

# Erasure/List Random Coding Error Exponents Are Not Universally Achievable

Wasim Huleihel      Nir Weinberger      Neri Merhav

Department of Electrical Engineering  
Technion - Israel Institute of Technology  
Haifa 3200003, ISRAEL

E-mail: {wh@campus, nirwein@campus, merhav@ee}.technion.ac.il

**Abstract**—We study the problem of universal decoding for unknown discrete memoryless channels in the presence of erasure/list option at the decoder, in the random coding regime. Specifically, we harness a universal version of Forney’s classical erasure/list decoder developed in earlier studies, which is based on the competitive minimax methodology, and guarantees universal achievability of a certain fraction of the optimum random coding error exponents. In this paper, we derive an exact single-letter expression for the maximum achievable fraction. Examples are given in which the maximal achievable fraction is strictly less than unity, which imply that, in general, there is no universal erasure/list decoder which achieves the same random coding error exponents as the optimal decoder for a known channel. This is in contrast to the situation in ordinary decoding (without the erasure/list option), where optimum exponents are universally achievable, as is well known. It is also demonstrated that previous lower bounds derived for the maximal achievable fraction are not tight in general. We then analyze a generalized random coding ensemble which incorporate a training sequence, in conjunction with a suboptimal practical decoder (“plug-in” decoder), which first estimates the channel using the known training sequence, and then decodes the remaining symbols of the codeword using the estimated channel. One of the implications of our results, is setting the stage for a reasonable criterion of optimal training. Finally, we compare the performance of the “plug-in” decoder and the universal decoder, in terms of the achievable error exponents, and show that the latter is noticeably better than the former.

**Index Terms**—Universal decoding, error exponents, erasure/list decoding, maximum-likelihood decoding, random coding, generalized likelihood ratio test, training sequence, plug-in decoder, channel uncertainty, competitive minimax.

## I. INTRODUCTION

**I**N many practical situations encountered in coded communication systems, the channel over which transmission takes place is unknown to the receiver. Typically, the optimal maximum likelihood (ML) decoder depends on the channel statistics, and therefore its usage is precluded. In such cases, universal decoders are sought which do not require knowledge of the actual channel, but still preform well just as if the channel was known to the decoder. The design of such universal decoders was extensively addressed for ordinary decoding

(without the erasure/list option), see, e.g., [1-7], and references therein. For example, for unknown discrete memoryless channels (DMCs), the maximum mutual information (MMI) decoder [1] is asymptotically optimal for ordinary decoding, in the sense that it achieves the same random coding error exponents as the ML decoder. However, for decoders with an erasure/list option, only partial results exist.

In this paper, we focus on universal erasure/list decoders proposed and analyzed by Forney for known channels [8]. Erasure/list decoding is especially attractive for unknown channels, since communicating at any fixed rate, however small, is inherently problematic, since this fixed rate might be larger than the unknown capacity of the underlying channel. It makes sense to try to adapt the coding rate to the channel conditions, which can be learned on-line at the transmitter whenever a feedback link from the receiver to the transmitter is available. A possible approach to handle the problem described above is the *rateless coding* methodology, see, for example [9-14], in which at every time instant the decoder either makes a decision on one of the transmitted messages or decides to request an additional symbol via the feedback line. The latter case can be considered as an “erasure” event for the decoder, and so universal erasure decoders are required (see discussion in [15]).

In [4, Chapter 10, Theorem 10.11], Csiszár and Körner proposed a family of universal erasure decoders, parametrized by some real parameter, for DMCs, and analyzed the resulting error exponents. While this family is in the spirit of the MMI decoder, it does not achieve the same exponents as Forney’s optimal erasure/list decoder. More recently, in [16], Moulin has generalized this family of decoders and proposed a family of decoders parametrized by a weighting function. An optimal weighting function was sought which maximizes the total error exponent of the worst channel in the family, under a constraint on the worst channel undetected-error exponent (the worst channel associated with the two exponents might be different). The decoder was considered universal if the above mentioned trade-off between the worst case exponents does not change even if the choice of specific decoder in the family of allowed decoders can depend on the channel (see [16, Eq. (3.11)], and the discussion that follows). However, this is a rather weak criterion, in the sense that the optimal decoder only depends on the worst case exponents. So, if the family of channels is rich enough (e.g. includes channels whose

This research was partially supported by The Israeli Science Foundation (ISF), grant no. 412/12. This paper was presented in part at the 2015 IEEE Information Theory Workshop (ITW), and the 2015 Information Theory and Applications (ITA) Workshop.

capacity is lower than the required rate), then the worst case exponents are simply zero, and any decoder is universal. To this end, a stronger criterion for universality was proposed, which states that a decoder is universal if it achieves Forney's exponents (for a known channel) for all channels in the family. In [16, Proposition 5.5], Moulin provided sufficient conditions under which the decoder of Csiszár and Körner is universal in the strong sense. Loosely speaking, it is required that the total error exponent is small enough for all channels in the family. These conditions, however, strongly limit the families of channels for which this decoder is universal.

In [15], Merhav and Feder studied the problem using a different approach. Specifically, they considered the problem of universal decoding with an erasure/list option for the class of DMCs indexed by an unknown parameter  $\theta$ . They invoked the competitive minimax methodology proposed in [17], in order to derive a universal version of Forney's classical erasure/list decoder. Recall that for a given DMC with parameter  $\theta$ , a given coding rate  $R$ , and a given threshold parameter  $T$  (all to be formally defined later), Forney's erasure/list decoder optimally trades off between the exponent,  $E_1(R, T, \theta)$ , of the probability of total error event,  $\mathcal{E}_1$ , and the exponent,  $E_2(R, T, \theta) = E_1(R, T, \theta) + T$ , of the probability of undetected error event,  $\mathcal{E}_2$ , for an erasure decoder (or, average list size for list decoder), in the random coding regime. The universal erasure/list decoder of [15] guarantees achievability of an exponent,  $\hat{E}_1(R, T, \theta)$ , which is at least as large as  $\xi \cdot E_1(R, T, \theta)$  for all  $\theta$ , for some constant  $\xi \in (0, 1]$  that is independent of  $\theta$  (but does depend on  $R$  and  $T$ ), and at the same time, an undetected error exponent for erasure decoder (or, average list size for list decoder)  $\hat{E}_2(R, T, \theta) \geq \xi \cdot \hat{E}_1(R, T, \theta) + T$  for all  $\theta$ . At the very least this guarantees that whenever the probabilities of  $\mathcal{E}_1$  and  $\mathcal{E}_2$  decay exponentially for a known channel, so they do even when the channel is unknown, using the proposed universal decoder. It should be remarked, that the benchmark exponents in [15] were the classical lower bounds on  $E_1(R, T, \theta)$  and  $E_2(R, T, \theta)$  derived by Forney [8].

Clearly, to maximize the guaranteed exponents obtained by the universal decoder of [15], the maximal  $\xi \in [0, 1]$  such that the above holds is of interest. This maximal fraction is the central quantity of this paper and will be denoted henceforth by  $\xi^*(R, T)$ . If, for example,  $\xi^*(R, T)$  is strictly less than unity, then it means that there is a major difference between universal ordinary decoding and universal erasure/list decoding: while for the former, it is well known that optimum random coding error exponents are universally achievable (at least for some classes of channels and certain random coding distributions), in the latter, when the erasure/list options are available, this may no longer be the case<sup>1</sup>. In [15], Merhav and Feder invoked Gallager's bounding techniques to analyze the exponential behavior of upper bounds on the probabilities

<sup>1</sup>We could have similarly required that the universal decoder would achieve an undetected error exponent of  $\hat{E}_2(R, T, \theta) \geq \tilde{\xi} \cdot E_2(R, T, \theta)$  for all  $\theta \in \Theta$ , and some  $\tilde{\xi} \in (0, 1]$ . While the numerical value of the maximal achievable  $\tilde{\xi}$ , say  $\tilde{\xi}^*(R, T, \theta)$ , will be different from  $\xi^*(R, T, \theta)$ , the main conclusions of the paper will not change. Specifically,  $\xi^*(R, T, \theta) < 1$  if and only if  $\tilde{\xi}^*(R, T, \theta) < 1$ .

$\mathcal{E}_1$  and  $\mathcal{E}_2$ . Accordingly, a single-letter expression for a lower bound to  $\xi^*(R, T)$  was obtained, which we denote henceforth by  $\xi_L(R, T)$ . Since  $\xi_L(R, T)$  was merely a lower bound, the question of achievability of Forney's erasure/list exponents was not fully settled in [15]<sup>2</sup>.

As was previously mentioned, even for a known channel, only lower bounds for the exponents were obtained by Forney [8]. More recently, inspired by a statistical-mechanical point of view on random code ensembles, Somekh-Baruch and Merhav [18] have found *exact* expressions for the exponents of the optimal erasure/list decoder, by assessing the moments of certain type class enumerators. In this paper, we tackle again the problem of erasure/list channel decoding using similar methods, and derive an *exact* expression for  $\xi^*(R, T)$  with respect to the *exact* erasure/list exponents of a known channels found in [18]. Unlike the lower bound of [15], the exact expression leads to the following conclusions:

- 1) In general,  $\xi^*(R, T)$  is strictly less than 1. Therefore, the known channel exponents in erasure/list decoding cannot be achieved universally. In this sense, channel knowledge is crucial for asymptotically optimum erasure/list decoding. This is in sharp contrast to the situation in ordinary decoding (without the erasure/list option), where, as said, optimum exponents are universally achievable, e.g., by the MMI decoder.
- 2) In general,  $\xi_L(R, T)$  is strictly less than  $\xi^*(R, T)$ . Therefore, the Gallager-style analysis technique in [15] is not always powerful enough to obtain  $\xi^*(R, T)$ .

Although the above universal decoder achieves  $\xi^*(R, T)$ , it may have a rather high implementation complexity. Usually, in practical communication systems with channel uncertainty, a portion of the blocklength is devoted to training which is a common part of all codewords. A possible practical decoder is the "plug-in" decoder, which first estimates the channel using the known training sequence, and then decodes the remaining symbols of the codeword using the estimated channel from the first stage. This suboptimal decoder, on the one hand, has a smaller complexity, and thus can be more easily incorporated into practical systems, but on the other hand, achieves only some  $\xi^e(R, T) \leq \xi^*(R, T)$ . For this sub-optimal decoder, we derive its error exponents and a closed-form formula for  $\xi^e(R, T)$ , which now depend also on the relative training time and the type of the sequence. One implication of our results, is setting the stage for a reasonable criterion of optimal training. Finally, we show numerically that there is a noticeable loss in the error exponents incurred by the plug-in decoder compared to the universal decoder.

The outline of the rest of the paper is as follows. In Section II, we establish notation conventions, and in Section III we detail necessary background on erasure/list decoding, both for known and unknown channels. Then, in Section IV, we present our main result of an exact expression for  $\xi^*(R, T)$ , and discuss the special case of binary symmetric channel (BSC).

<sup>2</sup>Note that universality in the weak sense in [16] does not guarantee that  $\xi^*(R, T)$  is larger than zero because this weak criterion only considers the worst case channels. A universal decoder in the stronger sense in [16] does imply that  $\xi^*(R, T) = 1$ , but, as previously mentioned, such universality was proved only for a restricted families of channels.

We then shed light on the differences between  $\xi^*(R, T)$  and  $\xi_L(R, T)$ , along with some numerical results, which illustrate the main result of this paper. In Section V, we analyze generalized random coding ensembles which incorporates a training sequence, in conjunction with the suboptimal plug-in decoder and the universal decoder, and compare its performance with the universal decoder and the optimal decoder (for known channel). Finally, in Section VI, we provide proofs for all our results.

## II. NOTATION CONVENTIONS

Throughout this paper, scalar random variables (RVs) will be denoted by capital letters, their sample values will be denoted by the respective lower case letters, and their alphabets will be denoted by the respective calligraphic letters, e.g.  $X$ ,  $x$ , and  $\mathcal{X}$ , respectively. A similar convention will apply to random vectors of dimension  $n$  and their sample values, which will be denoted with the same symbols in the boldface font. The set of all  $n$ -vectors with components taking values in a certain finite alphabet, will be denoted as the same alphabet superscripted by  $n$ , e.g.,  $\mathcal{X}^n$ . Generic channels will be usually denoted by the letters  $P$ ,  $Q$ , or  $W$ . We shall mainly consider joint distributions of two RVs  $(X, Y)$  over the Cartesian product of two finite alphabets  $\mathcal{X}$  and  $\mathcal{Y}$ . For brevity, we will denote any joint distribution, e.g.  $Q_{XY}$ , simply by  $Q$ , the marginals will be denoted by  $Q_X$  and  $Q_Y$ , and the conditional distributions will be denoted by  $Q_{X|Y}$  and  $Q_{Y|X}$ . The joint distribution induced by  $Q_X$  and  $Q_{Y|X}$  will be denoted by  $Q_X \times Q_{Y|X}$ , and a similar notation will be used when the roles of  $X$  and  $Y$  are switched.

The expectation operator will be denoted by  $\mathbb{E}\{\cdot\}$ , and when we wish to make the dependence on the underlying distribution  $Q$  clear, we denote it by  $\mathbb{E}_Q\{\cdot\}$ . The entropy of  $X$  and the conditional entropy of  $X$  given  $Y$ , will be denoted  $H_X(Q)$ ,  $H_{X|Y}(Q)$ , respectively, where  $Q$  is the underlying probability distribution. The mutual information of the joint distribution  $Q$  will be denoted by  $I(Q)$ . The divergence (or, Kullback-Liebler distance) between two probability measures  $Q$  and  $P$  will be denoted by  $D(Q||P)$ . For two numbers  $0 \leq q, p \leq 1$ ,  $D(q||p)$  will stand for the divergence between the binary measures  $\{q, 1 - q\}$  and  $\{p, 1 - p\}$ .

For a given vector  $\mathbf{x}$ , let  $\hat{Q}_{\mathbf{x}}$  denote the empirical distribution, that is, the vector  $\{\hat{Q}_{\mathbf{x}}(x), x \in \mathcal{X}\}$ , where  $\hat{Q}_{\mathbf{x}}(x)$  is the relative frequency of the letter  $x$  in the vector  $\mathbf{x}$ . Let  $\mathcal{T}_P$  denote the type class associated with  $P$ , that is, the set of all sequences  $\mathbf{x}$  for which  $\hat{Q}_{\mathbf{x}} = P$ . Similarly, for a pair of vectors  $(\mathbf{x}, \mathbf{y})$ , the empirical joint distribution will be denoted by  $\hat{Q}_{\mathbf{x}\mathbf{y}}$ , or simply by  $\hat{Q}$ , for short. All the previously defined notations for regular distributions will also be used for empirical distributions.

The cardinality of a finite set  $\mathcal{A}$  will be denoted by  $|\mathcal{A}|$ , its complement will be denoted by  $\mathcal{A}^c$ . The probability of an event  $\mathcal{E}$  will be denoted by  $\Pr\{\mathcal{E}\}$ . The indicator function of an event  $\mathcal{E}$  will be denoted by  $\mathcal{I}\{\mathcal{E}\}$ . For two sequences of positive numbers,  $\{a_n\}$  and  $\{b_n\}$ , the notation  $a_n \doteq b_n$  means that  $\{a_n\}$  and  $\{b_n\}$  are of the same exponential order, i.e.,  $n^{-1} \log a_n/b_n \rightarrow 0$  as  $n \rightarrow \infty$ , where in this paper,

logarithms are defined with respect to (w.r.t.) the natural basis, that is,  $\log(\cdot) \equiv \ln(\cdot)$ . Finally, for a real number  $x$ , we let  $|x|^+ \triangleq \max\{0, x\}$ .

## III. MODEL FORMULATION AND SHORT BACKGROUND

### A. Known Channel

Consider a DMC with a finite input alphabet  $\mathcal{X}$ , finite output alphabet  $\mathcal{Y}$ , and a matrix of single-letter transition probabilities  $\{W(y|x), x \in \mathcal{X}, y \in \mathcal{Y}\}$ . A rate- $R$  codebook consists of  $M = \lceil e^{nR} \rceil$  length- $n$  codewords  $\mathbf{x}_m \in \mathcal{X}^n$ ,  $m = 1, 2, \dots, M$ , representing the  $M$  messages. It will be assumed that all messages are a-priori equiprobable. We assume the ensemble of fixed composition random codes of blocklength  $n$ , where each codeword is selected at random, uniformly within a type class  $\mathcal{T}(P_X)$  for some given random coding distribution  $P_X$  over the alphabet  $\mathcal{X}$ .

In the following, we give a short description on the operation of the erasure decoder and then the list decoder. A decoder with an erasure option is a partition of the observation space  $\mathcal{Y}^n$  into  $(M + 1)$  regions, denoted by  $\{\mathcal{R}_m\}_{m=0}^M$ . An erasure decoder works as follows: If  $\mathbf{y} \in \mathcal{Y}^n$  falls into the  $m$ th region,  $\mathcal{R}_m$ , for  $m = 1, 2, \dots, M$ , then a decision is made in favor of message number  $m$ . If  $\mathbf{y} \in \mathcal{R}_0$ , then no decision is made and an erasure is declared. Accordingly, we shall refer to  $\mathbf{y} \in \mathcal{R}_0$  as an *erasure event*. Given a code  $\mathcal{C} \triangleq \{\mathbf{x}_1, \dots, \mathbf{x}_M\}$  and a decoder  $\mathcal{R} \triangleq (\mathcal{R}_0, \dots, \mathcal{R}_M)$ , we define two error events. The event  $\mathcal{E}_1$  is the event of deciding on erroneous codeword or making an erasure, and the event  $\mathcal{E}_2$  which is the undetected error event, namely, the event of deciding on erroneous codeword. It is evident that  $\mathcal{E}_1$  is the disjoint union of the erasure event and  $\mathcal{E}_2$ . The probabilities of all the aforementioned events are given by:

$$\Pr\{\mathcal{E}_1\} = \frac{1}{M} \sum_{m=1}^M \sum_{\mathbf{y} \in \mathcal{R}_m^c} W(\mathbf{y}|\mathbf{x}_m), \quad (1)$$

$$\Pr\{\mathcal{E}_2\} = \frac{1}{M} \sum_{m=1}^M \sum_{\mathbf{y} \in \mathcal{R}_m} \sum_{m' \neq m} W(\mathbf{y}|\mathbf{x}_{m'}), \quad (2)$$

and

$$\Pr\{\mathcal{R}_0\} = \Pr\{\mathcal{E}_1\} - \Pr\{\mathcal{E}_2\}. \quad (3)$$

A list decoder is a mapping from the space of received vectors  $\mathcal{Y}^n$  into a collection of the subsets of  $\{1, \dots, M\}$ . Alternatively, a list decoder is uniquely defined by a set of  $M + 1$  (not necessarily disjoint) decoding regions  $\{\mathcal{R}_m\}_{m=0}^M$  such that  $\mathcal{R}_m \subseteq \mathcal{Y}^n$  and  $\mathcal{R}_0 = \mathcal{Y}^n \setminus \bigcup_{m=1}^M \mathcal{R}_m$ . Given a received vector  $\mathbf{y}$ , the  $m$ th codeword belongs to the output list if  $\mathbf{y} \in \mathcal{R}_m$ , and if  $\mathbf{y}$  does not belong to any of the regions  $\mathcal{R}_m$  then  $\mathbf{y} \in \mathcal{R}_0$ , and an erasure is declared. The average error probability of a list decoder and a codebook  $\mathcal{C}$  is the probability that the actual transmitted codeword does not belong to the output list, and it is defined similarly to (1). The average list size is the expected (w.r.t. the output of the channel) number of erroneous codewords in the output list, and it is easily verified that it is defined exactly as in (2) (see [8, Eq. (13)]).

Since the error events for the erasure and list decoders are defined in the same way, they can be treated on the same footing. Nonetheless, for descriptive purposes, we will refer to the erasure decoder, but we emphasize that all the following analysis and results are true also for the list decoder. When knowledge on the specific DMC is available at the decoder, Forney has shown in [8], using the Neyman-Pearson methodology, that the optimal trade-off between  $\Pr\{\mathcal{E}_1\}$  and  $\Pr\{\mathcal{E}_2\}$  is attained by the decision regions  $\mathcal{R}^* \triangleq (\mathcal{R}_0^*, \dots, \mathcal{R}_M^*)$  given by:

$$\mathcal{R}_m^* \triangleq \left\{ \mathbf{y} : \frac{W(\mathbf{y}|\mathbf{x}_m)}{\sum_{m' \neq m} W(\mathbf{y}|\mathbf{x}_{m'})} \geq e^{nT} \right\}, \quad m = 1, 2, \dots, M, \quad (4)$$

and

$$\mathcal{R}_0^* \triangleq \bigcap_{m=1}^M (\mathcal{R}_m^*)^c, \quad (5)$$

where  $T$  is a parameter, henceforth referred as the *threshold*, which controls the balance between the probabilities of  $\mathcal{E}_1$  and  $\mathcal{E}_2$ . When  $T \geq 0$  the decoder operates in the erasure mode, and when it is in the list mode then  $T < 0$ . No other decision rule gives both a lower  $\Pr\{\mathcal{E}_1\}$  and a lower  $\Pr\{\mathcal{E}_2\}$  than the above choice. Finally, we define the error exponents  $E_i(R, T)$ ,  $i = 1, 2$ , as the exponents of the average probabilities of errors  $\overline{\Pr}\{\mathcal{E}_i\}$  (associated with the optimal decoder  $\mathcal{R}^*$ ), where the average is taken w.r.t. a given ensemble of the randomly selected codes, that is,

$$E_i(R, T) \triangleq -\liminf_{n \rightarrow \infty} \frac{1}{n} \log \overline{\Pr}\{\mathcal{E}_i\}, \quad i = 1, 2. \quad (6)$$

An important observation is that Forney's decision rule for known DMCs can also be obtained by formulating the following optimization problem: Find a decoder  $\mathcal{R}$  that minimizes  $\Gamma(\mathcal{C}, \mathcal{R})$  where

$$\Gamma(\mathcal{C}, \mathcal{R}) \triangleq \Pr\{\mathcal{E}_2\} + e^{-nT} \Pr\{\mathcal{E}_1\} \quad (7)$$

$$= \frac{1}{M} \sum_{m=1}^M \left[ \sum_{\mathbf{y} \in \mathcal{R}_m} \sum_{m' \neq m} W(\mathbf{y}|\mathbf{x}_{m'}) + \sum_{\mathbf{y} \in \mathcal{R}_m^c} e^{-nT} W(\mathbf{y}|\mathbf{x}_m) \right] \quad (8)$$

for a given codebook  $\mathcal{C}$  and a given threshold  $T$ . Indeed, noting that (8) can be rewritten as

$$\Gamma(\mathcal{C}, \mathcal{R}) = \sum_{\mathbf{y} \in \mathcal{Y}^n} \frac{1}{M} \sum_{m=1}^M \left[ \sum_{m' \neq m} W(\mathbf{y}|\mathbf{x}_{m'}) \mathcal{I}\{\mathbf{y} \in \mathcal{R}_m\} + e^{-nT} W(\mathbf{y}|\mathbf{x}_m) \mathcal{I}\{\mathbf{y} \in \mathcal{R}_m^c\} \right], \quad (9)$$

it is evident that for each  $m$ , the bracketed expression is minimized by  $\mathcal{R}_m^*$  as defined above. By taking the ensemble average, we have

$$\mathbb{E}\{\Gamma(\mathcal{C}, \mathcal{R}^*)\} \triangleq \overline{\Pr}\{\mathcal{E}_2\} + e^{-nT} \overline{\Pr}\{\mathcal{E}_1\}. \quad (10)$$

In [18], it was stated (without a proof) that, in the exponential scale, there is a balance between the two terms at the right hand side of (10), namely, the exponent of  $\overline{\Pr}\{\mathcal{E}_2\}$  equals to the exponent of  $e^{-nT} \overline{\Pr}\{\mathcal{E}_1\}$ , for the optimal decoder  $\mathcal{R}^*$ . We rigorously assert this property in the following lemma, the proof of which appears in Appendix A.

*Lemma 1* For all  $R$  and  $T$ , the optimal decoder  $\mathcal{R}^*$  satisfies:

$$E_2(R, T) = T + E_1(R, T). \quad (11)$$

The significance of Lemma 1 is attributed to the fact that now we only need to assess the exponential behavior of either  $\overline{\Pr}\{\mathcal{E}_1\}$ , or,  $\overline{\Pr}\{\mathcal{E}_2\}$ , but not both. As was mentioned in the Introduction, in [18], Somekh-Baruch and Merhav have obtained exact single-letter formulas for the error exponents  $E_1(R, T)$  and  $E_2(R, T)$  associated with  $\overline{\Pr}\{\mathcal{E}_1\}$  and  $\overline{\Pr}\{\mathcal{E}_2\}$ , respectively. Specifically, they show, that for the ensemble of fixed composition codes [18, Theorem 1]<sup>3,4</sup>:

$$E_1(R, T) = \min \{E_a(R, T), E_b(R, T)\}, \quad (12)$$

where

$$E_a(R, T) \triangleq \min_{(Q, \tilde{Q}) \in \tilde{\mathcal{Q}}} \left[ D(\tilde{Q} \| P_X \times W) + I(Q) - R \right] \quad (13)$$

and

$$E_b(R, T) \triangleq \min_{\tilde{Q} \in \hat{\mathcal{L}}} D(\tilde{Q} \| P_X \times W) \quad (14)$$

where  $\tilde{\mathcal{Q}}$  is a probability distribution on  $\mathcal{X} \times \mathcal{Y}$ , and

$$\tilde{\mathcal{Q}} \triangleq \left\{ (Q, \tilde{Q}) \in \mathcal{D} : I(Q) \geq R, \hat{\Omega}(Q, \tilde{Q}) \leq 0 \right\}, \quad (15)$$

$$\mathcal{D} \triangleq \left\{ (Q, \tilde{Q}) : Q_X = \tilde{Q}_X = P_X, Q_Y = \tilde{Q}_Y \right\}, \quad (16)$$

$$\hat{\Omega}(Q, \tilde{Q}) \triangleq \mathbb{E}_{\tilde{Q}} \log W(Y|X) - \mathbb{E}_Q \log W(Y|X) - T, \quad (17)$$

and

$$\hat{\mathcal{L}} \triangleq \left\{ \tilde{Q} : \mathbb{E}_{\tilde{Q}} \log W(Y|X) \leq R + T + \max_{Q: (Q, \tilde{Q}) \in \mathcal{D}: I(Q) \leq R} [\mathbb{E}_Q \log W(Y|X) - I(Q)] \right\}. \quad (18)$$

As a special case, we shall consider in the sequel the problem of universal erasure/list decoding for the BSC, and to this end, we will use the exact expression of  $E_1(R, T)$ . Accordingly, for the BSC with crossover probability  $\theta$ , it was shown that [18, Corollary 2]

$$E_{1, \text{BSC}}(R, T) = \min \{E_{a, \text{BSC}}(R, T), E_{b, \text{BSC}}(R, T)\}, \quad (19)$$

where

$$E_{a, \text{BSC}}(R, T) \triangleq \log 2 - R$$

<sup>3</sup>In [18], each codeword in the codebook was drawn independently of all other codewords, and its symbols were drawn from an independent and identically (i.i.d.) distribution (identical for all the codewords). Nonetheless, the modification to the ensemble of fixed composition codes is straightforward.

<sup>4</sup>We note that there is an error at the end of the proof of Theorem 1 in [18], where it was claimed that  $\min \{E_a(R, T), E_b(R, T)\} = E_a(R, T)$ , which may not be true in general. The correct expression is as in (12).

$$+ \min_{\tilde{q} \in [\theta, \delta_{\text{GV}}(R) - T/\beta]} \left[ D(\tilde{q} \parallel \theta) - h\left(\tilde{q} + \frac{T}{\beta}\right) \right], \quad (20)$$

and

$$E_{b,\text{BSC}}(R, T) \triangleq \min_{\tilde{q} \in \hat{\mathcal{L}}_{\text{BSC}}} D(\tilde{q} \parallel \theta), \quad (21)$$

where  $\beta(\theta) \triangleq \log[(1-\theta)/\theta]$ , and  $\delta_{\text{GV}}(R)$  denote the normalized Gilbert-Varshamov (GV) distance, i.e., the smaller solution,  $\delta$ , to the equation

$$h(\delta) = \log 2 - R, \quad (22)$$

where  $h(\delta) \triangleq -\delta \log \delta - (1-\delta) \log(1-\delta)$  is the binary entropy function, and

$$\hat{\mathcal{L}}_{\text{BSC}} \triangleq \left\{ \tilde{q} : -\tilde{q} \cdot \beta(\theta) \leq R + T \right. \\ \left. + \max_{q: R \geq \log 2 - h(q)} [-q \cdot \beta(\theta) + h(q) - \log 2] \right\}. \quad (23)$$

### B. Unknown Channel

We now move on to the case of an unknown channel. Consider a family of DMCs

$$\mathcal{W}_\Theta \triangleq \{W_\theta(y|x), x \in \mathcal{X}, y \in \mathcal{Y}, \theta \in \Theta\}, \quad (24)$$

with a finite input alphabet  $\mathcal{X}$ , a finite output alphabet  $\mathcal{Y}$ , and a matrix of single-letter transition probabilities  $\{W_\theta(y|x)\}$ , where  $\theta$  is a parameter, or the index of the channel in the class, taking values in some set  $\Theta$ , which may be countable or uncountable. For example,  $\theta$  may represent the set of all  $|\mathcal{X}| \cdot (|\mathcal{Y}| - 1)$  single-letter transition probabilities that define the DMC with the given input and output alphabets. In our problem, the channel is unknown to the receiver designer, and the designer only knows that the channel belongs to the family of channels  $\mathcal{W}_\Theta$ , that is,  $\theta$  itself is unknown.

When the channel is unknown, the competitive minimax methodology, proposed and developed in [15], proves useful. Specifically, let  $\Gamma_\theta(\mathcal{C}, \mathcal{R})$  in (7) designate the above defined Lagrangian, where we now emphasize the dependence on the index of the channel,  $\theta$ . Similarly, henceforth we shall denote the error exponents in (6) by  $E_1(R, T, \theta)$  and  $E_2(R, T, \theta)$ . Also, let  $\bar{\Gamma}_\theta^* \triangleq \mathbb{E} \{\min_{\mathcal{R}} \Gamma_\theta(\mathcal{C}, \mathcal{R})\}$ , which is the ensemble average of the minimum of the above Lagrangian (achieved by Forney's optimum decision rule) w.r.t. the channel  $W_\theta(y|x)$ , for a given  $\theta$ . Note that by Lemma 1, the exponential order of  $\bar{\Gamma}_\theta^*$  is  $e^{-n(E_1(R, T, \theta) + T)}$ . A *competitive minimax decision rule*  $\mathcal{R}$  is one that achieves

$$\min_{\mathcal{R}} \max_{\theta \in \Theta} \frac{\Gamma_\theta(\mathcal{C}, \mathcal{R})}{\bar{\Gamma}_\theta^*}, \quad (25)$$

which is asymptotically equivalent to

$$\min_{\mathcal{R}} \max_{\theta \in \Theta} \frac{\Gamma_\theta(\mathcal{C}, \mathcal{R})}{e^{-n[E_1(R, T, \theta) + T]}}. \quad (26)$$

However, as discussed in [15], such a minimax criterion, of competing with the optimum performance, may be too ambitious, and the value of the minimization problem in (26) may diverge to infinity for every  $R$ , as  $n \rightarrow \infty$ . A possible remedy for this situation is to compete with only a fraction

$\xi \in [0, 1]$  of  $E_1(R, T, \theta)$ , which we would like to choose as large as possible. To wit, we are interested in the competitive minimax criterion

$$K_n(\mathcal{C}) = \min_{\mathcal{R}} K_n(\mathcal{C}, \mathcal{R}), \quad (27)$$

in which

$$K_n(\mathcal{C}, \mathcal{R}) = \max_{\theta \in \Theta} \frac{\Gamma_\theta(\mathcal{C}, \mathcal{R})}{e^{-n(\xi E_1(R, T, \theta) + T)}}. \quad (28)$$

Accordingly, for a given rate  $R$  and threshold  $T$ , we wish to find  $\xi^*(R, T)$ , defined as:

$$\xi^*(R, T) \triangleq \sup \left\{ \xi \in [0, 1] : \limsup_{n \rightarrow \infty} \frac{1}{n} \log \bar{K}_n \leq 0 \right\}, \quad (29)$$

that is, the largest value of  $\xi$  such that the ensemble average  $\bar{K}_n \triangleq \mathbb{E} \{K_n(\mathcal{C})\}$  would *not* grow exponentially fast.

In [15], the following universal decoding metric was defined

$$f(\mathbf{x}_m, \mathbf{y}) \triangleq \max_{\theta \in \Theta} \left\{ e^{n[\xi E_1(R, T, \theta) + T]} W_\theta(\mathbf{y} | \mathbf{x}_m) \right\}, \quad (30)$$

and a universal erasure/list decoder was proposed which has the following decision regions

$$\hat{\mathcal{R}}_m \triangleq \left\{ \mathbf{y} : \frac{f(\mathbf{x}_m, \mathbf{y})}{\sum_{m' \neq m} f(\mathbf{x}_{m'}, \mathbf{y})} \geq e^{nT} \right\}, \quad m = 1, 2, \dots, M, \quad (31)$$

and

$$\hat{\mathcal{R}}_0 \triangleq \bigcap_{m=1}^M \hat{\mathcal{R}}_m^c. \quad (32)$$

The property that makes  $\hat{\mathcal{R}} \triangleq (\hat{\mathcal{R}}_0, \hat{\mathcal{R}}_1, \dots, \hat{\mathcal{R}}_M)$  interesting is that it was shown in [15], that it is asymptotically optimal, i.e., for any given  $\xi$ ,  $K_n(\mathcal{C}, \hat{\mathcal{R}})$  may only be sub-exponentially larger than  $K_n(\mathcal{C})$ . Thus, the largest  $\xi$  such that  $\bar{K}_n$  is sub-exponential is also attained by  $\hat{\mathcal{R}}$ . Hence, in order to find the largest achievable  $\xi$ , we would like to evaluate exactly the exponential order of  $\mathbb{E}[K_n(\mathcal{C}, \hat{\mathcal{R}})]$ , as a function of  $\xi$ .

We conclude this section with a few remarks:

- 1) Note that the results in this paper can be generalized to other random coding ensembles which assign equal probabilities within every type class (for more details see [15, Section V]). For conceptual simplicity, we confine attention to fixed-composition random coding.
- 2) We have assumed that the input distribution  $P_X$  is fixed, and so the dependence of  $\xi^*(R, T)$  in  $P_X$  was omitted. While, in essence, the input distribution may be optimized to maximize  $\xi^*(R, T, P_X)$  over some set of input distributions (where, for the moment, we make the dependence in  $P_X$  explicit), the meaning of the resulting maximal value should be examined very carefully. Specifically, if we maximize over the entire simplex, the resulting  $\max_{P_X} \xi^*(R, T, P_X)$  is simply 1, which is achieved, trivially and uninterestingly, by any input assignment that puts all its mass on a single codeword. Of course the resultant communication system is completely useless. The point is that the minimax criterion is relative (competitive minimax), i.e., it looks at the difference between the ML exponent and the best universally achievable exponent, allowing (among other

things) both exponents to be poor. It seems that any other conceivable approach for universality will also suffer from a difficulty to define a reasonable criterion for a good choice of  $P_X$ .

- 3) For  $T = 0$  it can be shown that the exponent (12) coincides with the ordinary random coding exponent. Since the MMI is a universal decoder which achieves the random coding exponent, then clearly any optimal erasure/list universal decoder may only have better exponents, and therefore  $\xi^*(R, 0) = 1$ .

#### IV. RESULTS

In this section, our results are presented and discussed. Proofs are relegated to Section VI.

##### A. Exact formula for the largest achievable fraction

We start with a few definitions. Let

$$G(R, T, \xi, \tilde{Q}) \triangleq \max_{\theta \in \Theta} \left\{ \xi E_1(R, T, \theta) + T + \mathbb{E}_{\tilde{Q}} \log W_\theta(Y|X) \right\}, \quad (33)$$

$$\Omega(R, T, \xi, Q, \tilde{Q}) \triangleq G(R, T, \xi, \tilde{Q}) - G(R, T, \xi, Q) - T, \quad (34)$$

where  $E_1(R, T, \theta)$  is given in (12). Finally, let

$$\mathcal{Q} \triangleq \left\{ (Q, \tilde{Q}) \in \mathcal{D} : I(Q) \geq R, \Omega(R, T, \xi, Q, \tilde{Q}) \leq 0 \right\} \quad (35)$$

and

$$\mathcal{L} \triangleq \left\{ \tilde{Q} : G(R, T, \xi, \tilde{Q}) \leq R + T + \max_{Q: (Q, \tilde{Q}) \in \mathcal{D}, I(Q) \leq R} [G(R, T, \xi, Q) - I(Q)] \right\}. \quad (36)$$

where  $\mathcal{D}$  is defined in (16).

*Theorem 1* Consider the ensemble of fixed composition codes of type  $\mathcal{T}(P_X)$ . Then, for any given  $T \in \mathbb{R}$  and  $R \geq 0$ ,  $\xi^*(R, T)$ , defined in (29), is equal to the largest number  $\xi$  that simultaneously satisfies:

$$\max_{\theta \in \Theta} \left\{ \xi E_1(R, T, \theta) - \min_{(Q, \tilde{Q}) \in \mathcal{Q}} \left\{ D(\tilde{Q} \| P_X \times W_\theta) + I(Q) - R \right\} \right\} \leq 0, \quad (37)$$

and

$$\max_{\theta \in \Theta} \left\{ \xi E_1(R, T, \theta) - \min_{\tilde{Q} \in \mathcal{L}} D(\tilde{Q} \| P_X \times W_\theta) \right\} \leq 0. \quad (38)$$

Notice that in order to find  $\xi^*(R, T)$  one can perform a simple line search over the interval  $[0, 1]$  using the condition in Theorem 1. Alternatively, in the following corollary, we also propose an analytical single-letter expression for  $\xi^*(R, T)$ .

*Corollary 1* Let  $\mathcal{G}(\tilde{Q}_Y) \triangleq \{Q : I(Q) \leq R, Q_Y = \tilde{Q}_Y\}$ , and define (39)-(42), shown at the top of the next page, where in the optimizations  $Q_X = \tilde{Q}_X = P_X$ . Then,

$$\xi^*(R, T) = \min \{ \xi_1^*(R, T), \xi_2^*(R, T) \}. \quad (43)$$

For the special case of the BSC, one can simplify the above minimization problems over the joint distributions  $(Q, \tilde{Q})$ , and obtain instead a one-dimensional minimization problem. Indeed, consider the family of BSCs where the unknown crossover probability  $\theta$  belongs to  $\Theta = [0, 1]$ . Recall that (c.f. end of Subsection III-A)  $\beta(\theta) = \log[(1 - \theta)/\theta]$ . Define

$$\phi(\theta) \triangleq \frac{\xi E_1(R, T, \theta) + \log(1 - \theta) + T}{\beta(\theta)} - \frac{\max_{\theta'} \{ \xi E_1(R, T, \theta') + \log(1 - \theta') - \beta(\theta') \cdot \tilde{q} \}}{\beta(\theta)} \quad (44)$$

and

$$q_1^* \triangleq \max_{\theta \leq 1/2} \phi(\theta), \quad (45)$$

$$q_2^* \triangleq \min_{\theta > 1/2} \phi(\theta). \quad (46)$$

Finally, let

$$g(q_1^*, q_2^*) \triangleq \begin{cases} \log 2, & \text{if } q_1^* > 1/2, \text{ or, } q_2^* < 1/2, \\ \max \{ h(q_1^*), h(q_2^*) \}, & \text{otherwise} \end{cases} \quad (47)$$

and

$$\mathcal{L}_{\text{BSC}} \triangleq \left\{ \tilde{q} : \max_{0 \leq \theta \leq 1} [\xi E_1(R, T, \theta) - \tilde{q} \cdot \beta(\theta) + \log \theta] \leq R + T + \max_{0 \leq \theta \leq 1} [\xi E_1(R, T, \theta) - \max \{ \theta, \delta_{\text{GV}}(R) \} \cdot \beta(\theta) + \log \theta + h(\max \{ \theta, \delta_{\text{GV}}(R) \}) - \log 2] \right\}. \quad (48)$$

We have the following result.

*Corollary 2* Consider a family of BSCs, where the unknown crossover probability  $\theta$  belongs to  $\Theta = [0, 1]$ , and with fixed composition codes of type  $P_X = (1/2, 1/2)$ . Then,  $\xi^*(R, T)$  is equal to the largest number  $\xi$  that simultaneously satisfies:

$$\max_{0 \leq \theta \leq 1} \left\{ \xi \cdot E_{1, \text{BSC}}(R, T, \theta) - \min_{\tilde{q}} \left[ D(\tilde{q} \| \theta) + |-g(q_1^*, q_2^*) + \log 2 - R|^+ \right] \right\} \leq 0, \quad (49)$$

and

$$\max_{0 \leq \theta \leq 1} \left\{ \xi \cdot E_{1, \text{BSC}}(R, T, \theta) - \min_{\tilde{q} \in \mathcal{L}_{\text{BSC}}} D(\tilde{q} \| \theta) \right\} \leq 0, \quad (50)$$

where  $E_{1, \text{BSC}}(R, T, \theta)$  is given in (19).

$$\hat{\xi}_1(R, T, Q, \tilde{Q}, \theta, \theta_1, \theta_2, \lambda) \triangleq \frac{D(\tilde{Q}||P_X \times W_\theta) + I(Q) - R + \lambda \mathbb{E}_{\tilde{Q}} [\log W_{\theta_1}(Y|X)] - \lambda \mathbb{E}_Q [\log W_{\theta_2}(Y|X)] - \lambda T}{E_1(R, T, \theta) - \lambda E_1(R, T, \theta_1) + \lambda E_1(R, T, \theta_2)}, \quad (39)$$

$$\xi_1^*(R, T) \triangleq \min_{\theta \in \Theta} \min_{(\tilde{Q}, Q) \in \mathcal{D}} \min_{Q \in \mathcal{G}^c(\tilde{Q}_Y)} \max_{\lambda \geq 0} \max_{\theta_1 \in \Theta} \min_{\theta_2 \in \Theta} \hat{\xi}_1(R, T, Q, \tilde{Q}, \theta, \theta_1, \theta_2, \lambda), \quad (40)$$

$$\hat{\xi}_2(R, T, Q, \tilde{Q}, \theta, \theta_1, \theta_2, \lambda) \triangleq \frac{D(\tilde{Q}||P_X \times W_\theta) + \lambda \mathbb{E}_{\tilde{Q}} [\log W_{\theta_1}(Y|X)] - \lambda \mathbb{E}_Q [\log W_{\theta_2}(Y|X)] - \lambda [R + T - I(Q)]}{E_1(R, T, \theta) - \lambda E_1(R, T, \theta_1) + \lambda E_1(R, T, \theta_2)}, \quad (41)$$

$$\xi_2^*(R, T) \triangleq \min_{\theta \in \Theta} \min_{\tilde{Q}} \max_{\lambda \geq 0} \max_{\theta_1 \in \Theta} \min_{Q \in \mathcal{G}(\tilde{Q}_Y)} \min_{\theta_2 \in \Theta} \hat{\xi}_2(R, T, Q, \tilde{Q}, \theta, \theta_1, \theta_2, \lambda), \quad (42)$$

## B. Discussion and Comparison with Previous Results

While in this work we have derived the exact maximal achievable  $\xi^*(R, T)$  for fixed composition coding of type  $P_X$ , in [15, Theorem 2], Merhav and Feder have obtained the following lower bound [15, Theorem 2]:

$$\xi^*(R, T) \geq \xi_L(R, T) \triangleq \min_{(\theta, \theta'') \in \Theta^2} \max_{0 \leq s \leq \rho \leq 1} \frac{E(\theta, \theta'', s, \rho) - \rho R - sT}{(1-s)E_1(R, T, \theta) + sE_1(R, T, \theta'')} \quad (51)$$

where

$$E(\theta, \tilde{\theta}, s, \rho) \triangleq \min_{Q_Y} [F(Q_Y, 1-s, \theta) + \rho F(Q_Y, s/\rho, \theta'') - H(Q_Y)] \quad (52)$$

and

$$F(Q_Y, 1-s, \theta) \triangleq \min_{Q_{X|Y}: (Q_Y \times Q_{X|Y})_X = P_X} [I(Q) - \lambda \mathbb{E}_Q \log W_\theta(Y|X)]. \quad (53)$$

Before we continue, we remark that in [15], Forney's lower bound on  $E_1(R, T, \theta)$  was used instead of its exact value as derived in [18], but for the sake of comparison any exponent can be used, and specifically, the exact exponent. Now, note that an alternative (equivalent) representation of  $\xi_L(R, T)$  in (51) is that it is given by the largest  $\xi$  such that for any pair  $(\theta, \theta'') \in \Theta^2$

$$\max_{0 \leq s \leq \rho \leq 1} E(\theta, \theta'', s, \rho) - \rho R - sT - \xi [(1-s)E_1(R, T, \theta) + sE_1(R, T, \theta'')] \geq 0. \quad (54)$$

Straightforward algebraic manipulations show that the last inequality can be rewritten as

$$\max_{0 \leq s \leq \rho \leq 1} \min_{(Q, \tilde{Q}) \in \mathcal{D}} \Psi(R, T, \theta, \theta'', Q, \tilde{Q}, \rho, s) \geq 0 \quad (55)$$

where

$$\begin{aligned} \Psi(R, T, \theta, \theta', \theta'', Q, \tilde{Q}, \rho, s, \xi) &\triangleq D(\tilde{Q}||P_X \times W_\theta) \\ &+ \rho [I(Q) - R] + s \cdot [\mathbb{E}_{\tilde{Q}} \log W_{\theta'}(Y|X) + \xi E_1(R, T, \theta') \\ &- \mathbb{E}_Q \log W_{\theta''}(Y|X) - \xi E_1(R, T, \theta'') - T] - \xi E_1(R, T, \theta). \end{aligned} \quad (56)$$

For any given  $(\theta, \theta'') \in \Theta^2$ , and  $(s, \rho)$ ,  $\Psi(R, T, \theta, \theta', \theta'', Q, \tilde{Q}, \rho, s, \xi)$  is convex in<sup>5</sup>  $(Q, \tilde{Q})$ , and for a given  $(Q, \tilde{Q})$ , it is linear (and hence concave) in  $(s, \rho)$ . Thus, the minimax theorem implies that (55) is equivalent to

$$\min_{(\theta, \theta'') \in \Theta^2} \min_{(Q, \tilde{Q}) \in \mathcal{D}} \max_{0 \leq s \leq \rho \leq 1} \Psi(R, T, \theta, \theta', \theta'', Q, \tilde{Q}, \rho, s, \xi) \geq 0. \quad (57)$$

On the other hand, the exact value of  $\xi^*(R, T)$  in Theorem 1 is determined by the two conditions (37)-(38). In what follows, we shall concentrate on the first condition in (37), as this condition can be compared to (57). Thus, let us focus on the case in which the condition in (37) is more stringent than the condition in (38). Then, according to (37), a fraction  $\xi$  is achievable if

$$\min_{\theta \in \Theta} \min_{(Q, \tilde{Q}) \in \mathcal{D}} D(\tilde{Q}||P_X \times W_\theta) + I(Q) - R - \xi E_1(R, T, \theta) \geq 0 \quad (58)$$

where the minimum over  $(Q, \tilde{Q})$  is such that  $I(Q) \geq R$  and  $\Omega(R, T, \xi, Q, \tilde{Q}) \leq 0$ . Now, the optimization problem in (58) is equivalent to

$$\min_{\theta \in \Theta} \min_{(Q, \tilde{Q}) \in \mathcal{D}} \max_{\rho' \geq 0} \max_{s \geq 0} [D(\tilde{Q}||P_X \times W_\theta) - \xi E_1(R, T, \theta) + (1-\rho') [I(Q) - R] + s\Omega(R, T, \xi, Q, \tilde{Q})] \geq 0, \quad (59)$$

or by letting  $\rho = 1 - \rho'$  we get

$$\min_{\theta \in \Theta} \min_{(Q, \tilde{Q}) \in \mathcal{D}} \max_{\rho \leq 1} \max_{s \geq 0} [D(\tilde{Q}||P_X \times W_\theta) + \rho [I(Q) - R] + s\Omega(R, T, \xi, Q, \tilde{Q}) - \xi E_1(R, T, \theta)] \geq 0, \quad (60)$$

which is equivalent to

$$\min_{\theta \in \Theta} \min_{(Q, \tilde{Q}) \in \mathcal{D}} \max_{\rho \leq 1} \max_{s \geq 0} \max_{\theta'' \in \Theta} \Psi(R, T, \theta, \theta', \theta'', Q, \tilde{Q}, \rho, s, \xi) \geq 0. \quad (61)$$

Moreover, for a given  $(\theta, Q, \tilde{Q})$ , we may write

$$\begin{aligned} &\max_{\rho \leq 1} \max_{s \geq 0} \max_{\theta' \in \Theta} \min_{\theta'' \in \Theta} \Psi(R, T, \theta, \theta', \theta'', Q, \tilde{Q}, \rho, s, \xi) \\ &= \min_{\theta'' \in \Theta} \max_{\theta' \in \Theta} \max_{0 \leq \rho \leq 1} \max_{s \geq 0} \Psi(R, T, \theta, \theta', \theta'', Q, \tilde{Q}, \rho, s, \xi), \end{aligned} \quad (62)$$

<sup>5</sup>The input distributions of both  $Q$  and  $\tilde{Q}$  are assumed fixed to  $P_X$ , and we are essentially only optimizing over the conditional distributions  $(Q_{Y|X}, \tilde{Q}_{Y|X})$ .

because under the constraint  $s \geq 0$ , the inner minimization over  $\theta'' \in \Theta$  does not depend on the value of  $(\rho, s, \theta')$ : it is simply the  $\theta'' \in \Theta$  which maximizes  $\mathbb{E}_Q \log W_{\theta''}(Y|X) + \xi E_1(R, T, \theta'')$ <sup>6</sup>. Thus, the resulting condition is

$$\min_{(\theta, \theta'') \in \Theta^2} \min_{(Q, \tilde{Q}) \in \mathcal{D}} \max_{0 \leq \rho \leq 1} \max_{s \geq 0} \max_{\theta' \in \Theta} \Psi(R, T, \theta, \theta', \theta'', Q, \tilde{Q}, \rho, s, \xi) \geq 0. \quad (63)$$

By comparing the condition in (63) to the condition of the lower bound of [15] in (57), the following differences are observed:

- 1) In (57) an additional constraint  $s \leq \rho$  is imposed.
- 2) In (57) a sub-optimal choice of  $\theta' = \theta$  is imposed.

Accordingly, these differences may cause the value of the minimax in (57) to be lower than the value of the optimization problem in (63), which results in a lower achievable  $\xi$  compared to  $\xi^*(R, T)$ , as one should expect. Next, we provide two examples, where in the first one these differences are immaterial, and in the second one they do matter. The former happens when the optimal solution in (63), denoted by  $(\theta^*, \theta''^*, Q^*, \tilde{Q}^*, \rho^*, s^*)$ , satisfies  $s^* \leq \rho^*$ , and the maximizer of  $\mathbb{E}_{\tilde{Q}^*} \log W_{\theta''^*}(Y|X) + \xi_L(R, T) \cdot E_1(R, T, \theta')$  is given by  $\theta^*$ . Accordingly, in this case, the value of (63) equals to (57). Since, in addition, in this example, the condition in (37) is more stringent than the condition in (38), we obtain  $\xi^*(R, T) = \xi_L(R, T)$ . The conclusion that stems from this observation is that, in this case, the analysis in [15] is tight.

*Example 1* In [15], a family of BSCs was considered where  $\theta \in \Theta$  designates the cross-over probability of the BSC, and  $\Theta = \{0, 1/100, 2/100, \dots, 1\}$ . The values of  $\xi_L(R, T)$  were computed for various values of  $R$  and  $T$ . It was assumed that  $T \geq 0$ , which means that the decoder operates in the erasure mode. Numerical calculations of the bound derived in this work (and the exact formula), result in exactly the same values as given in [15, Table 1], and so in all these cases, the analysis of [15] was sufficient to provide tight results. For example, for  $(R, T) = (0.05, 0.15)$ , and codebook type  $P_X = (1/2, 1/2)$ , we obtain  $\xi_L(R, T) = 0.495$ . Also, the two worst case channels (i.e., the solutions to (63)) are  $\theta^* = 0.18$  and  $\theta''^* = 0.22$  while  $\theta'^* = \theta^*$  and  $\rho^* = 0.36 > s^* = 0.185$ . So, since  $s^* < \rho^*$  and  $\theta'^* = \theta^*$ , the discussion above implies that a tight result is obtained, that is,  $\xi^*(R, T) = \xi_L(R, T) = 0.495$ . Thus, in the worst case over all  $\theta \in \Theta$ , the exponent  $\hat{E}_1(R, T, \theta)$  is not less than  $0.495 \cdot E_1(R, T, \theta)$ .

Since  $\xi^*(R, T) < 1$  for some  $R$  and  $T$ , we arrive at the following conclusion: *In general, in the random coding regime of erasure/list decoding, there is no universal decoder which achieves the same error exponent as Forney's decoder for every channel in the class.* This fact is in contrast to ordinary decoding, in which the MMI decoder achieves the exact same error exponent as the ML decoder. In this sense, knowledge of

<sup>6</sup>If for a given real function  $f(u, v)$  the minimizer  $v^*$  w.r.t.  $v$  does not depend on  $u$ , then  $\max_{u \in \mathcal{U}} \min_{v \in \mathcal{V}} f(u, v) = \max_{u \in \mathcal{U}} f(u, v^*) \geq \min_{v \in \mathcal{V}} \max_{u \in \mathcal{U}} f(u, v)$ , and the minimax inequality results  $\max_{u \in \mathcal{U}} \min_{v \in \mathcal{V}} f(u, v) = \min_{v \in \mathcal{V}} \max_{u \in \mathcal{U}} f(u, v)$ , assuming that  $\mathcal{U}$  and  $\mathcal{V}$  are two independent sets (i.e., rectangular).

the channel is crucial when erasure/list options are allowed. The possible difficulty of universalizing an erasure decoder is apparent for the BSC: While for ordinary decoding, the optimal detector depends only on whether  $\theta \leq 1/2$  or  $\theta > 1/2$  (i.e., minimum distance versus maximum distance decoders, respectively), and thus rather easy to universalize, the optimal erasure decoder depends on the exact value of  $\theta$ .

Nonetheless, in general, we might have that  $\xi_L(R, T)$  is strictly less than  $\xi^*(R, T)$ . Again, assume that the condition in (37) dominates  $\xi^*(R, T)$ . To provide intuition, notice that in (63) *triplets*  $(\theta, \theta', \theta'') \in \Theta^3$  are optimized, in contrast to (57), where only *pairs* of channels  $(\theta, \theta'') \in \Theta^2$  are optimized. Thus, for a family of only two channels, namely,  $|\Theta| = 2$ , typically (but not necessarily) the second difference above, of imposing the constraint  $\theta' = \theta$ , is immaterial. Then, the only difference between the conditions in (57) and (63) is the constraint  $s \leq \rho$ . Let us assume that this is indeed the case, and let us notice that  $s$  can be thought as a Lagrange multiplier for the constraint

$$\mathbb{E}_{\tilde{Q}} \log W_{\theta'}(Y|X) + \xi E_1(R, T, \theta') - \mathbb{E}_Q \log W_{\theta''}(Y|X) - \xi E_1(R, T, \theta'') - T \leq 0. \quad (64)$$

Now, if the constraint, at the optimal solution, is slack, then the optimal Lagrange multiplier is  $s^* = 0$ . In this case, the constraint  $s \leq \rho$  is immaterial and so (57) and (63) are exactly the same. However, as we shall see in the sequel, it is possible that  $s^* > \rho^*$  in (63), and then the values of the objective in (57) and (63) are different. Observing (64), it is apparent that as  $T$  decreases, and especially in the list mode of  $T < 0$ , the optimal  $s^*$  of (63) increases, perhaps beyond the optimal  $\rho^*$ . Thus, if both  $s^* > \rho^*$  and the condition in (37) dominates  $\xi^*(R, T)$ , we get that  $\xi_L(R, T) < \xi^*(R, T)$ . The following example provides such a simple case. We remark, that such a phenomenon was already observed in a Slepian-Wolf erasure/list decoding scenario, for a known source [19]. There too, in the list regime of  $T < 0$ , there is a gap between the Forney-style bound and the exact random binning error exponents.

*Example 2* Consider a family of two BSCs, where  $\Theta = \{0.1, 0.15\}$ , and a type  $P_X = (1/2, 1/2)$  for the random fixed composition codebook. We take  $(R, T) = (0.4, -0.25)$ , and since  $T < 0$ , the decoder operates in the list mode. We obtain that  $\xi_L(R, T) = 0.716$  which is strictly less than  $\xi^*(R, T) = 0.727$ . In the optimization problem (57), the optimal values are  $\rho^* = s^* = 0.231$ , while if the constraint  $s \leq \rho$  is relaxed, then the optimal values are  $s = 0.231 > \rho = 0.217$ . The resulting value of the optimization problem is exactly 0.727, just as  $\xi^*(R, T)$ . Moreover, for this example, the largest achievable  $\xi$  which satisfies condition (37) is the same for condition (38). While the difference between  $\xi_L(R, T)$  and  $\xi^*(R, T)$  is not very large, it is nevertheless existent and in more intricate scenarios, the differences might be more significant.

## V. DECODING WITH TRAINING

Usually, in practical communication systems with channel uncertainty, a portion of the blocklength is devoted to a

training sequence which is common to all codewords. This sequence is aimed for learning the unknown channel. In this section, we will first define random coding ensembles which incorporate a training sequence. Then, we shall propose and compare two decoders for this scenario: the (asymptotically optimal) universal decoder in (31), and a “plug-in” decoder, which first estimates the channel using the training sequence, and then decodes the remaining symbols of the codeword using the estimated channel.

### A. Definition of training ensembles

For reasons that will be clear in the sequel, we consider two variants of an ensemble which incorporate a training sequence. In the first ensemble, we fix a portion<sup>7</sup>  $\alpha \in [0, 1)$  of the blocklength  $n$ . Then, a training sequence<sup>8</sup>  $\bar{x} \in \mathcal{X}^{\alpha n}$  is chosen<sup>9</sup> within type  $\bar{P}_X$ , and  $M = e^{nR}$  codewords  $\tilde{x}_m \in \mathcal{X}^{(1-\alpha)n}$ ,  $m = 1, 2, \dots, M$ , are selected at random, uniformly within a type class  $\mathcal{T}(P_X)$  for some given random coding distribution  $P_X$  over the alphabet  $\mathcal{X}$ . The transmitted codewords are then the concatenations  $x_m = (\bar{x}, \tilde{x}_m)$  for  $1 \leq m \leq M$ . In the second ensemble, the blocklength of  $M = e^{nR}$  codewords  $\tilde{x}_m \in \mathcal{X}^n$ ,  $m = 1, 2, \dots, M$ , remains  $n$ , but the codewords are prefixed with a training sequence of length  $\beta n$ , where  $\beta \geq 0$ . The later ensemble leads of course to a reduction of the effective rate to  $R_{\text{eff}} = R/(1 + \beta)$ . Since the channel is a DMC, it can be easily verified that only the type of the training sequence  $\bar{P}_X$  will affect performance, but not the particular sequence within the type class  $\mathcal{T}(\bar{P}_X)$ . Evidently, when  $\alpha = 0$  or  $\beta = 0$ , we revert to the ordinary random coding ensemble. Finally, it is important to emphasize that there is an inherent trade-off in using training (i.e., taking  $\alpha > 0$  or  $\beta > 0$ ): learning time comes at the expense of effective blocklength and vice-versa.

### B. Universal decoder

Whenever  $\xi^*(R, T) < 1$ , one can hope to improve  $\xi^*(R, T)$  by using the training ensemble<sup>10</sup> defined above with  $\alpha > 0$ , along with the *asymptotically optimal decoder* in (31). That is, even though the first  $\alpha n$  symbols are the same for all codewords, the decoder computes the metric  $f(x_m, \mathbf{y})$  for the entire codeword. With a slight abuse of notation, we may denote the maximal fraction achieved by this decoder as  $\xi^*(R, T, \alpha, \bar{P}_X)$ , for  $\alpha \in [0, 1)$ , and then  $\alpha = 0$  corresponds to the ordinary fixed-composition ensemble, considered in Subsection IV-A. The methods used to prove Theorem 1, can be generalized to obtain  $\xi^*(R, T, \alpha, \bar{P}_X)$ , and in Appendix

<sup>7</sup>As discussed in [7, Appendix I], achieving the random coding error exponent when using a plug-in decoder with a training sequence of length  $\alpha n$  such that  $\alpha n \rightarrow 0$  is not possible, even for ordinary decoding. In a nutshell, the error exponent of the plug-in decoder is not degraded by the estimation error of the channel only when the length of the training sequence is a linear function of  $n$ . For this reason, we consider a training sequence of length  $\alpha n$ , where  $\alpha$  is a constant fraction.

<sup>8</sup>Henceforth, over-bar will indicate quantities which are related to the training part.

<sup>9</sup>For brevity, integer constraints will be omitted.

<sup>10</sup>In this subsection, we will describe our results only for the first ensemble (defined by  $\alpha$ ), but similar results can be readily derived for the second ensemble (defined by  $\beta$ ).

B, a closed-form formula for  $\xi^*(R, T, \alpha, \bar{P}_X)$ , with a proof outline, are provided. Nonetheless, we suspect that, in fact,  $\xi^*(R, T, \alpha, \bar{P}_X)$  cannot be improved in this way, namely, choosing  $\alpha = 0$  is optimal.

To gain intuition for the explanation of this phenomena, we focus on two codewords only,  $\tilde{x}_1$  and  $\tilde{x}_2$ , of length  $(1 - \alpha)n$ . In ordinary decoding for a known channel, the decision on the decoded codeword is made only on the basis of the *order* between the likelihoods of both codewords, i.e.,  $W_\theta(\tilde{\mathbf{y}}|\tilde{x}_1) \leq W_\theta(\tilde{\mathbf{y}}|\tilde{x}_2)$ . On the other hand, in erasure/list decoding for a known channel, the actual likelihood *values* are of importance due to the multiplication of the competing likelihood by  $e^{(1-\alpha)nT}$  (recall that, for example, the first codeword is selected only if  $W_\theta(\tilde{\mathbf{y}}|\tilde{x}_1) > e^{(1-\alpha)nT} \cdot W_\theta(\tilde{\mathbf{y}}|\tilde{x}_2)$ ). Now, if a common prefix (training sequence) is added to both codewords (and transmitted over the channel), clearly the likelihood of the first part  $W_\theta(\bar{\mathbf{y}}|\bar{x})$  is the same for both codewords. Let the combined codewords be  $x_1 = (\bar{x}, \tilde{x}_1)$  and  $x_2 = (\bar{x}, \tilde{x}_2)$ , and the combined channel output be  $\mathbf{y} = (\bar{\mathbf{y}}, \tilde{\mathbf{y}})$ . Then, while the order between the combined likelihoods is preserved  $W_\theta(\mathbf{y}|x_1) \leq W_\theta(\mathbf{y}|x_2)$ , as the blocklength is now  $n$  and not  $(1 - \alpha)n$ , the ratio between the values of the two likelihoods (or its inverse), now has to exceed  $e^{nT}$ , rather than the smaller value of  $e^{(1-\alpha)nT}$ , so that erasure will not be decided.

This occurs also in the case of an unknown channel, namely, for the universal decoder in (31), and in the extreme cases for which  $\alpha$  is close to 1, it may happen that only erasures are decided, which leads to a zero total error exponent. For small and moderate values of  $\alpha$  the total error exponent may not be zero, but is still nonetheless worse than the exponent achieved with  $\alpha = 0$ . For the family of BSCs in Example 1, we have numerically verified that  $\alpha = 0$  for all rates and thresholds. We conjecture that this holds for more general families of channels.

### C. Plug-in decoder

A possible practical decoder (termed “plug-in” decoder), for the training ensembles defined, works in two stages: First, the decoder estimates the channel using the known training sequence, and then uses this estimated channel in place of the true (unknown) channel in using Forney’s decoder (4)-(5), for the remaining symbols of the codeword. This sub-optimal decoder, and the competitive minimax decoder in (31), are two extremes. Indeed, the decoder in (31) achieves  $\xi^*(R, T)$  but may have rather high implementation complexity. The plug-in decoder, on the one hand, has smaller complexity, and thus can be more easily incorporated into practical systems<sup>11</sup>, but on the other hand, achieves only some  $\xi^e(R, T) \leq \xi^*(R, T)$  (to be rigorously defined in the sequel). Therefore, if  $\xi^e(R, T) \ll \xi^*(R, T)$  then there is substantial motivation to use the more complex decoder (31). If, however,  $\xi^e(R, T) \approx \xi^*(R, T)$  then the plug-in decoder is sufficient to almost achieves the optimal performance, while still keeping a reasonable implementation

<sup>11</sup>If, e.g., the code has some structure and the decoder for a known channel can be implemented for any  $\theta \in \Theta$ , then the plug-in decoder for an unknown channel only requires an additional estimation step.

complexity. In this subsection, we analyze the competitive minimax performance of the plug-in decoder.

As mentioned above, the training part,  $\bar{x}$ , shall be used by the decoder to estimate the channel (this is the first stage). Let us split the output vector  $\mathbf{y}$  into two parts  $(\bar{\mathbf{y}}, \hat{\mathbf{y}})$ , where the first part corresponds to the training. The channel estimator is a function  $\hat{\theta}(\bar{Q}) \in \Theta$ , where  $\bar{Q} = \bar{Q}_{\bar{x}\bar{\mathbf{y}}}$ . Then, in the second stage, optimal decoding (for a known channel) is employed for the remaining symbols of the codeword, assuming that the channel is  $W_{\hat{\theta}(\bar{Q})}$ . Let us denote this plug-in decoder by  $\mathcal{R}^e$ , and its associated exponents by  $E_i^e(R, T, \theta, \alpha)$ , for  $i = 1, 2$  for the first ensemble, and  $E_i^e(R, T, \theta, \beta)$  for the second ensemble. To analyze these exponents let  $E_i^m(R, T, \theta, \hat{\theta})$  for  $i = 1, 2$ , designate the error exponents associated with the optimal decoder for a known channel, when tuned to the channel  $W_{\hat{\theta}(\bar{Q})}$ , but used over the channel  $W_\theta$  (i.e., *mismatched decoder*), for the ordinary fixed-composition ensemble (without training). Then, a routine method of types argument reveals that

$$E_i^e(R, T, \theta, \alpha) = \min_{\bar{Q}: \bar{Q}_X = \bar{P}_X} \left\{ \alpha \cdot D(\bar{Q} \| \bar{P}_X \times W_\theta) + (1 - \alpha) \cdot E_i^m(R, T, \theta, \hat{\theta}(\bar{Q})) \right\}, \quad (65)$$

$$\check{E}_i^e(R, T, \theta, \beta) = \min_{\bar{Q}: \bar{Q}_X = \bar{P}_X} \left\{ \beta \cdot D(\bar{Q} \| \bar{P}_X \times W_\theta) + E_i^m(R, T, \theta, \hat{\theta}(\bar{Q})) \right\}, \quad (66)$$

for  $i = 1, 2$ . Now,  $E_i^m(R, T, \theta, \hat{\theta})$  can be obtained by simply replacing every instance of  $\mathbb{E}_{\bar{Q}} \log W_\theta(Y|X)$ , which represent the log-likelihoods assuming the correct channel, with the mismatched log-likelihoods  $\mathbb{E}_{\bar{Q}} \log W_{\hat{\theta}(\bar{Q})}(Y|X)$  in the exponent expressions of [18, Theorem 1 and Theorem 2]<sup>12</sup>. Note, however, that since a mismatched decoder is, in general, sub-optimal, Lemma 1 *cannot* be used, and the equality  $E_2^m(R, T, \theta, \hat{\theta}) = E_1^m(R, T, \theta, \hat{\theta}) + T$  may not necessarily hold. Thus, in the mismatched case, the expression for  $E_2^m(R, T, \theta, \hat{\theta})$  (see, [18, Theorem 2]) must be used, along with the above replacement (to obtain  $E_2^m(R, T, \theta, \hat{\theta})$ ). It should be stressed, however, that the expression for  $E_2^m(R, T, \theta, \hat{\theta})$  in [18, Theorem 2] is valid only for the erasure mode<sup>13</sup>, i.e.,  $T \geq 0$ , which shall be assumed henceforth. Finally, as can be seen from the above expressions, we need to define/find the estimator  $\hat{\theta}(\bar{Q})$ . If, e.g.,  $\Theta$  is the family of all DMCs, with input alphabet  $\mathcal{X}$  and output alphabet  $\mathcal{Y}$ , then the *maximum likelihood estimator* can be used, which in this case, is just the parameter  $\theta$  which corresponds to  $\bar{Q}_{Y|X}$  where  $\bar{Q} = \hat{Q}_{\bar{x}\bar{\mathbf{y}}}$ . A different example is the family of all BSCs, and

<sup>12</sup>As mentioned before, in [18] the i.i.d. ensemble was assumed. The modification to the fixed-composition ensemble is straightforward, and only requires removing the  $D(Q_X \| P_X)$  terms.

<sup>13</sup>In general, the undetected error probability event (pertaining to the error exponent  $E_2$ ), is more difficult to analyze than the total error event (pertaining to the error exponent  $E_1$ ), and in [18],  $E_2$  was only analyzed for the erasure regime. The difficulty stems from the fact that the analysis in [18] is possible only for disjoint decoding regions, which is not the case in the list regime. Unfortunately, a direct analysis (namely, without relying on the relation  $E_2 = E_1 + T$ , which might be wrong for the plug-in decoder) of the undetected error exponent in the list regime is much more challenging.

in this case the maximum likelihood (ML) estimator is simply  $\hat{Q}_{\bar{x}\bar{\mathbf{y}}}(X \neq Y)$ .

At this point, we can use the definition of the competitive criterion  $K_n(\mathcal{C}, \mathcal{R}^e)$  in (28), and define  $\bar{K}_n^e \triangleq \mathbb{E} \{K_n(\mathcal{C}, \mathcal{R}^e)\}$ , where the expectation is w.r.t. the first training ensemble defined above. As before, for a given rate  $R$  and threshold  $T$ , we will be interested in the maximal achievable  $\xi$  such that

$$\xi^e(R, T, \alpha, \bar{P}_X) \triangleq \sup \left\{ \xi \in [0, 1] : \limsup_{n \rightarrow \infty} \frac{1}{n} \log \bar{K}_n^e \leq 0 \right\}. \quad (67)$$

The above definition sets the stage for a reasonable criterion of optimal training, which includes both the relative training time and the optimal (type of the) training sequence. In other words, the training fraction  $\alpha$  and training type  $\bar{P}_X$  can be optimized to obtain,

$$\xi^e(R, T) \triangleq \max_{0 < \alpha < 1} \max_{\bar{P}_X} \xi^e(R, T, \alpha, \bar{P}_X). \quad (68)$$

Contrary to the universal decoder considered in the previous subsections, here, we can easily extract  $\xi^e(R, T, \alpha, \bar{P}_X)$ , as it appears only in the denominator of (28). Indeed, letting  $E_i^e(R, T, \theta)$ , for  $i = 1, 2$ , be the error exponents associated with the plug-in decoder  $\mathcal{R}^e$ , and the training ensemble defined above, using (28) and (67), it is easy to verify that (69)-(71), shown at the top of the next page, hold. Similar results can be obtained for the second training ensemble. Note that for the second ensemble  $\xi$  should be monotonically increasing with  $\beta$ , because the more we train the plug-in decoder, the better we compete with the informed decoder. Accordingly, when  $\beta \rightarrow \infty$  the plug-in decoder actually knows the channel, so the maximal  $\xi$  should be trivially one, but  $R_{\text{eff}}$  is zero. In between these two extremes, we get the entire spectrum of trade-offs between the maximal  $\xi$  and  $R_{\text{eff}}$ .

#### D. Numerical examples

Consider the setting of Example 1, in which a family of BSCs is studied where  $\theta \in \Theta$  designates the cross-over probability of the BSC, and  $\Theta = \{0, 1/100, 2/100, \dots, 1\}$ . Due to the symmetry of the channels, we take  $P_X = \bar{P}_X = (1/2, 1/2)$ . The plug-in decoder employs the ML estimator in the initial estimation stage to estimate the unknown crossover probability.

For a given rate  $R$  and threshold  $T$  we will plot the error exponent achieved for any given  $\theta \in \Theta$  by the various decoders. In light of the discussion in Subsection V-B, for both the optimal decoder for a known channel and the universal decoder (31), we will assume that there is no training, i.e.,  $\alpha = 0$  (or,  $\beta = 0$ ). From the proof of Theorem 1, it is evident that the exponents achieved by the universal decoder (31) are given by

$$E_1^u(R, T, \theta) \triangleq \min \left\{ \min_{\tilde{Q} \in \mathcal{L}} D(\tilde{Q} \| P_X \times W_\theta), \min_{(\tilde{Q}, \tilde{Q}) \in \mathcal{Q}} \left\{ D(\tilde{Q} \| P_X \times W_\theta) + I(\tilde{Q}) - R \right\} \right\}, \quad (72)$$

$$\xi^e(R, T, \alpha, \bar{P}_X) = \min_{\theta \in \Theta} \left\{ -\frac{1}{E_1(R, T, \theta)} \left[ T + \limsup_{n \rightarrow \infty} \frac{1}{n} \mathbb{E} \{ \Gamma_\theta(\mathcal{C}, \mathcal{R}^e) \} \right] \right\} \quad (69)$$

$$= \min_{\theta \in \Theta} \left\{ -\frac{1}{E_1(R, T, \theta)} [T - \min \{ E_1^e(R, T, \theta) + T, E_2^e(R, T, \theta) \}] \right\} \quad (70)$$

$$= \min_{\theta \in \Theta} \left\{ \frac{1}{E_1(R, T, \theta)} [\min \{ E_1^e(R, T, \theta), E_2^e(R, T, \theta) - T \}] \right\}. \quad (71)$$

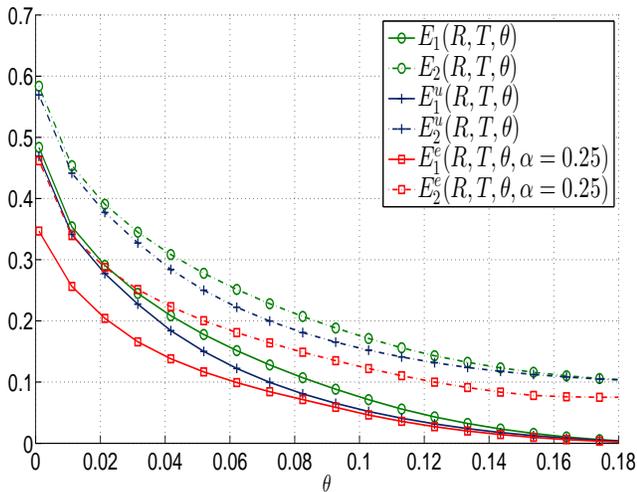


Fig. 1. Comparison of the error exponents achieved by the optimal decoder for known channel, universal decoder, and the plug-in decoder, as a function of  $\theta$ , for  $R = T = 0.1$ ,  $\xi^*(R, T) = 0.66$ , and using the first ensemble with  $\alpha = 0.25$ .

and  $E_2^u(R, T, \theta) = E_1^u(R, T, \theta) + T$ , due to Lemma 2 (see, Appendix A). To evaluate (72), in every instance of  $\xi$  (e.g., (33)), we substitute  $\xi^*(R, T)$  which was already calculated in Example 1. Finally, the exponents of the plug-in decoder are given in (65) and (66), for the two ensembles, respectively. In our simulations, we choose  $R = T = 0.1$ , for which  $\xi^*(R, T) = 0.66$ , and we use  $\alpha = 0.25$ , which turns out to be the (approximately) optimal length of the training sequence, for all  $\theta \in \Theta$ . Fig. 1 compares the error exponents achieved by the various decoders (i.e., optimal decoder for known channel, universal decoder, and plug-in decoder), as a function of  $\theta$ , using the first ensemble (defined via  $\alpha$ ) for the plug-in decoder. It can be seen that there is a noticeable loss in using the plug-in decoder compared to the universal decoder. Fig. 2 compares the error exponents achieved by the various decoders, as a function of  $\theta$ , using the second ensemble (defined via  $\beta$ ) for the plug-in decoder, using two values of  $\beta$ . From this figure, it can be seen that for  $\beta = 0.32$  the performance of the plug-in decoder are close to the universal decoder, and for  $\beta = 0.5$  the performance are fairly close to the known channel decoder. Recall, however, that the price in using  $\beta = 0.32$  and  $\beta = 0.5$  is an effective rate of  $R_{\text{eff}} = 0.76 \cdot R$  and  $R_{\text{eff}} = (2/3) \cdot R$ , respectively.

*Remark 1* Remarkably, in our numerical calculations we get that  $\xi^e(R, T) = 0$  (defined in (68)), for all  $R \geq 0$  and

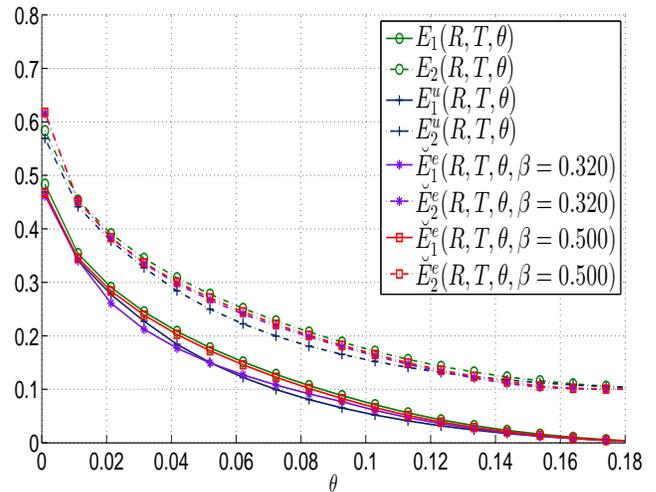


Fig. 2. Comparison of the error exponents achieved by the optimal decoder for known channel, universal decoder, and the plug-in decoder, as a function of  $\theta$ , for  $R = T = 0.1$ ,  $\xi^*(R, T) = 0.66$ , and using the second ensemble with  $\beta = 0.32, 0.5$ .

$T > 0$ . This result may be attributed to the fact that our competitive criterion implicitly assumes that the difference between the total error exponent and the undetected error exponent is  $T$  (and rightfully, as this is true for both the optimal decoder in the case of a known channel, and for the asymptotically optimal decoder in the case of unknown channel). However, this is not necessarily true for the plug-in decoder, and  $E_2^e(R, T, \theta)$  maybe less than  $E_1^e(R, T, \theta) + T$ , and so the undetected error exponent of the plug-in decoder poorly competes with  $\xi \cdot E_1(R, T, \theta) + T$  (recall the definition in (26)). For this example, no value of  $\alpha$  has produced  $E_2^e(R, T, \theta) \geq T$  uniformly over  $\theta \in \Theta$  and this resulted in the zero values  $\xi^e(R, T)$  (recall (71)). So, even in this relatively simple example, using a plug-in decoder will cause a significant loss in error exponents. In light of this result, a less pessimistic criterion, could be

$$\min_{\mathcal{R}} \max_{\theta \in \Theta} \frac{\Gamma_\theta(\mathcal{C}, \mathcal{R})}{e^{-n[\bar{\xi} \cdot E_1(R, T, \theta) + \bar{\xi} T]}}, \quad (73)$$

where now  $T$  is also multiplied by  $\bar{\xi}$ . A fraction  $\bar{\xi}$  achieved under this criterion implies that the plug-in decoder simultaneously achieves exponents of  $E_1^e(R, T, \theta) \geq \bar{\xi} \cdot E_1(R, T, \theta)$  and  $E_2^e(R, T, \theta) \geq \bar{\xi} \cdot E_2(R, T, \theta) = \bar{\xi} \cdot (E_1(R, T, \theta) + T)$  for all  $\theta \in \Theta$ . The analysis of the maximal achievable fraction  $\bar{\xi}(R, T)$  that pertains to (73) is the same as for  $\xi^e(R, T)$  under the original criterion. Of course, this alternative criterion will

lead to different numerical values for  $\xi^e(R, T)$  (specifically, positive values for  $T > 0$ ).

## VI. PROOFS

In the following, for simplicity of notations, we omit the dependency of the various quantities on  $R, T$ , and  $\xi$ , as they remain constants along the proofs, e.g.,  $\Omega(R, T, \xi, Q, \tilde{Q})$  will be replaced with  $\Omega(Q, \tilde{Q})$ .

*Proof of Theorem 1:* We analyze the total error term, following the steps of [18, Section V]. As was mentioned earlier, we want to assess the (exact) exponential behavior of  $\mathbb{E} [K_n(\mathcal{C}, \hat{\mathcal{R}})]$ . In [15, Theorem 2], an upper bound was derived on this quantity, so here we seek a tight lower bound. Let  $\Theta_n$  denote the set of values of  $\theta$  that achieve the maximum at the right-hand side of (30) for some  $\mathbf{x} \in \mathcal{X}^n, \mathbf{y} \in \mathcal{Y}^n$ . Note that the elements of  $\Theta_n$  depend on  $\mathbf{x}$  and  $\mathbf{y}$  only through their joint type, and whence, we have that  $|\Theta_n| \leq (n+1)^{|\mathcal{X}^n| |\mathcal{Y}^n| - 1}$ , i.e. the size of  $\Theta_n$  is a polynomial function of  $n$ . Now,

$$\begin{aligned}
\mathbb{E} [K_n(\mathcal{C}, \hat{\mathcal{R}})] &= \mathbb{E} \left\{ \max_{\theta \in \Theta} \frac{\Gamma_\theta(\mathcal{C}, \hat{\mathcal{R}})}{e^{-n(\xi E_1(\theta) + T)}} \right\} \\
&\geq \mathbb{E} \left\{ \max_{\theta \in \Theta_n} \frac{\Gamma_\theta(\mathcal{C}, \hat{\mathcal{R}})}{e^{-n(\xi E_1(\theta) + T)}} \right\} \\
&\stackrel{(a)}{=} \mathbb{E} \left\{ \sum_{\theta \in \Theta_n} \frac{\Gamma_\theta(\mathcal{C}, \hat{\mathcal{R}})}{e^{-n(\xi E_1(\theta) + T)}} \right\} \\
&\stackrel{(b)}{=} \mathbb{E} \left\{ \sum_{\theta \in \Theta_n} \frac{\frac{1}{M} \sum_{m=1}^M \sum_{\mathbf{y} \in \hat{\mathcal{R}}_m} \sum_{m' \neq m} W_\theta(\mathbf{y} | \mathbf{X}_{m'})}{e^{-n(\xi E_1(\theta) + T)}} \right. \\
&\quad \left. + \frac{\frac{1}{M} \sum_{m=1}^M \sum_{\mathbf{y} \in \hat{\mathcal{R}}_m^c} e^{-nT} W_\theta(\mathbf{y} | \mathbf{X}_m)}{e^{-n(\xi E_1(\theta) + T)}} \right\} \\
&= \mathbb{E} \left\{ \frac{1}{M} \sum_{m=1}^M \sum_{\mathbf{y} \in \hat{\mathcal{R}}_m} \sum_{m' \neq m} \sum_{\theta \in \Theta_n} e^{n(\xi E_1(\theta) + T)} W_\theta(\mathbf{y} | \mathbf{X}_{m'}) \right\} \\
&\quad + \mathbb{E} \left\{ \frac{1}{M} \sum_{m=1}^M \sum_{\mathbf{y} \in \hat{\mathcal{R}}_m^c} \sum_{\theta \in \Theta_n} e^{n\xi E_1(\theta)} W_\theta(\mathbf{y} | \mathbf{X}_m) \right\} \\
&\stackrel{(c)}{=} \mathbb{E} \left\{ \frac{1}{M} \sum_{m=1}^M \sum_{\mathbf{y} \in \hat{\mathcal{R}}_m} \sum_{m' \neq m} \max_{\theta \in \Theta_n} e^{n(\xi E_1(\theta) + T)} W_\theta(\mathbf{y} | \mathbf{X}_{m'}) \right\} \\
&\quad + \mathbb{E} \left\{ \frac{1}{M} \sum_{m=1}^M \sum_{\mathbf{y} \in \hat{\mathcal{R}}_m^c} \max_{\theta \in \Theta_n} e^{n\xi E_1(\theta)} W_\theta(\mathbf{y} | \mathbf{X}_m) \right\} \\
&= \mathbb{E} \left\{ \frac{1}{M} \sum_{m=1}^M \sum_{\mathbf{y} \in \hat{\mathcal{R}}_m} \sum_{m' \neq m} f(\mathbf{X}_{m'}, \mathbf{y}) \right\} \\
&\quad + \mathbb{E} \left\{ \frac{1}{M} \sum_{m=1}^M \sum_{\mathbf{y} \in \hat{\mathcal{R}}_m^c} e^{-nT} f(\mathbf{X}_m, \mathbf{y}) \right\} \tag{74}
\end{aligned}$$

where in (a) and (c) we have used the fact that the size of  $\Theta_n$  is polynomial, and thus can be absorbed in the  $e^{nT}$  factor (see, [18, pp. 5, footnote 2]), and (b) follows from (8). As was shown in [15, eq. after (A.1)], the lower bound in (74) is, in

fact, also an upper bound on  $\mathbb{E} [K_n(\mathcal{C}, \hat{\mathcal{R}})]$ . Therefore, in the exponential scale, nothing was lost due to the above bounding, and we essentially have that

$$\begin{aligned}
\mathbb{E} [K_n(\mathcal{C}, \hat{\mathcal{R}})] &\doteq \mathbb{E} \left\{ \frac{1}{M} \sum_{m=1}^M \sum_{\mathbf{y} \in \hat{\mathcal{R}}_m} \sum_{m' \neq m} f(\mathbf{X}_{m'}, \mathbf{y}) \right\} \\
&\quad + \mathbb{E} \left\{ \frac{1}{M} \sum_{m=1}^M \sum_{\mathbf{y} \in \hat{\mathcal{R}}_m^c} e^{-nT} f(\mathbf{X}_m, \mathbf{y}) \right\}. \tag{75}
\end{aligned}$$

Contrary to the proof technique used in [15] to assess the exponential behavior of (75), where Chernoff and Jensen bounds were invoked, here, we will evaluate the *exact* exponential scale of the two terms on the right hand side of (75). It can be noticed that the first expression is related to undetected errors (or average number of incorrect codewords on the list), and the second one is related to the total error (erasures and undetected errors). For brevity, we define

$$A_1 \triangleq e^{-nT} \cdot \mathbb{E} \left\{ \frac{1}{M} \sum_{m=1}^M \sum_{\mathbf{y} \in \hat{\mathcal{R}}_m^c} f(\mathbf{X}_m, \mathbf{y}) \right\}, \tag{76}$$

and

$$A_2 \triangleq \mathbb{E} \left\{ \frac{1}{M} \sum_{m=1}^M \sum_{\mathbf{y} \in \hat{\mathcal{R}}_m} \sum_{m' \neq m} f(\mathbf{X}_{m'}, \mathbf{y}) \right\}, \tag{77}$$

and so

$$\mathbb{E} [K_n(\mathcal{C}, \hat{\mathcal{R}})] \doteq A_1 + A_2. \tag{78}$$

As was mentioned before, we would like to analyze the exponential rate of (75), or, equivalently, of (76) and (77). Now, note that,

$$\begin{aligned}
\lim_{n \rightarrow \infty} \frac{1}{n} \log \mathbb{E} [K_n(\mathcal{C}, \hat{\mathcal{R}})] \\
= \max \left\{ \lim_{n \rightarrow \infty} \frac{1}{n} \log A_1, \lim_{n \rightarrow \infty} \frac{1}{n} \log A_2 \right\}, \tag{79}
\end{aligned}$$

whenever all the limits exist. Then, a fraction  $\xi$  is *achievable* if both  $n^{-1} \log A_1$  and  $n^{-1} \log A_2$  converge to a non-positive constant as  $n \rightarrow \infty$ . Let us begin with the evaluation of  $A_1$ . Continuing from (76), we get (80)-(84), shown at the top of the next page, where (a) follows from the symmetry of the random coding mechanism, and the probability in the last equation is over the random choice of  $\{\mathbf{X}_{m'}\}_{m' \neq m}$ , which determines  $\hat{\mathcal{R}}_m$ . Now, if  $Q$  is the joint empirical probability distribution (defined on  $\mathcal{X} \times \mathcal{Y}$ ) of  $\mathbf{x}_{m'}$  and  $\mathbf{y}$ , then,

$$f(\mathbf{x}_{m'}, \mathbf{y}) = \max_{\theta \in \Theta} \left\{ e^{n(\xi E_1(\theta) + T)} W_\theta(\mathbf{y} | \mathbf{x}_{m'}) \right\} \tag{85}$$

$$= \max_{\theta \in \Theta} \left\{ e^{n(\xi E_1(\theta) + T)} e^{n\mathbb{E}_Q \log W_\theta(Y|X)} \right\} \tag{86}$$

$$= \exp \left[ n \cdot \max_{\theta \in \Theta} \{ (\xi E_1(\theta) + T) + \mathbb{E}_Q \log W_\theta(Y|X) \} \right] \tag{87}$$

$$= \exp [n \cdot G(Q)], \tag{88}$$

where

$$G(Q) \triangleq \max_{\theta \in \Theta} \left\{ \xi E_1(\theta) + T + \mathbb{E}_Q \log W_\theta(Y|X) \right\}. \tag{89}$$

$$A_1 = e^{-nT} \mathbb{E} \left\{ \frac{1}{M} \sum_{m=1}^M \sum_{\mathbf{y}} f(\mathbf{X}_m, \mathbf{y}) \cdot \mathcal{I}\{\mathbf{y} \in \hat{\mathcal{R}}_m^c\} \right\} \quad (80)$$

$$\stackrel{(a)}{=} e^{-nT} \mathbb{E} \left\{ \sum_{\mathbf{y}} f(\mathbf{X}_m, \mathbf{y}) \cdot \mathcal{I}\{\mathbf{y} \in \hat{\mathcal{R}}_m^c\} \middle| m\text{th message transmitted} \right\} \quad (81)$$

$$= e^{-nT} \sum_{\mathbf{y}} \mathbb{E} \left\{ f(\mathbf{X}_m, \mathbf{y}) \cdot \mathcal{I}\{\mathbf{y} \in \hat{\mathcal{R}}_m^c\} \middle| m\text{th message transmitted} \right\} \quad (82)$$

$$= e^{-nT} \sum_{\mathbf{x}_m} P_X(\mathbf{X}_m = \mathbf{x}_m) \sum_{\mathbf{y}} \mathbb{E} \left\{ f(\mathbf{X}_m, \mathbf{y}) \cdot \mathcal{I}\{\mathbf{y} \in \hat{\mathcal{R}}_m^c\} \middle| \mathbf{X}_m = \mathbf{x}_m, m\text{th message transmitted} \right\} \quad (83)$$

$$= e^{-nT} \sum_{\mathbf{x}_m} P_X(\mathbf{X}_m = \mathbf{x}_m) \sum_{\mathbf{y}} f(\mathbf{x}_m, \mathbf{y}) \cdot \Pr \left\{ \mathbf{y} \in \hat{\mathcal{R}}_m^c \middle| \mathbf{X}_m = \mathbf{x}_m, m\text{th message transmitted} \right\} \quad (84)$$

Next, we shall focus on the latter probability in (84). For a given  $\mathbf{x}_m$  and  $\mathbf{y}$ , let  $\tilde{Q} = \hat{P}_{\mathbf{x}_m \mathbf{y}}$ , and let  $N_{\mathbf{y}}(Q)$  denote the number of codewords (excluding  $\mathbf{x}_m$ ) whose joint empirical probability distribution with a given  $\mathbf{y}$  is  $Q$ . Accordingly, we have that

$$\begin{aligned} & \Pr \left\{ \mathbf{y} \in \hat{\mathcal{R}}_m^c \middle| \mathbf{X}_m = \mathbf{x}_m, \mathbf{Y} = \mathbf{y} \right\} \\ &= \Pr \left\{ \sum_{m' \neq m} f(\mathbf{X}_{m'}, \mathbf{y}) \geq f(\mathbf{x}_m, \mathbf{y}) e^{-nT} \right\} \\ &= \Pr \left\{ \sum_Q N_{\mathbf{y}}(Q) \exp[n \cdot G(Q)] \geq \exp[n \cdot G(\tilde{Q})] e^{-nT} \right\} \\ &\doteq \Pr \left\{ \max_Q N_{\mathbf{y}}(Q) \exp[n \cdot G(Q)] \geq \exp[n \cdot G(\tilde{Q})] e^{-nT} \right\} \\ &= \Pr \left\{ \bigcup_Q N_{\mathbf{y}}(Q) \exp[n \cdot G(Q)] \geq \exp[n \cdot G(\tilde{Q})] e^{-nT} \right\} \\ &\doteq \sum_Q \Pr \left\{ N_{\mathbf{y}}(Q) \exp[n \cdot G(Q)] \geq \exp[n \cdot G(\tilde{Q})] e^{-nT} \right\} \\ &\doteq \max_Q \Pr \left\{ N_{\mathbf{y}}(Q) \exp[n \cdot G(Q)] \geq \exp[n \cdot G(\tilde{Q})] e^{-nT} \right\} \\ &= \max_{Q \in \mathcal{S}(\hat{P}_{\mathbf{y}})} \Pr \left\{ N_{\mathbf{y}}(Q) \geq \exp[n \cdot \Omega(Q, \tilde{Q})] \right\} \quad (90) \end{aligned}$$

where

$$\Omega(Q, \tilde{Q}) \triangleq G(R, T, \xi, \tilde{Q}) - G(R, T, \xi, Q) - T \quad (91)$$

and for a given  $\tilde{Q}_Y$ ,  $\mathcal{S}(\tilde{Q}_Y) \triangleq \{Q : Q_Y = \tilde{Q}_Y\}$ . The asymptotic analysis of the probability in (90) was carried out in [18, Section V] for any given  $\Omega$ , and it is not different here. The result relies on the exponential decay of the probability that the joint type of a given  $\mathbf{y}$  with a randomly chosen  $\mathbf{x}_{m'}$  is  $Q$ , namely

$$p \triangleq \Pr \left\{ \hat{P}_{\mathbf{X}_{m'}, \mathbf{y}} = Q \right\}. \quad (92)$$

Under the assumed random coding ensemble, a simple application of the method of types reveals that [4]

$$p \doteq \exp \{-nI(Q)\}. \quad (93)$$

Next, standard large deviations arguments (cf. [18, Section V]) reveal that for  $Q \in \mathcal{S}(\hat{P}_{\mathbf{y}})$ , we have (94), shown at the

top of the next page, where by  $a_n \doteq 0$  we mean that  $a_n$  decreases to 0 super-exponentially fast. Define  $U(\tilde{Q})$  in (95). Thus, substituting (94) in (90) and then in (84), we obtain, using the method of types,

$$\begin{aligned} A_1 &\doteq e^{-nT} \sum_{\mathbf{x}_m} P(\mathbf{X}_m = \mathbf{x}_m) \sum_{\mathbf{y}} f(\mathbf{x}_m, \mathbf{y}) \cdot U(\tilde{Q}) \quad (96) \\ &\doteq e^{-nT} \max_{\tilde{Q}} \exp[nH_{Y|X}(\tilde{Q})] \exp[nG(\tilde{Q})] U(\tilde{Q}). \quad (97) \end{aligned}$$

Note that the condition:

$$\Omega(Q, \tilde{Q}) \leq R - I(Q) \quad (98)$$

in (95) is equivalent to

$$G(\tilde{Q}) \leq G(Q) - I(Q) + R + T. \quad (99)$$

Thus, we obtain that the exponent of  $A_1$  is given by

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log A_1 = -T - \min \left\{ \tilde{E}_a(R, T, \xi), \tilde{E}_b(R, T, \xi) \right\}, \quad (100)$$

in which

$$\tilde{E}_a(R, T, \xi) \triangleq \min_{(Q, \tilde{Q}) \in \mathcal{Q}} \left[ -H_{Y|X}(\tilde{Q}) - G(\tilde{Q}) + I(Q) - R \right] \quad (101)$$

where

$$\mathcal{Q} \triangleq \left\{ (Q, \tilde{Q}) \in \mathcal{D} : I(Q) \geq R, \Omega(R, T, \xi, Q, \tilde{Q}) \leq 0 \right\}, \quad (102)$$

and

$$\tilde{E}_b(R, T, \xi) \triangleq \min_{\tilde{Q} \in \mathcal{L}} \left[ -H_{Y|X}(\tilde{Q}) - G(\tilde{Q}) \right] \quad (103)$$

where

$$\begin{aligned} \mathcal{L} &\triangleq \left\{ \tilde{Q} : G(R, T, \xi, \tilde{Q}) \leq R + T \right. \\ &\quad \left. + \max_{Q: (Q, \tilde{Q}) \in \mathcal{D}, I(Q) \leq R} [G(R, T, \xi, Q) - I(Q)] \right\}. \quad (104) \end{aligned}$$

Now, we want to find the maximal  $\xi$  for which

$$-T - \tilde{E}_a(R, T, \xi) \leq 0, \quad (105)$$

$$\Pr \left\{ N_{\mathbf{y}}(Q) \geq e^{n\Omega(Q, \tilde{Q})} \right\} \doteq \begin{cases} \exp \left\{ -n |I(Q) - R|^+ \right\} & \Omega(Q, \tilde{Q}) \leq 0 \\ 1 & 0 < \Omega(Q, \tilde{Q}) \leq R - I(Q), \\ 0 & \Omega(Q, \tilde{Q}) > R - I(Q) \end{cases} \quad (94)$$

$$U(\tilde{Q}) \triangleq \max_{Q \in \mathcal{S}(\tilde{Q}_Y)} \begin{cases} \exp[-n(I(Q) - R)] & \Omega(Q, \tilde{Q}) \leq 0, I(Q) > R \\ 1 & I(Q) \leq R, \Omega(Q, \tilde{Q}) \leq R - I(Q). \\ 0 & \text{otherwise} \end{cases} \quad (95)$$

$$-T - \tilde{E}_b(R, T, \xi) \leq 0. \quad (106)$$

For  $\tilde{E}_a(R, T, \xi)$ , substituting  $G(Q)$ , given in (89), in (101), we obtain (107)-(110), shown at the top of the page, which is exactly the condition in (37). In a similar manner, one obtains

$$- \tilde{E}_b(R, T, \xi) - T \\ = \max_{\theta} \left\{ \xi E_1(\theta) - \min_{\tilde{Q} \in \mathcal{L}} D(\tilde{Q} \| P_X \times W_{\theta}) \right\}, \quad (111)$$

which is exactly the condition in (38). This concludes the analysis of  $A_1$ , and we next consider  $A_2$ . In essence, we can derive the exponential behavior of  $A_2$ , using similar methods to the derivation of  $E_2(R, T, \theta)$  in [18]. However, since the resulting exponent  $\lim_{n \rightarrow \infty} \frac{1}{n} \log A_2$  is continuous in  $T$ , just as  $\lim_{n \rightarrow \infty} \frac{1}{n} \log A_1$ , we may invoke the following lemma, which is analogue to Lemma 1, and is proved in Appendix A:

*Lemma 2* For all  $R$  and  $T$ :

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log A_2 = T + \lim_{n \rightarrow \infty} \frac{1}{n} \log A_1. \quad (112)$$

Thus, it suffices to assess the exponent of either  $A_1$  or  $A_2$ , and then the other one is immediately obtained. While both  $A_1$  and  $A_2$  can be analyzed, the analytical formula for the exponent of  $A_1$  is more compact, and thus we only presented it. ■

*Proof of Corollary 1:* Define the set  $\mathcal{G}(\tilde{Q}_Y) \triangleq \{Q : I(Q) < R, Q_Y = \tilde{Q}_Y\}$ . We start from the first condition in Theorem 1, which is equivalent to requiring that for all  $\theta$  and  $\tilde{Q}$

$$\xi E_1(R, T, \theta) \leq D(\tilde{Q} \| P_X \times W_{\theta}) \\ + \min_{Q \in \mathcal{G}^c(\tilde{Q}_Y)} \max_{\lambda \geq 0} \left[ I(Q) - R + \lambda \cdot \Omega(R, T, \xi, Q, \tilde{Q}) \right]. \quad (113)$$

Letting

$$\Omega_{\theta_1, \theta_2}(R, T, \xi, Q, \tilde{Q}) \triangleq \xi E_1(R, T, \theta_1) + \mathbb{E}_{\tilde{Q}} [\log W_{\theta_1}(Y|X)] \\ - [\xi E_1(R, T, \theta_2) + \mathbb{E}_{\tilde{Q}} [\log W_{\theta_2}(Y|X)]] - T, \quad (114)$$

we have by definition,

$$\Omega(R, T, \xi, Q, \tilde{Q}) = \max_{\theta_1} \min_{\theta_2} \Omega_{\theta_1, \theta_2}(R, T, \xi, Q, \tilde{Q}). \quad (115)$$

Substituting (115) in (113), we get

$$\xi E_1(R, T, \theta) \leq D(\tilde{Q} \| P_X \times W_{\theta})$$

$$+ \min_{Q \in \mathcal{G}^c(\tilde{Q}_Y)} \max_{\lambda \geq 0} \max_{\theta_1} \min_{\theta_2} \left[ I(Q) - R \\ + \lambda \cdot \Omega_{\theta_1, \theta_2}(R, T, \xi, Q, \tilde{Q}) \right], \quad (116)$$

which is equivalent to demanding that for all  $Q \in \mathcal{G}_R^c(\tilde{Q}_Y)$  there exist some  $\lambda \geq 0$  and  $\theta_1 \in \Theta$ , such that for all  $\theta_2 \in \Theta$  we have

$$\xi E_1(R, T, \theta) \leq D(\tilde{Q} \| P_X \times W_{\theta}) + I(Q) - R \\ + \lambda \cdot \Omega_{\theta_1, \theta_2}(R, T, \xi, Q, \tilde{Q}). \quad (117)$$

Upon substitution of (114) in (117), after rearranging the terms, we obtain  $\xi \leq \hat{\xi}_1(R, T, Q, \tilde{Q}, \theta, \theta_1, \theta_2, \lambda)$ , where  $\hat{\xi}_1$  is defined in (39). Thus, the largest achievable  $\xi$  which satisfies the first condition is  $\xi_1^*(R, T)$ . In the same way, the second condition yields  $\xi_2^*(R, T)$ , and thus,  $\xi^*(R, T) = \min \{\xi_1^*(R, T), \xi_2^*(R, T)\}$ . ■

*Proof of Corollary 2:* In the following, we analyze the objective in (37) for any  $\theta$ . Starting with the left term,  $E_1(\theta)$ , note that this is just the expression that was considered in [18, pp. 6450-6451, eqs. (64)-(73)]. For completeness, we present here the main steps in the simplification of this term to the BSC. We start with the analysis of  $E_a(R, T)$  given in (13). First, note that

$$\mathbb{E}_{\tilde{Q}} \log W_{\theta}(Y|X) - \mathbb{E}_{\tilde{Q}} \log W_{\theta}(Y|X) \\ = \left[ Q(X \neq Y) - \hat{Q}(X \neq Y) \right] \beta \quad (118)$$

where  $\beta = \log[(1 - \theta)/\theta]$ . Thus, recalling (12),  $E_1(\theta)$  takes the form

$$\min_{\tilde{Q}} \left\{ D(\tilde{Q} \| P_X \times W_{\theta}) \right. \\ \left. + \left| \min_{Q \in \hat{\mathcal{Q}}_{\text{BSC}}(\tilde{Q})} (-H_{X|Y}(Q) + \log 2 - R) \right|^+ \right\} \quad (119)$$

where

$$\hat{\mathcal{Q}}_{\text{BSC}}(\tilde{Q}) \triangleq \left\{ Q : Q_Y = \tilde{Q}_Y, \right. \\ \left. Q(X \neq Y) \leq \tilde{Q}(X \neq Y) + \frac{T}{\beta} \right\}. \quad (120)$$

Now, note that

$$H_{X|Y}(Q) = H_{\mathcal{I}\{X \neq Y\}|Y}(Q) \leq H_{\mathcal{I}\{X \neq Y\}}(Q), \quad (121)$$

$$-\tilde{E}_a(R, T, \xi) - T = \max_{(Q, \tilde{Q}) \in \mathcal{Q}} \left[ H_{Y|X}(\tilde{Q}) + G(\tilde{Q}) - I(Q) + R \right] - T \quad (107)$$

$$= \max_{(Q, \tilde{Q}) \in \mathcal{Q}} \left[ H_{Y|X}(\tilde{Q}) + \max_{\theta} \left\{ \xi E_1(\theta) + \mathbb{E}_{\tilde{Q}} \log W_{\theta}(Y|X) \right\} - I(Q) + R \right] \quad (108)$$

$$= \max_{\theta} \left\{ \xi E_1(\theta) + \max_{(Q, \tilde{Q}) \in \mathcal{Q}} \left\{ H_{Y|X}(\tilde{Q}) - I(Q) + R + \mathbb{E}_{\tilde{Q}} \log W_{\theta}(Y|X) \right\} \right\} \quad (109)$$

$$= \max_{\theta} \left\{ \xi E_1(\theta) - \min_{(Q, \tilde{Q}) \in \mathcal{Q}} \left\{ D(\tilde{Q} \| P_X \times W_{\theta}) + I(Q) - R \right\} \right\}, \quad (110)$$

and thus

$$\begin{aligned} & \min_{\tilde{Q}} \left\{ D(\tilde{Q} \| P_X \times W_{\theta}) \right. \\ & \quad \left. + \left| \min_{Q \in \hat{\mathcal{Q}}_{\text{BSC}}(\tilde{Q})} (-H_{X|Y}(Q) + \log 2 - R) \right|^+ \right\} \\ & \geq \min_{\tilde{Q}} \left\{ D(\tilde{Q} \| P_X \times W_{\theta}) \right. \\ & \quad \left. + \left| \min_{Q \in \hat{\mathcal{Q}}_{\text{BSC}}(\tilde{Q})} (-H_{\mathcal{I}\{X \neq Y\}}(Q) + \log 2 - R) \right|^+ \right\} \quad (122) \\ & = \min_{\tilde{q}} \left\{ D(\tilde{q} \| \theta) + \left| \min_{q \leq \tilde{q} + T/\beta} (-h(q) + \log 2 - R) \right|^+ \right\} \quad (123) \end{aligned}$$

$$= \min_{\tilde{q}} \left\{ D(\tilde{q} \| \theta) + \left| -h \left( \min \left\{ \frac{1}{2}, \tilde{q} + \frac{T}{\beta} \right\} \right) + \log 2 - R \right|^+ \right\}$$

$$= \min_{\tilde{q}} \left\{ D(\tilde{q} \| \theta) - h \left( \min \left\{ \delta_{GV}(R), \tilde{q} + \frac{T}{\beta} \right\} \right) + \log 2 - R \right\}$$

$$= \min_{\tilde{q} \in [\theta, \delta_{GV}(R) - T/\beta]} \left[ D(\tilde{q} \| \theta) - h \left( \tilde{q} + \frac{T}{\beta} \right) \right] + \log 2 - R \quad (126)$$

where the last step follows since the minimizing  $\tilde{Q}$  is such that  $\tilde{Q}_X = P_X$  to obtain minimal  $D(\tilde{Q} \| P_X \times W_{\theta})$ , and it is easy to verify using convexity arguments that given  $\tilde{Q}(X \neq Y) = \tilde{q}$  the divergence  $D(\tilde{Q} \| P_X \times W_{\theta})$  is minimized for a symmetric  $\tilde{Q}_{Y|X}$ , namely,

$$\tilde{Q}_{Y|X}(y|x) = \begin{cases} \tilde{q} & x = y \\ 1 - \tilde{q} & x \neq y \end{cases}, \quad (124)$$

for which  $D(\tilde{Q} \| P_X \times W_{\theta}) = D(\tilde{q} \| \theta)$ . Finally, it is evident that we have equality in (122) if we choose

$$Q_{Y|X}(y|x) = \begin{cases} q & x = y \\ 1 - q & x \neq y \end{cases}, \quad (125)$$

and thus it is the minimizer. Next, we observe that  $-h(q)$  is a decreasing function of  $q$  for  $q \in [0, 1/2]$  and increasing for  $q \in [1/2, 1]$ . Thus,

$$\begin{aligned} & \min_{\tilde{q}} \left\{ D(\tilde{q} \| \theta) \right. \\ & \quad \left. + \left| \min_{q \leq \tilde{q} + T/\beta} (-h(q) + \log 2 - R) \right|^+ \right\} \\ & = \min_{\tilde{q}} \left\{ D(\tilde{q} \| \theta) \right. \end{aligned}$$

where the last step can be easily verified using monotonicity properties of the binary entropy and divergence [18, p. 6451 after eq. (72)]. Now, we analyze  $E_b(R, T)$  given in (14). Note that there is no conceptual difference between  $E_a(R, T)$  and  $E_b(R, T)$ , and it can be verified that the latter can be written as

$$\min_{\tilde{q} \in \hat{\mathcal{L}}_{\text{BSC}}} D(\tilde{q} \| \theta) \quad (127)$$

where

$$\begin{aligned} \hat{\mathcal{L}}_{\text{BSC}} \triangleq & \left\{ \tilde{q} : -\tilde{q} \cdot \beta \leq R + T \right. \\ & \left. + \max_{q: R \geq \log 2 - h(q)} [-q \cdot \beta + h(q) - \log 2] \right\}. \quad (128) \end{aligned}$$

Next, for any  $\theta$ , consider the right term in objective of (37). Note that the only difference between the left and the right terms in (37) is just the inner minimization region. Accordingly, the right term takes the form

$$\begin{aligned} & \min_{\tilde{Q}} \left\{ D(\tilde{Q} \| P_X \times W_{\theta}) \right. \\ & \quad \left. + \left| \min_{Q \in \mathcal{Q}_{\text{BSC}}(\tilde{Q})} (-H_{X|Y}(Q) + \log 2 - R) \right|^+ \right\} \quad (129) \end{aligned}$$

where

$$\begin{aligned} \mathcal{Q}_{\text{BSC}}(\tilde{Q}) \triangleq & \left\{ Q : Q_Y = \tilde{Q}_Y, \right. \\ & \max_{\theta'} \left\{ \xi E_1(\theta') - \beta(\theta') \tilde{Q}(X \neq Y) + \log(1 - \theta') \right\} \\ & - \max_{\theta'} \left\{ \xi E_1(\theta') - \beta(\theta') Q(X \neq Y) + \log(1 - \theta') \right\} \\ & \left. - T \leq 0 \right\}. \quad (130) \end{aligned}$$

Let  $\tilde{E}_1(\theta) \triangleq E_1(\theta) + \log(1 - \theta)/\xi$ . Then, using exactly the same steps as before, we get

$$\begin{aligned} & \min_{\tilde{Q}} \left\{ D(\tilde{Q} \| P_X \times W_\theta) \right. \\ & \quad \left. + \left| \min_{Q \in \mathcal{Q}_{\text{BSC}}(\tilde{Q})} (-H_{X|Y}(Q) + \log 2 - R) \right|^+ \right\} \\ & \geq \min_{\tilde{Q}} \left\{ D(\tilde{Q} \| P_X \times W_\theta) \right. \\ & \quad \left. + \left| \min_{Q \in \mathcal{Q}_{\text{BSC}}(\tilde{Q})} (-H_{\mathcal{I}\{X \neq Y\}}(Q) + \log 2 - R) \right|^+ \right\} \quad (131) \\ & = \min_{\tilde{q}} \left\{ D(\tilde{q} \| \theta) + \left| \min_{q \in \tilde{\mathcal{Q}}_{\text{BSC}}(\tilde{q})} (-h(q) + \log 2 - R) \right|^+ \right\}, \quad (132) \end{aligned}$$

and equality can be achieved choosing  $Q$  to be symmetric, as before, and

$$\begin{aligned} \tilde{\mathcal{Q}}_{\text{BSC}}(\tilde{q}) \triangleq & \left\{ q : \max_{\theta'} \left\{ \xi \tilde{E}_1(\theta') - \beta(\theta') \cdot \tilde{q} \right\} \right. \\ & \left. - \max_{\theta'} \left\{ \xi \tilde{E}_1(\theta') - \beta(\theta') \cdot q \right\} - T \leq 0 \right\}. \quad (133) \end{aligned}$$

Next, we simplify the set  $\tilde{\mathcal{Q}}_{\text{BSC}}(\tilde{q})$ . The constraint on  $q$  in the definition of  $\tilde{\mathcal{Q}}_{\text{BSC}}(\tilde{q})$ , is equivalent to demanding that there exist some  $\theta' \in \Theta$  such that the following holds

$$\beta(\theta')q - \xi \tilde{E}_1(\theta') \leq T - \max_{\theta''} \left\{ \xi \tilde{E}_1(\theta'') - \beta(\theta'') \cdot \tilde{q} \right\}, \quad (134)$$

or equivalently

$$\beta(\theta')q \leq \xi \tilde{E}_1(\theta') + T - \max_{\theta''} \left\{ \xi \tilde{E}_1(\theta'') - \beta(\theta'') \cdot \tilde{q} \right\}. \quad (135)$$

Now, note that  $\beta(\theta') \geq 0$  if and only if  $\theta' \leq 1/2$ . Accordingly, this means that, in terms of  $q$ ,  $\tilde{\mathcal{Q}}_{\text{BSC}}(\tilde{q})$  is equivalent to  $q \leq q_1^*$  or  $q \geq q_2^*$ , where  $q_1^*$  and  $q_2^*$  are given in (45) and (46), respectively. Consequently,

$$\begin{aligned} & \min_{\tilde{q}} \left\{ D(\tilde{q} \| \theta) + \left| \min_{q \in \tilde{\mathcal{Q}}_{\text{BSC}}(\tilde{q})} (-h(q) + \log 2 - R) \right|^+ \right\} \\ & = \min_{\tilde{q}} \left\{ D(\tilde{q} \| \theta) + |(-g(q_1^*, q_2^*) + \log 2 - R)|^+ \right\} \quad (136) \end{aligned}$$

where  $g(q_1^*, q_2^*)$  is defined in (47). Finally, we consider the right term in (38). Using the same steps as above we obtain that

$$\min_{\tilde{Q} \in \mathcal{L}} D(\tilde{Q} \| P_X \times W_\theta) = \min_{\tilde{q} \in \mathcal{L}_{\text{BSC}}} D(\tilde{q} \| \theta) \quad (137)$$

where  $\mathcal{L}_{\text{BSC}}$  is defined in (138)-(139), shown at the top of the next page, where the last step in (139) follows from the fact that the maximizer  $q$  in the optimization problem in (138) is given by  $\max\{\theta, \delta_{\text{GV}}(R)\}$ . ■

## APPENDIX A PROOF OF LEMMAS 1 AND 2

We begin with the proof of Lemma 1. For the sake of this proof, we will explicitly designate the dependence on  $T$ , and denote the decoder in (4)-(5), with parameter  $T$ , by  $\mathcal{R}^*(T)$ . Similarly, we will denote the value of (7) as  $\Gamma(\mathcal{C}, \mathcal{R}, T)$ . As we have mentioned, the decoder minimizing  $\Gamma(\mathcal{C}, \mathcal{R}, T)$  can be easily seen to be given by  $\mathcal{R}^*(T)$ . Now, assume conversely, that the exponents associated with  $\mathbb{E}[\Gamma(\mathcal{C}, \mathcal{R}^*(T), T)]$  satisfy

$$E_2(R, T) < T + E_1(R, T). \quad (\text{A.1})$$

The opposite case, where the inequality in (A.1) is reversed, can be handled analogously. Accordingly, this means that in the exponential scale, we have

$$\mathbb{E}[\Gamma(\mathcal{C}, \mathcal{R}^*(T), T)] \doteq e^{-nE_2(R, T)}. \quad (\text{A.2})$$

Now, it is evident that  $E_1(R, T)$  is a monotonically decreasing function of  $T$  (allowing more erasures increases  $\overline{\text{Pr}}\{\mathcal{E}_1\}$ ), and  $E_2(R, T)$  is a monotonically increasing function of  $T$  (allowing more erasures decreases  $\overline{\text{Pr}}\{\mathcal{E}_2\}$ ) [18]. Now, due to the fact that  $E_1(R, T)$  and  $E_2(R, T)$  are continuous functions of  $T$  [18, eqs. (23) and (31)], without loss of essential generality, there exists  $\epsilon > 0$  and  $\delta_1 \geq 0, \delta_2 > 0$  such that

$$E_1(R, T + \epsilon) = E_1(R, T) - \delta_1 \quad (\text{A.3})$$

and

$$E_2(R, T + \epsilon) = E_2(R, T) + \delta_2 \quad (\text{A.4})$$

yet

$$E_2(R, T + \epsilon) < T + E_1(R, T + \epsilon). \quad (\text{A.5})$$

Note that since it is not guaranteed that  $E_1(R, T)$  or  $E_2(R, T)$  are strictly monotonic, as it might be the case that  $\delta_2 = 0$  too, i.e., regions of plateau. Accordingly, there are several cases to consider. First, if just  $E_1(R, T)$  is within a plateau region, then the above arguments remain the same since  $\delta_1 = 0$  but  $\delta_2 > 0$ . Secondly, if just  $E_2(R, T)$  is within a plateau region, then we claim that this contradicts the optimality of Forney's decoder. Indeed, in this case, if we increase  $T$  by some small  $\epsilon > 0$  (such that  $E_2(R, T + \epsilon)$  is within the plateau), we obtain a decoder with exponents  $E_2(R, T + \epsilon) = E_2(R, T)$  and  $E_1(R, T + \epsilon) < E_1(R, T)$ , and yet, due to continuity,  $E_2(R, T) < E_1(R, T + \epsilon)$ . Thus, we obtained that the optimal decoder  $\mathcal{R}^*(T + \epsilon)$  has the same performance as  $\mathcal{R}^*(T)$ , in terms of  $\mathbb{E}[\Gamma(\mathcal{C}, \mathcal{R}^*(T), T)]$ , but with worse  $\overline{\text{Pr}}\{\mathcal{E}_1\}$ , which means not the best trade-off between  $\overline{\text{Pr}}\{\mathcal{E}_1\}$  and  $\overline{\text{Pr}}\{\mathcal{E}_2\}$ , and thus contradicting the optimality of Forney's decoder at  $T + \epsilon$ . Finally, if both exponents are within a region of plateau, we can simply vary  $T$  until we leave this region, and thus we can assume that  $\delta_2 > 0$ . To conclude, we obtained that

$$\mathbb{E}[\Gamma(\mathcal{C}, \mathcal{R}(T + \epsilon), T)] \doteq e^{-nE_2(R, T + \epsilon)} \quad (\text{A.6})$$

$$< e^{-nE_2(R, T)} \quad (\text{A.7})$$

$$\doteq \mathbb{E}[\Gamma(\mathcal{C}, \mathcal{R}(T), T)] \quad (\text{A.8})$$

which contradicts the property that  $\mathcal{R}^*(T)$  is the minimizer of  $\Gamma(\mathcal{C}, \mathcal{R}, T)$ .

$$\mathcal{L}_{\text{BSC}} \triangleq \left\{ \tilde{q} : \max_{\theta} [\xi E_1(\theta) - \tilde{q} \cdot \beta + \log \theta] \leq R + T + \max_{q: R \geq \log 2^{-h(q)}} \left\{ \max_{\theta} [\xi E_1(\theta) - q \cdot \beta + \log \theta] + h(q) - \log 2 \right\} \right\} \quad (138)$$

$$= \left\{ \tilde{q} : \max_{\theta} [\xi E_1(R, T, \theta) - \tilde{q} \cdot \beta(\theta) + \log \theta] \leq R + T + \max_{\theta} [\xi E_1(R, T, \theta) - \max\{\theta, \delta_{\text{GV}}(R)\} \cdot \beta(\theta) + \log \theta + h(\max\{\theta, \delta_{\text{GV}}(R)\}) - \log 2] \right\} \quad (139)$$

The proof of Lemma 2 follows the same steps as above. Indeed, the Lagrangian associated with the universal erasure decoder (see, (75)), has a similar structure to the Lagrangian associated with the optimal (known channel) decoder (see, (8)). As was mentioned in the proof of Theorem 1, the exponents of  $A_1$  and  $A_2$  are both continuous. So, just as the difference between the exponents of  $\overline{\text{Pr}}\{\mathcal{E}_1\}$  and  $\overline{\text{Pr}}\{\mathcal{E}_2\}$  is  $T$ , the difference between the exponents of  $A_1$  and  $A_2$  is also  $T$ .

#### APPENDIX B UNIVERSAL DECODER WITH TRAINING

To present the achieved fraction for the ensemble which includes training, we need to slightly generalize the definitions preceding Theorem 1. The definitions of  $G(R, T, \xi, \bar{Q})$  in (33) and  $\Omega(R, T, \xi, Q, \bar{Q})$  in (34) remain exactly the same. Define,

$$J(Q, \bar{Q}) \triangleq (1 - \alpha) \cdot I \left( \frac{Q - \alpha \bar{Q}}{1 - \alpha} \right). \quad (\text{B.1})$$

For a given joint type  $\bar{Q}$ , we replace the definition of  $\mathcal{Q}$  in (35) with

$$\mathcal{Q}(\bar{Q}) \triangleq \left\{ (Q, \bar{Q}) \in \mathcal{D}(\bar{Q}) : J(Q, \bar{Q}) \geq R, \Omega(R, T, \xi, Q, \bar{Q}) \leq 0 \right\}, \quad (\text{B.2})$$

and replace the definition of  $\mathcal{L}$  in (36) with

$$\mathcal{L}(\bar{Q}) \triangleq \left\{ \tilde{Q} : G(R, T, \xi, \tilde{Q}) \leq R + T + \max_{Q: (Q, \tilde{Q}) \in \mathcal{D}(\tilde{Q}), J(Q, \tilde{Q}) \leq R} [G(R, T, \xi, Q) - J(Q, \tilde{Q})] \right\}, \quad (\text{B.3})$$

where  $\mathcal{D}$  defined in (16) is replaced by

$$\mathcal{D}(\bar{Q}) \triangleq \left\{ (Q, \bar{Q}) : Q_X = \bar{Q}_X = P_X, Q_Y = \bar{Q}_Y, \frac{Q - \alpha \bar{Q}}{1 - \alpha} \text{ is a probability distribution} \right\}. \quad (\text{B.4})$$

Finally, define

$$\Delta_{\theta}(Q, \bar{Q}) \triangleq \alpha \cdot D(\bar{Q} \| \bar{P}_X \times W_{\theta}) + (1 - \alpha) \cdot D \left( \frac{Q - \alpha \bar{Q}}{1 - \alpha} \middle\| P_X \times W_{\theta} \right). \quad (\text{B.5})$$

*Theorem 2* Consider the ensemble defined above with types  $\bar{P}_X$  and  $P_X$ , and a fixed  $\alpha \in [0, 1)$ . Then,  $\xi^*(R, T, \alpha, \bar{P}_X)$ ,

defined in (29), is equal to the largest number  $\xi$  that simultaneously satisfies:

$$\max_{\theta \in \Theta} \left\{ \xi E_1(R, T, \theta) - \min_{\bar{Q}: \bar{Q}_X = \bar{P}_X} \min_{(Q, \bar{Q}) \in \mathcal{Q}(\bar{Q})} \left\{ \Delta_{\theta}(\bar{Q}, \bar{Q}) + J(Q, \bar{Q}) - R \right\} \right\} \leq 0, \quad (\text{B.6})$$

and

$$\max_{\theta \in \Theta} \left\{ \xi E_1(R, T, \theta) - \min_{\bar{Q}: \bar{Q}_X = \bar{P}_X} \min_{Q \in \mathcal{L}(\bar{Q})} \Delta_{\theta}(\bar{Q}, \bar{Q}) \right\} \leq 0. \quad (\text{B.7})$$

Choosing a strictly positive  $\alpha$  has the potential to increase  $\xi^*(R, T, 0, \bar{P}_X)$ . However, the behavior of  $\xi^*(R, T, \alpha, \bar{P}_X)$  as a function of  $\alpha$ , is typically not monotonic. Indeed, as was mentioned before, on the one hand, as  $\alpha$  increases, the decoder has better knowledge of the channel, even if it does not estimate it explicit. On the other hand, the number of available symbols  $(1 - \alpha)n$  that are used to distinguish the  $M = \lceil e^{nR} \rceil$  codewords from one another decreases<sup>14</sup>. Thus, we expect that, in general,  $\xi^*(R, T, \alpha, \bar{P}_X)$  will be maximized by some  $\alpha^* \in (0, 1)$ . In addition, the type of the training part  $\bar{P}_X$  may also be optimized. Evidently, Theorem 2 sets the stage for a reasonable criterion of optimal training, which includes both the relative training time and the optimal (type of the) training sequence. Similarly to Corollary 1, one can derive a formula for  $\xi^*(R, T, \alpha, \bar{P}_X)$ , and then, a reasonable objective would be to optimize  $\xi^*(R, T, \alpha, \bar{P}_X)$  over both  $\alpha$  and  $\bar{P}_X$ .

*Proof of Theorem 2:* The proof follows the same lines of the proof Theorem 1 so we mainly highlight the differences. We will represent the joint type of the training sequence  $\bar{x}$  and the training part of  $\mathbf{y}$  by  $\bar{Q}$ . Also, for a given  $\mathbf{y}$  we will denote by  $\bar{\mathbf{y}}$  the first  $\alpha \cdot n$  symbols of  $\mathbf{y}$  (i.e. the output symbols for the training sequence). We continue (84) as shown in (B.8)-(B.12), presented at the top of the next page. Now, if the joint type of the training sequence  $\bar{x}$  and the training part of  $\mathbf{y}$  is  $\bar{Q}$ , and the type of the entire codeword  $\mathbf{x}_m$  and  $\mathbf{y}$  is  $Q$ , then the type of the last  $(1 - \alpha)n$  symbols of  $\mathbf{x}_m$  and  $\mathbf{y}$  is  $\frac{Q - \alpha \bar{Q}}{1 - \alpha}$ . So, the probability in Eq. (92) should now be replaced by

$$p \doteq \exp \left\{ -n \cdot J(Q, \bar{Q}) \right\}. \quad (\text{B.13})$$

Consequently, for  $Q \in \mathcal{S}(\hat{P}_{\mathbf{y}})$ , we have (B.14), and we define (B.15), both shown at the top of the next page. Thus, using

<sup>14</sup>Note that the blocklength which is used to gauge the rate is still  $n$ .

$$A_1 = e^{-nT} \sum_{\mathbf{x}_m} P_X(\mathbf{X}_m = \mathbf{x}_m) \sum_{\mathbf{y}} f(\mathbf{x}_m, \mathbf{y}) \cdot \Pr \left\{ \mathbf{y} \in \hat{\mathcal{R}}_m^c \mid \mathbf{X}_m = \mathbf{x}_m \text{ transmitted} \right\} \quad (\text{B.8})$$

$$= e^{-nT} \sum_{\mathbf{x}_m} P_X(\mathbf{X}_m = \mathbf{x}_m) \sum_{\bar{Q}} \sum_{\mathbf{y}: \hat{P}_{\mathbf{x}_m \mathbf{y}} = \bar{Q}} f(\mathbf{x}_m, \mathbf{y}) \cdot \Pr \left\{ \mathbf{y} \in \hat{\mathcal{R}}_m^c \mid \mathbf{X}_m = \mathbf{x}_m \text{ transmitted} \right\} \quad (\text{B.9})$$

$$\doteq e^{-nT} \max_{\bar{Q}} \sum_{\mathbf{x}_m} P_X(\mathbf{X}_m = \mathbf{x}_m) \sum_{\mathbf{y}: \hat{P}_{\mathbf{x}_m \mathbf{y}} = \bar{Q}} f(\mathbf{x}_m, \mathbf{y}) \cdot \Pr \left\{ \mathbf{y} \in \hat{\mathcal{R}}_m^c \mid \mathbf{X}_m = \mathbf{x}_m \text{ transmitted} \right\} \quad (\text{B.10})$$

$$\doteq e^{-nT} \max_{\bar{Q}} \max_{\mathbf{x}_m} \sum_{\mathbf{y}: \hat{P}_{\mathbf{x}_m \mathbf{y}} = \bar{Q}, \hat{P}_{\mathbf{x}_m \mathbf{y}} = \bar{Q}} P_X(\mathbf{X}_m = \mathbf{x}_m) f(\mathbf{x}_m, \mathbf{y}) \cdot \Pr \left\{ \mathbf{y} \in \hat{\mathcal{R}}_m^c \mid \mathbf{X}_m = \mathbf{x}_m \text{ transmitted} \right\} \quad (\text{B.11})$$

$$\doteq e^{-nT} \max_{\bar{Q}} \max_{\mathbf{x}_m} \sum_{\mathbf{y}: \hat{P}_{\mathbf{x}_m \mathbf{y}} = \bar{Q}, \hat{P}_{\mathbf{x}_m \mathbf{y}} = \bar{Q}} P_X(\mathbf{X}_m = \mathbf{x}_m) f(\mathbf{x}_m, \mathbf{y}) \cdot \Pr \left\{ \mathbf{y} \in \hat{\mathcal{R}}_m^c \mid \mathbf{X}_m = \mathbf{x}_m \text{ transmitted} \right\}. \quad (\text{B.12})$$

$$\Pr \left\{ N_{\mathbf{y}}(Q) \geq e^{n\Omega(Q, \bar{Q})} \right\} \doteq \begin{cases} \exp \left\{ -n |J(Q, \bar{Q}) - R|^+ \right\} & \Omega(Q, \bar{Q}) \leq 0 \\ 1 & 0 < \Omega(Q, \bar{Q}) \leq R - J(Q, \bar{Q}) \\ 0 & \Omega(Q, \bar{Q}) > R - J(Q, \bar{Q}) \end{cases} \quad (\text{B.14})$$

$$U(\bar{Q}, \bar{Q}) \triangleq \max_{Q \in \mathcal{S}(\bar{Q}_Y)} \begin{cases} \exp \left[ -n(J(Q, \bar{Q}) - R) \right] & \Omega(Q, \bar{Q}) \leq 0, J(Q, \bar{Q}) > R \\ 1 & J(Q, \bar{Q}) \leq R, \Omega(Q, \bar{Q}) \leq R - J(Q, \bar{Q}) \\ 0 & \text{otherwise} \end{cases} \quad (\text{B.15})$$

the same derivation as in (90), but with (B.14) replacing (94), we may continue (B.12) as follows:

$$A_1 \doteq e^{-nT} \max_{\bar{Q}} \max_{\mathbf{x}_m} \exp \left[ \alpha n H_{Y|X}(\bar{Q}) \right] \cdot \exp \left[ (1 - \alpha) n H_{Y|X} \left( \frac{Q - \alpha \bar{Q}}{1 - \alpha} \right) \right] \exp \left[ n G(\bar{Q}) \right] U(\bar{Q}, \bar{Q}). \quad (\text{B.16})$$

Thus, we obtain that the exponent of  $A_1$  is given by

$$\lim_{n \rightarrow \infty} \frac{1}{n} \log A_1 = -T - \min \left\{ \tilde{E}_a(R, T, \xi), \tilde{E}_b(R, T, \xi) \right\}, \quad (\text{B.17})$$

in which

$$\tilde{E}_a(R, T, \xi) \triangleq \min_{\bar{Q}} \min_{(Q, \bar{Q}) \in \mathcal{Q}(\bar{Q})} \left[ -\alpha H_{Y|X}(\bar{Q}) - (1 - \alpha) H_{Y|X} \left( \frac{Q - \alpha \bar{Q}}{1 - \alpha} \right) - G(\bar{Q}) + J(Q, \bar{Q}) - R \right] \quad (\text{B.18})$$

where  $\mathcal{Q}(\bar{Q})$  is defined in (B.2), and

$$\tilde{E}_b(R, T, \xi) \triangleq \min_{\bar{Q}} \min_{\bar{Q} \in \mathcal{L}(\bar{Q})} \left[ -\alpha H_{Y|X}(\bar{Q}) - (1 - \alpha) H_{Y|X} \left( \frac{Q - \alpha \bar{Q}}{1 - \alpha} \right) - G(\bar{Q}) \right] \quad (\text{B.19})$$

where  $\mathcal{L}(\bar{Q})$  is defined in (B.3). Now, we want to find the maximal  $\xi$  for which

$$-T - \tilde{E}_a(R, T, \xi) \leq 0, \quad (\text{B.20})$$

$$-T - \tilde{E}_b(R, T, \xi) \leq 0. \quad (\text{B.21})$$

The expressions for  $\tilde{E}_a(R, T, \xi)$  and  $\tilde{E}_b(R, T, \xi)$  can be simplified just as in the proof of Theorem 1 (see Eqs. (110) and (111)). This results the conditions appearing in the theorem. ■

#### ACKNOWLEDGMENT

The authors would like to thank the associate editor, Jun Chen, and the anonymous referees for their suggestions which helped improving the content of this paper.

#### REFERENCES

- [1] V. D. Goppa, "Nonprobabilistic mutual information without memory," *Probl. Cont. Information Theory*, vol. 4, pp. 97–102, 1975.
- [2] J. Ziv, "Universal decoding for finite-state channels," *IEEE Trans. Inf. Theory*, vol. IT-31, no. 4, pp. 453–460, July 1985.
- [3] I. Csiszár, "Linear codes for sources and source networks: error exponents, universal coding," *IEEE Trans. Inf. Theory*, vol. IT-28, no. 4, pp. 585–592, July 1982.
- [4] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge University Press, 2011.
- [5] N. Merhav, "Universal decoding for memoryless Gaussian channels with a deterministic interference," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1261–1269, July 1993.
- [6] —, "Universal decoding for arbitrary channels relative to a given class of decoding metrics," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5566–576, Sep. 2013.
- [7] M. Feder and A. Lapidoth, "Universal decoding for channels with memory," *IEEE Trans. Inf. Theory*, vol. 44, no. 5, pp. 1726–1745, Sep. 1998.
- [8] G. D. Forney, Jr., "Exponential error bounds for erasure, list, and decision feedback schemes," *IEEE Trans. Inf. Theory*, vol. 14, no. 2, pp. 206–220, 1968.
- [9] M. V. Burnashev, "Data transmission over a discrete channel with feedback," *Problems of Information Transmission*, pp. 250–265, 1976.

- [10] N. Shulman, “*Communication over an unknown channel via common broadcasting*,” Ph.D. dissertation, Tel-Aviv University, 2003, [http://www.eng.tau.ac.il/shulman/papers/Nadav\\_PhD.pdf](http://www.eng.tau.ac.il/shulman/papers/Nadav_PhD.pdf).
- [11] S. Draper, B. J. Frey, and F. R. Kschischang, “Rateless coding for non-ergodic channels with decoder channel state information,” *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4119–4133, 2009.
- [12] U. Erez, G. W. Wornell, and M. D. Trott, “Rateless space-time coding,” in *Proc. ISIT 2005*, Sep. 2005, pp. 1937–1941.
- [13] J. Jiang and K. R. Narayanan, “Multilevel coding for channels with non-uniform inputs and rateless transmission over the bsc,” in *Proc. ISIT 2006*, 2006, pp. 518–522.
- [14] A. Tchamkerten and E. I. Telatar, “Variable length codes over unknown channels,” *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2126–2145, 2006.
- [15] N. Merhav and M. Feder, “Minimax universal decoding with an erasure option,” *IEEE Trans. Inf. Theory*, vol. 53, no. 5, pp. 1664–1675, May, 2007.
- [16] P. Moulin, “A Neyman-Pearson approach to universal erasure and list decoding,” *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4462–4478, 2009.
- [17] M. Feder and N. Merhav, “Universal composite hypothesis testing: a competitive minimax approach,” *IEEE Trans. Inf. Theory special issue in memory of Aaron D. Wyner*, vol. 48, no. 6, pp. 1504–1517, June 2002.
- [18] A. Somekh-Baruch and N. Merhav, “Exact random coding exponents for erasure decoding,” *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6444–6454, 2011.
- [19] N. Merhav, “Erasure/list exponents for Slepian-Wolf decoding,” *IEEE Trans. Inf. Theory*, vol. 60, no. 8, pp. 4463–4471, Aug. 2014.

**Wasim Huleihel** (S’14) received the B.Sc. and the M.Sc. degrees in electrical engineering from the Ben-Gurion University of the Negev, Beer-Sheva, Israel, in 2012 and 2013, respectively. Currently, he is working toward the Ph.D. degree in electrical engineering at the Technion Institute of Technology, Haifa, Israel. His research interests are in the areas of information theory, and relationships between information theory, statistics, detection, and estimation.

**Nir Weinberger** (S’14) received the B.Sc. and M.Sc. degrees (both *summa cum laude*) from Tel-Aviv University, Tel-Aviv, Israel, in 2006 and 2009, respectively. From 2006 to 2013 he served as an algorithms Engineer in the Israeli Defense Forces. Currently, he is pursuing his Ph.D. degree at the Technion - Israel Institute of Technology, Haifa, Israel. His research interest is information theory, with emphasis on large deviations aspects in coding problems.

**Neri Merhav** (S’86–M’87–SM’93–F’99) was born in Haifa, Israel, on March 16, 1957. He received the B.Sc., M.Sc., and D.Sc. degrees from the Technion, Israel Institute of Technology, in 1982, 1985, and 1988, respectively, all in electrical engineering.

From 1988 to 1990 he was with AT&T Bell Laboratories, Murray Hill, NJ, USA. Since 1990 he has been with the Electrical Engineering Department of the Technion, where he is now the Irving Shepard Professor. During 1994–2000 he was also serving as a consultant to the Hewlett–Packard Laboratories – Israel (HPL-I). His research interests include information theory, statistical communications, and statistical signal processing. He is especially interested in the areas of lossless/lossy source coding and prediction/filtering, relationships between information theory and statistics, detection, estimation, as well as in the area of Shannon Theory, including topics in joint source–channel coding, source/channel simulation, and coding with side information with applications to information hiding and watermarking systems. Another recent research interest concerns the relationships between Information Theory and statistical physics.

Dr. Merhav was a co-recipient of the 1993 Paper Award of the IEEE Information Theory Society and he is a Fellow of the IEEE since 1999. He also received the 1994 American Technion Society Award for Academic Excellence and the 2002 Technion Henry Taub Prize for Excellence in Research. From 1996 until 1999 he served as an Associate Editor for Source Coding to the IEEE TRANSACTIONS ON INFORMATION THEORY. He also served as a co-chairman of the Program Committee of the 2001 IEEE International Symposium on Information Theory. He is currently on the Editorial Board of FOUNDATIONS AND TRENDS IN COMMUNICATIONS AND INFORMATION THEORY.