Error Exponents of Erasure/List Decoding Revisited via Moments of Distance Enumerators [*]

Neri Merhav

September 17, 2008

Department of Electrical Engineering
Technion - Israel Institute of Technology
Haifa 32000, ISRAEL

Abstract

The analysis of random coding error exponents pertaining to erasure/list decoding, due to Forney, is revisited. Instead of using Jensen's inequality as well as some other inequalities in the derivation, we demonstrate that an exponentially tight analysis can be carried out by assessing the relevant moments of a certain distance enumerator. The resulting bound has the following advantages: (i) it is at least as tight as Forney's bound, (ii) under certain symmetry conditions associated with the channel and the random coding distribution, it is simpler than Forney's bound in the sense that it involves an optimization over one parameter only (rather than two), and (iii) in certain special cases, like the binary symmetric channel (BSC), the optimum value of this parameter can be found in closed form, and so, there is no need to conduct a numerical search. We have not found yet a numerical example where this new bound is strictly better than Forney's bound and this may provide an additional evidence to support Forney's conjecture that his bound is tight for the average code. However, when applying the proposed analysis technique to a certain *universal* decoder with erasures, we demonstrate that it may yield significantly tighter exponential error bounds. We believe that this technique can be useful in simplifying and improving exponential error bounds in other problem settings as well.

Index Terms: random coding, erasure, list, error exponent, distance enumerator.

1 Introduction

In his celebrated paper [6], Forney extended Gallager's bounding techniques [5] and found exponential error bounds for the ensemble performance of optimum generalized decoding rules that include

[*] This research was supported by the Israel Science Foundation (ISF), grant no. 223/05.

the options of erasure, variable size lists, and decision feedback (see also later studies, e.g., [1], [8],[9], [11], [14], and [17]).

Stated informally, Forney [6] considered a communication system where a code of block length n and size $M = e^{nR}$ (R being the coding rate), drawn independently at random under a distribution $\{P(x)\}$, is used for a discrete memoryless channel (DMC) $\{P(y|x)\}$ and decoded with an erasure/list option. For the erasure case, in which we focus hereafter, an optimum tradeoff was sought between the probability of erasure (no decoding) and the probability of undetected decoding error. This tradeoff is optimally controlled by a threshold parameter T of the function e^{nT} to which one compares the ratio between the likelihood of each hypothesized message and the sum of likelihoods of all other messages. If this ratio exceeds e^{nT} for some message, a decision is made in favor of that message, otherwise, an erasure is declared.

Forney's main result is a lower bound $E_1(R,T)$ to the exponent of the probability of the event $\mathcal{E}_1$ of not making the correct decision, namely, either erasing or making the wrong decision. This lower bound is given by

$$E_1(R,T) = \max_{0\leq s\leq\rho\leq 1}[E_0(s,\rho) - \rho R - sT] \tag{1}$$

where

$$E_0(s,\rho) = -\ln\left[\sum_y\left(\sum_x P(x)P^{1-s}(y|x)\right)\cdot\left(\sum_{x'}P(x')P^{s/\rho}(y|x')\right)^{\rho}\right]. \tag{2}$$

The probability of the undetected error event $\mathcal{E}_2$ (i.e., the event of not erasing but making a wrong estimate of the transmitted message) is given by $E_2(R,T) = E_1(R,T) + T$. As is seen, the computation of $E_1(R,T)$ involves an optimization over two parameters, ρ and s, which in general requires a two–dimensional search by some method. This is different from Gallager's random coding error exponent for ordinary decoding (without erasures), which is given by:

$$E_r(R) = \max_{0\le\rho\le 1}[E_0(\rho) - \rho R], \tag{3}$$

with $E_0(\rho)$ being defined as

$$E_0(\rho) = -\ln\left[\sum_y\left(\sum_x P(x)P^{1/(1+\rho)}(y|x)\right)^{1+\rho}\right], \tag{4}$$

where there is only one parameter to optimize. In [6], one of the steps in the derivation involves the inequality $(\sum_i a_i)^r \le \sum_i a_i^r$, which holds for $r \le 1$ and non–negative $\{a_i\}$ (cf. eq. (90) in [6]), and another step (eq. (91e) therein) applies Jensen's inequality. The former inequality introduces an additional parameter, denoted ρ, to be optimized together with s.

Here, we offer a different technique for deriving a lower bound to the exponent of $\Pr\{\mathcal{E}_1\}$, which avoids the use of these inequalities. Instead, an exponentially tight evaluation of the relevant expression is derived by assessing the moments of a certain distance enumerator, and so, the resulting bound is at least as tight as Forney's bound. Since the first above–mentioned inequality is bypassed, there is no need for the parameter ρ, and so, under certain symmetry conditions (that often hold) on the random coding distribution and the channel, the resulting bound is also simpler in the sense that there is only one parameter to optimize rather than two. Moreover, this optimization can be carried out in closed form at least in some special cases like the binary symmetric channel (BSC). We have not found yet a convincing numerical example where the new bound is *strictly* better than Forney's bound. This may serve as an additional evidence to support Forney's conjecture that his bound is tight for the average code. Nevertheless, when applying the same analysis technique to a certain universal decoder with erasures, we demonstrate by numerical examples that significantly tighter exponential error bounds can be obtained compared to the technique used in [6].

We wish to emphasize that the main message of this contribution, is not merely in the simplification or the improvement of the error exponent bound in this specific problem of decoding with erasures, but more importantly, in the analysis technique we offer here, which is applicable to other problem settings as well, e.g., the interference channel [7] and the degraded broadcast channel [10]. The underlying ideas behind this technique are inspired from the statistical mechanical point of view on random code ensembles, offered in [15] and further developed in [12] (see also [2]).

The outline of this paper is as follows. In Section 2, we establish notation conventions and give some necessary background. In Section 3, we present the main result and discuss it. In Section 4, we derive the new bound, first for the special case of the BSC, and then more generally. Finally, in Section 5, we analyze a universal decoder as described above.

2 Notation and Preliminaries

Throughout this paper, scalar random variables (RV's) are denoted by capital letters, their sample values are denoted by the respective lower case letters, and their alphabets are denoted by the respective calligraphic letters. A similar convention applies to random vectors of dimension n and their sample values, which will be denoted with same symbols in the bold face font. The set of all n–vectors with components taking values in a certain finite alphabet, will be denoted as the same alphabet superscripted by n. Sources and channels will be denoted generically by the letter P or Q. Information theoretic quantities like entropies and conditional entropies, will be denoted following the usual conventions e.g., $H(X)$, $H(X|Y)$, etc. When we wish to emphasize the dependence of the entropy on a certain underlying probability distribution Q we subscript it by Q, i.e., use $H_Q(X)$, $H_Q(X|Y)$, etc. The expectation operator will be denoted by $\boldsymbol{E}\{\cdot\}$, and again, when we wish to emphasize the dependence on Q, we denote it by $\boldsymbol{E}_Q\{\cdot\}$. The cardinality of a finite set $\mathcal{A}$ is denoted by $|\mathcal{A}|$. The indicator function of an event $\mathcal{E}$ is denoted by $1\{\mathcal{E}\}$. For a given sequence $\boldsymbol{y} \in \mathcal{Y}^n$, $\mathcal{Y}$ being a finite alphabet, $\hat{P}_{\boldsymbol{y}}$ denotes the empirical distribution on $\mathcal{Y}$ extracted from $\boldsymbol{y}$, in other words, $\hat{P}_{\boldsymbol{y}}$ is the vector $\{\hat{P}_{\boldsymbol{y}}(y),\ y \in \mathcal{Y}\}$, where $\hat{P}_{\boldsymbol{y}}(y)$ is the relative frequency of the letter y in the vector $\boldsymbol{y}$. For two sequences of positive numbers, $\{a_n\}$ and $\{b_n\}$, the notation $a_n \doteq b_n$ means that $\frac{1}{n}\ln\frac{a_n}{b_n} \to 0$ as $n \to \infty$. Similarly, $a_n \overset{\cdot}{\le} b_n$ means that $\limsup_{n\to\infty}\frac{1}{n}\ln\frac{a_n}{b_n} \le 0$, and so on.

Consider a discrete memoryless channel (DMC) with a finite input alphabet $\mathcal{X}$, finite output alphabet $\mathcal{Y}$, and single–letter transition probabilities $\{P(y|x),\ x \in \mathcal{X},\ y \in \mathcal{Y}\}$. As the channel is fed by an input vector $\boldsymbol{x} \in \mathcal{X}^n$, it generates an output vector $\boldsymbol{y} \in \mathcal{Y}^n$ according to the sequence conditional probability distributions $P(y_i|x_1,\ldots,x_i,y_1,\ldots,y_{i-1}) = P(y_i|x_i)$, $i = 1,2,\ldots,n$, where for $i = 1$, $(y_1,\ldots,y_{i-1})$ is understood as the null string. A rate–R block code of length n consists of $M = e^{nR}$ n–vectors $\boldsymbol{x}_m \in \mathcal{X}^n$, $m = 1,2,\ldots,M$, which represent M different messages. We assume that all messages are equiprobable.

A decoder with an erasure option is a partition of $\mathcal{Y}^n$ into $(M+1)$ regions, $\mathcal{R}_0,\mathcal{R}_1,\ldots,\mathcal{R}_M$. This decoder works as follows: If $\boldsymbol{y}$ falls into $\mathcal{R}_m$, $m = 1,2,\ldots,M$, a decision is made in favor of message m. If $\boldsymbol{y} \in \mathcal{R}_0$, no decision is made and an erasure is declared. We will refer to $\mathcal{R}_0$ as the *erasure event.* Given a code $\mathcal{C} = \{\boldsymbol{x}_1,\ldots,\boldsymbol{x}_M\}$ and a decoder $\mathcal{R} = (\mathcal{R}_0,\mathcal{R}_1,\ldots,\mathcal{R}_m)$, we define two additional undesired events. The event $\mathcal{E}_1$ is the event of not making the right decision. This event is the disjoint union of the erasure event and the it undetected error event $\mathcal{E}_2$, namely, the event of making the wrong decision. The probabilities of these events are as follows:

$$\Pr\{\mathcal{E}_1\} = \sum_{m=1}^{M}\sum_{\boldsymbol{y}\in\mathcal{R}_m^c} P(\boldsymbol{x}_m,\boldsymbol{y}) = \frac{1}{M}\sum_{m=1}^{M}\sum_{\boldsymbol{y}\in\mathcal{R}_m^c} P(\boldsymbol{y}|\boldsymbol{x}_m) \tag{5}$$

$$\Pr\{\mathcal{E}_2\} = \sum_{m=1}^{M}\sum_{\boldsymbol{y}\in\mathcal{R}_m}\sum_{m'\neq m} P(\boldsymbol{x}_{m'},\boldsymbol{y}) = \frac{1}{M}\sum_{m=1}^{M}\sum_{\boldsymbol{y}\in\mathcal{R}_m}\sum_{m'\neq m} P(\boldsymbol{y}|\boldsymbol{x}_{m'}) \tag{6}$$

$$\Pr\{\mathcal{R}_0\} = \Pr\{\mathcal{E}_1\} - \Pr\{\mathcal{E}_2\}. \tag{7}$$

Forney [6] shows that the best tradeoff between $\Pr\{\mathcal{E}_1\}$ and $\Pr\{\mathcal{E}_2\}$ is attained by the decoder $\mathcal{R}^* = (\mathcal{R}_0^*, \mathcal{R}_1^*, \ldots, \mathcal{R}_M^*)$ defined by

$$\begin{aligned}
\mathcal{R}_m^* &= \left\{\boldsymbol{y}:\ \frac{P(\boldsymbol{y}|\boldsymbol{x}_m)}{\sum_{m'\neq m} P(\boldsymbol{y}|\boldsymbol{x}_{m'})} \geq e^{nT}\right\}, \quad m = 1, 2, \ldots, M \\
\mathcal{R}_0^* &= \bigcap_{m=1}^{M} (\mathcal{R}_m^*)^c, \qquad (8)
\end{aligned}$$

where $(\mathcal{R}_m^*)^c$ is the complement of $\mathcal{R}_m^*$, and where $T \geq 0$ is a parameter, henceforth referred to as the *threshold*, which controls the balance between the probabilities of $\mathcal{E}_1$ and $\mathcal{E}_2$. Forney devotes the remaining part of his paper [6] to derive lower bounds, as well as to investigate properties, of the random coding exponents (associated with $\mathcal{R}^*$), $E_1(R,T)$ and $E_2(R,T)$, of $\overline{\Pr}\{\mathcal{E}_1\}$ and $\overline{\Pr}\{\mathcal{E}_2\}$, the average probabilities of $\mathcal{E}_1$ and $\mathcal{E}_2$, respectively, (w.r.t.) the ensemble of randomly selected codes, drawn independently according to an i.i.d. distribution $P(\boldsymbol{x}) = \prod_{i=1}^n P(x_i)$.

3 Main Result

Our main result in this paper is the following:

Theorem 1 *Assume that the random coding distribution $\{P(x),\ x \in \mathcal{X}\}$ and the channel transition matrix $\{P(y|x),\ x \in \mathcal{X},\ y \in \mathcal{Y}\}$ are such that for every real s,*

$$\gamma_y(s) \stackrel{\Delta}{=} -\ln\left[\sum_{x\in\mathcal{X}} P(x)P^s(y|x)\right] \qquad (9)$$

is independent of y, in which case, it will be denoted by $\gamma(s)$. Let s_R be the solution to the equation

$$\gamma(s) - s\gamma'(s) = R, \qquad (10)$$

where $\gamma'(s)$ is the derivative of $\gamma(s)$. Finally, let

$$E_1^*(R,T,s) = \Lambda(R,s) + \gamma(1-s) - sT - \ln|\mathcal{Y}| \qquad (11)$$

where

$$\Lambda(R,s) = \begin{cases} \gamma(s) - R & s \geq s_R \\ s\gamma'(s_R) & s < s_R \end{cases} \tag{12}$$

Then,

$$\overline{Pr}\{\mathcal{E}_1\} \stackrel{\cdot}{\leq} e^{-nE_1^*(R,T)} \tag{13}$$

where $E_1^*(R,T) = \sup_{s\geq 0} E_1^*(R,T,s)$ *and*

$$\overline{Pr}\{\mathcal{E}_2\} \stackrel{\cdot}{\leq} e^{-nE_2^*(R,T)} \tag{14}$$

where $E_2^*(R,T) = E_1^*(R,T) + T$*. Also,* $E_1^*(R,T) \geq E_1(R,T)$*, where* $E_1(R,T)$ *is given in (1).*

Three comments are in order regarding the condition that $\gamma_y(s)$ of eq. (9) is independent of y.

First, observe that this condition is obviously satisfied when $\{P(x)\}$ is uniform and the columns of the matrix $\{a_{xy}\} = \{P(y|x)\}$ are permutations of each other, because then the summations $\sum_x P(x)P^s(y|x)$, for the various y's, consist of exactly the same terms, just in a different order. This is the case, for example, when $\mathcal{X} = \mathcal{Y}$ is a group endowed with an addition/subtraction operation (e.g., addition/subtraction modulo the alphabet size), and the channel is additive in the sense that the 'noise' $(Y - X)$ is statistically independent of X. Somewhat more generally, the condition $\gamma_y(s) = \gamma(s)$ for all y holds when the different columns of the matrix $\{P(y|x)\}$ are formed by permutations of each other subject to the following rule: $P(y|x)$ can be permuted with $P(y|x')$ if $P(x) = P(x')$.

Second, the derivation of the bound can be carried out, in principle, even without this condition. In this case, one obtains an exponential expression that depends, for each $\boldsymbol{y}$, on the empirical distribution $\hat{P}_{\boldsymbol{y}}$, and its summation over $\boldsymbol{y}$ can then be handled using the method of types, which involves optimization over $\{\hat{P}_{\boldsymbol{y}}\}$. But then we are loosing the simplicity of the bound.

Finally, even when the condition holds, it is not apparent that the expression of Forney's bound $E_1(R,T)$ can be simplified directly in a trivial manner, nor can we see how the optimum parameters ρ and s can be found analytically in closed form.

4 Derivation of the New Bound

4.1 Background

The first few steps of the derivation are similar to those in [6]: For a given code and for every $s \geq 0$,

$$\begin{aligned}
\Pr\{\mathcal{E}_1\} &= \frac{1}{M}\sum_{m=1}^{M}\sum_{\boldsymbol{y}\in(\mathcal{R}_m^*)^c} P(\boldsymbol{y}|\boldsymbol{x}_m) \\
&= \frac{1}{M}\sum_{m=1}^{M}\sum_{\boldsymbol{y}\in\mathcal{Y}^n} P(\boldsymbol{y}|\boldsymbol{x}_m)\cdot 1\left\{\frac{e^{nT}\sum_{m'\neq m}P(\boldsymbol{y}|\boldsymbol{x}_{m'})}{P(\boldsymbol{y}|\boldsymbol{x}_m)}\geq 1\right\} \\
&\leq \frac{1}{M}\sum_{m=1}^{M}\sum_{\boldsymbol{y}\in\mathcal{Y}^n} P(\boldsymbol{y}|\boldsymbol{x}_m)\left(\frac{e^{nT}\sum_{m'\neq m}P(\boldsymbol{y}|\boldsymbol{x}_{m'})}{P(\boldsymbol{y}|\boldsymbol{x}_m)}\right)^s \\
&= \frac{e^{nsT}}{M}\sum_{m=1}^{M}\sum_{\boldsymbol{y}\in\mathcal{Y}^n} P^{1-s}(\boldsymbol{y}|\boldsymbol{x}_m)\left(\sum_{m'\neq m}P(\boldsymbol{y}|\boldsymbol{x}_{m'})\right)^s. \qquad (15)
\end{aligned}$$

As for $\mathcal{E}_2$, we have similarly,

$$\Pr\{\mathcal{E}_2\} \leq e^{-n(1-s)T}\sum_{\boldsymbol{y}\in\mathcal{Y}^n} P^{1-s}(\boldsymbol{y}|\boldsymbol{X}_m)\left(\sum_{m'\neq m}P(\boldsymbol{y}|\boldsymbol{X}_{m'})\right)^s. \qquad (16)$$

Since this differs from the bound on $\Pr\{\mathcal{E}_1\}$ only by the constant factor e^{-nT}, it will be sufficient to focus on $\mathcal{E}_1$ only. Taking now the expectation w.r.t. the ensemble of codes, and using the fact that $\boldsymbol{X}_m$ is independent of all other codewords, we get:

$$\overline{\Pr}\{\mathcal{E}_1\} \leq e^{nsT}\sum_{\boldsymbol{y}\in\mathcal{Y}^n}\boldsymbol{E}\{P^{1-s}(\boldsymbol{y}|\boldsymbol{X}_m)\}\cdot\boldsymbol{E}\left\{\left(\sum_{m'\neq m}P(\boldsymbol{y}|\boldsymbol{X}_{m'})\right)^s\right\}. \qquad (17)$$

The first factor of the summand is easy to handle:

$$\boldsymbol{E}\{P^{1-s}(\boldsymbol{y}|\boldsymbol{X}_m)\} = \sum_{\boldsymbol{x}\in\mathcal{X}^n}P(\boldsymbol{x})P^{1-s}(\boldsymbol{y}|\boldsymbol{x}) = \prod_{i=1}^{n}[\sum_{x\in\mathcal{X}}P(x)P^{1-s}(y_i|x)] = e^{-n\gamma(1-s)}. \qquad (18)$$

Concerning the second factor, Forney's approach is to use the inequality $(\sum_i a_i)^r \le \sum_i a_i^r$, which holds when $\{a_i\}$ are positive and $r \le 1$, in order to upper bound $\boldsymbol{E}\{(\sum_{m'\ne m} P(\boldsymbol{y}|\boldsymbol{X}_{m'}))^s\}$ by $\boldsymbol{E}\{(\sum_{m'\ne m} P(\boldsymbol{y}|\boldsymbol{X}_{m'})^{s/\rho})^\rho\}$ for $\rho \ge s$, and then use Jensen's inequality to insert the expectation into the brackets, which is allowed by limiting ρ to lie in $[0,1]$. In other words, the above expression is further upper bounded in [6] by $(\sum_{m'\ne m} \boldsymbol{E}\{P(\boldsymbol{y}|\boldsymbol{X}_{m'})^{s/\rho}\})^\rho$, $0 \le \rho \le 1$.

We will use a different route, where all steps of the derivation will be clearly exponentially tight, and without introducing the additional parameter ρ. To simplify the exposition and make it easier to gain some geometrical insight, it will be instructive to begin with the special case of the BSC and the uniform random coding distribution. The extension to more general DMC's and random coding distributions will be given in Subsection 4.3.

4.2 The BSC with the uniform random coding distribution

Consider the case where $\mathcal{X} = \mathcal{Y} = \{0,1\}$, the channel is a BSC with a crossover probability p, and the random coding distribution is $P(\boldsymbol{x}) = 2^{-n}$ for all $\boldsymbol{x} \in \{0,1\}^n$. First, concerning the first factor in the summand of (17), we have, in this special case:

$$\gamma(1-s) = -\ln\left[\frac{1}{2}p^{1-s} + \frac{1}{2}(1-p)^{1-s}\right] = \ln 2 - \ln[p^{1-s} + (1-p)^{1-s}]. \tag{19}$$

As for the second factor, we proceed as follows. Define $\alpha = \ln\frac{1-p}{p}$ and for a given $\boldsymbol{y}$, let $N_{\boldsymbol{y}}(d)$ denote distance enumerator relative to $\boldsymbol{y}$, that is, the number of incorrect codewords $\{\boldsymbol{x}_{m'},\ m' \ne m\}$ at Hamming distance d from $\boldsymbol{y}$. We then have:

$$\begin{aligned}
\boldsymbol{E}\left\{\left(\sum_{m'\ne m} P(\boldsymbol{y}|\boldsymbol{X}_{m'})\right)^s\right\} &= \boldsymbol{E}\left\{\left[(1-p)^n \sum_{d=0}^{n} N_{\boldsymbol{y}}(d)e^{-\alpha d}\right]^s\right\} \\
&\doteq \boldsymbol{E}\left\{\left[(1-p)^n \max_d N_{\boldsymbol{y}}(d)e^{-\alpha d}\right]^s\right\} \\
&\doteq (1-p)^{ns}\boldsymbol{E}\left\{\max_d N_{\boldsymbol{y}}^s(d)e^{-\alpha s d}\right\}
\end{aligned}$$

$$
\begin{aligned}
&\doteq \quad (1-p)^{ns}\boldsymbol{E}\left\{\sum_{d=0}^{n} N_{\boldsymbol{y}}^{s}(d)e^{-\alpha s d}\right\} \\
&\doteq \quad (1-p)^{ns}\sum_{d=0}^{n}\boldsymbol{E}\{N_{\boldsymbol{y}}^{s}(d)\}e^{-\alpha s d}. \qquad (20)
\end{aligned}
$$

The exponential equalities form the *first main point* in our approach: They hold, even before taking the expectations, because the summation over d consists of a *subexponential* number of terms (as opposed to the exponential number of terms in the original summation over the codewords). Thus, the key issue here is how to assess the power–s moments of the distance enumerator $N_{\boldsymbol{y}}(d)$. To this end, we have to distinguish between two ranges of d, or equivalently, $\delta = d/n$. Let $\delta_{GV}(R)$ denote the normalized Gilbert–Varshamov (GV) distance, $\delta_{GV} = d_{GV}/n$, i.e., the smaller solution, δ, to the equation $h(\delta) = \ln 2 - R$, where $h(\delta) = -\delta\ln\delta - (1-\delta)\ln(1-\delta), \quad \delta \in [0,1]$.

Now, the *second main point* of the proposed approach is that $\boldsymbol{E}\{N_{\boldsymbol{y}}^{s}(d)\}$ behaves differently[1] for the case $\delta_{GV}(R) \le \delta \le 1-\delta_{GV}(R)$ and for the case $\delta < \delta_{GV}(R)$ or $\delta > 1-\delta_{GV}(R)$. Let us define then $\mathcal{G}_R = \{\delta : \ \delta_{GV}(R) \le \delta \le 1-\delta_{GV}(R)\}$. In particular, using the large deviations behavior of $N_{\boldsymbol{y}}(n\delta)$, $\delta \in [0,1]$, as the sum of $e^{nR}-1$ binary i.i.d. RV's, it is easily seen[2] that

$$
\boldsymbol{E}\{N_{\boldsymbol{y}}^{s}(n\delta)\} \doteq \begin{cases} e^{ns[R+h(\delta)-\ln 2]} & \delta \in \mathcal{G}_R \\ e^{n[R+h(\delta)-\ln 2]} & \delta \in \mathcal{G}_R^c. \end{cases} \qquad (21)
$$

Thus,

$$
\begin{aligned}
&\boldsymbol{E}\left\{\left(\sum_{m'\neq m} P(\boldsymbol{y}|\boldsymbol{X}_{m'})\right)^{s}\right\} \\
&\doteq \quad (1-p)^{ns}\left[\sum_{\delta\in\mathcal{G}_R} e^{ns[R+h(\delta)-\ln 2]}\cdot e^{-\alpha s n\delta} + \sum_{\delta\in\mathcal{G}_R^c} e^{n[R+h(\delta)-\ln 2]}\cdot e^{-\alpha s n\delta}\right]
\end{aligned}
$$

[1] The intuition behind this different behavior is that when $h(\delta)+R-\ln 2 > 0$, the RV $N_{\boldsymbol{y}}(d)$, which is the sum of $e^{nR}-1$ many i.i.d. binary RV's, $1\{d(\boldsymbol{X}_{m'},\boldsymbol{y}) = d\}$, concentrates extremely (double–exponentially) rapidly around its expectation $e^{n[R+h(\delta)-\ln 2]}$, whereas for $h(\delta)+R-\ln 2 < 0$, $N_{\boldsymbol{y}}(d)$ is typically zero, and so, the dominant term of $\boldsymbol{E}\{N_{\boldsymbol{y}}^{s}(d)\}$ is $1^s \cdot \Pr\{N_{\boldsymbol{y}}(d) = 1\} \approx e^{n[R+h(\delta)-\ln 2]}$. This is analogous to the behavior observed in the random energy model (REM) of spin glasses (cf. [4]) where this change in behavior yields a phase transition.

[2] See the Appendix of the ArXiv version [13] of this paper, which is omitted here for the sake of brevity.

$$\doteq \quad (1-p)^{ns}\left[e^{ns(R-\ln 2)}\cdot\exp\{ns\max_{\delta\in\mathcal{G}_R}[h(\delta)-\alpha\delta]\}+e^{n(R-\ln 2)}\cdot\exp\{n\max_{\delta\in\mathcal{G}_R^c}[h(\delta)-\alpha s\delta]\}\right] \tag{22}$$

As we are considering rates below capacity, $p<\delta_{GV}(R)$ or $p>1-\delta_{GV}(R)$. We also assume that $p<1/2$, which will leave us only with the first possibility of $p<\delta_{GV}(R)$. Therefore, the global (unconstrained) maximum of $h(\delta)-\alpha\delta$, which is attained at $\delta=p$, falls outside $\mathcal{G}_R$, and so, $\max_{\delta\in\mathcal{G}_R}[h(\delta)-\alpha\delta]$ is attained at $\delta=\delta_{GV}(R)$ which yields

$$\max_{\delta\in\mathcal{G}_R}[h(\delta)-\alpha\delta]=h(\delta_{GV}(R))-\alpha\delta_{GV}(R)=\ln 2-R-\alpha\delta_{GV}(R).$$

Thus, the first term in the large square brackets of the r.h.s. of (22) is of the exponential order of $e^{-ns\alpha\delta_{GV}(R)}$. As for the second term, the unconstrained maximum of $h(\delta)-\alpha s\delta$ is obtained at $\delta=p_s\stackrel{\Delta}{=}\frac{p^s}{p^s+(1-p)^s}$, which can be either larger or smaller than $\delta_{GV}(R)$, depending on s. Specifically,

$$\max_{\delta\in\mathcal{G}_R^c}[h(\delta)-\alpha s\delta]=\left\{\begin{array}{ll} h(p_s)-\alpha s p_s & p_s\le\delta_{GV}(R)\\ \ln 2-R-\alpha s\delta_{GV}(R) & p_s>\delta_{GV}(R)\end{array}\right. \tag{23}$$

The condition $p_s\le\delta_{GV}(R)$ is equivalent to $s\ge s_R\stackrel{\Delta}{=}(\ln[(1-\delta_{GV}(R))/\delta_{GV}(R)])/\alpha$. Thus, the second term in the square brackets of the r.h.s. of eq. (22) is of the order of $e^{-n\mu(s,R)}$, where

$$\mu(s,R)=\left\{\begin{array}{ll}\mu_0(s,R) & s\ge s_R\\ \alpha s\delta_{GV}(R) & s<s_R\end{array}\right. \tag{24}$$

and where

$$\begin{aligned}\mu_0(s,R) &= \alpha s p_s-h(p_s)+\ln 2-R\\ &= s\ln(1-p)-\ln[p^s+(1-p)^s]+\ln 2-R.\end{aligned} \tag{25}$$

Next, observe that the second term, $e^{-n\mu(s,R)}$, is always the dominant term: For $s<s_R$, this is trivial as both terms behave like $e^{-n\alpha s\delta_{GV}(R)}$. For $s\ge s_R$ (namely, $p_s\le\delta_{GV}(R)$), as $\delta=p_s$ achieves the *global* minimum of the function $f(\delta)\stackrel{\Delta}{=}\alpha s\delta-h(\delta)+\ln 2-R$, we have

$$\mu_0(s,R)=f(p_s)\le f(\delta_{GV}(R))=\alpha s\delta_{GV}(R).$$

Therefore, we have established that

$$\boldsymbol{E}\left\{\left(\sum_{m'\neq m} P(\boldsymbol{y}|\boldsymbol{X}_{m'})\right)^s\right\} \doteq \exp\left\{-n\left[s\ln\frac{1}{1-p}+\mu(s,R)\right]\right\} \tag{26}$$

independently of $\boldsymbol{y}$. Finally, we get:

$$\overline{\Pr}\{\mathcal{E}_1\} \stackrel{\cdot}{\leq} e^{nsT}\cdot 2^n \cdot e^{-n[\ln 2-\ln(p^{1-s}+(1-p)^{1-s})]}\cdot\exp\left\{-n\left[s\ln\frac{1}{1-p}+\mu(s,R)\right]\right\} = e^{-nE_1(R,T,s)} \tag{27}$$

where

$$E_1(R,T,s) \stackrel{\Delta}{=} \mu(s,R)+s\ln\frac{1}{1-p}-\ln[p^{1-s}+(1-p)^{1-s}]-sT.$$

We next derive closed form expressions for the optimum value of s, denoted s_{opt}, using the following consideration: We have seen that $E_1^*(R,T,s)$ is given by

$$F(s) \stackrel{\Delta}{=} \mu_0(s,R)+s\ln\frac{1}{1-p}-\ln[p^{1-s}+(1-p)^{1-s}]-sT$$

for $s\geq s_R$, and by

$$G(s) \stackrel{\Delta}{=} \alpha s\delta_{GV}(R)+s\ln\frac{1}{1-p}-\ln[p^{1-s}+(1-p)^{1-s}]-sT$$

for $s<s_R$. Both $F(s)$ and $G(s)$ are concave functions and hence have a unique maximum each. We have also seen that $F(s)\leq G(s)$ for all s, with equality at $s=s_R$ and only at that point. This means that $F(s)$ and $G(s)$ are tangential to each other at $s=s_R$, i.e., $F(s_R)=G(s_R)$ and $F'(s_R)=G'(s_R)$, where F' and G' are the derivatives of F and G, respectively. Now, there are three possibilities: If $F'(s_R)=G'(s_R)=0$, then $s_{\mathrm{opt}}=s_R$. If $F'(s_R)=G'(s_R)<0$, then $s_{\mathrm{opt}}<s_R$ is found by solving the equation $G'(s)=0$. If $F'(s_R)=G'(s_R)>0$, then $s_{\mathrm{opt}}>s_R$ is found by solving the equation $F'(s)=0$.

Assume first that $s_{\mathrm{opt}}<s_R$. Then, the equation $G'(s)=0$ is equivalent to:

$$\alpha\delta_{GV}(R)+\ln\frac{1}{1-p}+p_{1-s}\ln p+(1-p_{1-s})\ln(1-p)-T=0$$

or $\alpha p_{1-s} = \alpha\delta_{GV}(R) - T$ whose solution is:

$$s^* = 1 - \frac{1}{\alpha}\ln\frac{\alpha(1-\delta_{GV}(R)) + T}{\alpha\delta_{GV}(R) - T}. \tag{28}$$

Of course, if the r.h.s. of (28) turns out to be negative, then $s_{\mbox{opt}} = 0$. Thus, overall

$$s_{\mbox{opt}} = s_1(p,R,T) \stackrel{\triangle}{=} \left[1 - \frac{1}{\alpha}\ln\frac{\alpha(1-\delta_{GV}(R)) + T}{\alpha\delta_{GV}(R) - T}\right]_+, \tag{29}$$

where $[x]_+ \stackrel{\triangle}{=} \max\{x, 0\}$.

Next, assume that $s_{\mbox{opt}} > s_R$. In this case,

$$\begin{aligned} E_1(R,T,s) &= F(s) \\ &= \ln 2 - \ln[p^s + (1-p)^s] - \ln[p^{1-s} + (1-p)^{1-s}] - R - sT. \end{aligned} \tag{30}$$

Thus, the optimum s minimizes the convex function

$$\begin{aligned} f(s) &= \ln[p^s + (1-p)^s] + \ln[p^{1-s} + (1-p)^{1-s}] + sT \\ &= \ln\left[1 + (1-p)\left(\frac{p}{1-p}\right)^s + p\left(\frac{1-p}{p}\right)^s\right] + sT. \end{aligned} \tag{31}$$

Equating the derivative to zero, we get:

$$f'(s) \equiv \frac{-\left(\frac{p}{1-p}\right)^s \cdot (1-p)\alpha + \left(\frac{1-p}{p}\right)^s \cdot p\alpha}{1 + (1-p)\left(\frac{p}{1-p}\right)^s + p\left(\frac{1-p}{p}\right)^s} + T = 0 \tag{32}$$

or equivalently, defining $z = e^{\alpha s}$ as the unknown, we get:

$$\frac{-(1-p)/z + pz}{1 + (1-p)/z + pz} = -\frac{T}{\alpha},$$

which is a quadratic equation whose relevant (positive) solution is:

$$z = z_0 \stackrel{\triangle}{=} \frac{\sqrt{T^2 + 4p(1-p)(\alpha^2 - T^2)} - T}{2p(T+\alpha)}$$

provided[3] that $T < \alpha$, and so the derivative vanishes at

$$s_{\text{opt}} = s_2(p,T) \stackrel{\triangle}{=} \frac{1}{\alpha}\ln\left[\frac{\sqrt{T^2+4p(1-p)(\alpha^2-T^2)}-T}{2p(T+\alpha)}\right].$$

It is not difficult to verify that s_{opt} never exceeds unity. Also, s_{opt} is always positive ($z_0 \geq 1$) since the condition $F'(s_R) > 0$, which is equivalent to the condition $T < \alpha(p_{s_R} - p_{1-s_R})$, implies $T < \alpha/2$, which in turn is the condition for $s_{\text{opt}} > 0$. Note that for $T = 0$, we obtain $s_2(p,0) = 1/2$, in agreement with the Bhattacharyya bound.

In summary, the behavior of the solution can be described as follows: As R increases from 0 to $C = \ln 2 - h(p)$, s_R increases correspondingly from 0 to 1, and so, the expression $\alpha(p_{s_R} - p_{1-s_R})$ (which is positive as long as $R < \ln 2 - h(p_{1/2})$) decreases. As long as this expression is still larger than T, we have $F'(s_R) > 0$ and the relevant expression of $E_1^*(R,T,s)$ is $F(s)$, which is maximized at $s = s_2(p,T)$ independently of R. At this range, the slope of $E_1^*(R,T)$, as a function of R, is -1. As R continues to increase, we cross the point where $F'(s_R) = 0$ (a point which can be thought of as an analogue to the critical rate of ordinary decoding) and enter into the region where $F'(s_R) < 0$, for which $E_1^*(R,T) = G(s_1(p,R,T))$.

4.3 More General DMC's and Random Coding Distributions

Assume now a general DMC $\{P(y|x),\ x \in \mathcal{X},\ y \in \mathcal{Y}\}$ and a general i.i.d. random coding distribution $P(\boldsymbol{x}) = \prod_{i=1}^n P(x_i)$ that satisfy the condition of Theorem 1. As for the second factor of the summand of (17), we have the following:

$$\begin{aligned}\boldsymbol{E}\left\{\left(\sum_{m'\neq m} P(\boldsymbol{y}|\boldsymbol{X}_{m'})\right)^s\right\} &= \boldsymbol{E}\left\{\left(\sum_{Q_{x|y}} N_{\boldsymbol{y}}(Q_{x|y})\cdot\exp\{n\boldsymbol{E}_Q\ln P(Y|X)\}\right)^s\right\}\\ &\doteq \sum_{Q_{x|y}} \boldsymbol{E}\{N_{\boldsymbol{y}}^s(Q_{x|y})\}\cdot\exp\{ns\boldsymbol{E}_Q\ln P(Y|X)\},\end{aligned} \quad (33)$$

[3] Note that if $T > \alpha$, the decoder will always erase (even for $R = 0$) since for $p < 1/2$, we have $P(\boldsymbol{y}|\boldsymbol{x}_m)/[\sum_{m'\neq m} P(\boldsymbol{y}|\boldsymbol{x}_{m'})] \leq (1-p)^n/p^n = e^{\alpha n} < e^{nT}$.

where $N_{\boldsymbol{y}}(Q_{x|y})$ is the number of incorrect codewords whose conditional empirical distribution[4] with $\boldsymbol{y}$ is $Q_{x|y}$ and $\boldsymbol{E}_Q$ is the expectation operator associated with $\hat{P}_{\boldsymbol{y}} \times Q_{x|y}$. Define

$$\mathcal{G}_R = \{Q_{x|y}:\ R + H_Q(X|Y) + \boldsymbol{E}_Q \ln P(X) \geq 0\},$$

where $H_Q(X|Y)$ is the conditional entropy induced by $\hat{P}_{\boldsymbol{y}} \times Q_{x|y}$. Analogously to the case of the BSC (see also [13, Appendix]), we have:

$$\boldsymbol{E}\{N^s_{\boldsymbol{y}}(Q_{x|y})\} \doteq \begin{cases} \exp\{ns[R + H_Q(X|Y) + \boldsymbol{E}_Q \ln P(X)]\} & Q_{x|y} \in \mathcal{G}_R \\ \exp\{n[R + H_Q(X|Y) + \boldsymbol{E}_Q \ln P(X)]\} & Q_{x|y} \in \mathcal{G}^c_R \end{cases} \tag{34}$$

Thus,

$$\begin{aligned} \boldsymbol{E}\left\{\left(\sum_{m'\neq m} P(\boldsymbol{y}|\boldsymbol{X}_{m'})\right)^s\right\} \quad &\doteq \quad \sum_{Q_{x|y}\in\mathcal{G}_R} \exp\{ns[R + H_Q(X|Y) + \boldsymbol{E}_Q \ln P(X)]\} \times \\ &\quad \exp\{ns\boldsymbol{E}_Q \ln P(Y|X)\} + \\ &\quad \sum_{Q_{x|y}\in\mathcal{G}^c_R} \exp\{n[R + H_Q(X|Y) + \boldsymbol{E}_Q \ln P(X)]\} \times \\ &\quad \exp\{ns\boldsymbol{E}_Q \ln P(Y|X)\} \\ &\stackrel{\triangle}{=} \quad A + B. \end{aligned} \tag{35}$$

As for A, we obtain:

$$A \doteq \exp\{ns[R + \max_{Q_{x|y}\in\mathcal{G}_R}(H_Q(X|Y) + \boldsymbol{E}_Q \ln[P(X)P(Y|X)])]\}. \tag{36}$$

Note that without the constraint $Q_{x|y} \in \mathcal{G}_R$, the maximum of $(H_Q(X|Y) + \boldsymbol{E}_Q \ln[P(X)P(Y|X)])$ is attained at

$$Q_{x|y}(x|y) = P_{x|y}(x|y) \stackrel{\triangle}{=} \frac{P(x)P(y|x)}{\sum_{x\in\mathcal{X}} P(x')P(y|x')}.$$

But since $R < I(X;Y)$, then $P_{x|y}$ is in $\mathcal{G}^c_R$. We argue then that the optimum $Q_{x|y}$ in $\mathcal{G}_R$ is on the boundary of $\mathcal{G}_R$, i.e., it satisfies $R + H_Q(X|Y) + \boldsymbol{E}_Q \ln P(X) = 0$. To see why this is true, consider

[4] By "conditional empirical distribution" we mean the relative frequency of the various symbols of x that appear as channel inputs for a given channel output symbol y.

the following argument: Let $Q^0_{x|y}$ be any internal point in $\mathcal{G}_R$ and consider the conditional pmf $Q^t=(1-t)Q^0_{x|y}+tP_{x|y}$, $t\in[0,1]$. Define $f(t)=H_{Q^t}(X|Y)+\boldsymbol{E}_{Q^t}\ln[P(X)P(Y|X)]$. Obviously, f is concave and $f(0)\le f(1)$. Now, since $Q^0\in\mathcal{G}_R$ and $Q^1=P_{x|y}\in\mathcal{G}^c_R$, then by the continuity of the function $R+H_{Q^t}(X|Y)+\boldsymbol{E}_{Q^t}\ln P(X)$, there must be some $t=t_0$ for which Q^{t_0} is on the boundary of $\mathcal{G}_R$. By the concavity of f, $f(t_0)\ge(1-t_0)f(0)+t_0f(1)\ge f(0)$. Thus, any internal point of $\mathcal{G}_R$ can be improved by a point on the boundary between $\mathcal{G}_R$ and $\mathcal{G}^c_R$. Therefore, we have

$$\begin{aligned}
&\max_{Q_{x|y}\in\mathcal{G}_R}(H_Q(X|Y)+\boldsymbol{E}_Q\ln[P(X)P(Y|X)]))\\
=&\max_{\{Q_{x|y}:\ H_Q(X|Y)+\boldsymbol{E}_Q\ln P(X)=-R\}}[H_Q(X|Y)+\boldsymbol{E}_Q\ln P(X)+\boldsymbol{E}_Q\ln P(Y|X)]\\
=&\max_{\{Q_{x|y}:\ H_Q(X|Y)+\boldsymbol{E}_Q\ln P(X)=-R\}}[-R+\boldsymbol{E}_Q\ln P(Y|X)]\\
=&\ -R+\max_{\{Q_{x|y}:\ H_Q(X|Y)+\boldsymbol{E}_Q\ln P(X)=-R\}}\boldsymbol{E}_Q\ln P(Y|X)\\
=&\ -R+\max_{Q_{x|y}\in\mathcal{G}_R}\boldsymbol{E}_Q\ln P(Y|X) \qquad (37)
\end{aligned}$$

which means that $A\doteq e^{-ns\Delta(R)}$, where

$$\Delta(R)=\min_{Q_{x|y}\in\mathcal{G}_R}\boldsymbol{E}_Q\ln[1/P(Y|X)].$$

The achiever of $\Delta(R)$ is of the form

$$Q(x|y)=\frac{P(x)P^{s_R}(y|x)}{\sum_{x'\in\mathcal{X}}P(x')P^{s_R}(y|x')},$$

where s_R is such that $H_Q(X|Y)+\boldsymbol{E}_Q\ln P(X)=-R$, or equivalently, s_R is the solution [5] to the equation $s\gamma'(s)-\gamma(s)=R$. In other words,

$$\Delta(R)=\frac{\sum_{x\in\mathcal{X}}P(x)P^{s_R}(y|x)\ln[1/P(y|x)]}{\sum_{x\in\mathcal{X}}P(x)P^{s_R}(y|x)}=\gamma'(s_R).$$

[5] Observe that for $s=0$, $H_Q(X|Y)+\boldsymbol{E}_Q\ln P(X)=0$ and for $s=1$, $H_Q(X|Y)+\boldsymbol{E}_Q\ln P(X)=-I(X;Y)<-R$. Thus for $R<I(X;Y)$, $s_R\in[0,1)$.

Considering next the expression of B, we have:

$$B \doteq \exp\{n[R + \max_{Q_{x|y}\in\mathcal{G}_R^c}(H_Q(X|Y) + \boldsymbol{E}_Q \ln P(X) + s\boldsymbol{E}_Q \ln P(Y|X))]\}.$$

The unconstrained maximizer of $(H_Q(X|Y) + \boldsymbol{E}_Q \ln P(X) + s\boldsymbol{E}_Q \ln P(Y|X))$ is

$$Q_{x|y}^{(s)}(x|y) = \frac{P(x)P^s(y|x)}{\sum_{x'\in\mathcal{X}} P(x')P^s(y|x')}.$$

Now, there are two cases, depending on the value of s: If s is such that $Q_{x|y}^{(s)} \in \mathcal{G}_R^c$, or equivalently, $s > s_R$, then $B \doteq e^{-n[\gamma(s)-R]}$. If $Q_{x|y}^{(s)} \in \mathcal{G}_R$, namely, $s \leq s_R$, then once again, the optimum is attained at the boundary between $\mathcal{G}_R$ and $\mathcal{G}_R^c$, and then $B \doteq e^{-ns\gamma'(s_R)}$. In summary, $B \doteq e^{-n\Lambda(R,s)}$, where

$$\Lambda(R,s) = \begin{cases} \gamma(s) - R & s > s_R \\ s\gamma'(s_R) & s \leq s_R \end{cases}$$

The dominant term between A and B is obviously always B because it is either of the same exponential order of A, in the case $s \leq s_R$, or has a slower exponential decay, when $s > s_R$, as then the global (unconstrained) maximum of $[H_Q(X|Y) + \boldsymbol{E}_Q \ln P(X) + s\boldsymbol{E}_Q \ln P(Y|X)]$ is achieved. Thus, putting it all together, we get:

$$\overline{\Pr}\{\mathcal{E}_1\} \overset{\cdot}{\leq} e^{nsT} \cdot |\mathcal{Y}|^n \cdot e^{-n\gamma(1-s)} \cdot e^{-n\Lambda(R,s)} = e^{-nE_1^*(R,T,s)} \tag{38}$$

and the optimum $s \geq 0$ gives $E_1^*(R,T)$. The fact that $E_1^*(R,T) \geq E_1(R,T)$ stems from the fact that for the former, the evaluation of the exponential order is tight starting from the r.h.s. of eq. (17), whereas for the latter there are two inequalities for which the tightness of the exponential order is not obvious.

5 Comparing the Analysis Techniques for a Universal Decoder

In the section, we demonstrate that the proposed analysis technique sometimes gives strictly better exponential error bounds than the alternative route of using Jensen's inequality, as described earlier.

Consider the BSC with $p < 1/2$, as in Subsection 4.2, but this time, the channel is unknown and one employs a universal detector that operates according to the following decision rule: Select the message m if

$$\frac{e^{-n\beta\hat{h}(\boldsymbol{x}_m \oplus \boldsymbol{y})}}{\sum_{m' \neq m} e^{-n\beta\hat{h}(\boldsymbol{x}_{m'} \oplus \boldsymbol{y})}} \geq e^{nT} \tag{39}$$

where $\beta > 0$ is a free parameter and $\hat{h}(\boldsymbol{x} \oplus \boldsymbol{y})$ is the binary entropy pertaining to the relative number of 1's in the vector resulting from bit–by–bit XOR of $\boldsymbol{x}$ and $\boldsymbol{y}$, namely, the binary entropy function computed at the normalized Hamming distance between $\boldsymbol{x}$ and $\boldsymbol{y}$. If no message m satisfies (39), then an erasure is declared.

We have no optimality claims regarding this decision rule, but arguably, it is a reasonable decision rule (and hence there is motivation to analyze it): The minimization of $\hat{h}(\boldsymbol{x}_m \oplus \boldsymbol{y})$ among all codevectors $\{\boldsymbol{x}_m\}$, namely, the *minimum conditional entropy decoder* is a well–known universal decoding rule in the ordinary decoding regime, without erasures, which in the simple case of the BSC, is equivalent to the *maximum mutual information* (MMI) decoder [3] and to the *generalized likelihood ratio test* (GLRT) decoder, which jointly maximizes the likelihood over both the message and the unknown parameter. Here we adapt the minimum conditional entropy decoder to the structure proposed by an optimum decoder with erasures (see also [14]), where the unknown likelihood of each $\boldsymbol{x}_m$ is replaced by its maximum $e^{-n\hat{h}(\boldsymbol{x}_m \oplus \boldsymbol{y})}$, but with an additional degree of freedom of scaling the exponent by β, a design parameter that controls the relative importance of the codeword with the second highest score. For example, when $\beta \to \infty$,[6] only the first and the second highest scores count in the decision. From the statistical–mechanical point of view, the parameter β plays the role of the *inverse temperature*. In fact, the notion of *finite–temperature decoding* is not new even in ordinary decoding without erasures – it is due to Ruján [16].

[6] As β varies it is plausible to let T scale linearly with β.

To demonstrate the advantage of the proposed analysis technique, we now apply it in comparison to the approach of using Jensen's inequality and supplementing the parameter ρ in the bound. Let us analyze the probability of the event $\mathcal{E}_1$ of this decoder, namely, the event that the transmitted codeword $\boldsymbol{x}_m$ does not satisfy (39). We then have the following chain of inequalities, similarly as the analysis in Subsection 4.2, where the first few steps are common to the two analysis methods to be compared:

$$\begin{aligned}
\Pr\{\mathcal{E}_1\} &= \frac{1}{M}\sum_{m=1}^{M}\sum_{\boldsymbol{y}} P(\boldsymbol{y}|\boldsymbol{x}_m)\cdot 1\left\{\frac{e^{nT}\sum_{m'\neq m} e^{-n\beta\hat{h}(\boldsymbol{x}_{m'}\oplus\boldsymbol{y})}}{e^{-n\beta\hat{h}(\boldsymbol{x}_m\oplus\boldsymbol{y})}} \geq 1\right\} \\
&\leq \frac{1}{M}\sum_{m=1}^{M}\sum_{\boldsymbol{y}} P(\boldsymbol{y}|\boldsymbol{x}_m)\cdot \left[\frac{e^{nT}\sum_{m'\neq m} e^{-n\beta\hat{h}(\boldsymbol{x}_{m'}\oplus\boldsymbol{y})}}{e^{-n\beta\hat{h}(\boldsymbol{x}_m\oplus\boldsymbol{y})}}\right]^s \\
&= \frac{e^{nsT}}{M}\sum_{m=1}^{M}\sum_{\boldsymbol{y}} P(\boldsymbol{y}|\boldsymbol{x}_m)\cdot e^{n\beta s\hat{h}(\boldsymbol{x}_m\oplus\boldsymbol{y})}\cdot\left[\sum_{m'\neq m} e^{-n\beta\hat{h}(\boldsymbol{x}_{m'}\oplus\boldsymbol{y})}\right]^s \qquad (40)
\end{aligned}$$

Considering now the ensemble of codewords drawn indepedently by fair coin tossing, we have:

$$\begin{aligned}
\overline{\Pr}\{\mathcal{E}_1\} &\leq e^{nsT}\sum_{\boldsymbol{y}} \boldsymbol{E}\left\{P(\boldsymbol{y}|\boldsymbol{X}_1)\cdot\exp[n\beta s\hat{h}(\boldsymbol{X}_1\oplus\boldsymbol{y})]\right\}\cdot\boldsymbol{E}\left\{\left[\sum_{m>1}\exp[-n\beta\hat{h}(\boldsymbol{X}_m\oplus\boldsymbol{y})]\right]^s\right\} \\
&\stackrel{\triangle}{=} e^{nsT}\sum_{\boldsymbol{y}} A(\boldsymbol{y})\cdot B(\boldsymbol{y}) \qquad (41)
\end{aligned}$$

The computation of $A(\boldsymbol{y})$ is as follows: Denoting the Hamming weight of a binary sequence $\boldsymbol{z}$ by $w(\boldsymbol{z})$, we have:

$$\begin{aligned}
A(\boldsymbol{y}) &= \sum_{\boldsymbol{x}} 2^{-n}(1-p)^n\cdot\left(\frac{p}{1-p}\right)^{w(\boldsymbol{x}\oplus\boldsymbol{y})}\exp[n\beta s\hat{h}(\boldsymbol{x}\oplus\boldsymbol{y})] \\
&= \left(\frac{1-p}{2}\right)^n\sum_{\boldsymbol{z}}\exp\left[n\left(w(\boldsymbol{z})\ln\frac{p}{1-p}+\beta s\hat{h}(\boldsymbol{z})\right)\right] \\
&\doteq \left(\frac{1-p}{2}\right)^n\sum_{\delta} e^{nh(\delta)}\cdot\exp\left[n\left(\beta sh(\delta)-\delta\ln\frac{1-p}{p}\right)\right] \\
&\doteq \left(\frac{1-p}{2}\right)^n\exp\left[n\max_{\delta}\left((1+\beta s)h(\delta)-\delta\ln\frac{1-p}{p}\right)\right]. \qquad (42)
\end{aligned}$$

It is readily seen by ordinary optimization that

$$\max_{\delta}\left[(1+\beta s)h(\delta)-\delta\ln\frac{1-p}{p}\right] = (1+\beta s)\ln\left[p^{1/(1+\beta s)}+(1-p)^{1/(1+\beta s)}\right]-\ln(1-p)$$

and so upon substituting back into the the bound on $\overline{\Pr}\{\mathcal{E}_1\}$, we get:

$$\overline{\Pr}\{\mathcal{E}_1\} \le \exp\left[n\left(sT + (1+\beta s)\ln\left[p^{1/(1+\beta s)} + (1-p)^{1/(1+\beta s)}\right] - \ln 2\right)\right] \cdot \sum_{\boldsymbol{y}} B(\boldsymbol{y}). \qquad (43)$$

It remains then to assess the exponential order of $B(\boldsymbol{y})$ and this will now be done in two different ways. The first is Forney's way of using Jensen's inequality and introducing the additional parameter ρ, i.e.,

$$\begin{aligned} B(\boldsymbol{y}) &\le \boldsymbol{E}\left\{\left(\sum_{m>1} \exp[n\beta s\hat{h}(\boldsymbol{X}_m \oplus \boldsymbol{y})/\rho]\right)^{\rho}\right\} \\ &\le e^{n\rho R}\left(\boldsymbol{E}\left\{\exp[n\beta s\hat{h}(\boldsymbol{X}_m \oplus \boldsymbol{y})/\rho]\right\}\right)^{\rho}. \qquad (44) \end{aligned}$$

Now,

$$\begin{aligned} \boldsymbol{E}\left\{\exp[n\beta s\hat{h}(\boldsymbol{X}_m \oplus \boldsymbol{y})/\rho]\right\} &= 2^{-n}\sum_{\boldsymbol{z}} \exp[n\beta s\hat{h}(\boldsymbol{z})/\rho] \\ &\doteq 2^{-n}\sum_{\delta} e^{nh(\delta)} \cdot e^{n\beta s h(\delta)/\rho} \\ &= \exp[n([1-\beta s/\rho]_+ - 1)\ln 2], \qquad (45) \end{aligned}$$

where $[u]_+ \stackrel{\triangle}{=} \max\{u, 0\}$. Thus, we get $B(\boldsymbol{y}) \le \exp(n[\rho(R - \ln 2) + [\rho - \beta s]_+])$, which when substituted back into the bound on $\overline{\Pr}\{\mathcal{E}_1\}$, yields an exponential rate of

$$\begin{aligned} \tilde{E}_1(R,T) &= \max_{0\le s\le\rho\le 1}\{(\rho - [\rho - \beta s]_+)\ln 2 - \\ &\quad -(1+\beta s)\ln\left[p^{1/(1+\beta s)} + (1-p)^{1/(1+\beta s)}\right] - \rho R - sT\right\}. \qquad (46) \end{aligned}$$

On the other hand, estimating $B(\boldsymbol{y})$ by the alternative method, we have, similarly as in the analysis of Subsection 4.2:

$$\begin{aligned} B(\boldsymbol{y}) &= \boldsymbol{E}\left\{\left[\sum_{m>1} \exp[-n\beta\hat{h}(\boldsymbol{X}_m \oplus \boldsymbol{y})]\right]^{s}\right\} \\ &= \boldsymbol{E}\left\{\left[\sum_{\delta} N_{\boldsymbol{y}}(n\delta)\exp[-n\beta h(\delta)]\right]^{s}\right\} \end{aligned}$$

$$
\begin{aligned}
&\doteq \sum_{\delta} \boldsymbol{E}\{N^s_{\boldsymbol{y}}(n\delta)\} \cdot \exp(-n\beta s h(\delta)) \\
&\doteq \sum_{\delta \in \mathcal{G}^c_R} e^{n[R+h(\delta)-\ln 2]} \cdot \exp[-n\beta s h(\delta)] + \sum_{\delta \in \mathcal{G}_R} e^{ns[R+h(\delta)-\ln 2]} \cdot \exp[-n\beta s h(\delta)] \\
&\stackrel{\Delta}{=} U + V. \qquad (47)
\end{aligned}
$$

Now, U is dominated by the term $\delta = 0$ if $\beta s > 1$ and $\delta = \delta_{GV}(R)$ if $\beta s < 1$. It is then easy to see that $U \doteq \exp[-n(\ln 2 - R)(1 - [1-\beta s]_+)]$. Similarly, V is dominated by the term $\delta = 1/2$ if $\beta < 1$ and $\delta = \delta_{GV}(R)$ if $\beta \geq 1$. Thus, $V \doteq \exp[-ns(\beta[\ln 2 - R] - R[1-\beta]_+)]$. Therefore, defining

$$\phi(R, \beta, s) = \min\{(\ln 2 - R)(1 - [1-\beta s]_+), s(\beta[\ln 2 - R] - R[1-\beta]_+)\},$$

the resulting exponent is

$$\hat{E}_1(R,T) = \max_{s \geq 0} \left\{\phi(R,\beta,s) - (1+\beta s)\ln\left[p^{1/(1+\beta s)} + (1-p)^{1/(1+\beta s)}\right] - sT\right\}.$$

To compare numerical values of $\tilde{E}_1(R,T)$ and $\hat{E}_1(R,T)$, we have explored various values of the parameters p, β, R and T. While there are many quadruples (p, β, R, T) for which the two exponents coincide, there are also situations where $\hat{E}_1(R,T)$ exceeds $\tilde{E}_1(R,T)$. To demonstrate these situations, consider the values $p = 0.1$, $\beta = 0.5$, $T = 0.001$, and let R vary from 0 to 0.06 in steps of 0.01. Table 1 summarizes numerical values of both exponents, where the optimizations over ρ and s were conducted by an exhaustive search with a step size of 0.005 in each parameter. In the case of $\hat{E}_1(R,T)$, where $s \geq 0$ is not limited to the interval $[0,1]$ (since Jensen's inequality is not used), the numerical search over s was limited to the interval $[0,5]$.[7]

As can be seen (see also Fig. 1), the numerical values of the exponent $\hat{E}_1(R,T)$ are considerably larger than those of $\tilde{E}_1(R,T)$ in this example, which means that the analysis technique proposed in

[7] It is interesting to note that for some values of R, the optimum value s^* of the parameter s was indeed larger than 1. For example, at rate $R = 0$, we have $s^* = 2$ in the above search resolution.

	$R = 0.00$	$R = 0.01$	$R = 0.02$	$R = 0.03$	$R = 0.04$	$R = 0.05$	$R = 0.06$
$\tilde{E}_1(R,T)$	0.1390	0.1290	0.1190	0.1090	0.0990	0.0890	0.0790
$\hat{E}_1(R,T)$	0.2211	0.2027	0.1838	0.1642	0.1441	0.1231	0.1015

Table 1: Numerical values of $\tilde{E}_1(R,T)$ and $\hat{E}_1(R,T)$ as functions of R for $p = 0.1$, $\beta = 0.5$, and $T = 0.001$.

this paper, not only simplifies exponential error bounds, but sometimes leads also to significantly tighter bounds.

Acknowledgement

I would like to thank the Associate Editor, Ioannis Kontoyiannis, and the three anonymous reviewers for their very useful comments.

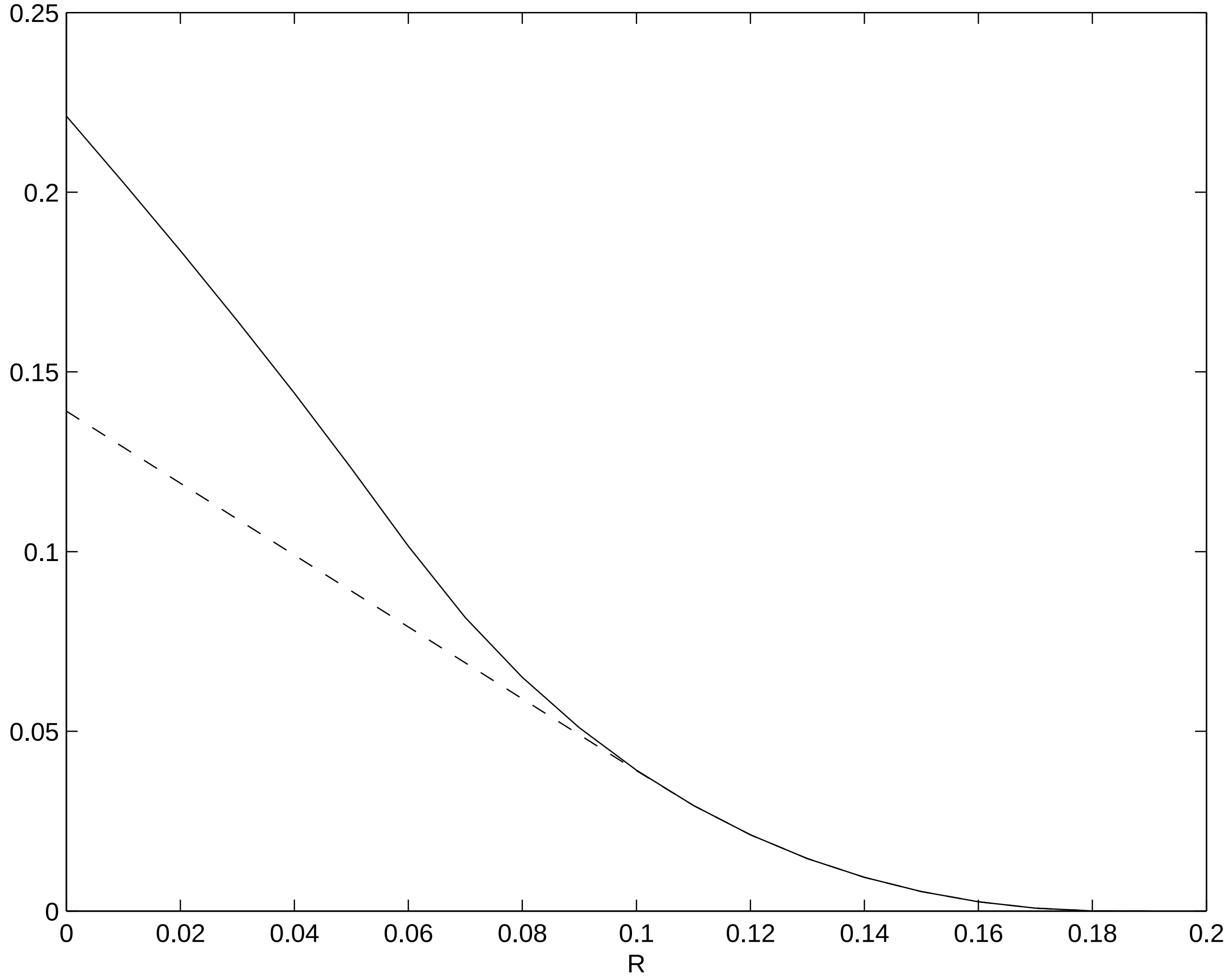

Figure 1: Graphs of $\hat{E}_1(R,T)$ (solid line) and $\tilde{E}_1(R,T)$ (dashed line) as functions of R for $p = 0.5$, $T = 0.001$ and $\beta = 0.5$.

References

[1] R. Ahlswede, N. Cai, and Z. Zhang, "Erasure, list, and detection zero–error capacities for low noise and a relation to identification," *IEEE Trans. Inform. Theory*, vol. 42, no. 1, pp. 55–62, January 1996.

[2] A. Barg and G. D. Forney, Jr., "Random codes: minimum distances and error exponents," *IEEE Trans. Inform. Theory*, vol. 48, no. 9, pp. 2568–2573, September 2002.

[3] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Academic Press 1981.

[4] B. Derrida, "The random energy model," *Physics Reports* (Review Section of Physics Letters), vol. 67, no. 1, pp. 29–35, 1980.

[5] R. G. Gallager, *Information Theory and Reliable Communication*, J. Wiley & Sons, 1968.

[6] G. D. Forney, Jr., "Exponential error bounds for erasure, list, and decision feedback schemes," *IEEE Trans. Inform. Theory*, vol. IT–14, no. 2, pp. 206–220, March 1968.

[7] R. Etkin, N. Merhav and E. Ordentlich, "Error exponents for the interference channel," to appear in *Proc. ISIT 2008*, Toronto, Canada, July 2008.

[8] T. Hashimoto, "Composite scheme LR+Th for decoding with erasures and its effective equivalence to Forney's rule," *IEEE Trans. Inform. Theory*, vol. 45, no. 1, pp. 78–93, January 1999.

[9] T. Hashimoto and M. Taguchi, "Performance and explicit error detection and threshold decision in decoding with erasures," *IEEE Trans. Inform. Theory*, vol. 43, no. 5, pp. 1650–1655, September 1997.

[10] Y. Kaspi and N. Merhav, ““Error exponents for degraded broadcast channels using statistics of distance enumerators,” in preparation.

[11] P. Kumar, Y.-H. Nam, and H. El Gamal, “On the error exponents of ARQ channels with deadlines,” *IEEE Trans. Inform. Theory*, vol. 53, no. 11, pp. 4265–4273, November 2007.

[12] N. Merhav, “Relations between random coding exponents and the statistical physics of random codes,” submitted to *IEEE Trans. Inform. Theory*, August 2007. Also, available on–line at: [http://www.ee.technion.ac.il/people/merhav/papers/p117.pdf].

[13] N. Merhav, “Error exponents of erasure/list decoding revisited via moments of distance enumerators,” [http://arxiv.org/PS_cache/arxiv/pdf/0711/0711.2501v1.pdf].

[14] N. Merhav and M. Feder, “Minimax universal decoding with an erasure option,” *IEEE Trans. Inform. Theory*, vol. 53, no. 5, pp. 1664–1675, May 2007.

[15] M. Mézard and A. Montanari, *Constraint satisfaction networks in physics and computation*, draft, February 27, 2006. [http://www.stanford.edu/∼montanar/BOOK/book.html].

[16] P. Ruján, “Finite temperature error–correcting codes,” *Phys. Rev. Let.*, vol. 70, no. 19, pp. 2968–2971, May 1993.

[17] A. J. Viterbi, “Error bounds for the white Gaussian and other very noisy memoryless channels with generalized decision regions,” *IEEE Trans. Inform. Theory*, vol. IT–15, no. 2, pp. 279–287, March 1969.