Saddlepoint Approximation of Random–Coding Bounds

Alfonso Martinez
Centrum Wiskunde & Informatica
1090 GB Amsterdam, The Netherlands
alfonso.martinez@ieee.org

Albert Guillén i Fàbregas
Department of Engineering
University of Cambridge
Cambridge, CB2 1PZ, UK
guillen@ieee.org

***Abstract*— This paper considers random-coding bounds to the decoding error probability with maximum-metric mismatched decoders. Their error exponents are determined and the saddlepoint approximation to the corresponding probability is derived. This approximation is accurate and allows for simple numerical evaluation, as verified for several channels of interest.**

I. Introduction

Two of the fundamental problems in the field of channel coding are characterizing the error probability attained by a given code construction and finding the largest achievable rate with vanishing error probability. While research has chiefly focused on the second problem, that of finding the channel capacity, recently, spurred by the construction of near-capacity achieving codes, renewed attention has been paid to the error probability in the finite-length regime. In particular, Polyanskiy *et al.* [1] have derived a number of new results, such as the random-coding union (RCU) bound, the dependence-testing bound (DT), and the $\kappa\beta$ bound among others. A key quantity in their development is the information density, defined as

$$i(\boldsymbol{x},\boldsymbol{y}) = \log\frac{P_{\boldsymbol{Y}|\boldsymbol{X}}(\boldsymbol{y}|\boldsymbol{x})}{P_{\boldsymbol{Y}}(\boldsymbol{y})} \tag{1}$$

where $P_{\boldsymbol{Y}|\boldsymbol{X}}(\boldsymbol{y}|\boldsymbol{x})$ is the vector channel transition probability and $\boldsymbol{x},\boldsymbol{y}$ are the channel input and output sequences, respectively. Moreover, these bounds have been coupled with Strassen's Gaussian approximation [2] to the error probability around capacity, thereby providing an estimate of the *effective* capacity for finite block length and non-zero error probability. Glossing over the details, the key observation is that, for memoryless channels, the information density is expressed as a sum of random variables, which suggests the application of the central limit theorem and leads to a Gaussian approximation.

In this paper, we rederive the RCU and DT bounds within the framework of *mismatched decoding*. Whereas maximum information-density decoders apply a maximum-likelihood decoding rule, a decoder is said mismatched [3], [4] if it selects the message $\hat{v}$ with largest decoding metric $q(\boldsymbol{x}(v),\boldsymbol{y})$, i. e.

$$\hat{v} = \arg\max_{v} q(\boldsymbol{x}(v),\boldsymbol{y}), \tag{2}$$

where $q(\boldsymbol{x}(v),\boldsymbol{y})$ need not be the channel likelihood metric. As we shall see, the information density is naturally replaced by a *generalized* information density $i_s(\boldsymbol{x},\boldsymbol{y})$, given by

$$i_s(\boldsymbol{x},\boldsymbol{y}) = \log\frac{q(\boldsymbol{x},\boldsymbol{y})^s}{\mathrm{E}[q(\boldsymbol{X}',\boldsymbol{y})^s]}, \tag{3}$$

where $s \geq 0$. The cumulant generating function of this generalized information density is closely related to Gallager's $E_0(\rho,s)$ function [5]. Indeed, for an i.i.d. codebook and a memoryless channel with metric $q(\boldsymbol{x},\boldsymbol{y}) = \prod_{i=1}^n q(x_i,y_i)$, letting τ be an arbitrary complex number, we have that

$$\begin{aligned}\kappa(\tau) &= \log\mathrm{E}[e^{\tau i_s(\boldsymbol{X},\boldsymbol{Y})}] &(4)\\ &= \sum_{i=1}^n \log\mathrm{E}\left[\left(\frac{q(X_i,Y_i)^s}{\mathrm{E}[q(X_i',Y_i)^s|Y_i]}\right)^\tau\right] &(5)\\ &= -n\hat{E}_0(-\tau,s), &(6)\end{aligned}$$

where $\hat{E}_0(\rho,s)$ is the Gallager function for mismatched decoding [3]. Setting $q(x,y) = P_{Y|X}(y|x)$ gives the usual $E_0(\rho,s)$.

More precisely, we express the RCU and DT bounds as the tail probability of a random variable, a form which allows us to determine the error exponent attained by these bounds in terms of Gallager's $E_0(\rho,s)$ function. Moreover, this form as a tail probability allows us to use the saddlepoint (or Laplace) approximation. While this approximation is essentially as easy to compute as the error exponent or the Gaussian approximation, it turns out to be more accurate, and thus provides an efficient method to estimate the *effective* capacity for finite block length and non-zero error probability.

Notation: Random variables are denoted by capital letters and their realization by small letters. Sequences are identified by a boldface font. The probability of an event is denoted by $\Pr\{\cdot\}$ and the expectation operator is denoted by $\mathrm{E}[\cdot]$. Logarithms are in natural units and information rates in nats, except in the examples, where bits are used.

II. Upper Bounds to the Error Probability

We adopt the conventional setup in channel coding. First, and for a given information message v, with $v \in \{1,2,\dots,M\}$, the encoder outputs a codeword of length n $\boldsymbol{x}(v) \in \mathcal{X}^n$, where $\mathcal{X}$ is the symbol channel input alphabet. One could consider more general vector alphabets and the

This work has been supported by the International Joint Project 2008/R2 of the Royal Society, the FP7 Network of Excellence in Wireless Communications (NEWCOM++), and the Isaac Newton Trust.

error probability analysis remains unchanged. The coding rate R is defined as $R \triangleq \frac{1}{n}\log M$. The corresponding channel output of length n, denoted by $\boldsymbol{y} \in \mathcal{Y}^n$, where $\mathcal{Y}$ is the symbol channel output alphabet. The output sequence is obtained from the input sequence according to the probability transition $P_{\boldsymbol{Y}|\boldsymbol{X}}(\boldsymbol{y}|\boldsymbol{x})$. Finally, the decoder selects the message $\hat{v}$ with largest decoding metric $q(\boldsymbol{x},\boldsymbol{y})$, i. e. $\hat{v} = \arg\max_v q(\boldsymbol{x}(v),\boldsymbol{y})$.

We study the probability that the decoder outputs a message different from the one sent, i. e. $\Pr\{\hat{V} \neq V\}$. Specifically, we consider the average (codeword) error probability $\bar{P}_e$ over the ensemble of (randomly selected) i.i.d. codewords.

We consider memoryless channels, for which $P_{\boldsymbol{Y}|\boldsymbol{X}}(\boldsymbol{y}|\boldsymbol{x}) = \prod_{i=1}^n P_{Y|X}(y_i|x_i)$, with $P_{Y|X}(y|x)$ the symbol transition probability. For maximum-likelihood (ML) decoding, the metric is given by $q(\boldsymbol{x},\boldsymbol{y}) = P_{\boldsymbol{Y}|\boldsymbol{X}}(\boldsymbol{y}|\boldsymbol{x})$. We study a general decoding metric, not necessarily ML; however, we assume that the codeword metric admits a symbolwise decomposition $q(\boldsymbol{x},\boldsymbol{y}) = \prod_{i=1}^n q(x_i,y_i)$, with some abuse of notation.

A. The Random Coding Union Bound

Polyanskiy's random coding union (RCU) bound to the average error probability under ML decoding [1] is given by

$$\bar{P}_e \leq \mathrm{E}\Big[\min\Big\{1,(M-1)\Pr\big\{i(\boldsymbol{X}',\boldsymbol{Y}) \geq i(\boldsymbol{X},\boldsymbol{Y})\big|\boldsymbol{X},\boldsymbol{Y}\big\}\Big\}\Big]. \tag{7}$$

The proof of this bound is easily extended to mismatched decoding, resulting in the following theorem.

Theorem 1: The error probability of a maximum-metric decoder with decoding metric $q(\boldsymbol{X},\boldsymbol{Y})$, averaged over all codebooks whose codewords are selected independently according to a distribution $P_{\boldsymbol{X}}(\boldsymbol{x})$ is upper bounded by

$$\bar{P}_e \leq \mathrm{E}\Big[\min\Big\{1,(M-1)\Pr\big\{q(\boldsymbol{X}',\boldsymbol{Y}) \geq q(\boldsymbol{X},\boldsymbol{Y})\big|\boldsymbol{X},\boldsymbol{Y}\big\}\Big\}\Big]. \tag{8}$$

Further, applying Markov's inequality to the probability $\Pr\big\{q(\boldsymbol{X}',\boldsymbol{y}) \geq q(\boldsymbol{x},\boldsymbol{y})\big\}$, the bound can be loosened to

$$\bar{P}_e \leq \mathrm{rcu}(n,M) \triangleq \mathrm{E}\left[\min\left\{1,(M-1)\frac{\mathrm{E}\big[q(\boldsymbol{X}',\boldsymbol{Y})^s|\boldsymbol{Y}\big]}{q(\boldsymbol{X},\boldsymbol{Y})^s}\right\}\right] \tag{9}$$

$$= \mathrm{E}\Big[e^{-\left(i_s(\boldsymbol{X},\boldsymbol{Y})-\log(M-1)\right)^+}\Big], \tag{10}$$

where $(a)^+ \triangleq \max(0,a)$.

The identity for non-negative random variables A [1],

$$\mathrm{E}\big[\min\{1,A\}\big] = \Pr\{A \geq U\}, \tag{11}$$

where U is a uniform $(0,1)$ random variable, allows us to express our loosened RCU in Eq. (10) as the the tail probability above zero of a random variable $Z \triangleq \log\frac{M-1}{U} - i_s(\boldsymbol{X},\boldsymbol{Y})$. This expression will prove fruitful later in the paper.

Remark 1: This bound may be combined with information-spectrum techniques to derive an formula for the achievable rate with mismatched decoding analogous to the inf-mutual information [6], [7].

B. The Dependence-Testing Bound

To derive the DT bound [1], one uses a threshold decoder which sequentially considers all messages, and outputs the first message whose metric exceeds a pre-determined threshold $\gamma(v)$, which we allow to depend on the message. An error is made if the metric does not exceed the threshold, $q(\boldsymbol{X}(i),\boldsymbol{Y}) \leq \gamma(i)$, or if there exists an alternative codeword with lower index and metric above the threshold, $q(\boldsymbol{X}(j),\boldsymbol{Y}) > \gamma(j)$, with $j < i$. Averaging over all messages and codebooks, we get that $\bar{P}_e$ is upper bounded by

$$\bar{P}_e \leq \frac{1}{M}\sum_i \Big(\Pr\big\{q(\boldsymbol{X}(i),\boldsymbol{Y}) \leq \gamma(i)\big\} + \\ + \sum_{j<i}\Pr\big\{q(\boldsymbol{X}(j),\boldsymbol{Y}) > \gamma(j)|\boldsymbol{X}(i)\big\}\Big) \tag{12}$$

$$= \frac{1}{M}\sum_i \Big(\Pr\big\{q(\boldsymbol{X}(i),\boldsymbol{Y}) \leq \gamma(i)\big\} + \\ + (M-i)\Pr\big\{q(\boldsymbol{X}(i),\boldsymbol{Y}) > \gamma(i)\big\}\Big). \tag{13}$$

In the last equation, the pair $(\boldsymbol{X}(i),\boldsymbol{Y})$ is distributed according to $P_{\boldsymbol{X}}P_{\boldsymbol{Y}|\boldsymbol{X}}$ in the first summand and according to $P_{\boldsymbol{X}}P_{\boldsymbol{Y}}$ in the second one.

This bound admits a simplified form for ML decoding. We may write the metric as $q(\boldsymbol{x},\boldsymbol{y}) = \frac{P_{\boldsymbol{Y}|\boldsymbol{X}}(\boldsymbol{y}|\boldsymbol{x})}{P_{\boldsymbol{Y}}(\boldsymbol{y})}$, which allows us to optimize the threshold as in [1]; we find that $\gamma(i) = M - i$ gives the tighest bound. Moreover, using the relation $P\big(\frac{dP}{dQ} \leq \gamma'\big) + \gamma' Q\big(\frac{dP}{dQ} > \gamma'\big) = \mathrm{E}_P\big[\min\{1,\gamma'\frac{dQ}{dP}\}\big]$ [1], we may compactly rewrite the bound in Eq. (13) as

$$\bar{P}_e \leq \frac{1}{M}\sum_i \mathrm{E}\left[\min\left\{1,(M-i)\frac{P_{\boldsymbol{Y}}(\boldsymbol{Y})}{P_{\boldsymbol{Y}|\boldsymbol{X}}(\boldsymbol{Y}|\boldsymbol{X})}\right\}\right]. \tag{14}$$

The expectation is done according to $P_{\boldsymbol{X}}P_{\boldsymbol{Y}|\boldsymbol{X}}$. Further, since $\frac{1}{M}\sum_i \gamma(i) = \frac{M-1}{2}$, and $\min[1,ax]$ is concave in x, applying Jensen's inequality relaxes Eq. (14) to the form in [1],

$$\bar{P}_e \leq \mathrm{dtb}(n,M) \triangleq \mathrm{E}\left[\min\left\{1,\frac{M-1}{2}\frac{P_{\boldsymbol{Y}}(\boldsymbol{Y})}{P_{\boldsymbol{Y}|\boldsymbol{X}}(\boldsymbol{Y}|\boldsymbol{X})}\right\}\right] \tag{15}$$

$$= \mathrm{E}\Big[e^{-\left(i(\boldsymbol{X},\boldsymbol{Y})-\log\frac{M-1}{2}\right)^+}\Big]. \tag{16}$$

In the general mismatched decoding case it may not be possible to express (13) in the compact form (16).

III. Chernoff Bound and Error Exponents

The RCU and DT bounds considered in Sect. II, being closely linked to the tail probability of the rv $i_s(\boldsymbol{X},\boldsymbol{Y})$, are amenable to analysis with large-deviations theory, which gives the rate of exponential decay. The Chernoff bound to the tail probability of a rv Z, $\Pr\{Z \geq \varepsilon\}$, with $\varepsilon > \mathrm{E}[Z]$, is given by

$$\Pr\{Z \geq \varepsilon\} \leq \inf_{\tau>0}\mathrm{E}[e^{\tau Z-\tau\varepsilon}] = \inf_{\tau>0}\big\{e^{\kappa(\tau)-\tau\varepsilon}\big\}, \tag{17}$$

where $\kappa(\tau) = \log\mathrm{E}[e^{\tau Z}]$ is the cumulant transform. It follows that the rate of exponential decay of the probability $\Pr\{Z \geq \varepsilon\}$

is bounded as

$$\lim_{n\to\infty} -\frac{1}{n}\log \Pr\{Z \geq \varepsilon\} \geq \sup_{\tau>0}\lim_{n\to\infty}\frac{1}{n}\bigl\{\tau\varepsilon - \kappa(\tau)\bigr\}. \quad (18)$$

We will use this identity to lower bound the channel reliability function, which gives the rate of exponential decay in the error probability of the best possible code.

We wish to bound the channel reliability function by finding the exponent $E_{\text{rcu}}(R)$, given by

$$E_{\text{rcu}}(R) \triangleq \sup_{s}\lim_{n\to\infty} -\frac{1}{n}\log \operatorname{rcu}(n,M). \quad (19)$$

We may thus concentrate on the tail of the random variable $Z = \log\frac{M-1}{U} - i_s(\boldsymbol{X},\boldsymbol{Y})$ above $\varepsilon = 0$. By definition, its cumulant transform $\kappa_{n,M}(\tau,s)$ is given by

$$\begin{aligned}\kappa_{n,M}(\tau,s) &\triangleq \log \mathrm{E}\left[e^{\tau\log\frac{M-1}{U} - \tau i_s(\boldsymbol{X},\boldsymbol{Y})}\right] &(20)\\ &= \tau\log(M-1) - \log(1-\tau)\\ &\quad + \log \mathrm{E}\left[\left(\frac{\mathrm{E}[q(\boldsymbol{X}',\boldsymbol{Y})^s|\boldsymbol{Y}]}{q(\boldsymbol{X},\boldsymbol{Y})^s}\right)^{\tau}\right]. &(21)\end{aligned}$$

The second term is due to the expectation over U, therefore, for the cumulant transform to converge we need $\tau < 1$.

For an i.i.d. codebook with $P_{\boldsymbol{X}}(\boldsymbol{x}) = \prod_{i=1}^n P_X(x_i)$ and memoryless channel and metric, we may follow Gallager and introduce the function $\hat{E}_0(\rho,s)$ given by

$$\hat{E}_0(\rho,s) = -\log \mathrm{E}\left[\left(\frac{\mathrm{E}[q(X',Y)^s|Y]}{q(X,Y)^s}\right)^{\rho}\right], \quad (22)$$

to write $\kappa_{n,M}(\tau,s)$ as

$$\kappa_{n,M}(\tau,s) = \tau\log(M-1) - \log(1-\tau) - n\hat{E}_0(\tau,s). \quad (23)$$

As τ is a dummy variable, we may safely replace it by ρ.

Applying the Chernoff bound, we lower bound the exponent as

$$\begin{aligned}E_{\text{rcu}}(R) &\geq \sup_{\substack{0<\tau<1\\ s\geq 0}}\lim_{n\to\infty} -\frac{1}{n}\kappa_{n,M}(\tau,s) &(24)\\ &= \sup_{\substack{0<\rho<1\\ s\geq 0}}\bigl\{\hat{E}_0(\rho,s) - \rho R\bigr\}, &(25)\end{aligned}$$

namely Gallager's random coding exponent with mismatched decoding, which we denote by $E_{\text{gb}}(R)$ [3].

Let $\hat{\rho}_0$ be the value maximizing $\hat{E}_0(\rho,s) - \rho R$; equivalently the only root of $\hat{E}_0'(\hat{\rho}_0,s) = R$. The critical rate is defined as the rate where $\hat{\rho} = 1$ [5]. Below the critical rate, $\hat{\rho}_0 \geq 1$, a value outside the range of the cumulant transform $\kappa_{n,M}(\tau,s)$. In this case, convexity of the latter shows that the supremum is attained at $\hat{\rho} = 1$, and we conclude that $\hat{\rho} = \min(1,\hat{\rho}_0)$ and $\hat{E}_0'(\rho,s) = R$.

Remark 2: This analysis shows the achievability of the generalized mutual information [3]. The exponent is negative as long as $R < \frac{\hat{E}_0(\rho,s)}{\rho}$. As $\rho \to 0$, the right-hand side is the first derivative of $\hat{E}_0(\rho,s)$ evaluated at $\rho = 0$, a quantity which coincides with the generalized mutual information.

The DT bound in Eq. (16) has a form very similar to the RCU bound, with Z given by $Z = \log\frac{M-1}{2U} - i_1(\boldsymbol{X},\boldsymbol{Y})$. It follows that the exponent of the DT bound $E_{\text{dtb}}(R)$ for ML decoding is thus given by

$$E_{\text{dtb}}(R) = \sup_{0<\rho<1}\bigl\{E_0(\rho,1) - \rho R\bigr\}. \quad (26)$$

Here $E_0(\rho,1)$ is the function $\hat{E}_0(\rho,s)$ evaluated for the ML metric and $s = 1$. The DT exponent may thus not exceed the RCU exponent. In particular, we have the obvious

$$E_{\text{dtb}}(R) \leq E_{\text{gb}}(R) = E_{\text{rcu}}(R) \quad (27)$$

This is because the DT is derived with the information density, for $s = 1$. As for the form in Eq. (14), the message-dependent threshold term $M - i$ adds an extra term to the cumulant transform $\kappa_{n,M}(\tau,s)$, namely

$$\begin{aligned}\log\left(\sum_{i=1}^{M}\frac{1}{M}(M-i)^{\tau}\right) &\simeq \log\left(M^{\tau}\int_0^1 (1-x)^{\tau}\,\mathrm{d}x\right) &(28)\\ &= \tau\log M - \log(1+\tau). &(29)\end{aligned}$$

This does not change the exponent of the DT bound.

IV. Saddlepoint Approximations

A. Motivation

Chernoff-type bounds provide a natural estimate of the tail probability via the cumulant transform, namely $\Pr\{Z \geq \varepsilon\} \sim e^{\kappa(\hat{\tau}) - \hat{\tau}\varepsilon}$, with $\hat{\tau} = \arg\min_{\tau}\bigl\{\kappa(\tau) - \tau\varepsilon\bigr\}$. Clearly, a more accurate estimate would be of the form $\Pr\{Z \geq \varepsilon\} \sim \alpha(\kappa,\hat{\tau})\cdot e^{\kappa(\hat{\tau}) - \hat{\tau}\varepsilon}$. Saddlepoint approximations provide such estimates [8]. In its classical form, the coefficient $\alpha(\kappa,\hat{\rho})$ of the saddlepoint approximation is given by

$$\alpha(\kappa,\hat{\tau}) = \frac{1}{\hat{\tau}\sqrt{2\pi\kappa''(\hat{\tau})}}. \quad (30)$$

However, this expression becomes inaccurate as $\hat{\tau} \to 0$, as it happens when ε is close to the mean $\mathrm{E}[Z]$. In such cases —and more generally—, a better coefficient is given by

$$\alpha(\kappa,\hat{\tau}) = \frac{1}{2}\operatorname{erfcx}\left(\hat{\tau}\sqrt{\frac{\kappa''(\hat{\tau})}{2}}\right), \quad (31)$$

where $\operatorname{erfcx}(x) \triangleq \operatorname{erfc}(x)\exp(x^2)$. An asymptotic expansion of $\operatorname{erfc}(x)$ at $x \to \infty$ recovers Eq. (30). As $\hat{\tau} \to 0$, however, we have $\hat{\tau} \to \frac{\mathrm{E}[Z]-\varepsilon}{\kappa''(0)}$, where $\kappa''(0)$ is the variance of Z, and

$$\begin{aligned}\Pr\{Z \geq \varepsilon\} &\sim \frac{1}{2}\operatorname{erfcx}\left(\hat{\tau}\sqrt{\frac{\kappa''(\hat{\tau})}{2}}\right)e^{\kappa(\hat{\tau}) - \hat{\tau}\varepsilon} &(32)\\ &\sim \mathrm{Q}\left(\frac{\mathrm{E}[Z]-\varepsilon}{\sqrt{\kappa''(0)}}\right), &(33)\end{aligned}$$

where $\mathrm{Q}(x) = \frac{1}{\sqrt{2\pi}}\int_x^{\infty} e^{-\frac{x^2}{2}}\,\mathrm{d}x$ is the Gaussian tail probability function. We thus recover a Gaussian approximation to the probability for values of ε close to the mean $\mathrm{E}[Z]$.

B. Approximation to the RCU Bound

We expressed in Eq. (10) the average error probability as the tail probability of a continuous random variable $Z = \log\frac{M-1}{U} - i_s(\boldsymbol{X},\boldsymbol{Y})$. We derived its cumulant transform $\kappa_{n,M}(\tau,s)$ in Sect. III. The parameter τ is a complex number for the purpose of deriving the saddlepoint approximation. As the cumulant transform is the Laplace transform of the probability density function $p_Z(z)$, the density function itself is expressable as an inverse Laplace transform [8], namely

$$p_Z(z) = \frac{1}{2\pi j}\int_{\hat\tau-j\infty}^{\hat\tau+j\infty} e^{\kappa_{n,M}(\tau,s)-\rho z}\,\mathrm{d}\tau, \tag{34}$$

where $\hat\tau < 1$ from the definition of $\kappa_{n,M}$. Since $\bar P_e$ is the tail above $\varepsilon = 0$, we compute it by integrating over $z \in [0,\infty)$. Changing the integration order, we get

$$\begin{aligned}
\mathrm{rcu}(n,M) &= \frac{1}{2\pi j}\int_{\hat\tau-j\infty}^{\hat\tau+j\infty}\int_0^\infty e^{\kappa_{n,M}(\tau,s)-\tau z}\,\mathrm{d}z\,\mathrm{d}\tau \qquad (35)\\
&= \frac{1}{2\pi j}\int_{\hat\tau-j\infty}^{\hat\tau+j\infty} e^{\kappa_{n,M}(\tau,s)}\left(\frac{e^{-\tau z}}{-\tau}\bigg|_0^\infty\right)\mathrm{d}\tau \qquad (36)\\
&= \frac{1}{2\pi j}\int_{\hat\tau-j\infty}^{\hat\tau+j\infty} e^{\kappa_{n,M}(\tau,s)}\frac{1}{\tau}\,\mathrm{d}\tau, \qquad (37)
\end{aligned}$$

where $\hat\tau > 0$ to guarantee convergence. For i.i.d. channels, and substituting the form of $\kappa_{n,M}(\tau,s)$ we get

$$\mathrm{rcu}(n,M) = \frac{1}{2\pi j}\int_{\hat\rho-j\infty}^{\hat\rho+j\infty} e^{\rho\log(M-1)-n\hat E_0(\rho,s)}\frac{1}{\rho(1-\rho)}\,\mathrm{d}\rho. \tag{38}$$

We next expand the exponent in the integrand as a Taylor series around $\hat\rho = \min(1,\hat\rho_0)$, with $\hat\rho_0$ given by the root of $\hat E_0'(\hat\rho_0,s) = R = \frac{1}{n}\log M$ (it is safe to replace $M-1$ by M here) discussed in Sect. III. Neglecting terms of order higher than 2 and up to a common factor n, we get

$$\begin{aligned}
\rho R - \hat E_0(\rho,s) \sim \hat\rho R - \hat E_0(\hat\rho,s) &+ \big(R - \hat E_0'(\hat\rho,s)\big)(\rho-\hat\rho)\\
&- \frac{1}{2}\hat E_0''(\hat\rho,s)(\rho-\hat\rho)^2. \qquad (39)
\end{aligned}$$

Let us define the following parameters W and V:

$$W \triangleq R - \hat E_0'(\hat\rho,s), \quad V \triangleq -\hat E_0''(\hat\rho,s). \tag{40}$$

We have $W = 0$ if $\hat\rho \le 1$. Beyond the critical rate, however, $W \ne 0$. We also have $V \ge 0$ and in general $V > 0$.

We proceed further by replacing the exponent in the integrand of Eq. (38) by Eq. (39) and using that $\frac{1}{\rho(1-\rho)} = \frac{1}{\rho} + \frac{1}{1-\rho}$. With the change of integration variable $\rho - \hat\rho = j\rho_i$, we must compute the following integrals (see [8, Section 2.1])

$$\begin{aligned}
\frac{1}{2\pi}\int_{-\infty}^{\infty} & e^{jnW\rho_i - \frac{1}{2}nV\rho_i^2}\frac{1}{\hat\rho + j\rho_i}\,\mathrm{d}\rho_i = \\
&= \frac{1}{2}\,\mathrm{erfcx}_1\left(\hat\rho\sqrt{\frac{nV}{2}}, W\sqrt{\frac{n}{2V}}\right) \qquad (41)\\
\frac{1}{2\pi}\int_{-\infty}^{\infty} & e^{jnW\rho_i - \frac{1}{2}nV\rho_i^2}\frac{1}{1-\hat\rho - j\rho_i}\,\mathrm{d}\rho_i = \\
&= \frac{1}{2}\,\mathrm{erfcx}_1\left((1-\hat\rho)\sqrt{\frac{nV}{2}}, -W\sqrt{\frac{n}{2V}}\right). \qquad (42)
\end{aligned}$$

where we used the function $\mathrm{erfcx}_1(x,y) \triangleq \mathrm{erfcx}(x-y)\exp(-y^2) = \mathrm{erfc}\,(x-y)\exp(x^2-2xy)$.

We thus obtain our desired saddlepoint approximation

$$\begin{aligned}
\mathrm{rcu}(n,M) \simeq e^{n(\hat\rho R - \hat E_0(\hat\rho,s))}\frac{1}{2}\Bigg(&\mathrm{erfcx}_1\left(\hat\rho\sqrt{\frac{nV}{2}}, W\sqrt{\frac{n}{2V}}\right)\\
&+ \mathrm{erfcx}_1\left((1-\hat\rho)\sqrt{\frac{nV}{2}}, -W\sqrt{\frac{n}{2V}}\right)\Bigg),
\end{aligned} \tag{43}$$

Remark 3: This analysis also extends to the DT bound in Eq. (16), for which $s = 1$ and M (for $M-1$) is replaced by $\frac{M}{2}$. The approximation is as in Eq. (43), with $s = 1$, an extra term $2^{-\hat\rho}$, and with $W = R - \hat E_0'(\hat\rho,s) - \frac{1}{n}\log 2$. As for the form in Eq. (14), the term $-\log(1+\rho)$ in $\kappa_{n,M}(\tau,s)$ induces the replacement of the factor $2^{-\hat\rho}$ by $1/(1+\hat\rho)$, thereby slightly reducing the error probability.

C. Channel Dispersion and the Gaussian Approximation

As discussed in the introduction to this section, the saddlepoint and Gaussian approximations are closely related. Since the Gaussian distribution is the only continuous distribution for which cumulants of order higher than 2 are zero, neglecting terms of order higher than 2 in the Taylor expansion of Eq. (39) may be seen as a form of Gaussian approximation.

For simplicity, we consider ML decoding. Let the rate R be rate close to the mutual information $I(X;Y)$. The comments here extend without difficulty to the generalized mutual information. Being close to $I(X;Y)$, we expect $\hat\rho$ to be small, and may carry out a Taylor expansion of $\rho R - \hat E_0(\rho,s)$ around $\hat\rho = 0$ (thus $s = 1$) keeping terms up to order 2. Moreover, we use that $E_0'(0;1) = I(X;Y)$ and define $V_0 = -E_0''(0;1)$. In general $V_0 \ge 0$, yet we assume $V_0 > 0$. This defines a Gaussian approximation to $\kappa_{n,M}(\tau,s)$, namely

$$\kappa_{n,M}(\tau,s) \simeq \kappa_{\mathrm{ga}}(\tau,s) \triangleq n\big(R - I(X;Y)\big)\tau + n\frac{1}{2}V_0\tau^2, \tag{44}$$

where we neglected the contribution from $\log(1-\tau)$. Proceeding as in the previous section, we solve for $\hat\tau$ by setting $R - \hat E_0(\hat\tau,s) \simeq \kappa_{\mathrm{ga}}'(\hat\rho,s) = 0$, with $\hat\tau = \hat\rho$, namely

$$\kappa_{\mathrm{ga}}'(\hat\rho,s) \simeq n\big(R - I(X;Y)\big) + nV_0\hat\rho = 0, \tag{45}$$

which implies that $\hat\rho = \dfrac{I(X;Y) - R}{V_0}$. Within the same order of accuracy, we may approximate the second derivative as

$$-n\hat E_0''(\rho,s) \simeq \kappa_{\mathrm{ga}}''(\rho,s) = nV_0. \tag{46}$$

Putting these values back in Eq. (43), we now obtain the following approximation

$$\mathrm{rcu}_{\mathrm{ga}}(n,M) = \frac{1}{2}\mathrm{erfc}\left(\big(I(X;Y) - R\big)\sqrt{\frac{n}{2V_0}}\right). \tag{47}$$

Setting $\bar P_e = \mathrm{rcu}_{\mathrm{ga}}(n,M)$, we solve for R_{ga} as

$$R_{\mathrm{ga}} = I(X;Y) - \sqrt{\frac{V_0}{n}}\mathrm{Q}^{-1}(\bar P_e). \tag{48}$$

This is a Gaussian approximation to the *effective* rate[1].

We are not able to recover Strassen's $\mathrm{O}(\log n)$ term in the expansion of the rate, a fact which may be traced back to the use of Markov's inequality in the RCU bound. Although a precise analysis of the loss incurred by invoking Markov's inequality in the RCU bound is open, consider a saddlepoint approximation to the probability $\Pr\{q(\boldsymbol{X}', \boldsymbol{y}) \geq q(\boldsymbol{x}, \boldsymbol{y})\}$,

$$\Pr\{q(\boldsymbol{X}', \boldsymbol{y}) \geq q(\boldsymbol{x}, \boldsymbol{y})\} \simeq \beta(n)\, \frac{\mathrm{E}[q(\boldsymbol{X}', \boldsymbol{y})^s]}{q(\boldsymbol{x}, \boldsymbol{y})^s} \tag{49}$$

in analogy to the motivation at the beginning of this section. We expect $\beta(n)$ to be similar to Eq. (31): it may either be $\mathrm{O}(1)$ or, for large enough n, be $\mathrm{O}(n^{-\frac{1}{2}})$. In the latter case the information density gets a new term $\frac{1}{2}\log n$, which appears as an extra summand in the Gaussian approximation, Eq. (48). To any extent, and from a practical point of view, the saddlepoint approximation often gives a better estimate that the Gaussian approximation, with or without the $\mathrm{O}(\log n)$ correction. In our case, the saddlepoint approximation accurately characterizes the RCU and DT bounds for all rates, while the Gaussian approximation does so for rates close to capacity.

Incidentally, the comments in this section illustrate the connection between the channel dispersion[2] V_0 and the error exponent, namely that the dispersion is equal to the inverse of the second derivative of the error exponent at capacity [9].

V. Applications

In this section we discuss some applications of the bounds and approximations described so far to the binary erasure channel (BEC), and the binary symmetric channel (BSC). For these channels, the maximum metric mismatched decoder is equivalent to ML. For ML decoding, the corresponding Gallager functions are given by

$$E_0^{\text{bec}}(\rho, s) = -\log\left(\varepsilon + (1-\varepsilon)2^{-\rho}\right), \tag{51}$$

$$E_0^{\text{bsc}}(\rho, s) = -\log\left(2^{-\rho}\left(\varepsilon^{\frac{1}{1+\rho}} + (1-\varepsilon)^{\frac{1}{1+\rho}}\right)^{1+\rho}\right) \tag{52}$$

The relevant channel parameter is denoted by ε.

A. Binary Erasure Channel

In general, the optimum $\hat{\rho}$ is to be found numerically. An exception is the BEC channel, for which[3]

$$E_0'(\rho, s) = \frac{(1-\varepsilon)\log 2}{(1-\varepsilon) + 2^{\rho}\varepsilon}, \tag{53}$$

which allows us to solve for the saddlepoint, giving

$$2^{\hat{\rho}_0} = \frac{(1-\varepsilon)(\log 2 - R)}{\varepsilon R}. \tag{54}$$

For the BEC, the saddlepoint approximations to the RCU and DT bounds admit a closed form expression. Fig. 1 depicts the *effective* coding rate for a given block length and average error probability. Clearly, the RCU and DT bounds outperform Gallager's and Feinstein's [10] bounds. In particular, the improvement in coefficient with respect to Gallager's bound makes more accurate the estimate of the *effective* coding rate. Also, the curves are indistinguishable from those in [1], confirming the accuracy of the saddlepoint approximation[4].

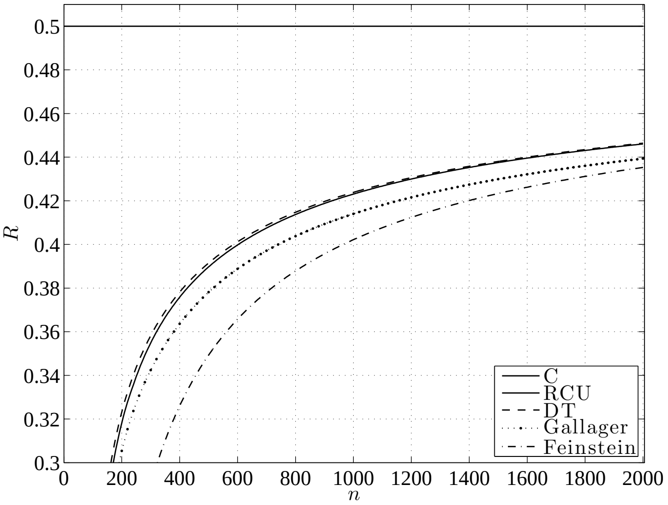

Fig. 1. Rate-length tradeoff for the BEC; $\varepsilon = 0.5$, $\bar{P}_e = 10^{-6}$.

Since $E_0(\rho, s)$ is independent of s, so is the generalized information density $i_s(x, y)$, which therefore coincides with the usual information density $i(x, y)$ for the BEC. Therefore, not only does the DT bound attain Gallager's random-coding exponent (thus tying with the RCU bound), but it is found to be slighly tighter than the RCU bound by a factor $2^{-\hat{\rho}}$ or $1/(1+\hat{\rho})$. This change translates into a small improvement in the estimate of the effective capacity.

As the information density is independent of the parameter s, no loss is incurred by invoking Markov's inequality in the RCU bound for the BEC. It is clear the number of erasures in the output, n_{e}, is a sufficient statistic for decoding, and the metric for the transmitted codeword $\boldsymbol{x}$ is is $q(\boldsymbol{x}, \boldsymbol{y}) = (1-\varepsilon)^{n-n_{\mathrm{e}}}\varepsilon^{n_{\mathrm{e}}}$. As for the alternative codewords, their metric is zero unless they coincide in the $n - n_{\mathrm{e}}$ non erased positions. There are $2^{n_{\mathrm{e}}}$ such sequences, each with metric $(1-\varepsilon)^{n-n_{\mathrm{e}}}\varepsilon^{n_{\mathrm{e}}}$. Since there are 2^n possible sequences of length n, the probability that a randomly generated alternative codeword is decoded instead of the transmitted one is given by

$$\Pr\left\{q(\boldsymbol{X}', \boldsymbol{y}) \geq q(\boldsymbol{x}, \boldsymbol{y})\right\} = \frac{2^{n_{\mathrm{e}}}}{2^n}. \tag{55}$$

[1] The channel dispersion V_0 (as well as the rates) is in base e. In bits, one has $V_0^{\text{bits}} = V_0/(\log 2)^2$.

[2] The channel dispersion is defined as

$$V_0 = \lim_{\bar{P}_e \to 0} \lim_{n\to\infty} n \frac{\left(C - R(n, \bar{P}_e))\right)^2}{-2\log \bar{P}_e}. \tag{50}$$

Close to the mutual information, we have $\bar{P}_e \simeq e^{n\frac{1}{2}E''_{\text{rcu}}(I)(I-R)^2} = e^{n\frac{(I-R)^2}{2E_0''(0)}}$, and conclude that $V_0 = \frac{1}{E_r''(C)} = -E_0''(0)$.

[3] Moreover, $E_0''(\hat{\rho}, s) = R(R - \log 2)$. As expected, $E_0'(0, s) = (1-\varepsilon)\log 2$, namely the channel capacity, and moreover $E_0''(0, s) = -\varepsilon(1-\varepsilon)(\log 2)^2$, in agreement with the channel dispersion $V_0 = \varepsilon(1-\varepsilon)(\log 2)^2$.

[4] It is shown in [1] that the same bounds are valid for both average and maximum error probability for the BEC and BSC.

An analogous computation gives

$$\frac{\mathrm{E}[q(\boldsymbol{X}',\boldsymbol{y})^s]}{q(\boldsymbol{x},\boldsymbol{y})^s}=\frac{\left(\frac{1}{2}(1-\varepsilon)^s\right)^{n-n_{\mathrm{e}}}\left(\frac{1}{2}\varepsilon^s+\frac{1}{2}\varepsilon^s\right)^{n_{\mathrm{e}}}}{(1-\varepsilon)^{s(n-n_{\mathrm{e}})}\varepsilon^{sn_{\mathrm{e}}}}=\frac{2^{n_{\mathrm{e}}}}{2^n} \tag{56}$$

This proves that our loosened RCU bound in Eq. (10) indeed coincides the original RCU bound in Eq. (8) [1].

B. Binary Symmetric Channel

We now examine the case of the BSC, where closed form expressions are not so simple to obtain. In this case, and for all our computations, we have chosen the free parameter s to be equal to Gallager's optimal value $s=\frac{1}{1+\hat{\rho}}$. While this choice might not be optimal, it is reasonable, as it maximises the error exponent, and, as we shall see, is valid for low rates.

Fig. 2 depicts the saddlepoint approximation and the exact numerical evaluation of the RCU for $n=50,100,200,500$. A very close match can be observed. While the Gaussian approximation, also shown in the figure, broadly agrees with the general behaviour of the probability, it does not provide an accurate estimate; its accuracy improves as n increases. For the BSC, comparison of the two versions of the RCU bound is not as straightforward as in the BEC channel. Using a saddlepoint approximation for the probability involved suggests that the true probability is $\mathrm{O}(\frac{1}{\sqrt{n}})$ smaller than the bound from Markov's inequality, an effect which translates into a loss in the saddlepoint approximation of order $\mathrm{O}(n^{-\frac{\hat{\rho}}{2}})$.

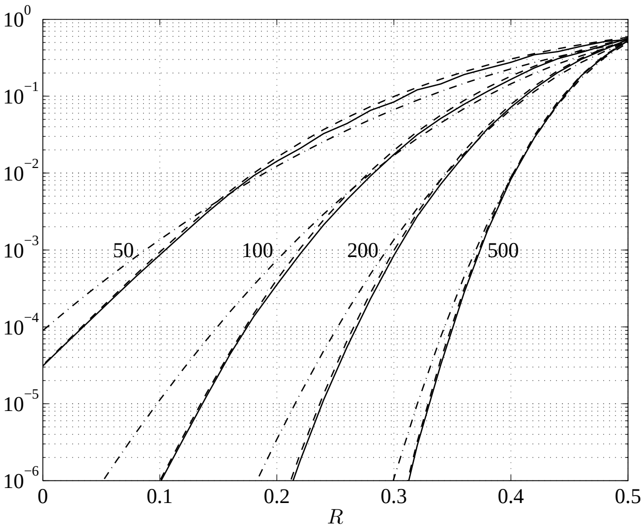

Fig. 2. RCU (solid lines), RCU saddlepoint approximation (dashed lines) and Gaussian approximation (dash-dotted lines) for a BSC with $\varepsilon=0.11$.

Fig. 3 compares the proposed saddlepoint approximations to the exact RCU and DT, the corresponding Chernoff bounds (Gallager's for the RCU) and the Gaussian approximation. Again, we observe a very close match between the bounds and saddlepoint approximations. We first observe that for low rates and low values of the error probability, the coefficient of the RCU saddlepoint approximation approaches 1, matching Gallager's bound. We observe a significant loss of the DT with respect to the RCU, mainly due to the loss in error exponent; the RCU has Gallager's exponent since it uses $s=\frac{1}{1+\rho}$, while the DT has a worse exponent due to using $s=1$.

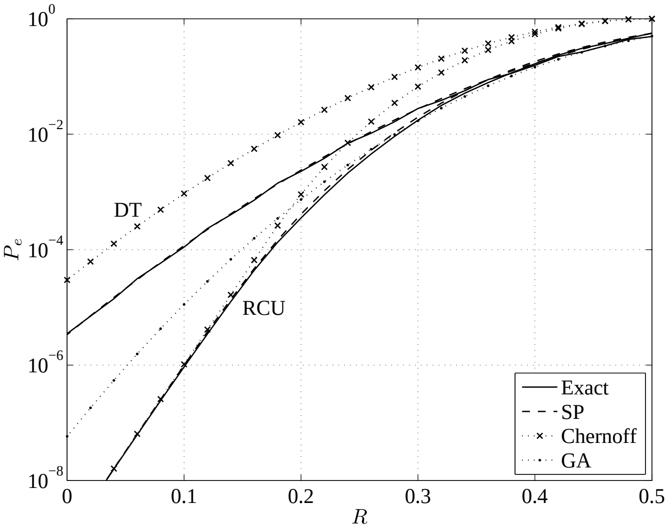

Fig. 3. Comparison of DT and RCU bounds, saddlepoint approximations, Chernoff bounds and Gaussian approximation for $n=100$ and a BSC with $\varepsilon=0.11$.

VI. Conclusions

In this paper, we have derived the error exponents and saddlepoint approximations of the random-coding union bound and the dependence-testing bound. These saddlepoint approximations are a versatile tool that allow to accurately calculate the corresponding bounds for arbitrary discrete-input memoryless channels (with or without mismatched decoding) with a complexity similar to that of the Gaussian approximation.

References

[1] Y. Polyanskiy, H. V Poor, and S. Verdú, "Channel coding rate in the finite blocklength regime," *IEEE Trans. Inf. Th.*, vol. 45, no. 5, pp. 2307–2359, May 2010.

[2] V. Strassen, "Asymptotische Abschätzungen in Shannons Informationstheorie," in *Trans. 3rd Prague Conf. Information Theory, Statist. Decision Functions, Random Processes*, 1962, pp. 689–723.

[3] G. Kaplan and S. Shamai, "Information rates and error exponents of compound channels with application to antipodal signaling in a fading environment," *AEU. Archiv für Elektronik und Übertragungstechnik*, vol. 47, no. 4, pp. 228–239, 1993.

[4] N. Merhav, G. Kaplan, A. Lapidoth, and S. Shamai (Shitz), "On information rates for mismatched decoders," *IEEE Trans. Inf. Theory*, vol. 40, no. 6, pp. 1953–1967, 1994.

[5] R. G. Gallager, *Information Theory and Reliable Communication*, John Wiley & Sons, Inc. New York, NY, USA, 1968.

[6] S. Verdú and T. S. Han, "A general formula for channel capacity," *IEEE Trans. Inf. Theory*, vol. 40, no. 4, pp. 1147–1157, 1994.

[7] A. Ganti, A. Lapidoth, and I. E. Telatar, "Mismatched decoding revisited: general alphabets, channels with memory, and the wideband limit," *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2315–2328, 2000.

[8] J. L. Jensen, *Saddlepoint Approximations*, Oxford University Press, USA, 1995.

[9] C. E. Shannon, "Certain Results in Coding Theory for Noisy Channels," *Inf. Control*, pp. 6–25, 1957.

[10] A. Feinstein, "A new basic theorem of information theory," *IRE Trans. Inf. Theory*, vol. 4, no. 4, pp. 2–22, 1954.