frac{1}{1+\rho} \right)^{\frac{\rho}{1+\rho}} \]
\[ B(\rho) \triangleq \sum_{y \in \mathcal{Y}} \left( \frac{1}{q} \sum_{x \in \mathcal{X}} p(y|x) \frac{1}{1+\rho} \right)^{\frac{\rho-1}{\rho}} \]
\[ C(\rho) \triangleq qA(\rho) - B(\rho). \]


IV. Examples

The new bounds are exemplified for the non-binary $(c,d)$-regular LDPC ensemble, proposed by Gallager in [16, Ch. 5]. This ensemble is characterized by a sparse parity-check matrix with binary elements (even for non-binary LDPC codes) and satisfies (8). An upper bound on the ensemble spectrum enumeration is provided in [16]. In addition, an exact enumeration is used based on a generalization of the analysis in [17] (the exact details are provided in [11]). The performance analysis of the considered ensemble is studied here for the the $q$-ary symmetric channel and the additive white Gaussian noise (AWGN) channel with a $q$-ary phase-shift keying (PSK) modulation.

The block error probabilities for some regular LDPC code ensembles with expurgation are presented in Figure 1 under ML decoding when the transmission takes place over the $q$-ary symmetric channel. The performance bounds introduced in this paper are compared to the union bound in order to show that the latter bound is useless beyond the crossover probability which corresponds to the cutoff rate. More specifically, for a $q$-ary symmetric channel, the cutoff rate is given by
\[ R_0 = 1 - 2\log_q \left( \sqrt{1-q} + \sqrt{q(q-1)} \right) \]
so the crossover probability which follows by setting the value of $R_0$ to the code rate, which is one-half symbol per channel use in Fig. 1, is equal to $p = 0.0670$ for quaternary input alphabet. The union bounds shown in this figure have a sharp decline around the crossover probability which corresponds to the cutoff rate of the quaternary symmetric channel (i.e., around $p = 0.0670$ for $q = 4$). This figure also exemplifies
for circle markers), the bound provided by Theorem 3 is presented for higher alphabet sizes (as is shown in [11]). D maintains its performance for a considerable range of to the bound in Theorem 3. In addition, the bound in (9) is evident that the bound in Theorem 2 is looser as compared is for $D$. The SFB in (6) is applicable only for higher values of $D$ values of $D_n$; the SFB is shown for $q = 4\), 8\), 16\), and 32\), whose transmission takes place over an AWGN channel with a q-ary PSK modulation. The capacity limit corresponds to a crossover probability

Fig. 1: Block error probability under ML decoding for the (8,16)-regular LDPC ensemble of Gallager, whose transmission takes place over the 4-ary symmetric channel. The capacity limit corresponds to a crossover probability of $p = 0.1893$ (marked as a solid vertical line). This figure depicts the upper bounds on the block error probability for the expurgated ensemble with a block length of 1008 symbols (in square marker), and 10,080 symbols (in dot-marker), based on Theorems 2 (in dashed lines) and Theorem 3 (in solid lines).

place over the AWGN channel with a q-ary PSK modulation.

All bounds are evaluated with the exact spectrum enumeration. The bound in (9), is evaluated for an alphabet size of $q = 4\) with $D_n$ values of 38 and 282, respective to the presented block lengths (i.e., $n = 1008$ and 10080). For $q = 8\), the two respective curves refer to $D_n$ values of 23 and 216; for $q = 16\), they refer to $D_n$ values of 15 and 132, and for $q = 32\), they refer to $D_n$ values of 12 and 102. The bound provided in Theorem 3 maintains its tightness for a considerably large range of $D_n$ values and alphabet cardinalities. The SFB in (6) is not applicable for the $D_n$ values above, but only for higher values of $D_n$ (the SFB is shown for $q = 4\) with $D_n$ values of 186 and 1851, respective to the presented block lengths; for $q = 8\), 16\), and 32\), the SFB refers to $D_n$ values of 191 and 1951, respective to the presented block lengths). Notice that the SFB in Theorem 2 deteriorates considerably as compared to the bound provided in Theorem 3, as the constellation order is increased. Except for the quaternary alphabet, when large $D_n$ values are used (for which the $\epsilon_n$ is around 0.1), for all other cases, the value of $\epsilon_n$ is below $10^{-12}$.

The upper bound in Theorem 3 is compared in Figure 3 to the SP59 lower bound and the improved sphere-packing (ISP) lower bound which is applicable for all symmetric memoryless channels and derived in [8] by improving the the bounding techniques in [9] and [10]. The upper bound is applied to the considered (8,32)-regular ensemble with octal alphabet cardinality and block lengths of 1024 and 10080 symbols with $D_n = 25$ and 95, respectively (the exact spectrum enumeration is applied). The ISP shows close proximity with the upper

Fig. 2: Upper bounds on the block error probability under ML decoding of the (8,16)-regular LDPC ensembles of Gallager with alphabet size of $q = 4\), 8\), 16\), and 32\), whose transmission takes place over an AWGN channel with a q-ary PSK modulation. The capacity limit corresponds to an $\epsilon_n$ threshold of $0.19\), $3.03\), $5.75\), and $8.57$ dB, respective to the constellation order (marked in vertical solid lines). This figure depicts the upper bounds on the block error probability for the expurgated ensemble with block lengths of 1008 symbols in square marker, and 10,080 symbols in dot-marker, based on Theorem 2 (in dashed lines) and Theorem 3 (in solid lines).

the potential application of the proposed bounds in this paper to properly assess the performance of efficient code ensembles (which perform reliably at rates exceeding the cutoff rate of the channel). The error performance is evaluated in Figure 1 using Theorem 2 (in dashed lines) and Theorem 3 (in solid lines), applied to the (8,16) Gallager expurgated ensemble with a quaternary alphabet. The resulting upper bounds on the decoding error, using the upper bound on the ensemble spectrum as given in [16], are presented with square and dot markers. When exact enumeration is applied, triangle and circle markers are used. The decoding error probability for a block length of $n = 1008$ symbols is shown with square and triangle markers where the bound in (9) is evaluated with $D_n = 99$ and a corresponding $\epsilon_n = 1.2 \cdot 10^{-4}$ (so a rather small fraction of the codebooks is actually expurgated). The SFB in (6) is applicable only for higher values of $D_n$, and is presented for $D_n = 173$ (and a corresponding $\epsilon_n = 0.1$). For a block length of 10,080 symbols (presented with dot and circle markers), the bound provided by Theorem 3 is presented for $D_n = 600$ (and a corresponding $\epsilon_n = 10^{-7}$). The SFB, is applicable only for higher values of $D_n$ (the presented curve is for $D_n = 1834$ symbol, with a corresponding $\epsilon_n = 0.11$). It is evident that the bound in Theorem 2 is looser as compared to the bound in Theorem 3. In addition, the bound in (9) maintains its performance for a considerable range of $D_n$ values. The inferiority of the SFB in (6) is further pronounced for higher alphabet sizes (as is shown in [11]).

The block error probability under ML decoding for the considered ensemble with an alphabet size of $q = 4\), 8\), 16\), and 32\) is depicted in Figure 2 when the transmission takes
This paper introduces new Gallager-type upper bounds on the decoding error probability of non-binary linear block codes whose transmission takes place over memoryless symmetric channels (these bounds are derived with full proofs in [11]). Under a symmetry property of the ensemble, the resulting bound is considerably simplified and even tightened. This simplifying assumption, which holds in particular for the considered non-binary low-density parity-check (LDPC) ensembles, yields a bound whose summations are over the Hamming weights of the non-zero codewords rather than their compositions (see Theorem 3). The tightness of the bounds presented in this paper is exemplified for the non-binary regular LDPC ensembles of Gallager [16] where transmission takes place over the $q$-ary symmetric channel and the AWGN channel with a $q$-ary PSK modulation. The bounds provided here are informative for the performance analysis of non-binary turbo-like codes over memoryless symmetric channels, and form a significantly tighter bounding technique as compared to the union bounds. As a particular case of this bounding technique, an adaptation of the Shulman-Feder bound (SFB) (see [5]) is provided for non-binary linear block codes. The latter approach which is related to the adaptation of the SFB to the non-binary setting is similar to the one provided by Bennatan and Burshtein [6] for a different setting of coding with a random coset mechanism.

The upper bound provided in this paper are compared to the sphere-packing 1959 (SP59) lower bound of Shannon [7] and the improved sphere-packing (ISP) lower bound provided in [8]; note that the latter bound improves the bounding techniques in [9] and [10] where this improvement is enhanced for codes with short to moderate block lengths.

The reader is referred to [11] for proofs and further applications and discussions.

Acknowledgment: This research work was supported in part by the Israel Science Foundation (grant no. 1070/07), and was also supported in part by the EU International Framework Programme via the NEWCOM++ Network of Excellence.

V. SUMMARY AND CONCLUSIONS

The upper bounds (in solid line) are provided for the $(8, 32)$ regular LDPC expurgated ensembles of Gallager. The lower bounds (the SP59 bound in dashed-dotted lines with empty markers and the ISP bound in dashed lines with filled markers), correspond to the ultimate performance of rate 0.75 block codes. The capacity limits in these cases correspond to $\frac{E_s}{N_0}$ threshold of 7.19 dB.

REFERENCES


