IRWIN AND JOAN JACOBS
CENTER FOR COMMUNICATION AND INFORMATION TECHNOLOGIES

Expurgated Random-Coding Ensembles: Exponents, Refinements and Connections

Jonathan Scarlett, Li Peng, Neri Merhav, Alfonso Martinez and Albert Guillén and Albert Guillén i Fàbregas

CCIT Report #837
July 2013

Electronics
Computers
Communications

DEPARTMENT OF ELECTRICAL ENGINEERING
TECHNION - ISRAEL INSTITUTE OF TECHNOLOGY, HAIFA 32000, ISRAEL

CCIT Report #837 July 2013

Expurgated Random-Coding Ensembles: Exponents, Refinements and Connections

Jonathan Scarlett, Li Peng, Neri Merhav, Alfonso Martinez and Albert Guillén i Fàbregas

Abstract

This paper studies expurgated random-coding bounds and exponents with a given (possibly suboptimal) decoding rule. Variations of Gallager's analysis are presented, yielding new asymptotic and non-asymptotic bounds on the error probability for an arbitrary codeword distribution. A simple non-asymptotic bound is shown to attain an exponent which coincides with that of Csiszár and Körner for discrete alphabets, while also remaining valid for continuous alphabets. The method of type class enumeration is studied for both discrete and continuous alphabets, and it is shown that this approach yields improved exponents for some codeword distributions. A refined analysis of expurgated i.i.d. random coding is given which yields an exponent with a $O\big(\frac{1}{\sqrt{n}}\big)$ prefactor, thus improving on Gallager's $O(1)$ prefactor.

I. Introduction

Achievable performance bounds for channel coding are typically obtained by analyzing the average error probability of an ensemble of codebooks with independently generated codewords. For memoryless channels, random codes with independent and identically distributed (i.i.d.) symbols achieve the channel capacity [1], characterize the error exponent of the best code at sufficiently high rates [2, Ch. 5], and provide tight bounds on the finite-length performance [3].

At low rates, the error probability of the best code in the random-coding ensemble can be significantly smaller than the average. In such cases, better performance bounds are obtained by considering an ensemble in which a subset of the randomly generated codewords are expurgated from the codebook. In particular, the error exponents resulting from such techniques are generally higher than the random-coding error exponent at low rates. Existing works exploring such techniques include those of Gallager [2, Sec. 5.7], Csiszár-Körner-Marton [4], [5, Ex. 10.18] and Csiszár-Körner [6]. The advantages of Gallager's approach include its simplicity and the fact that the analysis is not restricted to discrete

J. Scarlett and L. Peng are with the Department of Engineering, University of Cambridge, Cambridge, CB2 1PZ, U.K. (e-mail: jmscarlett@gmail.com, lp327@cam.ac.uk). N. Merhav is with the Department of Electrical Engineering, Technion - Israel Institute of Technology, Technion City, Haifa 32000, Israel. (e-mail: merhav@ee.technion.ac.il). A. Martinez is with the Department of Information and Communication Technologies, Universitat Pompeu Fabra, 08018 Barcelona, Spain (e-mail: alfonso.martinez@ieee.org). A. Guillén i Fàbregas is with the Institució Catalana de Recerca i Estudis Avançats (ICREA), the Department of Information and Communication Technologies, Universitat Pompeu Fabra, 08018 Barcelona, Spain, and also with the Department of Engineering, University of Cambridge, Cambridge, CB2 1PZ, U.K. (e-mail: guillen@ieee.org).

This work has been funded in part by the European Research Council under ERC grant agreement 259663, by the European Union's 7th Framework Programme (PEOPLE-2011-CIG) under grant agreement 303633 and by the Spanish Ministry of Economy and Competitiveness under grants RYC-2011-08150 and TEC2012-38800-C03-03. The work of N. Merhav was partially supported by the Israeli Science Foundation (ISF), grant no. 412/12.

alphabets. On the other hand, the exponents of [4]–[6] can be applied to channels with cost constraints. Furthermore, as we will see in Section III, these exponents can improve on that of Gallager for a given input distribution or decoding rule.

In this paper, we provide techniques that attain the best of each of the above approaches. Using variations of Gallager's analysis, we obtain a number of asymptotic and non-asymptotic bounds on the error probability, including exponents for channels with continuous alphabets, cost constraints, and mismatched decoders [7]–[10]. Furthermore, we explore the method of type class enumerators (e.g. see [11]–[13]) for both discrete and continuous channels, and discuss its extension to channels with memory.

A. System Setup

The input and output alphabets are denoted by $\mathcal{X}$ and $\mathcal{Y}$ respectively. The channel is assumed to be memoryless, and the associated conditional distribution is denoted by $W(y|x)$. In the case that both $\mathcal{X}$ and $\mathcal{Y}$ are finite, the channel is a discrete memoryless channel (DMC), but we do not assume this to be true in general. We consider block coding, in which a codebook $\mathcal{C} = \{\boldsymbol{x}^{(1)}, \dots, \boldsymbol{x}^{(M)}\}$ is known at both the encoder and decoder. The encoder takes as input a message m, uniformly distributed on the set $\{1, \dots, M\}$, and transmits the corresponding codeword $\boldsymbol{x}^{(m)}$ of length n. The decoder receives the vector $\boldsymbol{y}$ at the output of the channel, and forms the estimate

$$\hat{m} = \operatorname*{arg\,max}_{j \in \{1,\dots,M\}} \prod_{i=1}^{n} q(x_i^{(j)}, y_i), \tag{1}$$

where n is the length of each codeword, $x_i^{(j)}$ is the i-th entry of $\boldsymbol{x}^{(j)}$ (similarly for y_i), and $q(x, y)$ is a non-negative function called the *decoding metric*. An error is said to have occurred if $\hat{m} \neq m$. We assume that ties are broken as errors. We define $q^n(\boldsymbol{x}, \boldsymbol{y}) \triangleq \prod_{i=1}^{n} q(x_i, y_i)$ and $W^n(\boldsymbol{y}|\boldsymbol{x}) \triangleq \prod_{i=1}^{n} W(y_i|x_i)$.

When $q(x, y) = W(y|x)$, (1) is the optimal maximum-likelihood (ML) decoding rule. For other decoding metrics, this setting is that of *mismatched decoding* [7]–[10], which is relevant when ML decoding is not feasible, e.g. due to channel uncertainty or implementation constraints.

Throughout the paper, we consider channels with both constrained and unconstrained inputs. In the former setting, each codeword $\boldsymbol{x}$ must satisfy a constraint of the form

$$\frac{1}{n} \sum_{i=1}^{n} c(x_i) \le \Gamma, \tag{2}$$

where $c(\cdot)$ is referred to as a cost function, and Γ is a constant. Unless stated otherwise, it will be assumed that the input is unconstrained, which corresponds to $\Gamma = \infty$.

For a given rate R, an error exponent $E(R)$ is said to be achievable if there exists a sequence of codebooks $\mathcal{C}_n$ of length n and rate R whose error probability $p_e(\mathcal{C}_n)$ satisfies

$$\liminf_{n \to \infty} -\frac{1}{n} \log p_e(\mathcal{C}_n) \ge E(R). \tag{3}$$

We focus on the maximal error probability rather than the average error probability, but the two are equivalent for the purposes of studying error exponents.

B. Previous Work

The first study of expurgated exponents (for ML decoding) was by Gallager [2, Ch. 5], who considered an ensemble in which $2M-1$ codewords are generated at random, and a subset of M codewords forms the codebook. Roughly speaking, the codewords which are kept are those which have the lowest error probability among the original codewords. A different approach was taken by Csiszár, Körner and Marton [4] (see also [5, Ex. 10.18]), who began by proving the existence of a collection of constant-composition codewords such that any two codewords have a joint empirical distribution satisfying certain properties. By analyzing this collection of codewords using the method of types, an error exponent was obtained which coincides with Gallager's after the optimization of the input distribution. An exponent for mismatched decoding was derived by Csiszár and Körner [6], and was shown to coincide with that of [4] under ML decoding.

As stated in the introduction, the exponents in [4], [6] have the advantage of being applicable to channels with cost constraints. In Section III, we will see that the exponents of [4], [6] can in fact improve on that of Gallager for a given input distribution. However, the proofs are based on the method of types and rely heavily on the packing lemma [5, Ch. 10], and are thus valid only when the input and output alphabets are finite.

In general, relatively little is known about the optimization of the above-mentioned expurgated exponents over the input distribution. Furthermore, better exponents can be obtained by considering higher-order products of the channel, e.g. $W^{(2)}((y_1,y_2)|(x_1,x_2))=W(y_1|x_1)W(y_2|x_2)$, for which the optimal input distribution is not necessarily a product of single-letter distributions. Sufficient conditions for the single-letter exponent equal its multi-letter counterparts were given by Jelinek [14] and Blahut [15]. As the rate approaches zero, Gallager's single-letter exponent is known to be tight, due to the matching converse by Shannon, Gallager and Berlekamp [16]. Omura [17] presented connections between expurgated exponents and distortion-rate functions, with the distortion measure given by the Bhattacharyya distance.

Overviews of the mismatched decoding problem can be found in [7]–[10]. Most of the literature has focused on achievable rates, whereas this paper is concerned with the performance at low rates. The mismatched decoding paper most relevant to this one is [10], which studies non-expurgated random-coding error exponents for various ensembles.

C. Contributions

The main contributions of this paper are as follows:

- In Section II, we present a number of variations of Gallager's analysis which yield new asymptotic and non-asymptotic bounds on the error probability.
- In Section III, we present an overview of the expurgated exponents. Using the method of Lagrange duality [18], we relate the exponents given in [2], [4], [6]. Generalizations of the exponents in [2], [4] to the setting of mismatched decoding are given.
- In Section IV, we present two derivations of the exponent in [6] using constant-composition random coding. The first applies well-known properties of types to a non-asymptotic bound, thus providing a simple and concise proof. The second uses the method of type class enumeration (e.g. see [11]–[13]), inspired by statistical-mechanical

methods. This approach guarantees exponential tightness starting from an earlier step than the former approach, and leads to better exponents for some codeword distributions.

- In Section V, we consider cost-constrained random coding [2, Sec. 7.3] [19], and present two derivations of an exponent which coincides with that of [6] in the discrete case, while also remaining valid for continuous alphabets. The first uses simple bounding techniques similar to those of Gallager, while the second extends the type class enumerator approach. We discuss the application of the latter method to channels with memory.
- In Section VI, we present a refined derivation of Gallager's exponent for i.i.d. random coding (and its generalization to mismatched decoding) with a $O\big(\frac{1}{\sqrt{n}}\big)$ prefactor, thus improving on the original $O(1)$ prefactor. Similar improvements for the non-expurgated random-coding error exponent have recently been obtained by Altug and Wagner [20]. The analysis in [20] can be considered a refinement of that of Fano [21, Ch. 9], whereas our analysis can be considered a refinement of that of Gallager [2, Ch. 5].

D. Notation

We use bold symbols for vectors (e.g. $\boldsymbol{x}$), and denote the corresponding i-th entry using a subscript (e.g. x_i).

The set of all probability distributions on an alphabet, say $\mathcal{X}$, is denoted by $\mathcal{P}(\mathcal{X})$, and the set of all empirical distributions on a vector in $\mathcal{X}^n$ (i.e. types [5, Ch. 2]) is denoted by $\mathcal{P}_n(\mathcal{X})$. For a given type $Q \in \mathcal{P}_n(\mathcal{X})$, the type class $T^n(Q)$ is defined to be the set of all sequences in $\mathcal{X}^n$ with type Q.

The probability of an event is denoted by $\mathbb{P}[\cdot]$, and the symbol $\sim$ means "distributed as". The marginals of a joint distribution $P_{XY}(x,y)$ are denoted by $P_X(x)$ and $P_Y(y)$. We write $P_X = \widetilde{P}_X$ to denote element-wise equality between two probability distributions on the same alphabet. Expectation with respect to a joint distribution $P_{XY}(x,y)$ is denoted by $\mathbb{E}_P[\cdot]$, or simply $\mathbb{E}[\cdot]$ when the associated probability distribution is understood from the context. Similarly, the mutual information with respect to P_{XY} is written as $I_P(X;Y)$, or simply $I(X;Y)$ when the distribution is understood from the context. Given a distribution $Q(x)$ and conditional distribution $W(y|x)$, we write $Q \times W$ to denote the joint distribution defined by $Q(x)W(y|x)$.

For two positive sequences f_n and g_n, we write $f_n \doteq g_n$ if $\lim_{n\to\infty} \frac{1}{n}\log\frac{f_n}{g_n} = 0$, and we write $f_n \,\dot{\leq}\, g_n$ if $\limsup_{n\to\infty} \frac{1}{n}\log\frac{f_n}{g_n} \le 0$ and analogously for $\dot{\geq}$. We write $f_n = O(g_n)$ if $|f_n| \le c|g_n|$ for some c and sufficiently large n, and $f_n = o(g_n)$ if $\lim_{n\to\infty}\frac{f_n}{g_n} = 0$. All logarithms have base e, and all rates are in units of nats except in the examples, where bits are used. We define $[c]^+ = \max\{0,c\}$, and denote the indicator function by $\mathbb{1}\{\cdot\}$, and the floor function by $\lfloor\cdot\rfloor$.

II. Expurgated Bounds

In this section, we provide a number of variations of Gallager's bounds and techniques which will provide the starting point of the derivations of the exponents in Sections IV–VI. We let $P_{\boldsymbol{X}}$ denote a codeword distribution, and we define the random variables $(\boldsymbol{X},\boldsymbol{Y},\overline{\boldsymbol{X}})$ distributed according to

$$(\boldsymbol{X},\boldsymbol{Y},\overline{\boldsymbol{X}}) \sim P_{\boldsymbol{X}}(\boldsymbol{x})W^n(\boldsymbol{y}|\boldsymbol{x})P_{\boldsymbol{X}}(\overline{\boldsymbol{x}}). \tag{4}$$

In the case that a cost constraint of the form (2) is present, we assume that $P_{\boldsymbol{X}}$ is chosen such that $\boldsymbol{X}$ satisfies the constraint with probability one.

We let $\mathsf{C} = \{\boldsymbol{X}^{(1)}, \cdots, \boldsymbol{X}^{(M')}\}$ be a random codebook of size M' with each codeword independently generated according to $P_{\boldsymbol{X}}$. The symbol $\mathcal{C}$ is used to denote an expurgated codebook containing $M < M'$ codewords. We let $p_{e,m}(\cdot)$ be the error probability induced by a codebook given that message m was sent. The maximal error probability is denoted by $p_e(\cdot) = \max_m p_{e,m}(\cdot)$.

We begin with the following straightforward generalization of [2, Lemma, p. 151].

Lemma 1. *Fix a function $f : [0,1] \to \mathbb{R}$ and a codeword distribution $P_{\boldsymbol{X}}$ such that $f(p_{e,m}(\mathsf{C}))$ is non-negative for all m with probability one. For any $\eta > 0$ there exists a codebook $\mathcal{C}$ of size $M > M'\frac{\eta}{1+\eta}$ such that*

$$f\big(p_{e,m}(\mathcal{C})\big) \leq (1+\eta)\mathbb{E}\big[f(p_{e,m}(\mathsf{C}))\big] \tag{5}$$

for $m = 1, \cdots, M$.

Proof: The proof is identical to [2, Lemma, p. 151], with the assumption of $f(p_{e,m}(\mathsf{C}))$ being non-negative ensuring the validity of Markov's inequality. ■

While Lemma 1 is valid for any function $f(\cdot)$, it is primarily of interest when $f(\cdot)$ is monotonically increasing, so that (5) can be inverted in order to obtain an upper bound on $p_{e,m}(\mathcal{C})$. Gallager [2] presented the lemma with the choices $\eta = 1$ and $f(\cdot) = (\cdot)^{1/\rho}$, where $\rho > 0$. This function is non-negative, and thus satisfies the assumption of the lemma for any codeword distribution. It follows that there exists a codebook $\mathcal{C}$ of size M such that

$$p_e(\mathcal{C}) \leq \Big(2\mathbb{E}\big[p_{e,m}(\mathsf{C})^{1/\rho}\big]\Big)^{\rho}, \tag{6}$$

where C contains $M' = 2M-1$ codewords. In the following theorem, we provide non-asymptotic bounds on the error probability which follow in a straightforward fashion from (6). The proof alters Gallager's arguments for the purpose of better characterizing the non-asymptotic performance, and also for dealing with suboptimal decoding rules.

Theorem 1. *For any pair (n, M), codeword distribution $P_{\boldsymbol{X}}$ and parameters $\rho \geq 1$ and $s \geq 0$, there exists a codebook $\mathcal{C}_n$ with M codewords of length n whose maximal error probability satisfies*

$$p_e(\mathcal{C}_n) \leq \mathrm{rcux}_{\rho}(n, M) \leq \mathrm{rcux}_{\rho,s}(n, M) \tag{7}$$

where

$$\mathrm{rcux}_{\rho}(n, M) \triangleq \left(4(M-1)\mathbb{E}\left[\mathbb{P}\Big[q^n(\overline{\boldsymbol{X}}, \boldsymbol{Y}) \geq q^n(\boldsymbol{X}, \boldsymbol{Y}) \,\Big|\, \boldsymbol{X}, \overline{\boldsymbol{X}}\Big]^{1/\rho}\right]\right)^{\rho} \tag{8}$$

$$\mathrm{rcux}_{\rho,s}(n, M) \triangleq \left(4(M-1)\mathbb{E}\left[\mathbb{E}\left[\left(\frac{q^n(\overline{\boldsymbol{X}}, \boldsymbol{Y})}{q^n(\boldsymbol{X}, \boldsymbol{Y})}\right)^{s} \,\middle|\, \boldsymbol{X}, \overline{\boldsymbol{X}}\right]^{1/\rho}\right]\right)^{\rho}. \tag{9}$$

Proof: We obtain (8) from (6) by weakening the expectation as follows:

$$\mathbb{E}\big[p_{e,m}(\mathsf{C})^{1/\rho}\big] \leq \mathbb{E}\left[\bigg(\sum_{\overline{m} \neq m} \mathbb{P}\Big[q^n(\boldsymbol{X}^{(\overline{m})}, \boldsymbol{Y}) \geq q^n(\boldsymbol{X}^{(m)}, \boldsymbol{Y}) \,\Big|\, \boldsymbol{X}^{(m)}, \boldsymbol{X}^{(\overline{m})}\Big]\bigg)^{1/\rho}\right] \tag{10}$$

$$\leq \mathbb{E}\left[2(M-1)\mathbb{P}\Big[q^n(\overline{\boldsymbol{X}}, \boldsymbol{Y}) \geq q^n(\boldsymbol{X}, \boldsymbol{Y}) \,\Big|\, \boldsymbol{X}, \overline{\boldsymbol{X}}\Big]^{1/\rho}\right], \tag{11}$$

where (10) follows from the union bound, and (11) follows using $M' = 2M-1$ along with the inequality

$$\Big(\sum_i a_i\Big)^{1/\rho} \leq \sum_i a_i^{1/\rho}, \tag{12}$$

which holds for any $\rho \geq 1$. We obtain (9) by an application of Markov's inequality. ■

Following the terminology of Polyanskiy *et al.* [3], we refer to the bounds in (8)–(9) as *expurgated random-coding union* (RCUX) bounds. These will be used as a starting point for derivations in Sections IV–VI. Furthermore, these bounds are computable, at least for sufficiently symmetric channels and metrics, and are thus of independent interest for characterizing the finite-length performance [3]. It should be noted that both rcux_{ρ} and $\mathrm{rcux}_{\rho,s}$ extend immediately to channels with memory and general decoding rules (not necessarily single-letter).

The bound $\mathrm{rcux}_{\rho,s}$ was presented by Gallager [2] under ML decoding with $s = \frac{1}{2}$. For the random-coding ensembles we consider, it will be seen that this choice of s is optimal for ML decoding, at least in terms of the error exponent obtained. However, for mismatched decoding it is important to allow for an arbitrary $s \geq 0$.

The following theorem gives an asymptotic bound which follows by using Lemma 1 with a choice of $f(\cdot)$ which differs from that of Gallager.

Theorem 2. *Consider a sequence of codebooks C_n containing $M_n' = \lfloor \exp(nR) \rfloor$ codewords which are generated independently according to $P_{\boldsymbol{X}}$. Suppose that there exists a non-negative sequence $E(n)$ growing subexponentially in n (i.e. $E(n) \doteq 1$) such that*

$$\mathbb{P}\big[q^n(\overline{\boldsymbol{x}}, \boldsymbol{Y}) \geq q^n(\boldsymbol{x}, \boldsymbol{Y}) \,\big|\, \boldsymbol{X} = \boldsymbol{x}\big] \geq \exp(-E(n)) \tag{13}$$

for all $(\boldsymbol{x}, \overline{\boldsymbol{x}})$ with $P_{\boldsymbol{X}}(\boldsymbol{x}) P_{\boldsymbol{X}}(\overline{\boldsymbol{x}}) > 0$. Then there exists a sequence of codebooks $\mathcal{C}_n$ with M_n codewords such that

$$\lim_{n \to \infty} \frac{1}{n} \log M_n = R \tag{14}$$

and

$$\begin{aligned} p_e(\mathcal{C}_n) &\dot{\leq} \exp\Big(\mathbb{E}[\log p_{e,m}(\mathsf{C}_n)]\Big) && (15) \\ &\leq \exp\Big(\rho \mathbb{E}\Big[\log \mathbb{E}\big[p_{e,m}(\mathsf{C}_n)^{1/\rho} \,\big|\, \boldsymbol{X}^{(m)}\big]\Big]\Big), && (16) \end{aligned}$$

where (16) *holds for any $\rho > 0$.*

Proof: The error probability associated with the transmitted codeword $\boldsymbol{x}$ is lower bounded by the left-hand side of (13), where $\overline{\boldsymbol{x}}$ is any incorrect codeword. The assumption in (13) thus implies that the function $f(p_{e,m}(\mathsf{C})) = E(n) + \log p_{e,m}(\mathsf{C})$ is non-negative for $m = 1, \cdots, M$. Applying Lemma 1, we obtain that for each n there exists a codebook $\mathcal{C}_n$ such that

$$E(n) + \log p_e(\mathcal{C}_n) \leq (1 + \eta_n)\big(E(n) + \mathbb{E}[\log p_{e,m}(\mathsf{C}_n)]\big) \tag{17}$$

for any $\eta_n > 0$. Since $\log \alpha \leq 0$ for $\alpha \in (0, 1]$, it follows that

$$\log p_e(\mathcal{C}_n) \leq \eta_n E(n) + \mathbb{E}[\log p_{e,m}(\mathsf{C}_n)]. \tag{18}$$

Choosing $\eta_n = \frac{1}{E(n)}$, we obtain (15). Furthermore, we have from Lemma 1 that $M_n = e^{nR} \frac{\eta_n}{1+\eta_n}$, which yields (14) since $\eta_n = \frac{1}{E(n)}$ decays subexponentially in n. We obtain (16) by writing $\log \alpha = \rho \log(\alpha^{1/\rho})$, conditioning on the transmitted codeword, and applying Jensen's inequality. ■

The assumption of Theorem 2 is mild, allowing ensembles for which the error probability associated with any two permissible codewords decays nearly *double*-exponentially fast. However, it is a multi-letter condition, and hence may be difficult to verify directly. A single-letter sufficient condition depending only on the channel, metric and cost constraint (2) is that

$$\lim_{\gamma\to\infty}\frac{1}{\gamma}\log\log\frac{1}{\pi(\gamma)}=0, \tag{19}$$

where

$$\pi(\gamma)\triangleq\min_{(x,\overline{x})\,:\,c(x)\le\gamma,c(\overline{x})\le\gamma}\mathbb{P}[Y_x\in\mathcal{E}(x,\overline{x})] \tag{20}$$

$$\mathcal{E}(x,\overline{x})\triangleq\big\{y\,:\,q(\overline{x},y)\ge q(x,y)\big\}, \tag{21}$$

where in (20) we define $Y_x\sim W(\cdot|x)$. Under this assumption, the probability in (13) is lower bounded by the probability that $Y_i\in\mathcal{E}(X_i,\overline{X}_i)$ for $i=1,\cdots,n$, which in turn is lower bounded by $\pi(n\Gamma)^n$. Since n times a subexponential sequence is also subexponential, the condition of Theorem 2 follows from (19). Further discussion is given in Appendix A, along with some examples.

From (15), we can see the advantage of the expurgated ensemble over the non-expurgated one. The former yields the exponent corresponding to $-\frac{1}{n}\mathbb{E}[\log p_{e,m}(\mathsf{C}_n)]$, which is higher in general than that of $-\frac{1}{n}\log\mathbb{E}[p_{e,m}(\mathsf{C}_n)]$ due to Jensen's inequality.

Using L'Hôpital's rule, it is easily shown that $\lim_{\rho\to\infty}\rho\log\mathbb{E}[Z^{1/\rho}]=\mathbb{E}[\log Z]$ for any random variable Z. It follows that the inequality in (16) is actually an equality in the limit as $\rho\to\infty$. At first glance, it may appear that a similar argument can be used to show that (6) yields the same exponent as (15). However, there is an issue with the order of the limits of n and ρ. If we take $\rho\to\infty$ in (6), the factor 2^ρ makes the right-hand side equal ∞. We cannot resolve this issue by letting ρ grow slowly with n, since the random variable $p_{e,m}(\mathsf{C})$ also varies with n.

While we do not have an example where Theorem 2 yields a strictly higher exponent than (6), we will see that the former is useful in simplifying the analysis.

III. Expurgated Ensembles and Exponents

In this section, we present an overview of expurgated exponents, some of which appear here for the first time.

A. *Expurgated Random-Coding Ensembles*

Throughout the paper, we study three expurgated ensembles, each of which depends on an input distribution $Q\in\mathcal{P}(\mathcal{X})$:

1) The i.i.d. ensemble is characterized by

$$P_{\boldsymbol{X}}(\boldsymbol{x})=\prod_{i=1}^{n}Q(x_i). \tag{22}$$

This codeword distribution is valid for both discrete and continuous alphabets, but it is not suitable for channels with cost constraints, since in all non-trivial cases there is a non-zero probability of violating the constraint.

2) The constant-composition ensemble is characterized by

$$P_{\boldsymbol{X}}(\boldsymbol{x})=\frac{1}{|T^n(Q_n)|}\mathbb{1}\big\{\boldsymbol{x}\in T^n(Q_n)\big\}, \tag{23}$$

where Q_n is a type with the same support as Q such that $|Q_n(x)-Q(x)|=O\big(\frac{1}{n}\big)$ for all x. This codeword distribution relies on $|\mathcal{X}|$ being finite. It is directly applicable to channels with cost constraints, since each codeword satisfies (2) with probability one provided that $\mathbb{E}_{Q_n}[c(X)] \le \Gamma$, which in turn can be achieved provided that $\mathbb{E}_Q[c(X)] \le \Gamma$.

3) The cost-constrained ensemble is characterized by

$$P_{\boldsymbol{X}}(\boldsymbol{x}) = \frac{1}{\mu_n} \prod_{i=1}^{n} Q(x_i) \mathbb{1}\{\boldsymbol{x} \in \mathcal{D}_n\}, \tag{24}$$

where

$$\mathcal{D}_n \triangleq \left\{ \boldsymbol{x} \,:\, \frac{1}{n}\sum_{i=1}^{n} c(x_i) \le \Gamma, \left| \frac{1}{n}\sum_{i=1}^{n} a_l(x_i) - \phi_l \right| \le \frac{\delta}{n}, \, l = 1, \dots, L \right\}, \tag{25}$$

and where δ is a positive constant (independent of n), $\{a_l(\cdot)\}_{l=1}^{L}$ are functions with means $\phi_l \triangleq \mathbb{E}_Q[a_l(X)]$, and μ_n is a normalizing constant. This codeword distribution is valid for both discrete and continuous alphabets, and ensures that each codeword satisfies (2) with probability one. Both $c(x)$ and $\{a_l(\cdot)\}$ can be thought of as cost functions, and we will distinguish between the two by referring to them as the *system cost* and *auxiliary costs* respectively. In contrast to the system cost, the auxiliary costs are functions which can be optimized. That is, while the system cost is given as part of the problem statement, the auxiliary costs are introduced to improve the performance of the random-coding ensemble itself [9], [10], [19].

B. Expurgated Exponents

Here we state and compare the exponents obtained by the above ensembles. Unless stated otherwise, we assume that the channel is a DMC with unconstrained inputs.

Substituting the i.i.d. distribution (22) into (9), we immediately obtain the exponent

$$E_{\mathrm{ex}}^{\mathrm{iid}}(Q,R) \triangleq \sup_{\rho \ge 1} E_{\mathrm{x}}^{\mathrm{iid}}(Q,\rho) - \rho R, \tag{26}$$

where

$$E_{\mathrm{x}}^{\mathrm{iid}}(Q,\rho) \triangleq \sup_{s \ge 0} -\rho \log \sum_{x,\overline{x}} Q(x)Q(\overline{x}) \left(\sum_{y} W(y|x) \left(\frac{q(\overline{x},y)}{q(x,y)} \right)^{s} \right)^{1/\rho}, \tag{27}$$

The objective in (27) is concave in s, and under ML decoding (i.e. $q(x,y) = W(y|x)$), it is also unchanged when s is replaced by $1-s$. From these properties, it follows that $s = \frac{1}{2}$ is optimal for ML decoding, and thus the exponent is the same as that of Gallager [2].

Csiszár and Körner [6] make use of the constant-composition codeword distribution in (23). The analysis is significantly different to that of Gallager, and yields an exponent in a different form, namely[1]

$$E_{\mathrm{ex}}^{\mathrm{cc}}(Q,R) \triangleq \min_{\substack{P_{X\overline{X}Y} \in \mathcal{T}^{\mathrm{cc}}(Q) \\ I_P(X;\overline{X}) \le R}} D(P_{X\overline{X}Y} \| Q \times Q \times W) - R, \tag{28}$$

where

$$\mathcal{T}^{\mathrm{cc}}(Q) \triangleq \left\{ P_{X\overline{X}Y} \in \mathcal{P}(\mathcal{X} \times \mathcal{X} \times \mathcal{Y}) \,:\, P_X = Q, P_{\overline{X}} = Q, \mathbb{E}_P[\log q(\overline{X},Y)] \ge \mathbb{E}_P[\log q(X,Y)] \right\}. \tag{29}$$

The objective in (28) follows from [6, Eq. (32)] and the identity

$$D(P_{X\overline{X}Y} \| Q \times Q \times W) = D(P_{X\overline{X}Y} \| P_{X\overline{X}} \times W) + I_P(X;\overline{X}), \tag{30}$$

[1] The notation $Q \times Q \times W$ denotes the distribution $Q(x)Q(\overline{x})W(y|x)$.

which holds for any $P_{X\overline{X}Y}$ such that $P_X = P_{\overline{X}} = Q$. Defining $P_Y(y) \triangleq \sum_x Q(x)W(y|x)$, it is easily seen that $E_{\rm ex}^{\rm cc}$ is positive for sufficiently small R provided that $\mathbb{E}_{Q\times W}[\log q(X,Y)] > \mathbb{E}_{Q\times P_Y}[\log q(X,Y)]$. It was shown in [8] that the mismatched capacity is in fact zero unless this condition holds for some Q.

The following theorem provides the means for comparing the above two exponents, as well as that of Csiszár, Körner and Marton [4].

Theorem 3. *For any input distribution Q and rate R, we have*

$$E_{\rm ex}^{\rm cc}(Q,R) = \sup_{s\ge 0} \min_{\substack{P_{X\overline{X}}\,:\,P_X=Q,P_{\overline{X}}=Q,\\ I_P(X;\overline{X})\le R}} \mathbb{E}_P[d_s(X,\overline{X})] + I_P(X;\overline{X}) - R \tag{31}$$

$$= \sup_{\rho\ge 1} E_{\rm x}^{\rm cc}(Q,\rho) - \rho R, \tag{32}$$

where

$$d_s(x,\overline{x}) \triangleq -\log\sum_y W(y|x)\left(\frac{q(\overline{x},y)}{q(x,y)}\right)^s \tag{33}$$

$$E_{\rm x}^{\rm cc}(Q,\rho) \triangleq \sup_{s\ge 0,a(\cdot)} -\rho\sum_x Q(x)\log\sum_{\overline{x}} Q(\overline{x})\frac{e^{a(\overline{x})}}{e^{a(x)}}\left(\sum_y W(y|x)\left(\frac{q(\overline{x},y)}{q(x,y)}\right)^s\right)^{1/\rho}. \tag{34}$$

Proof: See Appendix B. ■

The expressions (32) and (34) strongly resemble (26)–(27). The expression in (31) is a generalization of the exponent in [4], which is recovered by setting $q(x,y) = W(y|x)$ and $s = \frac{1}{2}$. Using the same argument as the one following (27), we see that the latter choice is optimal. From the proof of Theorem 3, this implies the optimality of $s = \frac{1}{2}$ in (34) under ML decoding, though the optimal choice of $a(\cdot)$ is unclear in general. To our knowledge, the expression in (34) has not appeared previously even for ML decoding.

As noted in [6], [17], we can write (31) in the language of rate-distortion theory [22, Ch. 10]. Fix any $s \ge 0$ and define

$$D_s(Q,R) \triangleq \min_{\substack{P_{X\overline{X}}\,:\,P_X=Q,P_{\overline{X}}=Q,\\ I_P(X;\overline{X})\le R}} \mathbb{E}_P[d_s(X,\overline{X})]. \tag{35}$$

This can be interpreted as the distortion-rate function of a source X with a reproduction variable $\overline{X}$, subject to the additional constraint that each reproduction codeword $\overline{\boldsymbol{x}}$ has empirical distribution Q. For any $s \ge 0$, the constraint on the mutual information in (31) is active for sufficiently small R. The supremum of all such rates is given by

$$R_s(Q) \triangleq I_{P^*}(X;\overline{X}), \tag{36}$$

where

$$P_{X\overline{X}}^* \triangleq \operatorname*{arg\,min}_{P_{X\overline{X}}\,:\,P_X=Q,P_{\overline{X}}=Q} \mathbb{E}_P[d_s(X,\overline{X})] + I_P(X;\overline{X}). \tag{37}$$

For $R \le R_s$ we have $I_P(X;\overline{X}) = R$ under the minimizing $P_{X\overline{X}Y}$, whereas for $R \ge R_s$ the minimum in (31) decreases linearly with R for any fixed s. It follows that

$$E_{\rm ex}^{\rm cc}(Q,R) = \sup_{s\ge 0} E_{\rm ex}^{\rm cc}(Q,R,s), \tag{38}$$

where

$$E_{\mathrm{ex}}^{\mathrm{cc}}(Q,R,s) \triangleq \begin{cases} D_s(Q,R) & R \le R_s(Q) \\ D_s(Q,R_s) + R_s(Q) - R & R > R_s(Q). \end{cases} \tag{39}$$

By applying Jensen's inequality to (34) and setting $a(x)=0$, we immediately obtain

$$E_{\mathrm{ex}}^{\mathrm{cc}}(Q,R) \ge E_{\mathrm{ex}}^{\mathrm{iid}}(Q,R). \tag{40}$$

It was shown in [5, Ex. 10.18] that (40) holds with equality under ML decoding with an optimized input distribution Q. However, when either the decoding rule or input distribution is fixed, the inequality in (40) can be strict (see Section III-C for an example).

In Section IV, we show that (31) remains valid in the case of continuous outputs when the summation over y in (33) is replaced by an integral. In Section V, we take this result one step further and show that (32) remains valid in the case of continuous input and output alphabets, with the summations in (34) replaced by integrals. This is proved using the cost-constrained ensemble in (24).

We conclude this discussion with the following theorem, which generalizes Gallager's expression for the expurgated exponent as $R \to 0^+$ for channels whose zero-error capacity [23] is zero, and shows that the inequality in (40) becomes an equality in the limit.

Theorem 4. *Fix any input distribution Q such that all pairs $(x,\overline{x})$ with $Q(x)Q(\overline{x})>0$ share a common output, i.e. $W(y|x)W(y|\overline{x})>0$ for some y. Then*

$$\lim_{R\to 0^+} E_{\mathrm{ex}}^{\mathrm{cc}}(Q,R) = \lim_{R\to 0^+} E_{\mathrm{ex}}^{\mathrm{iid}}(Q,R) = \sup_{s\ge 0} \mathbb{E}[d_s(X,\overline{X})], \tag{41}$$

where d_s is defined in (33)*, and the expectation is taken with respect to $Q(x)Q(\overline{x})$.*

Proof: See Appendix C. ■

C. Numerical Example

In this subsection, we provide numerical results in the setting of Bit-Interleaved Coded Modulation (BICM), which was studied from a mismatched decoding perspective in [24]. We briefly state the setup here, and refer the reader to [24] for further details and discussion.

We assume that $|\mathcal{X}| = 2^t$ for some integer t. The codebook $\mathcal{C}$ containing codewords in $\mathcal{X}^n$ is obtained from a binary codebook containing codewords in $\{0,1\}^{nt}$. A given codeword $\boldsymbol{x} = (x_1, \cdots, x_n)$ is obtained by passing the corresponding binary codeword $\boldsymbol{b} = (b_1, \cdots, b_{nt})$ through a length-nt interleaver, and then applying a binary labeling function $\psi : \{0,1\}^t \to \mathcal{X}$ in blocks of t bits. As noted in [24], the interleaver can be ignored in the random coding setting, and we can thus write $x_i = \psi(b_{t(i-1)+1}, \dots, b_{ti}), i = 1, \cdots, n$.

We denote the inverse labeling function by $b_j : \mathcal{X} \to \{0,1\}$, so that $b_j(x)$ is the j-th bit in the binary label of x for $j = 1, \cdots, t$. We consider uniform input distributions on the bits and symbols, yielding $Q(x) = \frac{1}{|\mathcal{X}|}$ for all x. The classical BICM decoder [24], [25] treats each of the t bits in a received symbol as being independent. This leads to a

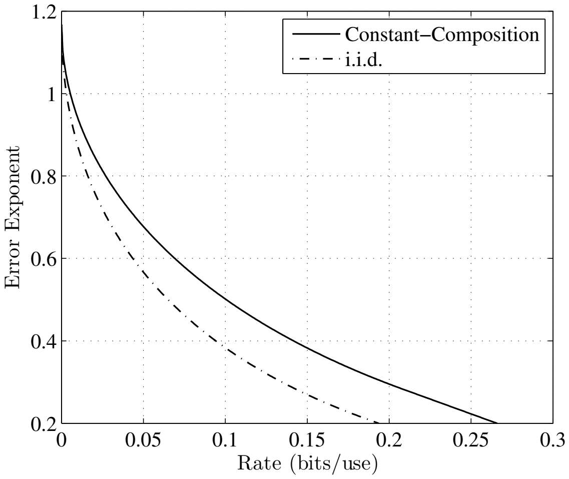

Figure 1. Expurgated exponents for BICM over the additive Gaussian noise channel with 8-PAM and the natural binary code labeling.

symbol decoding metric $q(x,y)$ which is equal to the product of bit metrics, namely [24]

$$q(x,y)=\prod_{j=1}^{t}q_j(b_j(x),y), \tag{42}$$

where

$$q_j(b,y)\overset{\triangle}{=}\sum_{x'\,:\,b_j(x')=b}W(y|x'). \tag{43}$$

As an example of the BICM setup, we consider the additive Gaussian noise channel $Y=X+Z$, where Z is normally distributed. We consider Pulse Amplitude Modulation (PAM) with $|\mathcal{X}|=8$ and hence $t=3$. We set the signal-to-noise ratio (SNR) to 5dB, and we let the binary labeler $\psi(\cdot)$ be the natural binary code, i.e. the 8 symbols are labeled in increasing order of their numerical x-value as $(0,0,0),(0,0,1),\cdots,(1,1,1)$.

Figure 1 plots the expurgated exponents for the i.i.d. and constant-composition ensembles, i.e. $E_{\mathrm{ex}}^{\mathrm{iid}}$ in (26) and $E_{\mathrm{ex}}^{\mathrm{cc}}$ in (32). The constant-composition exponent yields a significant improvement over the i.i.d. one. Consistent with Theorem 4, the exponents approach the same value as $R\to 0$.

As stated above, the gap between the two exponents vanishes under ML decoding with an optimally chosen input distribution Q. However, it should be noted that the gap remains present under ML decoding with a suboptimal Q, and also under mismatched decoding with an optimal Q.

IV. Derivations for Discrete Alphabets

In this section, we provide techniques for deriving the exponent $E_{\mathrm{ex}}^{\mathrm{cc}}$ in the forms given in (28) and (31), making use of the constant-composition ensemble in (23). Unless stated otherwise, we assume that the channel is a DMC.

We define the sets

$$\mathcal{S}^{\mathrm{cc}}(Q) \triangleq \Big\{\widetilde{P}_{X\overline{X}} \in \mathcal{P}(\mathcal{X}\times\mathcal{X}) \,:\, \widetilde{P}_{X} = Q, \widetilde{P}_{\overline{X}} = Q\Big\} \tag{44}$$

$$\mathcal{T}^{\mathrm{cc}}(\widetilde{P}_{X\overline{X}}) \triangleq \Big\{P_{X\overline{X}Y} \in \mathcal{P}(\mathcal{X}\times\mathcal{X}\times\mathcal{Y}) \,:\, P_{X\overline{X}} = \widetilde{P}_{X\overline{X}}, \mathbb{E}_P[\log q(\overline{X},Y)] \ge \mathbb{E}_P[\log q(X,Y)]\Big\} \tag{45}$$

$$\mathcal{S}_n^{\mathrm{cc}}(Q) \triangleq \mathcal{S}^{\mathrm{cc}}(Q) \cap \mathcal{P}_n(\mathcal{X}\times\mathcal{X}) \tag{46}$$

$$\mathcal{T}_n^{\mathrm{cc}}(\widetilde{P}_{X\overline{X}}) \triangleq \mathcal{T}^{\mathrm{cc}}(\widetilde{P}_{X\overline{X}}) \cap \mathcal{P}_n(\mathcal{X}\times\mathcal{X}\times\mathcal{Y}), \tag{47}$$

where we overload the symbol $\mathcal{T}^{\mathrm{cc}}$ (see (29)). It follows from these definitions that $P_{X\overline{X}Y} \in \mathcal{T}^{\mathrm{cc}}(Q)$ if and only if $P_{X\overline{X}Y} \in \mathcal{T}^{\mathrm{cc}}(\widetilde{P}_{X\overline{X}})$ for some $\widetilde{P}_{X\overline{X}} \in \mathcal{S}^{\mathrm{cc}}(Q)$. Furthermore, we have the following properties of types (e.g. see [5, Ch. 2]):

1) For any $\widetilde{P}_{X\overline{X}} \in \mathcal{S}_n^{\mathrm{cc}}(Q_n)$,

$$\mathbb{P}\big[(\boldsymbol{X},\overline{\boldsymbol{X}}) \in T^n(\widetilde{P}_{X\overline{X}})\big] \doteq \exp\big(-nI_{\widetilde{P}}(X;\overline{X})\big). \tag{48}$$

2) If $(\boldsymbol{x},\overline{\boldsymbol{x}}) \in T^n(\widetilde{P}_{X\overline{X}})$, then for any $P_{X\overline{X}Y} \in \mathcal{T}_n^{\mathrm{cc}}(\widetilde{P}_{X\overline{X}})$,

$$\mathbb{P}\big[(\boldsymbol{x},\overline{\boldsymbol{x}},\boldsymbol{Y}) \in T^n(P_{X\overline{X}Y}) \,\big|\, \boldsymbol{X} = \boldsymbol{x}\big] \doteq \exp\big(-nD(P_{X\overline{X}Y}\|\widetilde{P}_{X\overline{X}}\times W)\big). \tag{49}$$

A. Derivation Using Theorem 1

Using the codeword distribution in (23) and expanding (8) in terms of types, we obtain

$$\mathrm{rcux}_\rho(n,M)^{1/\rho}$$

$$= 4(M-1) \sum_{\widetilde{P}_{X\overline{X}} \in \mathcal{S}_n^{\mathrm{cc}}(Q_n)} \mathbb{P}\Big[(\boldsymbol{X},\overline{\boldsymbol{X}}) \in T^n(P_{X\overline{X}})\Big] \sum_{P_{X\overline{X}Y} \in \mathcal{T}_n^{\mathrm{cc}}(\widetilde{P}_{X\overline{X}})} \mathbb{P}\Big[(\boldsymbol{x},\overline{\boldsymbol{x}},\boldsymbol{Y}) \in T^n(P_{X\overline{X}Y}) \,\Big|\, \boldsymbol{X} = \boldsymbol{x}\Big]^{1/\rho} \tag{50}$$

$$\doteq M \max_{\widetilde{P}_{X\overline{X}} \in \mathcal{S}_n^{\mathrm{cc}}(Q_n)} \max_{P_{X\overline{X}Y} \in \mathcal{T}_n^{\mathrm{cc}}(\widetilde{P}_{X\overline{X}})} \exp\Big(-nI_{\widetilde{P}}(X;\overline{X})\Big) \exp\Big(-n\cdot\frac{1}{\rho}D\big(P_{X\overline{X}Y}\|\widetilde{P}_{X\overline{X}}\times W\big)\Big) \tag{51}$$

$$\doteq M \max_{P_{X\overline{X}Y} \in \mathcal{T}^{\mathrm{cc}}(Q)} \exp\Big(-n\Big(\frac{1}{\rho}D\big(P_{X\overline{X}Y}\|P_{X\overline{X}}\times W\big) + I_P(X;\overline{X})\Big)\Big), \tag{52}$$

where in (50) we define $(\boldsymbol{x},\overline{\boldsymbol{x}})$ to be an arbitrary pair with joint type $\widetilde{P}_{X\overline{X}}$, (51) follows from the properties of types in (48)–(49) and the fact that the number of joint types is polynomial in n, and (52) follows from the definitions of $\mathcal{S}_n^{\mathrm{cc}}$, $\mathcal{T}_n^{\mathrm{cc}}$ and $\mathcal{T}^{\mathrm{cc}}$. We thus obtain the exponent

$$\sup_{\rho\ge1} \min_{P_{X\overline{X}Y} \in \mathcal{T}^{\mathrm{cc}}(Q)} D(P_{X\overline{X}Y}\|P_{X\overline{X}}\times W) + \rho\big(I_P(X;\overline{X}) - R\big) \tag{53}$$

$$= \min_{P_{X\overline{X}Y} \in \mathcal{T}^{\mathrm{cc}}(Q)} \sup_{\rho\ge1} D(P_{X\overline{X}Y}\|P_{X\overline{X}}\times W) + \rho\big(I_P(X;\overline{X}) - R\big), \tag{54}$$

where (54) follows from Fan's minimax theorem [26], the conditions of which are satisfied here since the objective is linear in ρ and convex in $P_{X\overline{X}Y}$. Using

$$\sup_{\rho\ge1} \rho\alpha = \begin{cases} \infty & \alpha > 0 \\ \alpha & \alpha \le 0 \end{cases} \tag{55}$$

and the identity in (30), it follows that (54) coincides with (28).

If we start with $\mathrm{rcux}_{\rho,s}$ in (9) in place of rcux_{ρ} in (8), then a nearly identical analysis yields the exponent $E_{\mathrm{ex}}^{\mathrm{cc}}$ in the form given in (31). Unlike the above derivation or those of [4], [6], this approach allows for continuous output alphabets, though the input alphabet must remain finite.

B. Derivation Using Type Class Enumerators

Here we provide an alternative derivation of (28) and (31) using the method of type class enumerators (e.g. see [11]–[13]). This approach guarantees exponential tightness starting from an earlier step, and provides further insight into the expurgated coding bounds, including connections with statistical mechanics (see Section VII). While the focus in this section is on discrete alphabets, the analysis has a natural extension to continuous alphabets (see Section V-B).

Substituting (10) into (6) and defining

$$d_q(\boldsymbol{x},\overline{\boldsymbol{x}}) \triangleq -\log \mathbb{P}\Big[q^n(\overline{\boldsymbol{x}},\boldsymbol{Y}) \ge q^n(\boldsymbol{x},\boldsymbol{Y}) \,\Big|\, \boldsymbol{X}=\boldsymbol{x}\Big], \tag{56}$$

we obtain the bound

$$p_e(\mathcal{C}) \le 2^{\rho}\mathbb{E}\left[\bigg(\sum_{\overline{m}\ne m} e^{-d_q(\boldsymbol{X}^{(m)},\boldsymbol{X}^{(\overline{m})})}\bigg)^{1/\rho}\right]^{\rho} \tag{57}$$

$$\triangleq 2^{\rho}A_n(R,\rho). \tag{58}$$

Since we have not made use of the inequality in (12), (57) is valid for all $\rho>0$ (see (6)), rather than just $\rho \ge 1$.

For $m=1,\cdots,M$ and each joint type $\widetilde{P}_{X\overline{X}}$, we define the random variable

$$N_m(\widetilde{P}_{X\overline{X}}) \triangleq \sum_{\overline{m}\ne m} \mathbb{1}\big\{(\boldsymbol{X}^{(m)},\boldsymbol{X}^{(\overline{m})}) \in T^n(\widetilde{P}_{X\overline{X}})\big\}. \tag{59}$$

Under the random-coding distribution in (23), we have $N_m(\widetilde{P}_{X\overline{X}})=0$ with probability one if $\widetilde{P}_{X\overline{X}} \notin \mathcal{S}_n^{\mathrm{cc}}(Q_n)$. That is, the marginal of each codeword must agree with Q. Since d_q depends only on the joint type of its arguments, we define $d_q(\widetilde{P}_{X\overline{X}}) \triangleq \frac{1}{n}d_q(\boldsymbol{x},\overline{\boldsymbol{x}})$, where $(\boldsymbol{x},\overline{\boldsymbol{x}}) \in T^n(\widetilde{P}_{X\overline{X}})$.

Making repeated use of the fact that the number of joint types is polynomial in n, we have the following:

$$A_n(R,\rho)^{1/\rho} = \mathbb{E}\left[\bigg(\sum_{\widetilde{P}_{X\overline{X}}} N_m(\widetilde{P}_{X\overline{X}})e^{-nd_q(\widetilde{P}_{X\overline{X}})}\bigg)^{1/\rho}\right] \tag{60}$$

$$\doteq \mathbb{E}\left[\bigg(\max_{\widetilde{P}_{X\overline{X}}} N_m(\widetilde{P}_{X\overline{X}})e^{-nd_q(\widetilde{P}_{X\overline{X}})}\bigg)^{1/\rho}\right] \tag{61}$$

$$= \mathbb{E}\left[\max_{\widetilde{P}_{X\overline{X}}} N_m(\widetilde{P}_{X\overline{X}})^{1/\rho}e^{-nd_q(\widetilde{P}_{X\overline{X}})/\rho}\right] \tag{62}$$

$$\doteq \mathbb{E}\left[\sum_{\widetilde{P}_{X\overline{X}}} N_m(\widetilde{P}_{X\overline{X}})^{1/\rho}e^{-nd_q(\widetilde{P}_{X\overline{X}})/\rho}\right] \tag{63}$$

$$= \sum_{\widetilde{P}_{X\overline{X}}} \mathbb{E}\Big[N_m(\widetilde{P}_{X\overline{X}})^{1/\rho}\Big]e^{-nd_q(\widetilde{P}_{X\overline{X}})/\rho} \tag{64}$$

$$\doteq \max_{\widetilde{P}_{X\overline{X}}} \mathbb{E}\Big[N_m(\widetilde{P}_{X\overline{X}})^{1/\rho}\Big]e^{-nd_q(\widetilde{P}_{X\overline{X}})/\rho}. \tag{65}$$

It follows that

$$2^{\rho}A_n(R,\rho) \doteq \max_{\widetilde{P}_{X\overline{X}}} \bigg(\mathbb{E}\Big[N_m(\widetilde{P}_{X\overline{X}})^{1/\rho}\Big]\bigg)^{\rho} e^{-nd_q(\widetilde{P}_{X\overline{X}})}. \tag{66}$$

Now, similarly to [11, Eq. (34)], we have for all $\widetilde{P}_{X\overline{X}} \in \mathcal{S}_n^{\mathrm{cc}}(Q_n)$ that

$$\mathbb{E}\Big[N_m(\widetilde{P}_{X\overline{X}})^{1/\rho}\Big] \doteq \begin{cases} \exp\big(n\big(R - I_{\widetilde{P}}(X;\overline{X})\big)\big) & R < I_{\widetilde{P}}(X;\overline{X}) \\ \exp\big(n\big(R - I_{\widetilde{P}}(X;\overline{X})\big)/\rho\big) & R \ge I_{\widetilde{P}}(X;\overline{X}). \end{cases} \tag{67}$$

This result follows from the fact that given $\boldsymbol{X}^{(m)} = \boldsymbol{x}$, $N_m(\widetilde{P}_{X\overline{X}})$ is the sum of $e^{nR}-1$ binary independent random variables,

$$U_{\overline{m}} \triangleq \mathbb{1}\Big\{(\boldsymbol{x}, \boldsymbol{X}^{(\overline{m})}) \in T^n(\widetilde{P}_{X\overline{X}})\Big\}, \tag{68}$$

whose expectations are of the exponential order of $\exp\big(-nI_{\widetilde{P}}(X;\overline{X})\big)$. Furthermore, similarly to (51), we have

$$e^{-nd_q(\widetilde{P}_{X\overline{X}})} \doteq \exp\bigg(-n \min_{P_{X\overline{X}Y} \in \mathcal{T}^{\mathrm{cc}}(\widetilde{P}_{X\overline{X}})} D\big(P_{X\overline{X}Y} \| \widetilde{P}_{X\overline{X}} \times W\big)\bigg) \tag{69}$$

$$\triangleq e^{-nD_q(\widetilde{P}_{X\overline{X}})}. \tag{70}$$

Upon taking into account all the possible empirical distributions $\{\widetilde{P}_{X\overline{X}}\}$, we readily obtain

$$2^{\rho}A_n(R,\rho) \doteq e^{-n\min\{E_1(R,\rho),E_2(R)\}}, \tag{71}$$

where

$$E_1(R,\rho) \triangleq \min_{\substack{\widetilde{P}_{X\overline{X}} \in \mathcal{S}^{\mathrm{cc}}(Q) \\ I_{\widetilde{P}}(X;\overline{X}) \ge R}} D_q(\widetilde{P}_{X\overline{X}}) + \rho\big(I_{\widetilde{P}}(X;\overline{X}) - R\big) \tag{72}$$

and

$$E_2(R) = \min_{\substack{\widetilde{P}_{X\overline{X}} \in \mathcal{S}^{\mathrm{cc}}(Q) \\ I_{\widetilde{P}}(X;\overline{X}) \le R}} D_q(\widetilde{P}_{X\overline{X}}) + I_{\widetilde{P}}(X;\overline{X}) - R. \tag{73}$$

Combining (30), (70) and (73), we see that $E_2(R)$ coincides with $E_{\mathrm{ex}}^{\mathrm{cc}}$ in the form given in (28). It remains to show that $E_1(R,\rho)$, for the optimum choice of ρ, is never smaller than $E_2(R)$. This can be seen by noting that since (72) contains the constraint $I_{\widetilde{P}}(X;\overline{X}) \ge R$, the term multiplying ρ in (72) is non-negative. Thus, the best choice of ρ is to take the limit as $\rho \to \infty$, and hence the minimum in (72) is achieved by some $\widetilde{P}_{X\overline{X}}$ satisfying $I_{\widetilde{P}}(X;\overline{X}) = R$. Since this joint distribution also satisfies the constraints in (73), we conclude that $E_1 \ge E_2$, thus completing the derivation.

If we apply Markov's inequality to the probability in (56), we obtain a weaker bound in (57) with the Chernoff distance

$$d_s^n(\boldsymbol{x}, \overline{\boldsymbol{x}}) \triangleq \sum_{i=1}^{n} d_s(x_i, \overline{x}_i) \tag{74}$$

replacing d_q, where d_s is defined in (33). Applying a nearly identical analysis to the one above, this leads to the equivalent form of $E_{\mathrm{ex}}^{\mathrm{cc}}$ given in (31). This approach allows for continuous output alphabets, and will also prove to be important for handling continuous input alphabets (see Section V-B). While d_q is more complex than d_s and does not admit a single-letter form, we have chosen to focus on d_q in this section for the sake of proving the exponential tightness of the analysis starting from the earliest step possible.

C. Comparison of Techniques

For the constant-composition codeword distribution considered in this section, the approaches of Sections IV-A and IV-B led to the same exponent, namely $E_{\mathrm{ex}}^{\mathrm{cc}}$. It should be noted, however, that the approach of Section IV-B can yield a strictly higher exponent than that of Section IV-A for some codeword distributions. Here we discuss the simple example of the i.i.d. distribution in (22).

Following the steps of Section IV-A, it is easily verified that the exponent of the quantity rcux_ρ in Theorem 1 is given by

$$\min_{\substack{P_{X\overline{X}Y}\,:\,D(P_{X\overline{X}}\|Q\times Q)\leq R,\\ \mathbb{E}_P[\log q(\overline{X},Y)]\geq\mathbb{E}_P[\log q(X,Y)]}} D(P_{X\overline{X}Y}\|Q\times Q\times W)-R. \tag{75}$$

On the other hand, the analysis of Section IV-B yields an exponent of the same form as (75) with an additional constraint $P_X = Q$ in the minimization. To see why this is true, we note that the quantity $N_m(\widetilde{P}_{X\overline{X}})$ defined in (59) satisfies

$$\mathbb{E}\Big[N_m(\widetilde{P}_{X\overline{X}})^{1/\rho}\Big] = \mathbb{P}\big[\boldsymbol{X}^{(m)}\in T^n(\widetilde{P}_X)\big]\mathbb{E}\Big[N_m(\widetilde{P}_{X\overline{X}})^{1/\rho}\,\Big|\,\boldsymbol{X}^{(m)}\in T^n(\widetilde{P}_X)\Big] \tag{76}$$

$$\doteq \begin{cases} \exp\big(-nD(\widetilde{P}_X\|Q)\big)\cdot\exp\big(n\big(R-D(\widetilde{P}_{X\overline{X}}\|\widetilde{P}_X\times Q)\big)\big) & R< I_{\widetilde{P}}(X;\overline{X}) \\ \exp\big(-nD(\widetilde{P}_X\|Q)\big)\cdot\exp\big(n\big(R-D(\widetilde{P}_{X\overline{X}}\|\widetilde{P}_X\times Q)\big)/\rho\big) & R\geq I_{\widetilde{P}}(X;\overline{X}). \end{cases} \tag{77}$$

The additional factor $\exp\big(-nD(\widetilde{P}_X\|Q)\big)$ leads to an additive $\rho D(\widetilde{P}_X\|Q)$ term in the exponent E_2 in (73). The optimal choice of ρ is again in the limit as $\rho\to\infty$, and under this choice the minimizing $\widetilde{P}_{X\overline{X}}$ must satisfy $\widetilde{P}_X = Q$ so that the divergence is forced to zero.

Since both derivations are exponentially tight from the step at which they start, we conclude that the weakness of the first derivation is in the inequality in (11), or more precisely the use of (12). While this step is useful for simplifying the derivations, the above example shows that it is not exponentially tight in general.

Another approach to recovering the constraint $\widetilde{P}_X = Q$ in the above example is to follow the steps of Theorem 1 and Section IV-A starting with Theorem 2. Since the expectation of the transmitted codeword is outside the logarithm in (16), it is straightforward to obtain the constraint $\widetilde{P}_X = Q$ in the final minimization using the fact that the empirical distribution of $\boldsymbol{X}$ is close to Q with high probability.

Stated differently, the inequality (12) is exponentially tight for the i.i.d. ensemble when we start with (16), but it is not tight when we start with (6). In the latter case, the exponentially tight analysis of Section IV-B is required to obtain the improved exponent.

More generally, we believe that the approach of Section IV-B and its generalization to continuous channels (see Section V-B) could prove useful in obtaining strictly higher exponents than those attained by Theorem 1 for channels with memory and more general decoding metrics. An analogous observation was shown to be true in [11] in the setting of erasure and list decoding.

V. Derivations for Continuous Alphabets

In this section, we derive the following generalization of (32):

$$E_{\mathrm{ex}}^{\mathrm{cc}}(Q,R) = \sup_{\rho\geq 1} E_{\mathrm{x}}^{\mathrm{cc}}(Q,\rho)-\rho R, \tag{78}$$

where

$$E_{\mathrm{x}}^{\mathrm{cost}}(Q,\rho) = \sup_{s\geq 0, a(\cdot)} -\rho \int dx Q(x) \log \int d\overline{x} Q(\overline{x}) \frac{e^{a(\overline{x})}}{e^{a(x)}} \left(\int dy W(y|x) \left(\frac{q(\overline{x},y)}{q(x,y)} \right)^s \right)^{1/\rho}. \tag{79}$$

We show that, subject to mild technical conditions, this exponent is achievable for continuous cost-constrained channels (see (2)) provided that $\mathbb{E}_Q[c(X)] \leq \Gamma$. For clarity of exposition, we focus on the case that the input and output alphabets are a subset of the real line $\mathbb{R}$, but our analysis applies more generally (e.g. to $\mathbb{R}^k$ with $k > 1$).

We consider the cost-constrained ensemble in (24). Before proceeding, we present a number of preliminary results regarding the ensemble. A key property which will prove useful in the derivations is

$$\boldsymbol{x} \in \mathcal{D}_n \implies e^{r\left(\sum_{i=1}^n a(x_i) - n\phi_a\right)} e^{|r|\delta} \geq 1, \tag{80}$$

which holds for any real number r, and follows immediately from the definition of $\mathcal{D}_n$ in (25). Furthermore, we have the following.

Proposition 1. [10, Prop. 1] *Fix any input distribution Q and set of cost functions $\{a_l\}_{l=1}^L$ such that $E_Q[c(X)] \leq \Gamma$, $E_Q[c(X)^2] < \infty$ and $E_Q[a_l(X)^2] < \infty$ for $l = 1, \cdots, L$. Then the normalizing constant μ_n in* (24) *satisfies*

$$\lim_{n\to\infty} \frac{1}{n} \log \mu_n = 0. \tag{81}$$

Proposition 2. *Fix any input distribution Q and set of cost functions $\{a_l\}_{l=1}^L$ satisfying the assumptions of Proposition 1. For any function $f(x)$, we have*

$$\lim_{n\to\infty} \mathbb{E}\left[\frac{1}{n}\sum_{i=1}^n f(X_i)\right] = \mathbb{E}_Q[f(X)]. \tag{82}$$

Proof: See Appendix D. ■

Throughout the section, we present the analysis for a given input distribution Q. We assume that this distribution and the auxiliary costs in (25) are chosen such that the conditions of Proposition 1 are satisfied.

A. Derivation Using Theorem 1

We begin by presenting an achievable error exponent for the cost-constrained ensemble with fixed auxiliary costs.

Theorem 5. *For any input distribution Q and set of functions $\{a_l\}$ satisfying the assumptions of Proposition 1, the cost-constrained ensemble in* (24)–(25) *achieves the expurgated exponent*

$$E_{\mathrm{ex}}^{\mathrm{cost}}(Q,R,\{a_l\}) \triangleq \sup_{\rho\geq 1} E_{\mathrm{x}}^{\mathrm{cost}}(Q,\rho,\{a_l\}) - \rho R, \tag{83}$$

where

$$E_{\mathrm{x}}^{\mathrm{cost}}(Q,R,\{a_l\}) \triangleq \sup_{s\geq 0, \{r_l\}, \{\overline{r}_l\}} -\rho \log \iint dx d\overline{x} Q(x) Q(\overline{x}) \frac{e^{\sum_{l=1}^L \overline{r}_l (a_l(\overline{x}) - \phi_l)}}{e^{\sum_{l=1}^L r_l (a_l(x) - \phi_l)}} \left(\int dy W(y|x) \left(\frac{q(\overline{x},y)}{q(x,y)} \right)^s \right)^{1/\rho}. \tag{84}$$

Proof: Throughout the proof, we define $a_l^n(\boldsymbol{x}) \triangleq \sum_{i=1}^n a_l(x_i)$ and $Q^n(\boldsymbol{x}) \triangleq \prod_{i=1}^n Q(x_i)$. We start with (9), and write

$$\mathrm{rcux}_{\rho,s}(n,M)^{1/\rho} = 4(M-1)\iint d\boldsymbol{x}d\overline{\boldsymbol{x}}P_{\boldsymbol{X}}(\boldsymbol{x})P_{\boldsymbol{X}}(\overline{\boldsymbol{x}})\left(\int d\boldsymbol{y}W^n(\boldsymbol{y}|\boldsymbol{x})\left(\frac{q^n(\overline{\boldsymbol{x}},\boldsymbol{y})}{q^n(\boldsymbol{x},\boldsymbol{y})}\right)^s\right)^{1/\rho} \tag{85}$$

$$\dot{\le} M\iint d\boldsymbol{x}d\overline{\boldsymbol{x}}P_{\boldsymbol{X}}(\boldsymbol{x})P_{\boldsymbol{X}}(\overline{\boldsymbol{x}})\frac{e^{\sum_{l=1}^{L}\overline{r}_l(a_l^n(\overline{\boldsymbol{x}})-n\phi_l)}}{e^{\sum_{l=1}^{L}r_l(a_l^n(\boldsymbol{x})-n\phi_l)}}\left(\int d\boldsymbol{y}W^n(\boldsymbol{y}|\boldsymbol{x})\left(\frac{q^n(\overline{\boldsymbol{x}},\boldsymbol{y})}{q^n(\boldsymbol{x},\boldsymbol{y})}\right)^s\right)^{1/\rho} \tag{86}$$

$$\dot{\le} M\iint d\boldsymbol{x}d\overline{\boldsymbol{x}}Q^n(\boldsymbol{x})Q^n(\overline{\boldsymbol{x}})\frac{e^{\sum_{l=1}^{L}\overline{r}_l(a_l^n(\overline{\boldsymbol{x}})-n\phi_l)}}{e^{\sum_{l=1}^{L}r_l(a_l^n(\boldsymbol{x})-n\phi_l)}}\left(\int d\boldsymbol{y}W^n(\boldsymbol{y}|\boldsymbol{x})\left(\frac{q^n(\overline{\boldsymbol{x}},\boldsymbol{y})}{q^n(\boldsymbol{x},\boldsymbol{y})}\right)^s\right)^{1/\rho}, \tag{87}$$

where (86) holds for any $\{r_l\}$ and $\{\overline{r}_l\}$ from (80),[2] and (87) follows from (24) and (81). The proof is concluded by expanding each term in (87) as a product from 1 to n and taking the supremum over ρ, s, $\{r_l\}$ and $\{\overline{r}_l\}$. ■

In order to obtain the exponent $E_{\mathrm{ex}}^{\mathrm{cc}}$ from $E_{\mathrm{ex}}^{\mathrm{cost}}$, we set $L=2$ and choose $\overline{r}_1 = r_2 = 1$ and $\overline{r}_2 = r_1 = 0$. Upon optimizing the auxiliary costs $a_1(\cdot)$ and $a_2(\cdot)$, we obtain

$$E_{\mathrm{x}}^{\mathrm{cost}}(Q,\rho) = \sup_{s\ge0,a_1(\cdot),a_2(\cdot)} -\rho\log\iint dxd\overline{x}Q(x)Q(\overline{x})\frac{e^{a_1(\overline{x})-\phi_1}}{e^{a_2(x)-\phi_2}}\left(\int dyW(y|x)\left(\frac{q(\overline{x},y)}{q(x,y)}\right)^s\right)^{1/\rho} \tag{88}$$

$$\le \sup_{s\ge0,a_1(\cdot),a_2(\cdot)} -\rho\int dxQ(x)\log\int d\overline{x}Q(\overline{x})\frac{e^{a_1(\overline{x})-\phi_1}}{e^{a_2(x)-\phi_2}}\left(\int dyW(y|x)\left(\frac{q(\overline{x},y)}{q(x,y)}\right)^s\right)^{1/\rho} \tag{89}$$

where (89) follows from Jensen's inequality.

For any s and $a_1(\cdot)$, there exists a choice of $a_2(\cdot)$ which makes Jensen's inequality hold with equality in (89), and hence the same is true after taking the supremum over each. Hence, and by writing

$$-\int dxQ(x)\log\frac{e^{-\phi_1}}{e^{a_2(x)-\phi_2}} = -\int dxQ(x)\log e^{-a_1(x)} = \phi_1, \tag{90}$$

we obtain that the $a_2(\cdot)$ achieving the supremum in (88) is the one yielding equality in (89). Renaming $a_1(\cdot)$ as $a(\cdot)$ and using the first equality in (90), we obtain (79).

It should be noted that, in accordance with Proposition 1, the supremum over s and $a(\cdot)$ in (79) is restricted to choices such that $E_Q[a(X)^2] < \infty$, and such that $E_Q[a_2(X)^2] < \infty$ for the choice of $a_2(\cdot)$ which makes Jensen's inequality hold with equality in (89) (expressed in terms of s and $a(\cdot)$).

While the parameters $\{r_l\}$ and $\{\overline{r}_l\}$ are not necessary in the derivation of (79), they improve the exponent for a given set of auxiliary costs [10]. That is, the more general exponent of Theorem 5 serves as an indicator of the performance when the auxiliary costs are chosen suboptimally (e.g. due to the codebook designer having imperfect channel knowledge). Using a similar argument to that of (88)–(90), it is easily shown that $E_{\mathrm{ex}}^{\mathrm{cost}}$ never improves on $E_{\mathrm{ex}}^{\mathrm{cc}}$, and hence one cannot improve on the exponent obtained using $L=2$ optimally chosen auxiliary costs.

B. Derivation Using Distance Enumerators

In this subsection, we extend the type enumerator analysis of Section IV-B to channels with continuous alphabets. We assume that the technical condition of Theorem 2 is satisfied (see Appendix A for discussion), and make use of

[2] We could introduce $c(x)$ into the bound similarly, but there is no real loss of generality in omitting this inclusion, since one can always choose $a_l(\cdot) = c(\cdot)$ for some l. Under such a choice, the one-sided constraint on $c(\cdot)$ in (25) can be removed provided that $\mathbb{E}_Q[c(X)] < \Gamma$, though it must remain present in the case that $\mathbb{E}_Q[c(X)] = \Gamma$.

(16). For clarity of exposition, we present the key steps and ideas here, and give the remaining details in Appendix E. Unlike Section IV-B, we do not attempt to prove the exponential tightness of each step.

We fix $s \geq 0$ and define the Chernoff distance

$$d_s(x,\overline{x}) \triangleq -\log \int dy W(y|x) \bigg(\frac{q(\overline{x},y)}{q(x,y)} \bigg)^s \tag{91}$$

and its multi-letter extension

$$d_s^n(\boldsymbol{x},\overline{\boldsymbol{x}}) \triangleq \sum_{i=1}^n d_s(x_i,\overline{x}_i). \tag{92}$$

Applying the union bound and Markov's inequality to (16), we conclude that analogously to (57), there exists a codebook $\mathcal{C}$ of rate R such that

$$p_e(\mathcal{C}) \,\dot{\leq}\, \exp\Big(\mathbb{E}\big[\log A_n(R,\rho,\boldsymbol{X}^{(m)}) \big] \Big), \tag{93}$$

where

$$A_n(R,\rho,\boldsymbol{X}^{(m)}) \triangleq \mathbb{E}\Bigg[\bigg(\sum_{\overline{m} \neq m} e^{-d_s^n(\boldsymbol{X}^{(m)},\boldsymbol{X}^{(\overline{m})})} \bigg)^{1/\rho} \,\bigg|\, \boldsymbol{X}^{(m)} \Bigg]^\rho. \tag{94}$$

For a fixed transmitted codeword $\boldsymbol{X}^{(m)} = \boldsymbol{x}$, we analyze $A_n(R,\rho,\boldsymbol{x})$ using *distance enumerators*:

$$\sum_{\overline{m} \neq m} e^{-d_s^n(\boldsymbol{x},\boldsymbol{X}^{(\overline{m})})} \leq \sum_{k=0}^\infty e^{-nk\delta} N_m(k,\boldsymbol{x}), \tag{95}$$

where $\delta > 0$ is arbitrary, and

$$N_m(k,\boldsymbol{x}) \triangleq \sum_{\overline{m} \neq m} \mathbb{1}\big\{ nk\delta \leq d_s^n(\boldsymbol{x},\boldsymbol{X}^{(\overline{m})}) < n(k+1)\delta \big\}. \tag{96}$$

Using Markov's inequality, we can upper-bound the left-hand side of (13) by $e^{-d_s^n(\boldsymbol{x},\overline{\boldsymbol{x}})}$. It follows from the assumption of Theorem 2 that the highest value of k,

$$k_{\max}(n) \triangleq \max_{\boldsymbol{x}\,:\,P_{\boldsymbol{X}}(\boldsymbol{x})>0} \max\big\{ k \,:\, \mathbb{P}\big[N_m(k,\boldsymbol{x}) > 0\big] \neq 0 \big\}, \tag{97}$$

grows subexponentially in n for all $s \geq 0$. Thus, analogously to (66), the quantity $A_n(R,\rho,\boldsymbol{x})$ defined in (93) satisfies

$$A_n(R,\rho,\boldsymbol{x}) \,\dot{\leq}\, \max_{k \geq 0} \Big(\mathbb{E}\big[N_m(k,\boldsymbol{x})^{1/\rho} \big] \Big)^\rho e^{-nk\delta}. \tag{98}$$

We can further upper bound this expression by removing the lower inequality in the indicator function in (96). The key issue is now to assess the exponential rate of decay of the binary random variable

$$U_{\overline{m}}(\boldsymbol{x}) \triangleq \mathbb{1}\big\{ d_s^n(\boldsymbol{x},\boldsymbol{X}^{(\overline{m})}) < n(k+1)\delta \big\} \tag{99}$$

for a given transmitted codeword $\boldsymbol{x}$, i.e. to find the exponent of $F(D,\boldsymbol{x}) \triangleq \mathbb{P}\big[d_s^n(\boldsymbol{x},\overline{\boldsymbol{X}}) < D\big]$. This can be done using standard large deviations techniques such as the Chernoff bound. Letting $R(D,\boldsymbol{x})$ be any function such that $F(D,\boldsymbol{x}) \,\dot{\leq}\, e^{-nR(D,\boldsymbol{x})}$ uniformly in $\boldsymbol{x}$, we have similarly to (71) that

$$A_n(R,\rho,\boldsymbol{x}) \,\dot{\leq}\, e^{-n\min\{E_1(R,\rho,\delta,\boldsymbol{x}),E_2(R,\delta,\boldsymbol{x})\}}, \tag{100}$$

where

$$E_1(R,\rho,\delta,\boldsymbol{x}) \triangleq \min_{k\,:\,R((k+1)\delta,\boldsymbol{x}) \geq R} k\delta + \rho\big(R((k+1)\delta,\boldsymbol{x}) - R \big) \tag{101}$$

$$E_2(R,\delta,\boldsymbol{x}) \triangleq \min_{k\,:\,R((k+1)\delta,\boldsymbol{x}) \leq R} k\delta + R((k+1)\delta,\boldsymbol{x}) - R. \tag{102}$$

Upon taking the limit $\delta \to 0$, these become

$$E_1(R,\rho,\boldsymbol{x}) \triangleq \inf_{D\,:\,R(D,\boldsymbol{x})\geq R} D + \rho\big(R(D,\boldsymbol{x}) - R\big) \tag{103}$$

$$E_2(R,\boldsymbol{x}) \triangleq \inf_{D\,:\,R(D,\boldsymbol{x})\leq R} D + R(D,\boldsymbol{x}) - R. \tag{104}$$

Analogously to Section IV-B, the optimal choice of ρ is in the limit as $\rho \to \infty$, and we obtain $E_2 \leq E_1$, and hence

$$A_n(R,\rho,\boldsymbol{x}) \mathrel{\dot{\leq}} e^{-nE_2(R,\rho,\boldsymbol{x})}. \tag{105}$$

Substituting (105) into (93), we obtain

$$\liminf_{n\to\infty} -\frac{1}{n}\log p_e(\mathcal{C}) \geq \mathbb{E}\big[E_2(R,\rho,\boldsymbol{X})\big] \tag{106}$$

$$= \mathbb{E}\bigg[\inf_{D\,:\,R(D,\boldsymbol{X})\leq R} D + R(D,\boldsymbol{X}) - R\bigg]. \tag{107}$$

Thus far, we have not made use of the specific choice of $P_{\boldsymbol{X}}$, and hence (107) can be applied fairly generally. In fact, after a suitable modification of the definition of $d_s^n(\boldsymbol{x},\overline{\boldsymbol{x}})$, (107) extends immediately to more general channels and metrics (e.g. channels with memory). The ability to simplify the exponent (e.g. to a single-letter expression) depends on the form of $R(D,\boldsymbol{x})$, which in turn depends strongly on the codeword distribution $P_{\boldsymbol{X}}$. In some cases, $P_{\boldsymbol{X}}$ can be chosen in such a way that $R(D,\boldsymbol{x})$ is the same for all $\boldsymbol{x}$ with $P_{\boldsymbol{X}}(\boldsymbol{x}) > 0$, thus greatly simplifying (107).

In Appendix E, we give the remaining details for the cost-constrained ensemble with a single auxiliary cost $a_1(x) = a(x)$, and show that after optimizing $a(\cdot)$, (107) yields the exponent $E_{\mathrm{ex}}^{\mathrm{cc}}(Q,R)$ in (78). We only require one auxiliary cost $a(\cdot)$ to have a finite second moment, as opposed to $a_1(\cdot)$ and $a_2(\cdot)$ used in Section V-A. However, this comes at the price of requiring the assumption of Theorem 2 to hold true.

C. Comparison of Techniques

A notable difference between the above derivations is the method for ensuring that the average over x is outside the logarithm in (79), which is desirable due to Jensen's inequality. In Theorem 5, the expectation is in fact inside the logarithm, but the desired result is obtained by choosing $a_2(x)$ to make Jensen's inequality hold with equality. On the other hand, in Section V-B (and Appendix E) the expectation naturally arises outside the logarithm without the need for the second cost function.

Provided that the assumption of Theorem 2 is met, we can combine the two approaches and apply the techniques of Theorem 1 and Section V-A to (16), in which case $E_{\mathrm{x}}^{\mathrm{cost}}$ in (84) is improved to

$$E_{\mathrm{x}}^{\mathrm{cost}^*}(Q,R,\{a_l\}) \triangleq \sup_{s\geq 0,\{\overline{r}_l\}} -\rho\int dx Q(x)\log\int d\overline{x}Q(\overline{x})e^{\sum_{l=1}^{L}\overline{r}_l(a_l(\overline{x})-\phi_l)}\left(\int dy W(y|x)\left(\frac{q(\overline{x},y)}{q(x,y)}\right)^s\right)^{1/\rho}, \tag{108}$$

where the outer-most integral arises using Proposition 2. This exponent can also be derived by extending the analysis of Appendix E to include multiple auxiliary costs.

In the case that $L=0$ (i.e. i.i.d. coding), the above discussion is analogous to that of Section IV-C. In the absence of auxiliary costs, the exponent of Theorem 5 coincides with $E_{\mathrm{ex}}^{\mathrm{iid}}$ in (26), and the variation in (108) yields a (possibly strict) improvement due to Jensen's inequality. In the discrete memoryless setting, the former exponent is identical to

(75), whereas the latter exponent is equivalent to the improved version of (75) with the additional constraint $P_X = Q$. These equivalences are proved in a nearly identical fashion to Theorem 3.

Finally, while the analysis of Section V-A is very specific to the memoryless setting with a single-letter decoding metric, the analysis of Section V-B yields the expression in (107) which holds in much greater generality.

VI. Subexponential Prefactor

For any achievable error exponent $E(R)$, we have for some sequence of codebooks $\mathcal{C}_n$ of rate R that

$$p_e(\mathcal{C}_n) \le \alpha(n, R) \exp(-nE(R)), \tag{109}$$

where $\alpha(n, R)$ is a subexponential prefactor. In particular, the analysis of Gallager [2, Ch. 5] yields $\alpha(n, R) = O(1)$ for both the random-coding exponent and the expurgated exponent. Early works on improving the $O(1)$ term for non-expurgated random coding include those of Elias [27], Dobrushin [28] and Gallager [29]. These results were recently generalized by Altug and Wagner [20], [30], who obtained prefactors for the random-coding bound at all rates below capacity, as well as converse results above the critical rate. To our knowledge, no such improvement to Gallager's $O(1)$ prefactor for the expurgated exponent has been reported previously. In this section, we obtain a $O\big(\frac{1}{\sqrt{n}}\big)$ prefactor for the expurgated i.i.d. ensemble defined in (22). Throughout the section, we assume that the channel is a DMC with unconstrained inputs.

In [31], we have applied similar techniques in the setting of non-expurgated random coding in order to provide an alternative proof of [20, Thm. 1], as well as generalizing the result to the setting of mismatched decoding. The analysis of [20] can be considered a refinement of that of Fano [21], whereas our analysis can be considered a refinement of that of Gallager [2].

A. Technical Assumptions

We define the sets

$$\mathcal{Y}_1(x, \overline{x}) \triangleq \Big\{ y \,:\, W(y|x)W(y|\overline{x}) > 0 \Big\} \tag{110}$$

$$\mathcal{A}(Q) \triangleq \left\{ (x, \overline{x}) \,:\, Q(x)Q(\overline{x}) > 0,\, \frac{q(\overline{x}, y)}{q(x, y)} \ne \frac{q(\overline{x}, y')}{q(x, y')} \text{ for some } y, y' \in \mathcal{Y}_1(x, \overline{x}) \right\} \tag{111}$$

and make the following technical assumptions:

$$q(x, y) = 0 \iff W(y|x) = 0 \tag{112}$$

$$\mathcal{A}(Q) \ne \emptyset. \tag{113}$$

In the case of ML decoding, (112) is trivial, and (113) reduces to

$$W(y|x) \ne W(y|\overline{x}) \text{ for some } (x, \overline{x}, y) \text{ such that } Q(x)Q(\overline{x})W(y|x)W(y|\overline{x}) > 0, \tag{114}$$

which is the *feasibility decoding is suboptimal* assumption of [20, Def. 1]. A notable example of a channel which fails this condition is the binary erasure channel. In general, however, the assumptions in (112)–(113) are are fairly mild, and are satisfied for most channels, decoding metrics and input distributions.

B. Statement of the Result

Theorem 6. *Fix any DMC $W(y|x)$, decoding metric $q(x,y)$ and input distribution $Q(x)$ satisfying* (112)–(113)*. For all n and $R>0$, there exists a codebook $\mathcal{C}_n$ with $M \ge \exp(nR)$ codewords whose maximal error probability satisfies*

$$p_e(\mathcal{C}_n) \le \frac{K}{\sqrt{n}} \exp\big(-nE_{\rm ex}^{\rm iid}(Q,R)\big) \tag{115}$$

for sufficiently large n, where K is a constant depending only on W, q, Q and R.

Proof: We introduce a number of preliminary lemmas in Section VI-C, and prove the theorem in Section VI-D. ■

It is interesting to note that under ML coding and any rate where the expurgated exponent and random-coding exponent coincide, Theorem 6 gives the same prefactor growth rate as that of [29], which studies the random-coding error probability below the critical rate. Of course, Theorem 6 is primarily of interest at low rates, where the expurgated exponent exceeds the random-coding exponent.

C. Preliminary Lemmas

The key tool in our analysis is the following lemma by Polyanskiy, Poor and Verdú [3].

Lemma 2. [3, Lemma 47] *Let $Z_1,...,Z_n$ be independent random variables with $\sigma^2 \triangleq \sum_{i=1}^n \mathrm{Var}[Z_i] > 0$ and $T \triangleq \sum_{i=1}^n \mathbb{E}[|Z_i - \mathbb{E}[Z_i]|^3] < \infty$. Then for any real number t,*

$$\mathbb{E}\bigg[\exp\Big(-\sum_i Z_i\Big)\mathbb{1}\Big\{\sum_i Z_i > t\Big\}\bigg] \le 2\bigg(\frac{\log 2}{\sqrt{2\pi}} + \frac{12T}{\sigma^2}\bigg)\frac{1}{\sigma}\exp\big(-t\big). \tag{116}$$

In general, it is possible that the supremum over $s>0$ in (27) is only achieved in the limit as $s \to \infty$. The following lemma shows that the assumptions in (112)–(113) rule out this possibility.

Lemma 3. *For any $\rho \ge 1$ and (W,q,Q) satisfying* (112)–(113)*, the objective in* (27) *tends to $-\infty$ as $s \to \infty$.*

Proof: Let $(x,\overline{x})$ be an arbitrary pair in $\mathcal{A}(Q)$, the existence of which is asserted in (113). Of the pair (y,y') given in (111), at least one must satisfy $\frac{q(\overline{x},\cdot)}{q(x,\cdot)} \ne 1$; assume without loss of generality that this is $y \in \mathcal{Y}_1(x,\overline{x})$. In the case that $\frac{q(\overline{x},y)}{q(x,y)} > 1$, we upper bound the objective in (27) by

$$-\rho \log Q(x)Q(\overline{x})W(y|x)\bigg(\frac{q(\overline{x},y)}{q(x,y)}\bigg)^s \tag{117}$$

which tends to $-\infty$ as $s \to \infty$, since $W(y|x) > 0$ due to the fact that $y \in \mathcal{Y}_1(x,\overline{x})$. In the case that $\frac{q(\overline{x},y)}{q(x,y)} < 1$, a similar argument applies with the roles of x and $\overline{x}$ reversed. ■

The following lemma is somewhat more technical, and ensures the existence of a sufficiently high probability set in which Lemma 2 can be applied with a value of σ which has $\sqrt{n}$ growth. We define the quantities

$$V_s(y|x,\overline{x}) \triangleq \frac{W(y|x)\left(\frac{q(\overline{x},y)}{q(x,y)}\right)^s}{\sum_{y'} W(y'|x)\left(\frac{q(\overline{x},y')}{q(x,y')}\right)^s} \tag{118}$$

$$V_s^n(\boldsymbol{y}|\boldsymbol{x},\overline{\boldsymbol{x}}) \triangleq \prod_{i=1}^n V_s(y_i|x_i,\overline{x}_i) \tag{119}$$

$$j_s(x,\overline{x},y) \triangleq \log\frac{V_s(y|x,\overline{x})}{W(y|x)} \tag{120}$$

$$j_s^n(\boldsymbol{x},\overline{\boldsymbol{x}},\boldsymbol{y}) \triangleq \sum_{i=1}^n j_s(x_i,\overline{x}_i,y_i). \tag{121}$$

Furthermore, we let $\hat{P}_{\boldsymbol{x}\overline{\boldsymbol{x}}}(x,\overline{x})$ denote the joint empirical distribution (i.e. type) of $(\boldsymbol{x},\overline{\boldsymbol{x}})$.

Lemma 4. *For any $R>0$ and (W,q,Q) satisfying* (112)–(113)*, the sequence of sets*

$$\mathcal{F}_{\delta,n} \triangleq \Big\{(\boldsymbol{x},\overline{\boldsymbol{x}})\,:\,\sum_{(x,\overline{x})\in\mathcal{A}(Q)} \hat{P}_{\boldsymbol{x}\overline{\boldsymbol{x}}}(x,\overline{x}) > \delta\Big\} \tag{122}$$

satisfies the following properties:

1) *For any $\delta>0$ and $(\boldsymbol{x},\overline{\boldsymbol{x}})\in\mathcal{F}_{\delta,n}$, the random variable $\boldsymbol{Y}_s \sim V_s^n(\cdot|\boldsymbol{x},\overline{\boldsymbol{x}})$ satisfies*

$$\mathrm{Var}[j_s^n(\boldsymbol{x},\overline{\boldsymbol{x}},\boldsymbol{Y}_s)] \ge n\delta v_s, \tag{123}$$

where

$$v_s \triangleq \min_{(x,\overline{x})\in\mathcal{A}(Q)} \mathrm{Var}_{Y_s\sim V_s(\cdot|x,\overline{x})}[j_s(x,\overline{x},Y_s)]. \tag{124}$$

Furthermore, $v_s>0$ for all $s>0$.

2) *For any $\rho\ge 1$ and $s\ge 0$, there exists a choice of $\delta>0$ such that*

$$\sum_{(\boldsymbol{x},\overline{\boldsymbol{x}})\notin\mathcal{F}_{\delta,n}} P_{\boldsymbol{X}}(\boldsymbol{x})P_{\boldsymbol{X}}(\overline{\boldsymbol{x}})\bigg(\sum_{\boldsymbol{y}} W^n(\boldsymbol{y}|\boldsymbol{x})\bigg(\frac{q(\overline{\boldsymbol{x}},\boldsymbol{y})}{q(\boldsymbol{x},\boldsymbol{y})}\bigg)^s\bigg)^{1/\rho} \tag{125}$$

has a strictly larger exponential rate of decay than

$$\sum_{\boldsymbol{x},\overline{\boldsymbol{x}}} P_{\boldsymbol{X}}(\boldsymbol{x})P_{\boldsymbol{X}}(\overline{\boldsymbol{x}})\bigg(\sum_{\boldsymbol{y}} W^n(\boldsymbol{y}|\boldsymbol{x})\bigg(\frac{q(\overline{\boldsymbol{x}},\boldsymbol{y})}{q(\boldsymbol{x},\boldsymbol{y})}\bigg)^s\bigg)^{1/\rho}. \tag{126}$$

Proof: We obtain (123) by expanding the variance as

$$\mathrm{Var}[j_s^n(\boldsymbol{x},\overline{\boldsymbol{x}},\boldsymbol{Y}_s)] = \sum_{i=1}^n \mathrm{Var}[j_s(x_i,\overline{x}_i,Y_{s,i})] \tag{127}$$

$$\ge \sum_{(x,\overline{x})\in\mathcal{A}(Q)} n\hat{P}_{\boldsymbol{x}\overline{\boldsymbol{x}}}(x,\overline{x})\mathrm{Var}[j_s(x,\overline{x},Y_s)] \tag{128}$$

and substituting the bound in the definition of $\mathcal{F}_{\delta,n}$ in (122). To prove that $v_s>0$, we note that the variance of a random variable is zero if and only if the variable is deterministic, and hence under $Y_s\sim V_s(\cdot|x,\overline{x})$ we have

$$\mathrm{Var}[j_s(x,\overline{x},Y_s)]=0 \iff j_s(x,\overline{x},y) \text{ is independent of } y \text{ wherever } V_s(y|x,\overline{x})>0 \tag{129}$$

$$\iff \frac{q(\overline{x},y)}{q(x,y)} \text{ is independent of } y \text{ wherever } W(y|x)q(\overline{x},y)>0 \tag{130}$$

$$\iff (x,\overline{x})\notin\mathcal{A}(Q), \tag{131}$$

where (130) follows from the definitions of j_s and V_s, and (131) follows from the assumption in (112) and the definition of $\mathcal{A}(Q)$.

To prove the second property, we note that a nearly identical argument to Section IV-A (e.g. see (50)–(51)) yields that the exponent of (126) is equal to

$$\min_{P_{X\overline{X}}} D(P_{X\overline{X}} \| Q \times Q) + \frac{1}{\rho}\mathbb{E}_P[d_s(X,\overline{X})], \tag{132}$$

where d_s is defined in (33). Similarly, the exponent of (125) is given by

$$\min_{P_{X\overline{X}} \,:\, \sum_{(x,\overline{x})\in\mathcal{A}(Q)} P_{X\overline{X}}(x,\overline{x}) \le \delta} D(P_{X\overline{X}} \| Q \times Q) + \frac{1}{\rho}\mathbb{E}_P[d_s(X,\overline{X})]. \tag{133}$$

By a straightforward analysis of the Karush-Kuhn-Tucker (KKT) conditions [18, Sec. 5.5.3], we obtain that (132) is uniquely minimized by

$$P^*_{X\overline{X}}(x,\overline{x}) = \frac{Q(x)Q(\overline{x})\Big(\sum_y W(y|x)\Big(\frac{q(\overline{x},y)}{q(x,y)}\Big)^s\Big)^{1/\rho}}{\sum_{x',\overline{x}'} Q(x')Q(\overline{x}')\Big(\sum_{y'} W(y'|x')\Big(\frac{q(\overline{x}',y')}{q(x',y')}\Big)^s\Big)^{1/\rho}}. \tag{134}$$

From the assumptions in (112)–(113), we can find a pair $(x^*,\overline{x}^*) \in \mathcal{A}(Q)$ such that $P^*_{X\overline{X}}(x^*,\overline{x}^*) > 0$. By choosing $\delta < P^*_{X\overline{X}}(x^*,\overline{x}^*)$, we conclude that $P^*_{X\overline{X}}$ does not satisfy the constraint in (133), and thus (133) is strictly higher than (132). ■

D. *Proof of Theorem 6*

Due to the subtraction of ρR in (26), the case $\rho \to \infty$ is only relevant as $R \to 0$, or in the case that the exponent is infinity and the error probability is zero [2]. The former case is not considered in the theorem statement, and in the latter case the prefactor is irrelevant. We therefore assume that the supremum in (26) is achieved by a finite value of ρ. From Lemma 3, we can assume the same of s in (27). Throughout the proof, (ρ, s) are assumed to achieve these suprema at the given rate R.

Using the bound rcux_ρ in Theorem 1 with the i.i.d. codeword distribution in (22), we have

$$\frac{1}{M}\mathrm{rcux}_\rho(n,M)^{1/\rho} = \sum_{\boldsymbol{x},\overline{\boldsymbol{x}}} Q^n(\boldsymbol{x})Q^n(\overline{\boldsymbol{x}})\mathbb{P}\Big[q^n(\overline{\boldsymbol{x}},\boldsymbol{Y}) \ge q^n(\boldsymbol{x},\boldsymbol{Y})\Big]^{1/\rho} \tag{135}$$

$$= \sum_{(\boldsymbol{x},\overline{\boldsymbol{x}})\in\mathcal{F}_{\delta,n}} Q^n(\boldsymbol{x})Q^n(\overline{\boldsymbol{x}})\mathbb{P}\Big[q^n(\overline{\boldsymbol{x}},\boldsymbol{Y}) \ge q^n(\boldsymbol{x},\boldsymbol{Y})\Big]^{1/\rho}$$

$$+ \sum_{(\boldsymbol{x},\overline{\boldsymbol{x}})\notin\mathcal{F}_{\delta,n}} Q^n(\boldsymbol{x})Q^n(\overline{\boldsymbol{x}})\mathbb{P}\Big[q^n(\overline{\boldsymbol{x}},\boldsymbol{Y}) \ge q^n(\boldsymbol{x},\boldsymbol{Y})\Big]^{1/\rho}, \tag{136}$$

where $Q^n(\boldsymbol{x}) \overset{\triangle}{=} \prod_{i=1}^n Q(x_i)$, and each probability is implicitly conditioned on $\boldsymbol{X} = \boldsymbol{x}$. The constant δ is assumed to be chosen to be sufficiently small so that the second part of Lemma 4 holds under (ρ, s).

We first analyze the summation over $\mathcal{F}_{\delta,n}$ in (136). In order to make the inner probability more amenable to an application of Lemma 2, we write it as

$$\mathbb{P}\Big[q^n(\overline{\boldsymbol{x}},\boldsymbol{Y}) \ge q^n(\boldsymbol{x},\boldsymbol{Y})\Big] = \mathbb{P}\bigg[\bigg(\frac{q^n(\overline{\boldsymbol{x}},\boldsymbol{Y})}{q^n(\boldsymbol{x},\boldsymbol{Y})}\bigg)^s \ge 1\bigg] \tag{137}$$

$$= \mathbb{P}\left[\frac{\Big(\frac{q^n(\overline{\boldsymbol{x}},\boldsymbol{Y})}{q^n(\boldsymbol{x},\boldsymbol{Y})}\Big)^s}{\sum_{\boldsymbol{y}} W^n(\boldsymbol{y}|\boldsymbol{x})\Big(\frac{q^n(\overline{\boldsymbol{x}},\boldsymbol{y})}{q^n(\boldsymbol{x},\boldsymbol{y})}\Big)^s} \ge \frac{1}{\sum_{\boldsymbol{y}} W^n(\boldsymbol{y}|\boldsymbol{x})\Big(\frac{q^n(\overline{\boldsymbol{x}},\boldsymbol{y})}{q^n(\boldsymbol{x},\boldsymbol{y})}\Big)^s}\right] \tag{138}$$

$$= \mathbb{P}\left[j_s^n(\boldsymbol{x},\overline{\boldsymbol{x}},\boldsymbol{Y}) \ge -\log\sum_{\boldsymbol{y}} W^n(\boldsymbol{y}|\boldsymbol{x})\bigg(\frac{q(\overline{\boldsymbol{x}},\boldsymbol{y})}{q(\boldsymbol{x},\boldsymbol{y})}\bigg)^s\right], \tag{139}$$

where j_s^n is defined in (121). Next, following [32, Sec. 3.4.5], we write

$$W^n(\boldsymbol{y}|\boldsymbol{x}) = W^n(\boldsymbol{y}|\boldsymbol{x})\frac{V_s^n(\boldsymbol{y}|\boldsymbol{x},\overline{\boldsymbol{x}})}{V_s^n(\boldsymbol{y}|\boldsymbol{x},\overline{\boldsymbol{x}})} \tag{140}$$

$$= V_s^n(\boldsymbol{y}|\boldsymbol{x},\overline{\boldsymbol{x}})\exp\big(-nj_s(\boldsymbol{x},\overline{\boldsymbol{x}},\boldsymbol{y})\big). \tag{141}$$

Summing (141) over all $\boldsymbol{y}$ such that $j_s(\boldsymbol{x},\overline{\boldsymbol{x}},\boldsymbol{y}) \ge t$, we obtain

$$\mathbb{P}\big[j_s^n(\boldsymbol{x},\overline{\boldsymbol{x}},\boldsymbol{Y}) \ge t\big] = \mathbb{E}\Big[\exp\big(-nj_s^n(\boldsymbol{x},\overline{\boldsymbol{x}},\boldsymbol{Y}_s)\big)\mathbb{1}\big\{j_s^n(\boldsymbol{x},\overline{\boldsymbol{x}},\boldsymbol{Y}_s) \ge t\big\}\Big], \tag{142}$$

where $\boldsymbol{Y}_s \sim V_s^n(\cdot|\boldsymbol{x},\overline{\boldsymbol{x}})$. For any $(\boldsymbol{x},\overline{\boldsymbol{x}}) \in \mathcal{F}_{\delta,n}$, Lemma 2 and the first part of Lemma 4 thus imply

$$\mathbb{P}\big[j_s^n(\boldsymbol{x},\overline{\boldsymbol{x}},\boldsymbol{Y}) \ge t\big] \le \frac{K_1}{\sqrt{n}}e^{-t} \tag{143}$$

for some constant K_1. Substituting (143) into (139), we obtain

$$\mathbb{P}\Big[q^n(\overline{\boldsymbol{x}},\boldsymbol{Y}) \ge q^n(\boldsymbol{x},\boldsymbol{Y})\Big] \le \frac{K_1}{\sqrt{n}}\sum_{\boldsymbol{y}} W^n(\boldsymbol{y}|\boldsymbol{x})\bigg(\frac{q(\overline{\boldsymbol{x}},\boldsymbol{y})}{q(\boldsymbol{x},\boldsymbol{y})}\bigg)^s, \tag{144}$$

and hence

$$\sum_{(\boldsymbol{x},\overline{\boldsymbol{x}})\in\mathcal{F}_{\delta,n}} Q^n(\boldsymbol{x})Q^n(\overline{\boldsymbol{x}})\mathbb{P}\Big[q^n(\overline{\boldsymbol{x}},\boldsymbol{Y}) \ge q^n(\boldsymbol{x},\boldsymbol{Y})\Big]^{1/\rho}$$
$$\le \sum_{\boldsymbol{x},\overline{\boldsymbol{x}}} Q^n(\boldsymbol{x})Q^n(\overline{\boldsymbol{x}})\bigg(\frac{K_1}{\sqrt{n}}\sum_{\boldsymbol{y}} W^n(\boldsymbol{y}|\boldsymbol{x})\bigg(\frac{q(\overline{\boldsymbol{x}},\boldsymbol{y})}{q(\boldsymbol{x},\boldsymbol{y})}\bigg)^s\bigg)^{1/\rho}. \tag{145}$$

We observe that the right-hand side of (145) has the same exponent as (126). Using Markov's inequality, the summation over $\mathcal{F}_{\delta,n}^c$ in (136) can be upper bounded by (125), and hence the second part of Lemma 4 implies

$$\frac{1}{M}\mathrm{rcux}_{\rho,s}(n,M)^{1/\rho} \le \big(1+o(1)\big)\sum_{\boldsymbol{x},\overline{\boldsymbol{x}}} Q^n(\boldsymbol{x})Q^n(\overline{\boldsymbol{x}})\bigg(\frac{K_1}{\sqrt{n}}\sum_{\boldsymbol{y}} W^n(\boldsymbol{y}|\boldsymbol{x})\bigg(\frac{q(\overline{\boldsymbol{x}},\boldsymbol{y})}{q(\boldsymbol{x},\boldsymbol{y})}\bigg)^s\bigg)^{1/\rho}, \tag{146}$$

and hence

$$\mathrm{rcux}_{\rho,s}(n,M) \le \frac{K_1\big(1+o(1)\big)}{\sqrt{n}}M^\rho\left(\sum_{\boldsymbol{x},\overline{\boldsymbol{x}}} Q^n(\boldsymbol{x})Q^n(\overline{\boldsymbol{x}})\bigg(\sum_{\boldsymbol{y}} W^n(\boldsymbol{y}|\boldsymbol{x})\bigg(\frac{q(\overline{\boldsymbol{x}},\boldsymbol{y})}{q(\boldsymbol{x},\boldsymbol{y})}\bigg)^s\bigg)^{1/\rho}\right)^\rho \tag{147}$$

$$= \frac{K_1\big(1+o(1)\big)}{\sqrt{n}}\exp\big(-nE_{\mathrm{ex}}^{\mathrm{iid}}(Q,R)\big), \tag{148}$$

where (148) follows by expanding each term as a product from 1 to n and using the assumption that ρ and s achieve the exponent $E_{\mathrm{ex}}^{\mathrm{iid}}$ at rate R. This concludes the proof.

VII. Discussion and Conclusion

We have presented several asymptotic and non-asymptotic expurgated bounds for channels with a given decoding rule. Derivations have been given for both the exponent of Csiszár and Körner [6] and its generalization to continuous alphabets. The type class enumerator approach has been shown to provide better exponents for some codeword distributions, better guarantees of exponential tightness, and the opportunity for deriving expurgated exponents for channels with memory.

The $O\big(\frac{1}{\sqrt{n}}\big)$ prefactor to the exponent for i.i.d. coding is perhaps most meaningful for ML decoding with an optimal input distribution, since otherwise one would expect to improve the exponent via constant-composition coding or cost-constrained coding. Obtaining improved prefactors for these ensembles appears to be a more difficult task, since their proofs generally involve a change of measure to the i.i.d. distribution, thus introducing a polynomial prefactor (e.g. $(n+1)^{|\mathcal{X}|-1}$ for the constant-composition ensemble).

Connections with Statistical Mechanics

It is instructive to look at the analysis of Sections IV-B and V-B from the statistical-mechanical perspective. Let us take another look at the expression

$$Z(\boldsymbol{x}) = \sum_{\overline{m}\neq m} e^{-d(\boldsymbol{x},\boldsymbol{X}^{(\overline{m})})}, \tag{149}$$

where d can represent either d_q in (56) or d_s^n in (74) (see also (92)). From the viewpoint of statistical physics, Z can be interpreted as the partition function of a physical system, where for a fixed $\boldsymbol{x}^{(m)} = \boldsymbol{x}$, the various configurations (microstates) are $\{\boldsymbol{x}^{(\overline{m})}\}_{\overline{m}\neq m}$ and the energy function (Hamiltonian) is given by $d(\boldsymbol{x},\overline{\boldsymbol{x}})$. The various "configurational energies" $\{d(\boldsymbol{x},\boldsymbol{X}^{(\overline{m})})\}$ are independent random variables, since the codewords are generated independently. As explained in [33, Ch. 5-6] (see also [13, Ch. 6-7] and references therein), this setting is analogous to the random energy model (REM) in the literature of statistical physics of magnetic materials. The REM was invented by Derrida [34]–[36], as a model of extremely disordered spin glasses. This model is exactly solvable and exhibits a phase transition: Below a certain critical temperature, the partition function becomes dominated by a subexponential number of configurations in the ground-state energy, which means that the system freezes and its entropy vanishes in the thermodynamic limit. This combination of freezing and disorder resembles the behavior of a glass, so this low temperature phase of zero entropy is called the *glassy phase*. Above the critical temperature, the partition function is dominated by an exponential number of configurations, so its entropy is positive. This high temperature phase is called the *paramagnetic phase.*

In the case that $d(\cdot,\cdot)$ represents the Chernoff distance d_s^n, we can link these phases to the exponent $E_{\rm ex}^{\rm cc}$ in the form given in (39). The graph of $E_{\rm ex}^{\rm cc}(Q,R,s)$ is curved at rates below R_s (see (36)), and is a straight line at rates above R_s. The curved part corresponds to the glassy phase of the REM associated with (149), because the dominant contribution to $\mathbb{E}[Z^{1/\rho}]$ (see (149)) is due to a subexponential number of codewords whose "distance" from $\boldsymbol{x}$ (i.e. their "energy") is roughly $nD_s(Q,R)$. The straight-line part, on the other hand, corresponds to the paramagnetic phase, where roughly $e^{n(R-R_s)}$ incorrect codewords at distance $nD_s(Q,R_s)$ dominate the behavior. Thus, the passage between the curved part and the straight-line part at $R=R_s$ can be interpreted as a glassy phase transition. A similar discussion applies for the multi-letter distance d_q used in Section IV-B, with $D_s(Q,R)$ replaced by

$$D_q(Q,R) \triangleq \min_{\widetilde{P}_{X\overline{X}} \in \mathcal{S}^{\mathrm{cc}}(Q) \,:\, I_{\widetilde{P}}(X;\overline{X}) \le R} D_q(\widetilde{P}_{X\overline{X}}), \tag{150}$$

where $D_q(\widetilde{P}_{X\overline{X}})$ is defined in (70).

Appendix

A. Technical Condition of Theorem 2

We begin by providing an example of a class of continuous channels and metrics satisfying the single-letter condition given in (19). Consider an additive noise channel $Y = X+Z$, and let $q(x,y)$ be any decreasing function of $|y-x|$.[3] If the cost constraint is of the form $c(x) = |x|^\beta$ for some constant β, then $c(x) \le \gamma$ if and only if $|x| \le \gamma^{1/\beta}$. Thus, any two permissible points are separated by a distance of at least $2\gamma^{1/\beta}$, and the single-letter condition is satisfied if the additive noise satisfies $\mathbb{P}[Z > 2\gamma^{1/\beta}] \ge e^{-E'(\gamma)}$ and $\mathbb{P}[Z < -2\gamma^{1/\beta}] \ge e^{-E'(\gamma)}$ for some $E'(\gamma)$ growing subexponentially in γ. In particular, this holds for additive noise distributions with exponential tails, such as the Gaussian distribution. On the other hand, if the cost function is logarithmic, say $c(x) = \log(1+|x|)$, then (19) fails for additive noise distributions with exponential tails, since in this case the limit on the left-hand side of (19) equals a positive constant.

For any DMC whose zero-error capacity [23] is zero, the condition of Theorem 2 is satisfied under ML decoding, since the error probability can only decay exponentially [37]. On the other hand, the condition could fail for sufficiently "bad" metrics (e.g. one for which there exists a pair $(x,\overline{x})$ such that $q(x,y) > q(\overline{x},y)$ for all y). Furthermore, the condition fails under ML decoding whenever the zero-error capacity is positive and Q has a support which includes two inputs not sharing a common output.

Finally, we remark that even if the above single-letter condition fails, we can still choose $P_{\boldsymbol{X}}$ to ensure that the multi-letter condition of Theorem 2 is satisfied. For example, this can be done using the notion of auxiliary costs introduced in Section II.

B. Proof of Theorem 3

We write (28) as

$$\hat{E}^{\mathrm{cc}}_{\mathrm{ex}}(Q,R) = \min_{\substack{\widetilde{P}_{X\overline{X}} \in \mathcal{S}^{\mathrm{cc}}(Q) \\ I_{\widetilde{P}}(X;\overline{X}) \le R}} \min_{P_{X\overline{X}Y} \in \mathcal{T}^{\mathrm{cc}}(\widetilde{P}_{X\overline{X}})} D(P_{X\overline{X}Y} \| \widetilde{P}_{X\overline{X}} \times W) + I_{\widetilde{P}}(X;\overline{X}) - R, \tag{151}$$

where the objective follows from (30). We will study (151) one minimization at a time.

Step 1: For a given $\widetilde{P}_{X\overline{X}} \in \mathcal{S}^{\mathrm{cc}}(Q)$, the quantity $I_{\widetilde{P}}(X;\overline{X}) - R$ is constant, and hence we consider the optimization problem

$$\min_{P_{X\overline{X}Y} \in \mathcal{T}^{\mathrm{cc}}(\widetilde{P}_{X\overline{X}})} D(P_{X\overline{X}Y} \| \widetilde{P}_{X\overline{X}} \times W). \tag{152}$$

[3] Not all such metrics are equivalent, e.g. minimizing $\prod_{i=1}^n |y_i - x_i|$ may give significantly different behavior to minimizing $\prod_{i=1}^n e^{(y_i - x_i)^2}$.

The Lagrangian [18, Sec. 5.1.1] is given by

$$L_1 = \sum_{x,\overline{x},y} P_{X\overline{X}Y}(x,\overline{x},y)\log\frac{P_{X\overline{X}Y}(x,\overline{x},y)}{\widetilde{P}_{X\overline{X}}(x,\overline{x})W(y|x)} \\ + s\bigg(\sum_{x,y} P_{XY}(x,y)\log q(x,y) - \sum_{\overline{x},y} P_{\overline{X}Y}(\overline{x},y)\log q(\overline{x},y)\bigg) + \sum_{x,\overline{x}}\mu(x,\overline{x})\Big(\widetilde{P}_{X\overline{X}}(x,\overline{x}) - P_{X\overline{X}}(x,\overline{x})\Big), \quad (153)$$

where $s \geq 0$ and $\mu(\cdot,\cdot)$ are Lagrange multipliers. The optimization problem is convex with affine constraints, and thus the optimal value is equal to L_1 for some choice of $P_{X\overline{X}Y}$ and the Lagrange multipliers satisfying the Karush-Kuhn-Tucker (KKT) conditions [18, Sec. 5.5.3].

The simplification of (153) using the KKT conditions is similar to [10, Appendix B], so we omit the details. Setting $\frac{\partial L_1}{\partial P_{X\overline{X}Y}(x,\overline{x},y)} = 0$, using the constraint $P_{X\overline{X}} = \widetilde{P}_{X\overline{X}}$ to solve for $\mu(\cdot,\cdot)$, and substituting the resulting expressions back into (153), we obtain

$$L_1 = -\sum_{x,\overline{x}}\widetilde{P}_{X\overline{X}}(x,\overline{x})\log\sum_y W(y|x)\bigg(\frac{q(\overline{x},y)}{q(x,y)}\bigg)^s. \quad (154)$$

Renaming $\widetilde{P}_{X\overline{X}}$ as $P_{X\overline{X}}$, taking the supremum over $s \geq 0$, and adding $I_P(X;\overline{X}) - R$ (see (151)–(152)), we obtain the right-hand side of (31) with the minimum and supremum in the opposite order. Using Fan's minimax theorem [26], we can safely interchange the two.

Since we have taken the supremum over $s \geq 0$ rather than choosing it to satisfy the KKT conditions, we have only proved that (31) holds with the equality replaced by an inequality ($\leq$). To prove that the opposite inequality holds, we make use of the log-sum inequality [22, Thm. 2.7.1] similarly to [7, Appendix A]. We have for any $P_{X\overline{X}Y} \in \mathcal{T}^{\mathrm{cc}}(\widetilde{P}_{X\overline{X}})$ and $s \geq 0$ that

$$D(P_{X\overline{X}Y}\|\widetilde{P}_{X\overline{X}}\times W) \geq D(P_{X\overline{X}Y}\|\widetilde{P}_{X\overline{X}}\times W) - s\sum_{x,\overline{x},y}P_{X\overline{X}Y}(x,\overline{x},y)\log\frac{q(\overline{x},y)}{q(x,y)} \quad (155)$$

$$= \sum_{x,\overline{x},y}P_{X\overline{X}Y}(x,\overline{x},y)\log\frac{P_{X\overline{X}Y}(x,\overline{x},y)}{\widetilde{P}_{X\overline{X}}(x,\overline{x})W(y|x)\Big(\frac{q(\overline{x},y)}{q(x,y)}\Big)^s} \quad (156)$$

$$\geq \sum_{x,\overline{x}}P_{X\overline{X}}(x,\overline{x})\log\frac{1}{\sum_y W(y|x)\Big(\frac{q(\overline{x},y)}{q(x,y)}\Big)^s}, \quad (157)$$

where (155) follows from the constraint $\mathbb{E}_P[\log q(\overline{X},Y)] \geq \mathbb{E}_P[\log q(X,Y)]$ in (29), (156) follows from the definition of divergence, and (157) follows using the log-sum inequality [22, Thm. 2.7.1] and the constraint $P_{X\overline{X}} = \widetilde{P}_{X\overline{X}}$. Equation (157) coincides with (154), thus completing the proof of (31).

Step 2: We now turn to the proof of (32). For any fixed $s \geq 0$, the Lagrangian corresponding to (31) is given by

$$L_2 = -\sum_{x,\overline{x}}P_{X\overline{X}}(x,\overline{x})\log\sum_y W(y|x)\bigg(\frac{q(\overline{x},y)}{q(x,y)}\bigg)^s + (1+\lambda)\sum_{x,\overline{x}}P_{X\overline{X}}(x,\overline{x})\log\frac{P_{X\overline{X}}(x,\overline{x})}{Q(x)Q(\overline{x})} - (1+\lambda)R \\ + \sum_x \nu_1(x)\Big(Q(x) - P_X(x)\Big) + \sum_{\overline{x}}\nu_2(\overline{x})\Big(Q(\overline{x}) - P_{\overline{X}}(\overline{x})\Big), \quad (158)$$

where $\lambda \geq 0$, $\nu_1(\cdot)$ and $\nu_2(\cdot)$ are Lagrange multipliers. Setting $\frac{\partial L_2}{\partial P_{X\overline{X}}(x,\overline{x})} = 0$, using the constraint $P_X = Q$ to solve for $\nu_1(\cdot)$, and substituting the resulting expressions back into (158), we obtain

$$L_2 = -(1+\lambda)\sum_x Q(x)\log\sum_{\overline{x}}Q(\overline{x})\Bigg(\sum_y W(y|x)\bigg(\frac{q(\overline{x},y)}{q(x,y)}\bigg)^s\Bigg)^{\frac{1}{1+\lambda}}e^{\frac{1}{1+\lambda}(\nu_2(\overline{x})-\nu_2(x))} - (1+\lambda)R. \quad (159)$$

Taking the supremum over all $\nu_2(\cdot)$, $s \geq 0$ and $\lambda \geq 0$, we obtain the right-hand side of (32) after suitable renaming.

Once again, we have only proved that (32) holds with an inequality ($\leq$) in place of the equality, and we obtain a matching lower bound similarly to (155)–(157). For any $\rho \geq 1$ and $P_{X\overline{X}} \in \mathcal{S}^{\mathrm{cc}}(Q)$ with $I_{\widetilde{P}}(X;\overline{X}) \leq R$, we can lower bound the objective in (31) as follows:

$$
\begin{aligned}
-\sum_{x,\overline{x}} & P_{X\overline{X}}(x,\overline{x}) \log \sum_y W(y|x)\left(\frac{q(\overline{x},y)}{q(x,y)}\right)^s + I_P(X;\overline{X}) - R \\
&\geq -\sum_{x,\overline{x}} P_{X\overline{X}}(x,\overline{x}) \log \sum_y W(y|x)\left(\frac{q(\overline{x},y)}{q(x,y)}\right)^s + \rho\big(I_P(X;\overline{X}) - R\big) && (160) \\
&= -\rho \sum_{x,\overline{x}} P_{X\overline{X}}(x,\overline{x}) \log \frac{Q(x)Q(\overline{x})\bigg(\sum_y W(y|x)\Big(\frac{q(\overline{x},y)}{q(x,y)}\Big)^s\bigg)^{1/\rho}}{P_{X\overline{X}}(x,\overline{x})} - \rho R && (161) \\
&= -\rho \sum_{x,\overline{x}} P_{X\overline{X}}(x,\overline{x}) \log \frac{Q(x)Q(\overline{x})\bigg(\sum_y W(y|x)\Big(\frac{q(\overline{x},y)}{q(x,y)}\Big)^s\bigg)^{1/\rho} e^{a(\overline{x})-\phi_a}}{P_{X\overline{X}}(x,\overline{x})} - \rho R && (162) \\
&\geq -\rho \sum_x Q(x) \log \sum_{\overline{x}} Q(\overline{x}) \bigg(\sum_y W(y|x)\Big(\frac{q(\overline{x},y)}{q(x,y)}\Big)^s\bigg)^{1/\rho} e^{a(\overline{x})-\phi_a} - \rho R, && (163) \\
&= -\rho \sum_x Q(x) \log \sum_{\overline{x}} Q(\overline{x}) \bigg(\sum_y W(y|x)\Big(\frac{q(\overline{x},y)}{q(x,y)}\Big)^s\bigg)^{1/\rho} \frac{e^{a(\overline{x})}}{e^{a(x)}} - \rho R, && (164)
\end{aligned}
$$

where (160) follows from the constraint $I_{\widetilde{P}}(X;\overline{X}) \leq R$, (161) follows from the definition of mutual information and simple manipulations, (162) holds for any function $a(x)$ with mean $\phi_a = \mathbb{E}_Q[a(X)]$ by expanding the logarithm, (163) follows from the log-sum inequality [22, Thm. 2.7.1], and (164) follows by again expanding the logarithm and using the definition of ϕ_a. We thus have a matching lower bound to (159), and the proof is complete.

C. Proof of Theorem 4

Let $E_{\mathrm{x}}^{\mathrm{iid}}(Q,\rho,s)$ be the function $E_{\mathrm{x}}^{\mathrm{iid}}$ in (27), with a fixed value of s rather than a supremum. We claim that

$$
\lim_{R\to 0^+} \sup_{\rho\geq 1, s\geq 0} E_{\mathrm{x}}^{\mathrm{iid}}(Q,\rho,s) - \rho R = \sup_{\rho\geq 1, s\geq 0} E_{\mathrm{x}}^{\mathrm{iid}}(Q,\rho,s). \tag{165}
$$

It is easily seen that the left-hand side of (165) cannot exceed the right-hand side, since ρR is positive for any sequence of R values approaching zero from above. It remains to prove the converse. We have for all R that

$$
\sup_{\rho\geq 1, s\geq 0} E_{\mathrm{x}}^{\mathrm{iid}}(Q,\rho,s) - \rho R \geq E_{\mathrm{x}}^{\mathrm{iid}}(Q,\rho,s) - \rho R. \tag{166}
$$

Taking $R \to 0$ and then taking the supremum over $s \geq 0$ and $\rho \geq 1$ yields

$$
\lim_{R\to 0} \sup_{\rho\geq 1, s\geq 0} E_{\mathrm{x}}^{\mathrm{iid}}(Q,\rho,s) - \rho R \geq \sup_{\rho\geq 1, s\geq 0} E_{\mathrm{x}}^{\mathrm{iid}}(Q,\rho,s), \tag{167}
$$

which proves (165). Using an identical argument, we have

$$
\lim_{R\to 0^+} \sup_{\rho\geq 1, s\geq 0, a_1(\cdot), a_2(\cdot)} E_{\mathrm{x}}^{\mathrm{cost}}(Q,\rho,s,a_1,a_2) - \rho R = \sup_{\rho\geq 1, s\geq 0, a_1(\cdot), a_2(\cdot)} E_{\mathrm{x}}^{\mathrm{cost}}(Q,\rho,s,a_1,a_2), \tag{168}
$$

where $E_{\mathrm{x}}^{\mathrm{cost}}(Q,\rho,s,a_1,a_2)$ denotes the right-hand side of (88) with fixed values of s, $a_1(\cdot)$ and $a_2(\cdot)$ in place of the supremum.

From (32), (168) and the identity $\sup_{s,a_1(\cdot),a_2(\cdot)} E_{\mathrm{x}}^{\mathrm{cost}}(Q,\rho,s,a_1,a_2) = E_{\mathrm{x}}^{\mathrm{cc}}(Q,\rho)$ (see Section V-A), we have

$$\lim_{R\to 0^+} E_{\mathrm{ex}}^{\mathrm{cc}}(Q,R) = \sup_{\rho\ge 1, s\ge 0, a_1(\cdot),a_2(\cdot)} -\rho\log\sum_{x,\overline{x}} Q(x)Q(\overline{x})\frac{e^{a_1(\overline{x})-\phi_1}}{e^{a_2(x)-\phi_2}}\left(\sum_y W(y|x)\left(\frac{q(\overline{x},y)}{q(x,y)}\right)^s\right)^{\frac{1}{\rho}} \tag{169}$$

$$= \sup_{\rho\ge 1, s\ge 0, a_1'(\cdot),a_2'(\cdot)} -\rho\log\sum_{x,\overline{x}} Q(x)Q(\overline{x})\left(\frac{e^{a_1'(\overline{x})-\phi_1'}}{e^{a_2'(x)-\phi_2'}}\sum_y W(y|x)\left(\frac{q(\overline{x},y)}{q(x,y)}\right)^s\right)^{\frac{1}{\rho}}, \tag{170}$$

where (170) is obtained by letting $a_l'(\cdot) = a_l(\cdot)\rho$ for $l = 1,2$. Similarly to [2, Appendix 5B], we can show that the objective of (170) is a non-decreasing concave function of $\rho > 0$ for any fixed s, $a_1'(\cdot)$ and $a_2'(\cdot)$. Hence, the supremum over $\rho \ge 1$ is achieved as $\rho \to \infty$. The assumption on Q in the theorem statement ensures that the error probability is non-zero, and that the resulting limit is finite. Evaluating the limit using L'Hôpital's rule, we have

$$\lim_{R\to 0^+}\sup_{L,\{a_l\}} E_{\mathrm{ex}}^{\mathrm{cost}}(Q,R,\{a_l\}) = \sup_{s\ge 0, a_1'(\cdot),a_2'(\cdot)} -\sum_{x,\overline{x}} Q(x)Q(\overline{x})\log\left(\frac{e^{a_1'(\overline{x})-\phi_1'}}{e^{a_2'(x)-\phi_2'}}\sum_y W(y|x)\left(\frac{q(\overline{x},y)}{q(x,y)}\right)^s\right) \tag{171}$$

$$= \sup_{s\ge 0} -\sum_{x,\overline{x}} Q(x)Q(\overline{x})\log\sum_y W(y|x)\left(\frac{q(\overline{x},y)}{q(x,y)}\right)^s. \tag{172}$$

From the last step, we see that the functions $a_1'(\cdot)$ and $a_2'(\cdot)$ do not affect the exponent as $R \to 0$, and thus the same expression is obtained for $\lim_{R\to 0^+} E_{\mathrm{ex}}^{\mathrm{iid}}(Q,R)$.

D. Proof of Proposition 2

We first present the proof in the case that there is $L = 1$ auxiliary cost $a(\cdot)$ (with mean ϕ_a) and no system cost constraint, and then discuss the changes required to handle the general case. Throughout the proof, we define $a^n(\boldsymbol{x}) \triangleq \sum_{i=1}^n a(x_i)$ and $f^n(\boldsymbol{x}) \triangleq \sum_{i=1}^n f(x_i)$.

Let $\boldsymbol{X}$ be the random cost-constrained codeword, and let $\boldsymbol{X}'$ be an i.i.d. codeword with distribution $Q^n(\boldsymbol{x}')$. From (24), we have

$$\mathbb{E}\big[f^n(\boldsymbol{X})\big] = \frac{1}{\mu_n}\mathbb{E}\Big[f^n(\boldsymbol{X}')\mathbb{1}\big\{|a^n(\boldsymbol{X}') - n\phi_a| \le \delta\big\}\Big]. \tag{173}$$

By a direct differentiation, this is equal to $\frac{d}{d\lambda}\big(\frac{1}{n}\log Z(\lambda)\big)$ evaluated at $\lambda = 0$, where

$$Z(\lambda) \triangleq \mathbb{E}\Big[e^{\lambda f^n(\boldsymbol{X}')}\mathbb{1}\big\{|a^n(\boldsymbol{X}') - n\phi_a| \le \delta\big\}\Big]. \tag{174}$$

Expanding the expectation and using the inverse Laplace transform relation

$$\mathbb{1}\{z \ge 0\} = \frac{1}{2\pi j}\int_{u-j\infty}^{u+j\infty} dt\frac{e^{tz}}{t} \tag{175}$$

for $u > 0$, we have the following:

$$Z(\lambda) = \int d\boldsymbol{x}'Q^n(\boldsymbol{x}')e^{\lambda f^n(\boldsymbol{x}')}\Big(\mathbb{1}\{a^n(\boldsymbol{x}') \le n\phi_a + \delta\} - \mathbb{1}\{a^n(\boldsymbol{x}') \le n\phi_a - \delta\}\Big) \tag{176}$$

$$= \frac{1}{2\pi j}\int d\boldsymbol{x}'Q^n(\boldsymbol{x}')e^{\lambda f^n(\boldsymbol{x}')}\int_{u-j\infty}^{u+j\infty} dt\, e^{t(n\phi_a - a^n(\boldsymbol{x}'))}\frac{e^{t\delta} - e^{-t\delta}}{t} \tag{177}$$

$$= \frac{1}{2\pi j}\int_{u-j\infty}^{u+j\infty} dt\frac{e^{t\delta} - e^{-t\delta}}{t}e^{n\phi_a t}\bigg(\int dx'Q(x')e^{-ta(x')+\lambda f(x')}\bigg)^n. \tag{178}$$

Denoting the derivative of $Z(\cdot)$ by $Z'(\cdot)$, we have

$$Z'(0) = \frac{n}{2\pi j}\int_{u-j\infty}^{u+j\infty} dt \frac{e^{t\delta}-e^{-t\delta}}{t} e^{n\phi_a t}\bigg(\int dx' Q(x') e^{-ta(x')}\bigg)^{n-1} \int dx' Q(x') f(x') e^{-ta(x')} \tag{179}$$

$$= \frac{n}{2\pi j}\int_{u-j\infty}^{u+j\infty} dt \frac{e^{t\delta}-e^{-t\delta}}{t} e^{n\phi_a t}\bigg(\int dx' Q(x') e^{-ta(x')}\bigg)^{n} \frac{\int dx' Q(x') f(x') e^{-ta(x')}}{\int dx' Q(x') e^{-ta(x')}}. \tag{180}$$

Finally, using the assumption that $\mathbb{E}_Q[a(X)^2] < \infty$ and applying the saddlepoint method [38, Ch. 4-5] (see also [13, Sec. 4.2-4.3]), we obtain

$$\frac{d}{d\lambda}\Big(\frac{1}{n}\log Z(\lambda)\Big)\Big|_{\lambda=0} = \frac{Z'(0)}{Z(0)} \to \frac{\int dx' Q(x') f(x') e^{-t_0 a(x')}}{\int dx' Q(x') e^{-t_0 a(x')}}, \tag{181}$$

where t_0 is the zero of the derivative (saddlepoint) of the function $h(t) = \phi_a t + \log \mathbb{E}_Q[e^{-ta(X)}]$. Since $\phi_a = \mathbb{E}_Q[a(X)]$ by definition, it is easily verified that $t_0 = 0$, and thus the right-hand side of (181) equals $\mathbb{E}_Q[f(X)]$, as desired.

In the case of multiple auxiliary costs, the argument is similar, but with $ta(\cdot)$ replaced by $\sum_l t_l a_l(\cdot)$. The system cost $c(x)$ in (25) can be handled similarly provided that $\mathbb{E}_Q[c(X)] \le \Gamma$, which is an assumption of the proposition.

E. Derivation of $E_{\rm ex}^{\rm cc}$ Using Distance Enumerators

In this section, we present the remaining details which, together with the analysis in Section V-B, yield the exponent $E_{\rm ex}^{\rm cc}$ in (78).

Using similar arguments to Section V-A, we can evaluate the lower tail probability of $d_s^n(\boldsymbol{x}, \overline{\boldsymbol{X}})$ as follows:

$$\int d\overline{\boldsymbol{x}} P_{\boldsymbol{X}}(\overline{\boldsymbol{x}}) \mathbb{1}\big\{d_s^n(\boldsymbol{x},\overline{\boldsymbol{x}}) \le nD\big\} \le \int d\overline{\boldsymbol{x}} P_{\boldsymbol{X}}(\overline{\boldsymbol{x}}) e^{t(nD - d_s^n(\boldsymbol{x},\overline{\boldsymbol{x}}))} \tag{182}$$

$$\dot{\le} \int d\overline{\boldsymbol{x}} Q^n(\overline{\boldsymbol{x}}) e^{t(nD - d_s^n(\boldsymbol{x},\overline{\boldsymbol{x}}))} e^{\overline{r}(a(\overline{\boldsymbol{x}}) - n\phi_a)} \tag{183}$$

$$= e^{n(tD - \overline{r}\phi_a)} \prod_{i=1}^n \int d\overline{x} Q(x) e^{\overline{r}a(\overline{x}) - t d_s(x_i,\overline{x})}, \tag{184}$$

where (182) holds or any $t \ge 0$ by upper bounding the indicator function, and (183) holds for any $\overline{r}$ using (80) and (81). We thus have

$$R(D,\boldsymbol{x}) \ge \sup_{t\ge 0,\overline{r}} \overline{r}\phi_a - tD - \frac{1}{n}\sum_{i=1}^n \theta(x_i,\overline{r},t), \tag{185}$$

where

$$\theta(x,\overline{r},t) \stackrel{\triangle}{=} \log \mathbb{E}_Q\big[e^{\overline{r}a(\overline{X}) - t d_s(x_i,\overline{X})}\big]. \tag{186}$$

We can now simplify the exponent in (107) as follows:

$$\mathbb{E}\Big[\inf_{D\,:\,R(D,\boldsymbol{X})\le R} D + R(D,\boldsymbol{X}) - R\Big] \tag{187}$$

$$= \mathbb{E}\Big[\inf_D \sup_{\rho\ge 1} D + \rho\big(R(D,\boldsymbol{X}) - R\big)\Big] \tag{188}$$

$$\ge \sup_{\rho\ge 1}\mathbb{E}\Big[\inf_D D + \rho\big(R(D,\boldsymbol{X}) - R\big)\Big] \tag{189}$$

$$\ge \sup_{\rho\ge 1}\mathbb{E}\Big[\inf_D \sup_{t\ge 0,\overline{r}} D(1-\rho t) - \rho\Big(-\overline{r}\phi_a + \frac{1}{n}\sum_{i=1}^n \theta(X_i,\overline{r},t) + R\Big)\Big] \tag{190}$$

$$\ge \sup_{\rho\ge 1}\mathbb{E}\Big[\sup_{t\ge 0,\overline{r}} \inf_D D(1-\rho t) - \rho\Big(-\overline{r}\phi_a + \frac{1}{n}\sum_{i=1}^n \theta(X_i,\overline{r},t) + R\Big)\Big] \tag{191}$$

$$= \sup_{\rho \geq 1} \mathbb{E}\Big[\sup_{t \in [0,1/\rho], \overline{r}} -\rho\Big(-\overline{r}\phi_a + \frac{1}{n}\sum_{i=1}^{n} \theta(X_i, \overline{r}, t) + R\Big)\Big] \tag{192}$$

$$\geq \sup_{\rho \geq 1} \sup_{\overline{r}} -\rho\Big(-\overline{r}\phi_a + \mathbb{E}\Big[\frac{1}{n}\sum_{i=1}^{n} \theta(X_i, \overline{r}, 1/\rho)\Big] + R\Big) \tag{193}$$

$$\to \sup_{\rho \geq 1} \sup_{\overline{r}} \rho\Big(\overline{r}\phi_a - \mathbb{E}_Q[\theta(X, \overline{r}, 1/\rho)] - R\Big)\Big], \tag{194}$$

where (188) follows from (55), (190) follows from (185), (192) follows since the infimum over D in (191) yields an objective of $-\infty$ unless $t \in [0, 1/\rho]$, (193) follows by setting $t = 1/\rho$, and (194) follows from Proposition 2.

Substituting (186) into (194) and performing simple rearrangements, we obtain (78)–(79) with $\overline{r}a(x)$ in place of $a(x)$, and with a supremum over $\overline{r}$ in place of the supremum over $a(\cdot)$. The derivation is concluded by setting $\overline{r} = 1$ and optimizing $a(\cdot)$.

References

[1] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. Journal*, vol. 27, pp. 379–423, July and Oct. 1948.

[2] R. Gallager, *Information Theory and Reliable Communication*. John Wiley & Sons, 1968.

[3] Y. Polyanskiy, V. Poor, and S. Verdú, "Channel coding rate in the finite blocklength regime," *IEEE Trans. Inf. Theory*, vol. 56, no. 5, pp. 2307–2359, May 2010.

[4] I. Csiszár, J. Körner, and K. Marton, "A new look at the error exponent of discrete memoryless channels," in *IEEE Int. Symp. Inf. Theory*, Ithaca, NY, 1977.

[5] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, 2nd ed. Cambridge University Press, 2011.

[6] ——, "Graph decomposition: A new key to coding theorems," *IEEE Trans. Inf. Theory*, vol. 27, no. 1, pp. 5–12, Jan. 1981.

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

[8] I. Csiszár and P. Narayan, "Channel capacity for a given decoding metric," *IEEE Trans. Inf. Theory*, vol. 45, no. 1, pp. 35–43, Jan. 1995.

[9] A. Ganti, A. Lapidoth, and E. Telatar, "Mismatched decoding revisited: General alphabets, channels with memory, and the wide-band limit," *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2315–2328, Nov. 2000.

[10] J. Scarlett, A. Martinez, and A. Guillén i Fàbregas, "Mismatched decoding: Finite-length bounds, error exponents and approximations," submitted to *IEEE Trans. Inf. Theory* [Online: http://arxiv.org/abs/1303.6166].

[11] N. Merhav, "Error exponents of erasure/list decoding revisited via moments of distance enumerators," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4439–4447, Oct. 2008.

[12] R. Etkin, N. Merhav, and E. Ordentlich, "Error exponents of optimum decoding for the interference channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 1, pp. 40–56, 2010.

[13] N. Merhav, "Statistical physics and information theory," *Foundations and Trends in Comms. and Inf. Theory*, vol. 6, no. 1-2, pp. 1–212, 2009.

[14] F. Jelinek, "Evaluation of expurgated bound exponents," *IEEE Trans. Inf. Theory*, vol. 14, no. 3, pp. 501–505, 1968.

[15] R. Blahut, "Composition bounds for channel block codes," *IEEE Trans. Inf. Theory*, vol. 23, no. 6, pp. 656–674, 1977.

[16] C. E. Shannon, R. Gallager, and E. Berlekamp, "Lower bounds to error probability for coding on discrete memoryless channels. II," *Information and Control*, vol. 10, no. 5, pp. 522–552, 1967.

[17] J. K. Omura, "Expurgated bounds, Bhattacharyya distance, and rate distortion functions," *Information and Control*, vol. 24, no. 4, pp. 358 – 383, 1974.

[18] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge University Press, 2004.

[19] J. Scarlett, A. Martinez, and A. Guillén i Fàbregas, "Cost-constrained random coding and applications," in *Inf. Theory and Apps. Workshop*, San Diego, CA, Feb. 2013.

[20] Y. Altug and A. B. Wagner, "A refinement of the random coding bound," in *50th Allerton Conf. on Comm., Control and Comp.*, Monticello, IL, Oct. 2012.

[21] R. Fano, *Transmission of information: A statistical theory of communications*. MIT Press, 1961.

[22] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. John Wiley & Sons, Inc., 2001.

[23] C. E. Shannon, “The zero error capacity of a noisy channel,” *IRE Trans. Inf. Theory*, vol. 2, no. 3, pp. 8–19, Sep. 1956.

[24] A. Martinez, A. Guillén i Fàbregas, G. Caire, and F. Willems, “Bit-interleaved coded modulation revisited: A mismatched decoding perspective,” *IEEE Trans. Inf. Theory*, vol. 55, no. 6, pp. 2756–2765, June 2009.

[25] G. Caire, G. Taricco, and E. Biglieri, “Bit-interleaved coded modulation,” *IEEE Trans. Inf. Theory*, vol. 44, no. 3, pp. 927–946, May 1998.

[26] K. Fan, “Minimax theorems,” *Proc. Nat. Acad. Sci.*, vol. 39, pp. 42–47, 1953.

[27] P. Elias, “Coding for two noisy channels,” in *Third London Symp. Inf. Theory*, 1955.

[28] R. L. Dobrushin, “Asymptotic estimates of the probability of error for transmission of messages over a discrete memoryless communication channel with a symmetric transition probability matrix,” *Theory Prob. Appl.*, vol. 7, no. e, pp. 270–300, 1962.

[29] R. Gallager, “The random coding bound is tight for the average code,” *IEEE Trans. Inf. Theory*, vol. 19, no. 2, pp. 244–246, March 1973.

[30] Y. Altug and A. Wagner, “Refinement of the sphere-packing bound,” in *IEEE Int. Symp. Inf. Theory*, 2012, pp. 2949–2953.

[31] J. Scarlett, A. Martinez, and A. Guillén i Fàbregas, “A derivation of the asymptotic random-coding prefactor,” submitted to *Allerton Conf. on Comm., Control and Comp.*, 2013.

[32] Y. Polyanskiy, “Channel coding: non-asymptotic fundamental limits,” Ph.D. dissertation, Princeton University, 2010.

[33] M. Mézard and A. Montanari, *Information, Physics and Computation*. Oxford University Press, 2009.

[34] B. Derrida, “Random-energy model: Limit of a family of disordered models,” *Phys. Rev. Lett.*, vol. 45, no. 2, pp. 79–82, 1980.

[35] ——, “The random energy model,” *Physics Reports*, vol. 67, no. 1, pp. 29–35, 1980.

[36] ——, “Random-energy model: An exactly solvable model for disordered systems,” *Phys. Rev. Lett.*, vol. 24, no. 5, pp. 2613–2626, 1981.

[37] C. E. Shannon, R. Gallager, and E. Berlekamp, “Lower bounds to error probability for coding on discrete memoryless channels. I,” *Information and Control*, vol. 10, no. 1, pp. 65–103, 1967.

[38] N. G. de Bruijn, *Asymptotic Methods in Analysis*. Dover Publications, 1981.