IRWIN AND JOAN JACOBS
CENTER FOR COMMUNICATION AND INFORMATION TECHNOLOGIES

Reliability of Universal Decoding Based on Vector-Quantized Codewords

Neri Merhav

CCIT Report #904
September 2016

THE ANDREW & ERNA VITERBI FACULTY OF ELECTRICAL ENGINEERING
TECHNION—ISRAEL INSTITUTE OF TECHNOLOGY, HAIFA 3200003, ISRAEL

CCIT Report #904 September 2016

Reliability of Universal Decoding Based on Vector–Quantized Codewords

Neri Merhav

The Andrew & Erna Viterbi Faculty of Electrical Engineering
Technion - Israel Institute of Technology
Technion City, Haifa 32000, ISRAEL
E–mail: merhav@ee.technion.ac.il

Abstract

Motivated by applications of biometric identification and content identification systems, we consider the problem of random coding for channels, where each codeword undergoes lossy compression (vector quantization), and where the decoder bases its decision only on the compressed codewords and the channel output, which is in turn, the channel's response to the transmission of an original codeword, before compression. For memoryless sources and memoryless channels with finite alphabets, we propose a new universal decoder and analyze its error exponent, which improves on an earlier result by Dasarathy and Draper (2011), who used the classic maximum mutual information (MMI) universal decoder. Further, we show that our universal decoder provides the same error exponent as that of the optimal, maximum likelihood (ML) decoder, at least as long as all single–letter transition probabilities of the channel are positive. We conjecture that the same argument remains true even without this positivity condition.

Index Terms: Content identification, biometric identification, channel capacity, error exponent, rate–distortion coding, universal decoding, MMI.

1 Introduction

The problems of biometric identification (see, e.g., [5, Chap. 5], [11], [14], [15] and references therein) and content identification ([2], [3] see also the related problem of pattern recognition [13]) have received some considerable attention in the last few years.

Both of these problems have a certain version that, in a nutshell, can be described in two phases, as follows. In the first phase, a.k.a. the *enrollment phase*, e^{nR} mutually independent, randomly drawn vectors of length n are quantized and stored in a database. In the second phases, a.k.a. the *identification phase*, a noisy version of one of the original random vectors (before quantization) is presented to the system, which in turn has to identify the index of the corresponding stored (compressed) vector. In the case of biometric identification systems, the various signals are biometric ones (e.g., voices, fingerprints, face photographs, irises, etc.) corresponding to a group of individuals who subscribe to the biometric system in the enrollment phase, and the storage of these signals (which are naturally analog in their original form), using a finite amount of memory, can be carried out, of course, within finite accuracy only, due to the quantization. In content identification, the scenario is similar except that the various signals represent contents (for example, documents, images or video files [12]), which are desired to be identified (in spite of some possible modifications) and found in the system, whenever existent therein.

From the information–theoretic point of view, this problem naturally falls within the framework of coded communication in the random coding regime,[1] where the decoder does not have direct access to the original transmitted codewords themselves, but only to distorted versions of these codewords, that are obtained after lossy compression. Nonetheless, the channel output that is presented to the decoder is obtained as the response of the channel to one of the original codewords, before the lossy compression. For a memoryless source and channel, the maximum achievable rate R (i.e., the capacity) of this model setting has already been established by Tuncel [11] (see also [13], [14], [15]). Two years later, Dasarathy and Draper [2] have derived a lower bound to the achievable reliability (achievable error exponent) at a given rate R, and then after three more years [3], the same authors have also derived an upper (converse) bound to the reliability function based on a

[1] While in classic information theory, the concept of random coding is, first and foremost, a trick for a non–constructive proof for the existence of good codes, here it is part of the model, which represents the biometric source, or the source that generates the contents, depending on the application.

sphere–packing argument.

In this paper, we improve on the analysis in [2]. In particular, while Dasarathy and Draper chose to analyze the performance of the well–known maximum mutual information (MMI) decoder [1], without an apparent explanation and justification for this choice of decoder, here we argue that, in this special setting, there is room for improvement over the MMI decoder, in two different aspects. The first is relevant even without lossy compression: the MMI decoding metric is universally optimal (in the sense of the random coding error exponent) when the code ensemble is defined by the uniform distribution within a given type class, but when the random coding distribution is i.i.d. (as in the model considered in [2] and here), the MMI decoding metric should be modified by adding a divergence term between the empirical distribution of the codeword being tested and the true random coding distribution (see [8, eq. (16)]). On top of that, when the compression ingredient is brought back into the picture, this divergence term should be modified too. The second aspect of the improvement over the MMI decoder, is that the MMI metric should also be modified to account to the fact that after compression, the support of the induced random coding distribution is limited to the reproduction codebook of the lossy source encoder. As a consequence, instead of the normalized log–cardinality of the conditional type of the codeword given the channel output (which appears in the analysis of the usual setting and yields the conditional empirical entropy term that is part of the MMI metric), it turns out that one should better use the normalized logarithm of the *number of reproduction vectors that are jointly typical* with the channel output.

The main part of this paper is in the performance analysis of a new universal decoder that is obtained after the two above described modifications, and our main contributions are as follows.

1. Exponentially tight error performance analysis for the new proposed universal decoder.

2. Comparison with the result in [2]. The error exponent of the proposed decoder is at least as large as that of [2], and often, strictly so.

3. It is shown that the new universal decoder provides the same random coding error exponent as the optimal maximum likelihood (ML) decoder at least as long as all single–letter transition probabilities of the channel are positive. We believe that this positivity limitation is merely a technical issue, and in fact, this finding continues to hold true even without this limitation.

The source of this belief is the fact that random coding exponents are normally continuous in the channel parameters.

4. The new proposed decoder is shown to be no worse than any other decoder that bases its decision solely on the joint empirical distribution of the codebook vector being tested and the channel output, and this holds for any memoryless channel, even without the positivity limitation mentioned in item 3.

5. As a byproduct of the above, we also provide a good approximation to the ML decoder that is based on empirical distributions only (in the sense of item 4). This approximation applies to the vast majority of lossy compression codebooks in the ensemble, as long as the channel satisfies the positivity condition. The approximation could be useful because even when the channel is known, the exact ML decoder is hard to implement, due to the compression part.

The outline of the remaining part of this paper is as follows. In Section 2, we establish notation conventions. Section 3 is devoted to the formal description of the problem. Section 4 provides an informal outline of the basic idea of this work. In Section 5, we formally introduce the proposed universal decoder, and then, state and prove the main result of this work, along with a discussion that contains, among other things, a comparison with [2]. In Section 6, we derive a matching lower bound to the average error probability of the ML decoder. Finally, in Section 7, we summarize and conclude.

2 Notation Conventions

Throughout the paper, random variables will be denoted by capital letters, specific values they may take will be denoted by the corresponding lower case letters, and their alphabets will be denoted by calligraphic letters. Random vectors and their realizations will be denoted, respectively, by capital letters and the corresponding lower case letters, both in the bold face font. Their alphabets will be superscripted by their dimensions. For example, the random vector $\boldsymbol{X} = (X_1, \ldots, X_n)$, ($n$ – positive integer) may take a specific vector value $\boldsymbol{x} = (x_1, \ldots, x_n)$ in $\mathcal{X}^n$, the n–th order Cartesian power of $\mathcal{X}$, which is the alphabet of each component of this vector. Sources and channels will be subscripted by the names of the relevant random variables/vectors and their conditionings, whenever needed

and if applicable, following the standard notation conventions, e.g., Q_X, $Q_{Y|X}$, and so on. When there is no room for ambiguity, these subscripts will be omitted. For a given Q_X and $Q_{Y|X}$, the notation $(Q_X \times Q_{Y|X})_Y$ will be used to denote the operation that returns the induced marginal of Y, that is, $Q_Y(y) = \sum_{x\in\mathcal{X}} Q_X(x)Q_{Y|X}(y|x)$, and a similar notation rule will apply to other pairs (or triples) of random variables. For a generic joint distribution $Q_{XY} = \{Q_{XY}(x,y),\ x \in \mathcal{X},\ y \in \mathcal{Y}\}$, which will often be abbreviated by Q, information measures will be denoted in the conventional manner, but with a subscript Q, that is $H_Q(X)$ is the marginal entropy of X, $H_Q(X|Y)$ is the conditional entropy of X given Y, $I_Q(X;Y) = H_Q(X) - H_Q(X|Y)$ is the mutual mutual information, $D(Q_X\|G)$ is the relative entropy between Q_X and another distribution $G = \{G(x),\ x \in \mathcal{X}\}$, and so on. The weighted divergence between two conditional distributions (channels), say, $Q_{Z|X}$ and $W = \{W(z|x), x \in \mathcal{X},\ z \in \mathcal{Z}\}$, with weighting Q_X is defined as

$$D(Q_{Z|X}\|W|Q_X) = \sum_{x\in\mathcal{X}} Q_X(x) \sum_{z\in\mathcal{Z}} Q_{Z|X}(z|x) \log \frac{Q_{Z|X}(z|x)}{W(z|x)}. \tag{1}$$

The probability of an event $\mathcal{E}$ under P will be denoted by $P[\mathcal{E}]$, and the expectation operator with respect to (w.r.t.) a probability distribution P will be denoted by $\boldsymbol{E}_P\{\cdot\}$. Again, the subscript will be omitted if the underlying probability distribution is clear from the context. For two positive sequences a_n and b_n, the notation $a_n \doteq b_n$ will stand for equality in the exponential scale, that is, $\lim_{n\to\infty} \frac{1}{n} \log \frac{a_n}{b_n} = 0$. Similarly, $a_n \stackrel{\cdot}{\leq} b_n$ means that $\limsup_{n\to\infty} \frac{1}{n} \log \frac{a_n}{b_n} \leq 0$, and so on. The indicator function of an event $\mathcal{E}$ will be denoted by $\mathcal{I}\{E\}$. The notation $[x]_+$ will stand for $\max\{0, x\}$.

The empirical distribution of a sequence $\boldsymbol{x} \in \mathcal{X}^n$, which will be denoted by $\hat{P}_{\boldsymbol{x}}$, is the vector of relative frequencies $\hat{P}_{\boldsymbol{x}}(x)$ of each symbol $x \in \mathcal{X}$ in $\boldsymbol{x}$. The type class of $\boldsymbol{x} \in \mathcal{X}^n$, denoted $\mathcal{T}(\boldsymbol{x})$, is the set of all vectors $\boldsymbol{x}'$ with $\hat{P}_{\boldsymbol{x}'} = \hat{P}_{\boldsymbol{x}}$. When we wish to emphasize the dependence of the type class on the empirical distribution $\hat{P}$, we will denote it by $\mathcal{T}(\hat{P})$. Information measures associated with empirical distributions will be denoted with 'hats' and will be subscripted by the sequences from which they are induced. For example, the entropy associated with $\hat{P}_{\boldsymbol{x}}$, which is the empirical entropy of $\boldsymbol{x}$, will be denoted by $\hat{H}_{\boldsymbol{x}}(X)$. Similar conventions will apply to the joint empirical distribution, the joint type class, the conditional empirical distributions and the conditional type classes associated with pairs (and multiples) of sequences of length n. Accordingly, $\hat{P}_{\boldsymbol{xy}}$ would be the joint empirical distribution of $(\boldsymbol{x}, \boldsymbol{y}) = \{(x_i, y_i)\}_{i=1}^n$, $\mathcal{T}(\boldsymbol{x}, \boldsymbol{y})$ or $\mathcal{T}(\hat{P}_{\boldsymbol{xy}})$ will

denote the joint type class of $(\boldsymbol{x}, \boldsymbol{y})$, $\mathcal{T}(\boldsymbol{x}|\boldsymbol{y})$ will stand for the conditional type class of $\boldsymbol{x}$ given $\boldsymbol{y}$, $\hat{H}_{\boldsymbol{xy}}(X,Y)$ will designate the empirical joint entropy of $\boldsymbol{x}$ and $\boldsymbol{y}$, $\hat{H}_{\boldsymbol{xy}}(X|Y)$ will be the empirical conditional entropy, $\hat{I}_{\boldsymbol{xy}}(X;Y)$ will denote empirical mutual information, and so on. When we wish to emphasize the dependence of $\mathcal{T}(\boldsymbol{x}|\boldsymbol{y})$ upon $\boldsymbol{y}$ and the relevant empirical conditional distribution, $Q_{X|Y} = \hat{P}_{\boldsymbol{x}|\boldsymbol{y}}$, we denote it by $\mathcal{T}(Q_{X|Y}|\boldsymbol{y})$. Similar conventions will apply to triples of sequences, say, $\{(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})\}$, etc. Likewise, when we wish to emphasize the dependence of empirical information measures upon a given empirical distribution given by Q, we denote them using the subscript Q, as described above.

3 Problem Formulation

3.1 General Setting

Consider a discrete memoryless source (DMS), G, which, in the enrollment phase, generates $M = e^{nR_{\mathrm{I}}}$ vectors of length n, $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_M$, $\boldsymbol{x}_m \in \mathcal{X}^n$, $m = 1, 2, \ldots, M$, $\mathcal{X}^n$ being the n–th Cartesian power of a finite alphabet $\mathcal{X}$, and R_{I} being the identification rate. Each such vector is generated according to

$$G(\boldsymbol{x}) = \prod_{i=1}^{n} G(x_i), \tag{2}$$

where $G = \{G(x),\ x \in \mathcal{X}\}$ designates the source. To complete the enrollment phase, each vector $\boldsymbol{x}_m$, $m = 1, 2, \ldots, M$, is fed into a lossy source encoder (vector quantizer), whose output is $\boldsymbol{y}_m = f(\boldsymbol{x}_m) \in \mathcal{Y}^n$ (the n–th Cartesian power of another finite alphabet, $\mathcal{Y}$), and then $\boldsymbol{y}_m$ is stored in the database. The construction of $f(\cdot)$, which must trade off between compression constraints and identification performance, will be described in Subsection 3.2.

In the identification phase, an index m is selected uniformly at random and then a noisy version $\boldsymbol{z}$, of $\boldsymbol{x}_m$, is presented to the system with the query to identify m, based on $\boldsymbol{z}$ and on the codebook $\mathcal{C} = \{\boldsymbol{y}_1, \ldots, \boldsymbol{y}_M\}$ of quantized enrollment vectors. This noisy version $\boldsymbol{z} \in \mathcal{Z}^n$ ($\mathcal{Z}^n$ being the n–th Cartesian power of yet another finite alphabet, $\mathcal{Z}$), is generated by a discrete memoryless channel (DMC), according to $W(\boldsymbol{z}|\boldsymbol{x}_m)$, where for a generic $\boldsymbol{x} \in \mathcal{X}^n$,

$$W(\boldsymbol{z}|\boldsymbol{x}) = \prod_{i=1}^{n} W(z_i|x_i), \tag{3}$$

and we denote by W the matrix of the single–letter transition probabilities, $\{W(z|x),\ x \in \mathcal{X},\ z \in \mathcal{Z}\}$.

As in [2], we are interested in an achievable exponential bound to the error probability in decoding the index m for the query in the identification phase. In principle, the problem falls in the ordinary framework of ML decoding with the likelihood function

$$P(\boldsymbol{z}|\boldsymbol{y}_m) = \frac{P(\boldsymbol{y}_m, \boldsymbol{z})}{P(\boldsymbol{y}_m)} = \frac{\sum_{\boldsymbol{x}\in\mathcal{X}^n} G(\boldsymbol{x})W(\boldsymbol{z}|\boldsymbol{x})\mathcal{I}\{\boldsymbol{x} \in f^{-1}(\boldsymbol{y}_m)\}}{\sum_{\boldsymbol{x}\in\mathcal{X}^n} G(\boldsymbol{x})\mathcal{I}\{\boldsymbol{x} \in f^{-1}(\boldsymbol{y}_m)\}}, \tag{4}$$

where $f^{-1}(\boldsymbol{y}_m) = \{\boldsymbol{x} \in \mathcal{X}^n :\ f(\boldsymbol{x}) = \boldsymbol{y}_m\}$ is the inverse image of $\boldsymbol{y}_m$ induced by the lossy encoder f. We would like to characterize an ensemble of source encoders $\{f\}$, that satisfy a certain compression constraint, and a universal decoder $\hat{m} = g(\boldsymbol{z}, \mathcal{C})$, whose average (over the ensemble of $\{f\}$) error probability,

$$\bar{\mathrm{P}}_{\mathrm{e}} = \frac{1}{M}\sum_{m=1}^{M} \Pr\{g(\boldsymbol{z}, \mathcal{C}) \neq m\}, \tag{5}$$

is as small as possible, or more precisely, its error exponent,

$$E(R) = \lim_{n\to\infty}\left[-\frac{\log \bar{\mathrm{P}}_{\mathrm{e}}}{n}\right], \tag{6}$$

is as large as possible (provided that the limit exists).

Let L be a length function of a lossless code, that is, a function from $\mathcal{C}$ to the positive integers, satisfying the Kraft inequality, $\sum_{\boldsymbol{y}\in\mathcal{C}} 2^{-L(\boldsymbol{y})} \leq 1$. Also, let $R_{\mathrm{C}} > 0$ be given. The compression constraint can be formalized in many ways. A few examples are the following.

1. *Expected length constraint:* $\boldsymbol{E}\{L(\boldsymbol{Y})\} \leq nR_{\mathrm{C}}$.
2. *Excess–length probability constraint:* $\Pr\{L(\boldsymbol{Y}) \geq nR_{\mathrm{C}}\} \leq e^{-nE_{\mathrm{C}}}$ for a given $E_{\mathrm{C}} > 0$.
3. *Exponential moment constraint:* $\boldsymbol{E}\{\exp[sL(\boldsymbol{Y})]\} \leq e^{n\Lambda}$ for given $s > 0$ and $\Lambda > 0$.

3.2 The Ensemble of Lossy Encoders

We now move on to describe the construction of lossy encoder $f : \mathcal{X}^n \to \mathcal{C}$, or more precisely, the ensemble of lossy encoders. In essence, it is similar to the one in [2], but there are a few technical differences, which we use mainly for convenience.

For certain technical reasons that will become apparent later, we will assume first that $|\mathcal{Y}| \geq |\mathcal{X}|$ (and in Section 5, we will discuss the case where this assumption is dropped). Fix an arbitrarily small number $\Delta > 0$. The codebook $\mathcal{C} = \{\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m\}$ is selected at random as as follows: For each $\boldsymbol{x}$ from a type class $\mathcal{T}(Q_X)$ with $H_Q(X) < \sqrt{\Delta}$, set the encoder output to be $\boldsymbol{y} \equiv \boldsymbol{x}$, that is, no distortion is incurred.[2] For each type class with $H_Q(X) \geq \sqrt{\Delta}$ choose a certain conditional type $Q_{Y|X} = \{Q_{Y|X}(y|x)\ x \in \mathcal{X},\ y \in \mathcal{Y}\}$ (depending on Q_X), and then select uniformly at random $M_Q = e^{nR_Q}$, $R_Q = I_Q(X;Y) + \Delta$ members of $\mathcal{T}(Q_Y)$ to form a sub-code $\mathcal{C}_Q = \{\boldsymbol{y}_\ell,\ \ell = 1, 2, \ldots, M_Q\}$. The choice of $Q_{Y|X}$ is subjected to a compression constraint, considering the fact that the compressed description of the encoder output is of length approximately nR_Q (plus an overhead of $O(\log n)$ bits that specify the type Q_X). For example, to meet the expected length constraint, $I_Q(X;Y)$ should not exceed $R_{\rm C}$ for all Q_X in the vicinity of G. For the excess length probability constraint, $I_Q(X;Y)$ must be kept less than $R_{\rm C}$ for every Q_X with $D(Q_X\|G) \leq E_{\rm C}$. For the exponential length moment constraint, $sI_Q(X,Y) - D(Q_X\|G)$ must not exceed Γ for any Q_X, namely, $I_Q(X;Y) \leq (\Lambda - D(Q_X\|G)/s$ for every Q_X.

For reasons that will become apparent later, we will assume that the choice of $Q_{Y|X}$, for each Q_X, is such that the induced mapping $Q_X \to Q_Y$ is one–to–one, namely, each Q_Y is induced by no more than one Q_X.[3] This means that given either Q_X or Q_Y, the entire joint type Q_{XY} is fully determined. Moreover, for technical reasons, we will assume that for each Q_X with $H_Q(X) \geq \sqrt{\Delta}$, $Q_{Y|X}$ is selected such that $H_Q(X|Y) \geq \Delta + 3\epsilon$, for some $0 < \epsilon \ll \Delta$. As said, each $\boldsymbol{y}_\ell \in \mathcal{C}_Q$ is selected independently at random under the uniform distribution within the type class of $Q_Y = \{Q_Y(y)\ y \in \mathcal{Y}\}$, where $Q_Y(y) = \sum_x Q_X(x)Q_{Y|X}(y|x)$. The rate–distortion encoding rule is as follows. Each conditional type $\mathcal{T}(Q_{Y|X}|\boldsymbol{x})$, $\boldsymbol{x} \in \mathcal{X}^n$ (with $Q_{Y|X}$ matched to the type of $\boldsymbol{x}$), undergoes ranking according to a randomly chosen ordering of the members of $\mathcal{T}(Q_{Y|X}|\boldsymbol{x})$, under the uniform distribution across all $|\mathcal{T}(Q_{Y|X}|\boldsymbol{x})|!$ possible permutations.[4] The orderings are independent for the various conditional types $\{\mathcal{T}(Q_{Y|X}|\boldsymbol{x}),\ \boldsymbol{x} \in \mathcal{X}^n\}$. Let $M(\boldsymbol{x}, \boldsymbol{y})$ denote the rank

[2]This distinction between $H_Q(X) < \sqrt{\Delta}$ and $H_Q(X) \geq \sqrt{\Delta}$ is carried out for technical reasons only, and it will be needed only in Section 6, where we derive the compatible lower bound on the error probability of the ML decoder (in other words, in Section 5, one can take $\Delta = 0$). In essence, for input sequences with very low empirical entropy, it makes sense to apply lossless compression. This can only improve the identification performance without compromising the compression constraint.

[3]As a consequence of this fact, for Q_X with $H_Q(X) < \sqrt{\Delta}$, we also have $H_Q(Y) < \sqrt{\Delta}$. To maintain the one–to–one relation, it then follows also that $H_Q(X) \geq \sqrt{\Delta}$ implies $H_Q(Y) \geq \sqrt{\Delta}$.

[4]The concept of ranking was already introduced in the dual context, of channel decoding [4], [6] as a convenient rule for resolving ties.

of $\boldsymbol{y} \in \mathcal{T}(Q_{Y|X}|\boldsymbol{x})$. Let $\mathcal{M}$ denote the set of randomly chosen ranking functions $\{M(\boldsymbol{x},\boldsymbol{y}),\ \boldsymbol{x} \in \mathcal{X}^n,\ \boldsymbol{y} \in \mathcal{Y}^n\}$. Now, each $\boldsymbol{x}_m \in \mathcal{T}(Q_X)$ is encoded into the member of $\mathcal{T}_{Q_{Y|X}}(\boldsymbol{x}_m) \bigcap \mathcal{C}_Q$ with the smallest rank, $M(\boldsymbol{x}_m, \boldsymbol{y})$. If $\mathcal{T}_{Q_{Y|X}}(\boldsymbol{x}_m) \bigcap \mathcal{C}_Q = \emptyset$, the encoder outputs an arbitrary n–tuple designating an error message (say, the all–zero sequence), without a hope for successful operation. Let f denote the resulting rate–distortion coding function, i.e., $\boldsymbol{y} = f(\boldsymbol{x})$. The rate–distortion encoder f is therefore defined by the independent random selection of both $\mathcal{C} = \cup_Q C_Q$ and $\mathcal{M}$.

4 The Basic Idea

The problem with the exact likelihood function (4) is that it is difficult to work with, both in the operative level, as an actual decoding metric, and in the theoretical level, of a single–letter performance analysis, and the reason, of course, is the multiplicative term $\mathcal{I}\{\boldsymbol{x} \in f^{-1}(\boldsymbol{y}_m)\}$, that appears both in the numerator and the denominator. Dasarathy and Draper [2] have therefore analyzed a simpler decoder – the well known MMI decoder, which estimates m according to the quantized enrollment vector $\boldsymbol{y}_m$ with the highest value of $\hat{I}_{\boldsymbol{y}_m \boldsymbol{z}}(Y;Z)$. They have derived an achievable error exponent for a random selection of f, which indicates that the MMI decoder is good enough to achieve the maximum rate R (channel capacity), given by $\max I(Y;Z)$, where the joint distribution of (Y,Z) is induced by a Markov chain $Y \to X \to Z$ and the maximization is over the conditional distribution of Y given X, which is subjected to a compression constraint, $I(X;Y) \leq R_{\mathrm{C}}$, R_{C} being the allowed compression rate (see also [11]).

While the MMI decoder was shown to be sufficiently good to achieve capacity, no further justification for this choice of decoder was provided in [2]. A somewhat closer inspection, however, reveals that there may be room for improvement in the choice of the universal decoder, in order to achieve a better error exponent for a given rate below capacity. This follows from the two following observations, which together form the basic idea of the paper.

The first observation is relevant even in the classical random coding scenario, without the ingredient of lossy compression (i.e., $\boldsymbol{y}_m \equiv \boldsymbol{x}_m$). Consider then the ordinary random coding regime, where each codeword is selected independently at random under the memoryless source G. Let the transmitted codeword $\boldsymbol{x}$ and the corresponding channel output $\boldsymbol{z}$ be given. The pairwise error event, that an independently generated competing codeword $\boldsymbol{x}'$ would pose a threat to the correct

decoding is lower bounded as follows:

$$\begin{aligned}\sum_{\{\boldsymbol{x}':\ W(\boldsymbol{z}|\boldsymbol{x}')\geq W(\boldsymbol{z}|\boldsymbol{x})\}} G(\boldsymbol{x}') &\geq \sum_{\boldsymbol{x}'\in\mathcal{T}(\boldsymbol{x}|\boldsymbol{z})} G(\boldsymbol{x}') \\ &= \sum_{\boldsymbol{x}'\in\mathcal{T}(\boldsymbol{x}|\boldsymbol{z})} G(\boldsymbol{x}) \\ &= |\mathcal{T}(\boldsymbol{x}|\boldsymbol{z})|\cdot G(\boldsymbol{x}) \\ &\doteq \exp\{-n[\hat{I}_{\boldsymbol{x}\boldsymbol{z}}(X;Z)+D(\hat{P}_{\boldsymbol{x}}\|G)]\}, \end{aligned} \tag{7}$$

which is easily shown (using the method of types) to be achieved by the universal decoder $\hat{m} = \arg\max_m[\hat{I}_{\boldsymbol{x}_m\boldsymbol{z}}(X;Z)+D(\hat{P}_{\boldsymbol{x}_m}\|G)]$ (see also [8, eq. (16)]). In other words, while the MMI decoding metric is asymptotically optimal (in the random coding sense) for the ensemble of *fixed composition codes*, when it comes to the ensemble of i.i.d. random codewords, under G, this metric should be supplemented with the divergence term, $D(\hat{P}_{\boldsymbol{x}_m}\|G)$.

The second observation comes about when we put back the lossy compression ingredient into our system model. In this case, the $\boldsymbol{x}$–vectors in eq. (7) should be replaced by $\boldsymbol{y}$-vectors from the given codebook $\mathcal{C}$, and the channel W should be replaced by the channel P defined in eq. (4). Similarly, $G(\boldsymbol{x}')$ should be replaced by $P(\boldsymbol{y}')$, which is the denominator of (4). Suppose now that we can[5] approximate $P(\boldsymbol{y}')$ by $e^{-n\alpha(\hat{P}_{\boldsymbol{y}'})}$ (for $\boldsymbol{y}'\in\mathcal{C}$) and $P(\boldsymbol{z}|\boldsymbol{y})$ by $e^{-n\beta(\hat{P}_{\boldsymbol{y}\boldsymbol{z}})}$, where $\alpha(\cdot)$ and $\beta(\cdot)$ are certain functions. Then, taking into account that $P(\boldsymbol{y}')>0$ only for $\boldsymbol{y}'\in\mathcal{C}$, the analogue of the third line of (7) would now read $|\mathcal{T}(\boldsymbol{y}|\boldsymbol{z})\cap\mathcal{C}|\cdot e^{-n\alpha(\hat{P}_{\boldsymbol{y}})}$, a lower bound, which is asymptotically achieved by the universal decoder,

$$\hat{m}_{\rm u} = \arg\min_m[\log N(\boldsymbol{y}_m|\boldsymbol{z}) - n\alpha(\hat{P}_{\boldsymbol{y}_m})], \tag{8}$$

where $N(\boldsymbol{y}|\boldsymbol{z}) = |\mathcal{T}(\boldsymbol{y}|\boldsymbol{z})\cap\mathcal{C}|$, i.e., the number of codebook vectors that are in the conditional type $\mathcal{T}(\boldsymbol{y}|\boldsymbol{z})$. In other words, our second observation is that in the problem setting considered here, the MMI decoder should be modified, not only to account for the non–uniform input distribution, as mentioned in the first observation above, but also to account for the fact the support of this distribution is only $\mathcal{C}$, and not $\mathcal{Y}^n$ in its entirety. In the next section, we will first specify the function $\alpha(\cdot)$ and thereby fully define the proposed universal decoder (8).

[5]This will indeed be shown later to be possible for most encoders $\{f\}$ in the ensemble.

5 Main Result

As mentioned in Section 3.2, since we assume that for each input assignment Q_X, the channel $Q_{Y|X}$ is selected such that the mapping from Q_X to $Q_Y = (Q_X \times Q_{Y|X})_Y$ is one–one, a given Q_Y can be induced from only one Q_X, which in turn dictates $Q_{Y|X}$, and hence also the entire joint distribution Q_{XY}. In view of this, for a given Q_Y (or equivalently, a given Q_{XY}), let us define

$$A_Q(Y) = I_Q(X;Y) + D(Q_X\|G). \tag{9}$$

To emphasize the dependence of $A_Q(Y)$ upon the empirical distribution of a given $\boldsymbol{y}$, we also use the alternative notation $\alpha(\hat{P}_{\boldsymbol{y}})$ instead of $A_Q(Y)$, for every $\boldsymbol{y} \in \mathcal{T}(Q_Y)$ (i.e., $\hat{P}_{\boldsymbol{y}} = Q_Y$). Defining the universal decoder (8) with this choice of the function $\alpha(\cdot)$, we are now ready to state our main result.

Theorem 1 *Consider the model and the assumptions described in Section 3 and the universal decoder (8) with the above definition of the function $\alpha(\cdot)$. Then, for a given choice of $Q_{Y|X}$ as a functional of Q_X, the random coding error exponent associated with the ensemble of codes, described in Subsection 3.2, is given by*

$$\begin{aligned} E(R_{\rm I}) \;=\; \min_{Q_X}\min_{Q_{Z|Y}}\Bigg\{ & D(Q_X\|G) + \min_{\tilde{Q}_{X|YZ}\in\mathcal{U}(Q_{X|Y})} D(\tilde{Q}_{XZ|Y}\|Q_{X|Y}\times W|Q_Y) + \\ & + \max\{[I_Q(Y;Z) - I_Q(X;Y)]_+, [I_Q(Y;Z) + D(Q_X\|G) - R_{\rm I}\}]_+\}\,, \end{aligned} \tag{10}$$

where, for a given Q_{YZ}, the set $\mathcal{U}(Q_{X|Y})$ is defined to consist of all conditional distributions $\{\tilde{Q}_{X|YZ}\}$ that are consistent with $Q_{X|Y}$, that is, $\sum_{z\in\mathcal{Z}}\tilde{Q}_{X|YZ}(x|y,z)Q_{Y|Z}(y|z) = Q_{X|Y}(x|y)$ for every $(x,y)\in\mathcal{X}\times\mathcal{Y}$.

Before we prove this theorem, a brief discussion is in order.

First, observe that the objective function to be minimized in (10) is a functional of Q_X (or equivalently, Q_{XY}) and Q_{YZ}, or, equivalently, $Q_{Z|Y}$, as Q_Y is already dictated by Q_X. Since Q_X and $Q_{Z|Y}$ are not subject to our control, they undergo minimization. The controllable part is the choice of $Q_{Y|X}$, which is allowed to depend on Q_X, but not on $Q_{Z|Y}$. Therefore, the expression of $E(R_{\rm I})$ should, in principle, include also maximization over $Q_{Y|X}$ in between $\min_{Q_X}$ and $\min_{Q_{Z|Y}}$. This maximization should be carried out, of course, subject to the compression constraint, which

limits $Q_{Y|X}$ to some subset denoted $\mathcal{Q}$. The caveat is, however, that there is no apparent guarantee that the optimal $Q_{Y|X}$, as a functional of Q_X, would induce a one–to–one mapping from Q_X to Q_Y, a requirement that was already mentioned in Subsection 3.2, and whose motivation will be explained in the next paragraph. Nonetheless, we show in the appendix (subsection A.1) that it is possible to slightly modify the optimal $Q_{Y|X}$ by an arbitrarily small perturbation (and thus lose an arbitrarily small amount from the optimal error exponent, due to continuity) and thereby make the mapping $Q_X \to Q_Y$ one–to–one. It follows then that we can approach arbitrarily closely the min–max–min expression,

$$\min_{Q_X} \max_{Q_{Y|X}\in\mathcal{Q}} \min_{Q_{Z|Y}} \Bigg\{ D(Q_X\|G) + \min_{\tilde{Q}_{X|YZ}\in\mathcal{U}(Q_{X|Y})} D(\tilde{Q}_{XZ|Y}\|Q_{X|Y}\times W|Q_Y) + \\ + \max\{[I_Q(Y;Z) - I_Q(X;Y)]_+, [I_Q(Y;Z) + D(Q_X\|G) - R_{\rm I}]_+\}\Bigg\}. \tag{11}$$

As promised in the previous paragraph (and earlier), we now explain the motivation for insisting on a one–to–one mapping $Q_X \to Q_Y$. The easiest way to see this is to look at the expression $|\mathcal{T}(\boldsymbol{y}|\boldsymbol{z})\cap\mathcal{C}|\cdot\exp\{-n\alpha(\hat{P}\boldsymbol{y})\}$, which appears in the last paragraph of Section 3, in the context of an achievable lower bound to the pairwise error probability for a given $(\boldsymbol{y},\boldsymbol{z})$. We would like, of course, to keep this quantity as small as possible. Now, in general, if $Q_X \to Q_Y$ is not necessarily one–to–one, $\mathcal{T}(\boldsymbol{y}|\boldsymbol{z})\cap\mathcal{C}$ may include reproduction vectors that correspond to $\boldsymbol{x}$–vectors from all types $\{Q_X\}$ that are mapped to the given $Q_Y = \hat{P}\boldsymbol{y}$, but if $Q_X \to Q_Y$ is one–to–one, then there is only one such Q_X. Moreover, a many–to–one relation $Q_X \to Q_Y$ may decrease the above exponential term $\alpha(\hat{P}\boldsymbol{y})$ (i.e., increase the factor $\exp\{-n\alpha(\hat{P}\boldsymbol{y})\}$) since the given $\boldsymbol{y}$ may have more types $\{Q_X\}$ of source vectors $\{\boldsymbol{x}\}$ that could yield the given $\boldsymbol{y}$ using the source encoder. In particular, the definition of $A_Q(Y)$ should then include also a minimization over all $\{Q_{X|Y}\}$ pertaining to $\{Q_X\}$ that are mapped to the given Q_Y, which may again result in degradation in performance. But when $Q_X \to Q_Y$ is one–to-one, as required, there is only one such Q_X. More precisely, in view of the above discussion, it is possible to show that if the requirement of a one–to–one mapping $Q_X \to Q_Y$ is dropped (and then there is no longer need to assume $|\mathcal{Y}| \geq |\mathcal{X}$, and we can also take $\Delta = 0$), then the term in the second line of (11) should be replaced by the following expression:

$$\left[I_Q(Y;Z) - \max_{\tilde{Q}_{X|Y}\in\mathcal{S}(Q_Y)} I_{\tilde{Q}}(X;Y)\right]_+ + \left[\min_{\tilde{Q}_{X|Y}\in\mathcal{S}(Q_Y)} \{I_{\tilde{Q}}(X;Y) + D(\tilde{Q}_X\|G)\} -\right.$$

$$\left[\max_{\tilde{Q}_{X|Y}\in\mathcal{S}(Q_Y)} I_{\tilde{Q}}(X;Y) - I_Q(Y;Z)\right]_+ - R_{\rm I}\Bigg]_+, \tag{12}$$

where $\mathcal{S}(Q_Y)$ is the collection of all $\tilde{Q}_{X|Y}$ such that $\tilde{Q}_X = (Q_Y \times \tilde{Q}_{X|Y})_X$ is mapped to Q_Y. Clearly, the larger is the set $\mathcal{S}(Q_Y)$, the smaller is the resulting expression, and so, the best one can hope for is that $\mathcal{S}(Q_Y)$ would be a singleton, in which case, it becomes identical to the term in the second line of (11). Nonetheless, it should be pointed out that even in the general case, where $Q_X \to Q_Y$ is not one–to–one, and hence $\mathcal{S}(Q_Y)$ is not a singleton, the resulting error exponent cannot be worse than that of [2], since our proposed universal decoder is at least as good as any other decoder whose metric depends only on the empirical joint distribution of $(\boldsymbol{y}_m, \boldsymbol{z})$ (see item 4 in the Introduction) and in particular, it is also as good as the ML decoder (see Section 6). Here, we should remark that the modification (12) significantly complicates the optimization of $Q_{Y|X}$ for a given Q_X, because (12) depends on the mapping $Q_X = U[Q_{Y|X}]$ in a *global* manner (via the sets $\mathcal{S}(Q_Y)$, induced by $U[\cdot]$) and not only in a local, pointwise manner, of optimizing $Q_{Y|X}$ for each given Q_X separately. Therefore, the appropriate way to present the error exponent expression, in this more general case, is in terms of the series of optimizations, $\sup_{U[\cdot]} \min_{Q_X} \min_{Q_{X|Y}}$, rather than the min–max–min as before. (Of course, the supremum over $U[\cdot]$ is subject to the compression constraint.)

Finally, a word on the comparison between our result (11) and the one in [2, Theorem 1], is in order. The first two terms in (11) are identical to those in [2, Theorem 1], as they are just the terms of the exponential probabilistic weighting of the dominant type Q_{YZ}, i.e., the one that contributes most to the probability of error. However, the third term in (11) is different from the one in [2], which, in our notation, is simply $[I_Q(Y;Z)-R_{\rm I}]_+$. Even if we ignore the term $[I_Q(Y;Z)-I_Q(X;Y)]_+$ in the second line of (11), and lower bound our third term just by $[I_Q(Y;Z)+D(Q_X\|G)-R_{\rm I}]_+$, it obviously cannot be smaller than $[I_Q(Y;Z)-R_{\rm I}]_+$, of [2], due to the divergence term, $D(Q_X\|G)$. It is clear then that, at least at low rates (say, even $R_{\rm I}=0$), the exponent (11) is strictly larger than that of [2] whenever the minimizing Q_X differs from G, which can indeed be the case in many situations (see Subsection A.2 of the appendix for a demonstration of this fact).

Proof of Theorem 1. We begin with a simple upper bound to $P(\boldsymbol{y})$ for $\boldsymbol{y} \in \mathcal{C} \in \mathcal{T}(Q_Y)$, which applies to every $f = (\mathcal{C}, \mathcal{M})$ since $f^{-1}(\boldsymbol{y}) \subseteq \mathcal{T}(Q_{X|Y}|\boldsymbol{y})$, where $Q_{X|Y}$ is the reverse channel that

corresponds to Q_Y:

$$\begin{aligned}
P(\boldsymbol{y}) &= \sum_{\boldsymbol{x}\in\mathcal{X}^n} G(\boldsymbol{x})\mathcal{I}\{\boldsymbol{x}\in f^{-1}(\boldsymbol{y})\} && (13)\\
&\leq |\mathcal{T}(Q_{X|Y}|\boldsymbol{y})|\cdot G(\boldsymbol{x}) && (14)\\
&\leq \exp\{nH_Q(X|Y)+O_1(\log n)\}\cdot\exp\{-n[H_Q(X)+D(Q_X\|G)]\} && (15)\\
&= \exp\{-n[I_Q(X;Y)+D(Q_X\|G)+O_1(\log n)]\} && (16)\\
&= e^{-nA_Q(Y)+O_1(\log n)}, && (17)
\end{aligned}$$

where $O_1(\log n)$ is a quantity (resulting from the method of types), whose leading term is proportional to $\log n$. Similarly, for $(\boldsymbol{y},\boldsymbol{z})\in\mathcal{T}(Q_{YZ})$ with $\boldsymbol{y}\in\mathcal{C}\in\mathcal{T}(Q_Y)$, we have

$$\begin{aligned}
P(\boldsymbol{y},\boldsymbol{z}) &= \sum_{\boldsymbol{x}\in\mathcal{X}^n} G(\boldsymbol{x})W(\boldsymbol{z}|\boldsymbol{x})\mathcal{I}\{\boldsymbol{x}\in f^{-1}(\boldsymbol{y})\} && (18)\\
&\leq \sum_{\{T(Q_{X|YZ}|\boldsymbol{y},\boldsymbol{z}):\ Q_{X|YZ}\in\mathcal{U}(Q_{X|Y})\}} |\mathcal{T}(Q_{X|YZ}|\boldsymbol{y}.\boldsymbol{z})|\cdot[G(\boldsymbol{x})W(\boldsymbol{z}|\boldsymbol{x})]_{(\boldsymbol{x},\boldsymbol{z})\in\mathcal{T}(Q_{XZ})} && (19)\\
&\leq \max_{Q_{X|YZ}\in\mathcal{U}(Q_{X|Y})} \exp\{nH_Q(X|Y,Z)+O_2(\log n)\}\times\\
&\quad \exp\{n\sum_{x,z} Q_{XZ}(x,z)\log[G(x)W(z|x)\} && (20)\\
&= \exp\left\{-n\min_{Q_{X|YZ}\in\mathcal{U}(Q_{X|Y})}\sum_{x,y,z} Q_{XYZ}(x,y,z)\log\frac{Q_{X|YZ}(x|y,z)}{G(x)W(z|x)}+O_2(\log n)\right\} && (21)\\
&\stackrel{\Delta}{=} e^{-nB_Q(Y,Z)+O_2(\log n)}, && (22)
\end{aligned}$$

where $O_2(\log n)$ is again a quantity dominated by a term proportional to $\log n$. For later use, the following algebraic manipulation will be found useful.

$$\begin{aligned}
B_Q(Y,Z) &= \min_{Q_{X|YZ}\in\mathcal{U}(Q_{X|Y},0)}\sum_{x,y,z} Q_{XYZ}(x,y,z)\log\frac{Q_{X|YZ}(x|y,z)}{G(x)W(z|x)}\\
&= \min_{Q_{X|YZ}\in\mathcal{U}(Q_{X|Y})}[H_Q(X,Z)+D(Q_{XZ}\|G\times W)-H_Q(X|Y,Z)]\\
&= \min_{Q_{X|YZ}\in\mathcal{U}(Q_{X|Y})}[H_Q(X)+H_Q(Z|X)-H_Q(X|Y,Z)+D(Q_{XZ}\|G\times W)]\\
&= \min_{Q_{X|YZ}\in\mathcal{U}(Q_{X|Y})}[I_Q(X;Y,Z)+H_Q(Z|X)+D(Q_{XZ}\|G\times W)]\\
&= \min_{Q_{X|YZ}\in\mathcal{U}(Q_{X|Y})}[H_Q(Y,Z)-H_Q(Y,Z|X)+H_Q(Z|X)+D(Q_{XZ}\|G\times W)]\\
&= H_Q(Y,Z)+\min_{Q_{X|YZ}\in\mathcal{U}(Q_{X|Y})}[D(Q_{XZ}\|G\times W)-H_Q(Y|X,Z)]. && (23)
\end{aligned}$$

Now, consider the universal decoding metric

$$d(\boldsymbol{y},\boldsymbol{z}) = \log N(\boldsymbol{y}|\boldsymbol{z}) - n\alpha(\hat{P}\boldsymbol{y}). \tag{24}$$

Then, defining $\mathcal{E}_{\mathrm{u}}(\boldsymbol{y},\boldsymbol{z}) = \{\boldsymbol{y}' :\ d(\boldsymbol{y}',\boldsymbol{z}) \le d(\boldsymbol{y},\boldsymbol{z})\} \cap \mathcal{C}$, we have

$$\begin{aligned}
\sum_{\boldsymbol{y}' \in \mathcal{E}_{\mathrm{u}}(\boldsymbol{y},\boldsymbol{z})} P(\boldsymbol{y}') &= \sum_{\{\mathcal{T}(\boldsymbol{y}'|\boldsymbol{z}):\ \mathcal{T}(\boldsymbol{y}'|\boldsymbol{z}) \cap \mathcal{C} \subseteq \mathcal{E}_{\mathrm{u}}(\boldsymbol{y},\boldsymbol{z})\}} P[\mathcal{C} \cap \mathcal{T}(\boldsymbol{y}'|\boldsymbol{z})] && (25)\\
&= \sum_{\{\mathcal{T}(\boldsymbol{y}'|\boldsymbol{z}):\ \mathcal{T}(\boldsymbol{y}'|\boldsymbol{z}) \cap \mathcal{C} \subseteq \mathcal{E}_{\mathrm{u}}(\boldsymbol{y},\boldsymbol{z})\}} |\mathcal{C} \cap \mathcal{T}(\boldsymbol{y}'|\boldsymbol{z})| \cdot P(\boldsymbol{y}') && (26)\\
&\dot{\le} \sum_{\{\mathcal{T}(\boldsymbol{y}'|\boldsymbol{z}):\ \mathcal{T}(\boldsymbol{y}'|\boldsymbol{z}) \cap \mathcal{C} \subseteq \mathcal{E}_{\mathrm{u}}(\boldsymbol{y},\boldsymbol{z})\}} N(\boldsymbol{y}'|\boldsymbol{z}) \cdot e^{-n\alpha(\hat{P}_{\boldsymbol{y}'})} && (27)\\
&\le \sum_{\{\mathcal{T}(\boldsymbol{y}'|\boldsymbol{z}):\ \mathcal{T}(\boldsymbol{y}'|\boldsymbol{z}) \cap \mathcal{C} \subseteq \mathcal{E}_{\mathrm{u}}(\boldsymbol{y},\boldsymbol{z})\}} N(\boldsymbol{y}|\boldsymbol{z}) \cdot e^{-n\alpha(\hat{P}_{\boldsymbol{y}})} && (28)\\
&\doteq N(\boldsymbol{y}|\boldsymbol{z}) \cdot e^{-n\alpha(\hat{P}_{\boldsymbol{y}})}. && (29)
\end{aligned}$$

Then, for a given $f = (\mathcal{C}, \mathcal{M})$, the probability of error of the universal decoder (8), $\mathrm{P}_{\mathrm{e,u}}(f)$, is upper bounded as follows.

$$\begin{aligned}
\mathrm{P}_{\mathrm{e,u}}(f) &= \sum_{\boldsymbol{y} \in \mathcal{C}} \sum_{\boldsymbol{z} \in \mathcal{Z}^n} P(\boldsymbol{y},\boldsymbol{z}) \cdot \min\left\{1, e^{nR_{\mathrm{I}}} \cdot \sum_{\boldsymbol{y}' \in \mathcal{E}_{\mathrm{u}}(\boldsymbol{y},\boldsymbol{z})} P(\boldsymbol{y}')\right\}\\
&\dot{\le} \sum_{\boldsymbol{y} \in \mathcal{C}} \sum_{\boldsymbol{z} \in \mathcal{Z}^n} P(\boldsymbol{y},\boldsymbol{z}) \cdot \min\left\{1, e^{n[R_{\mathrm{I}} - \alpha(\hat{P}_{\boldsymbol{y}})]} \cdot N(\boldsymbol{y}|\boldsymbol{z})\right\}\\
&= \sum_{\boldsymbol{y} \in \mathcal{Y}^n} \mathcal{I}\{\boldsymbol{y} \in \mathcal{C}\} \cdot \sum_{\boldsymbol{z} \in \mathcal{Z}^n} P(\boldsymbol{y},\boldsymbol{z}) \cdot \min\left\{1, e^{n[R_{\mathrm{I}} - \alpha(\hat{P}_{\boldsymbol{y}})]} \cdot N(\boldsymbol{y}|\boldsymbol{z})\right\}. \qquad (30)
\end{aligned}$$

From this point onward, we will average the upper bound on $\mathrm{P}_{\mathrm{e,u}}(f)$ across the ensemble of $\{f\}$. This will be done in two steps. In the first step, we average over all incorrect codewords, whose contributions are expressed in the random variable $N(\boldsymbol{y}|\boldsymbol{z})$. In the second step, we average over the correct codeword (which is drawn independently of all incorrect codewords), that is expressed in the factor $\mathcal{I}\{\boldsymbol{y} \in \mathcal{C}\}$ in the last expression. Now, for a given pair $(\boldsymbol{y},\boldsymbol{z}) \in \mathcal{T}(Q_{YZ})$, the number $N(\boldsymbol{y}|\boldsymbol{z})$ is a binomial random variable (RV) with $e^{n[I_Q(X;Y)+\Delta]}$ trials and probability of success of the exponential order of $e^{-nI_Q(Y;Z)}$. Thus, for a given $\epsilon > 0$, if $I_Q(X;Y)+\Delta \ge I_Q(Y;Z)$, then $N(\boldsymbol{y}|\boldsymbol{z}) \le e^{n[I_Q(X;Y)-I_Q(Y;Z)+\Delta+\epsilon]}$ with probability at least as larger as $1 - \exp[-(n\epsilon - 1)e^{n\epsilon}]$ (as can easily been seen from a derivation similar to the one in [7, pp. 167–168]). For $I_Q(X;Y) + \Delta < I_Q(Y;Z)$, the RV $N(\boldsymbol{y}|\boldsymbol{z})$ exceeds unity with probability of the exponential order of $e^{-n[I_Q(Y;Z)-I_Q(X;Y)-\Delta]}$ (similarly to [7, eq. (6.36)]) and it exceeds the value $e^{n\epsilon}$, with probability less than $\exp[-(n\epsilon-1)e^{n\epsilon}]$. It follows then that for a given deterministic s, and for $I_Q(X;Y) + \Delta \ge I_Q(Y;Z)$,

$$\begin{aligned}
\boldsymbol{E}\left[\min\left\{1, e^{-ns} N(\boldsymbol{y}|\boldsymbol{z})\right\}\right] &\dot{\le} \min\left\{1, e^{-ns} \cdot e^{n[I_Q(X;Y)-I_Q(Y;Z)+\Delta+\epsilon]}\right\} && (31)\\
&\doteq \exp\{-n[s + I_Q(Y;Z) - I_Q(X;Y) - \Delta - \epsilon]_+\}, && (32)
\end{aligned}$$

whereas for $I_Q(X;Y)+\Delta < I_Q(Y;Z)$,

$$\begin{aligned}\boldsymbol{E}\left[\min\left\{1, e^{-ns}N(\boldsymbol{y}|\boldsymbol{z})\right\}\right] &\stackrel{\cdot}{\leq} e^{-n[I_Q(Y;Z)-I_Q(X;Y)-\Delta]}\cdot\min\left\{1,e^{-ns}\right\} \quad (33)\\ &= \exp\{-n[I_Q(Y;Z)-I_Q(X;Y)-\Delta+[s]_+]\}. \quad (34)\end{aligned}$$

Since we are interested merely in the exponential order, from now on, we shall neglect the Δ and ϵ terms, which eventually tends to zero anyway. The last two equations can now be unified as follows:

$$\begin{aligned}&\boldsymbol{E}\left[\min\left\{1, e^{-ns}N(\boldsymbol{y}|\boldsymbol{z})\right\}\right]\\ \stackrel{\cdot}{\leq}\ &\exp\left\{-n\left([I_Q(Y;Z)-I_Q(X;Y)]_+ + [s-[I_Q(X;Y)-I_Q(Y;Z)]_+]_+\right)\right\}. \quad (35)\end{aligned}$$

This exponential upper bound will be applied with the assignment $s=\alpha(\hat{P}_{\boldsymbol{y}})-R_{\rm I}$ (or equivalently, $s=A_Q(Y)-R_{\rm I}$). As for averaging over the randomness of the correct codeword, note that for a given $\boldsymbol{y}\in\mathcal{T}(Q_Y)$,

$$\boldsymbol{E}[\mathcal{I}\{\boldsymbol{y}\in\mathcal{C}\}]=\Pr\{\boldsymbol{y}\in\mathcal{C}\}=1-\left(1-\frac{1}{|\mathcal{T}(Q_Y)|}\right)^{e^{n[I_Q(X;Y)+\Delta]}}\stackrel{\cdot}{=}e^{-n[H_Q(Y|X)-\Delta]}. \quad (36)$$

Putting all this altogether, we obtain (again, neglecting Δ):

$$\begin{aligned}\bar{\rm P}_{\rm e,u} &\stackrel{\Delta}{=} \boldsymbol{E}\left\{{\rm P}_{\rm e}(f)\right\}\\ &\stackrel{\cdot}{\leq} \sum_{Q_Y}|\mathcal{T}(Q_Y)|\cdot e^{-nH_Q(Y|X)}\sum_{Q_{Z|Y}}|\mathcal{T}(Q_{Z|Y})|\cdot e^{-nB_Q(Y,Z)}\times\\ &\quad \exp\left\{-n\left([I_Q(Y;Z)-I_Q(X;Y)]_+ + [A_Q(Y)-[I_Q(X;Y)-I_Q(Y;Z)]_+-R_{\rm I}]_+\right)\right\}\\ &\stackrel{\cdot}{=} \exp\left\{-n\min_{Q_{YZ}}\left(B_Q(Y,Z)-H_Q(Z|Y)-H_Q(Y)+H_Q(Y|X)+\right.\right.\\ &\quad \left.\left.[I_Q(Y;Z)-I_Q(X;Y)]_+ + [A_Q(Y)-[I_Q(X;Y)-I_Q(Y;Z)]_+-R_{\rm I}]_+\right)\right\}\\ &= \exp\left\{-n\min_{Q_{YZ}}\left(B_Q(Y,Z)-H_Q(Y,Z)+H_Q(Y|X)+[I_Q(Y;Z)-I_Q(X;Y)]_+ + \right.\right.\\ &\quad \left.\left.+[I_Q(X;Y)+D(Q_X\|G)-[I_Q(X;Y)-I_Q(Y;Z)]_+-R_{\rm I}]_+\right)\right\}\\ &= \exp\left\{-n\min_{Q_X,Q_{Z|Y}}\left(B_Q(Y,Z)-H_Q(Y,Z)+H_Q(Y|X)+[I_Q(Y;Z)-I_Q(X;Y)]_+ + \right.\right.\\ &\quad \left.\left.[I_Q(X;Y)+D(Q_X\|G)-[I_Q(X;Y)-I_Q(Y;Z)]_+-R_{\rm I}]_+\right)\right\}. \quad (37)\end{aligned}$$

To simplify the above expression, and to modify its form to one that is more easily comparable to [2], we first observe (using (23)) that

$$B_Q(Y,Z)-H_Q(Y,Z)+H_Q(Y|X)$$

$$
\begin{aligned}
&= \min_{\tilde{Q}_{X|YZ}\in\mathcal{U}(Q_{X|Y})} [D(Q_{XZ}\|G\times W) - H_Q(Y|X,Z)] + H_Q(Y|X) && (38)\\
&= \min_{\tilde{Q}_{X|YZ}\in\mathcal{U}(Q_{X|Y})} [D(Q_{XZ}\|G\times W) + I_{\tilde{Q}}(Y;Z|X)] && (39)\\
&= D(Q_X\|G) + \min_{\tilde{Q}_{X|YZ}\in\mathcal{U}(Q_{X|Y})} [D(\tilde{Q}_{Z|X}\|W|Q_X) + I_{\tilde{Q}}(Y;Z|X)] && (40)\\
&= D(Q_X\|G) + \min_{\tilde{Q}_{X|YZ}\in\mathcal{U}(Q_{X|Y})} \sum_{y,z} Q_{YZ}(y,z)\times && (41)\\
&\quad \sum_x \tilde{Q}_{X|YZ}(x|y,z)\log\left[\frac{\tilde{Q}_{Z|X}(z|x)}{W(z|x)}\cdot\frac{\tilde{Q}_{YZ|X}(y,z|x)}{\tilde{Q}_{Z|X}(z|x)Q_{Y|X}(y|x)}\right] && (42)\\
&= D(Q_X\|G) + \min_{\tilde{Q}_{X|YZ}\in\mathcal{U}(Q_{X|Y})} \sum_{y,z} Q_{YZ}(y,z)\times && (43)\\
&\quad \sum_x \tilde{Q}_{X|YZ}(x|y,z)\log\left[\frac{\tilde{Q}_{YZ|X}(y,z|x)}{W(z|x)Q_{Y|X}(y|x)}\right] && (44)\\
&= D(Q_X\|G) + \min_{\tilde{Q}_{X|YZ}\in\mathcal{U}(Q_{X|Y})} \sum_{y,z} Q_{YZ}(y,z)\times && (45)\\
&\quad \sum_x \tilde{Q}_{X|YZ}(x|y,z)\log\left[\frac{\tilde{Q}_{Z|XY}(z|x,y)}{W(z|x)}\right] && (46)\\
&= D(Q_X\|G) + \min_{\tilde{Q}_{X|YZ}\in\mathcal{U}(Q_{X|Y})} \sum_{y,z} Q_{YZ}(y,z)\times && (47)\\
&\quad \sum_x \tilde{Q}_{X|YZ}(x|y,z)\log\left[\frac{\tilde{Q}_{Z|XY}(z|x,y)Q_{X|Y}(x|y)}{W(z|x)Q_{X|Y}(x|y)}\right] && (48)\\
&= D(Q_X\|G) + \min_{\tilde{Q}_{X|YZ}\in\mathcal{U}(Q_{X|Y})} \sum_{y,z} Q_{YZ}(y,z)\times && (49)\\
&\quad \sum_x \tilde{Q}_{X|YZ}(x|y,z)\log\left[\frac{\tilde{Q}_{XZ|Y}(x,z|y)}{W(z|x)Q_{X|Y}(x|y)}\right] && (50)\\
&= D(Q_X\|G) + \min_{\tilde{Q}_{X|YZ}\in\mathcal{U}(Q_{X|Y})} D(\tilde{Q}_{XZ|Y}\|Q_{X|Y}\times W|Q_Y), && (51)
\end{aligned}
$$

which are the first two terms in (10). As for the other terms of (37), we use the identities $a-[a-b]_+ \equiv b-[b-a]_+ \equiv \min\{a,b\}$ and $b+[a-b]_+ \equiv \max\{a,b\}$ to obtain

$$
\begin{aligned}
&[I_Q(Y;Z) - I_Q(X;Y)]_+ + [I_Q(X;Y) + D(Q_X\|G) - [I_Q(X;Y) - I_Q(Y;Z)]_+ - R_{\rm I}]_+ && (52)\\
&= [I_Q(Y;Z) - I_Q(X;Y)]_+ + [I_Q(Y;Z) + D(Q_X\|G) - [I_Q(Y;Z) - I_Q(X;Y)]_+ - R_{\rm I}]_+ && (53)\\
&= \max\{[I_Q(Y;Z) - I_Q(X;Y)]_+, I_Q(Y;Z) + D(Q_X\|G) - R_{\rm I}\} && (54)\\
&= \max\{[I_Q(Y;Z) - I_Q(X;Y)]_+, [I_Q(Y;Z) + D(Q_X\|G) - R_{\rm I}]_+\}, && (55)
\end{aligned}
$$

which is the last term in (10). This completes the proof of Theorem 1.

6 A Matching Lower Bound on ML Decoding Performance

In this section, we argue that the proposed universal decoder is asymptotically optimal in the sense that its error exponent is the same as that of the ML decoder, at least for channels with strictly positive single–letter transition probabilities, $\{W(z|x)\}$. The limitation to strictly positive $\{W(z|x)\}$ is rather technical, but it is conjectured that this argument continues to hold true even without this restriction. The reason for this belief is that random coding error exponents are normally continuous functionals of the channel parameters, and therefore, it is seems inconceivable that there would be significant differences between the error exponent of a channel where some $\{W(z|x)\}$ vanish and the one of a nearby channel where the parameters are slightly altered so that all $\{W(z|x)\}$ are positive.

Theorem 2 *Let W be a DMC with strictly positive single–letter probabilities, $\{W(z|x)\}$ and consider the model described in Section 3 along with the ML decoder, based on (4). Then, for a given choice of $Q_{Y|X}$ as a functional of Q_X, the random coding error exponent associated with the ensemble of codes, described in Subsection 3.2 and ML decoding, is given by eq. (10).*

Proof of Theorem 2. Since the ML decoder cannot be worse than the universal decoder (8), it is enough to prove that average error probability of the ML decoder is lower bounded by an expression of the exponential order of $e^{-nE(R_{\rm I})}$. The analysis is basically with the same method as in the proof of Theorem 1, except that here, we are after lower bounds (rather than upper bounds) to certain expressions.

We begin with lower bounds on $P(\boldsymbol{y})$ and $P(\boldsymbol{y},\boldsymbol{z})$, but to this end, we first need some preparatory steps. For a given $\boldsymbol{x}\in\mathcal{T}(Q_X)$ and $\boldsymbol{y}\in\mathcal{C}_Q\cap\mathcal{T}(Q_{Y|X}|\boldsymbol{x})$, we first observe that

$$\mathcal{I}\{\boldsymbol{x}\in f^{-1}(\boldsymbol{y})\}=\prod_{\boldsymbol{y}'\in\mathcal{C}_Q\cap\mathcal{T}(Q_{Y|X}|\boldsymbol{x})}[1-\mathcal{I}\{M(\boldsymbol{x},\boldsymbol{y}')<M(\boldsymbol{x},\boldsymbol{y})\}]. \tag{56}$$

Due to the symmetry of the random selection of $\mathcal{M}$, it is clear that for a given $\boldsymbol{x}\in\mathcal{T}(Q_X)$ and $\mathcal{C}_Q$, every $\boldsymbol{y}\in\mathcal{C}_Q\cap\mathcal{T}(Q_{Y|X}|\boldsymbol{x})$ has exactly the same probability to have the smallest rank among all members of $\mathcal{C}_Q\cap\mathcal{T}(Q_{Y|X}|\boldsymbol{x})$, and so, this probability is $1/|\mathcal{C}_Q\cap\mathcal{T}(Q_{Y|X}|\boldsymbol{x})|$. Next observe that $|\mathcal{C}_Q\cap\mathcal{T}(Q_{Y|X}|\boldsymbol{x})|$ is a binomial RV with $|\mathcal{C}_Q|=e^{n[I_Q(X;Y)+\Delta]}$ trials and probability of success of the exponential order of $e^{-nI_Q(X;Y)}$, therefore $|\mathcal{C}_Q\cap\mathcal{T}(Q_{Y|X}|\boldsymbol{x})|$ concentrates double–exponentially

rapidly around $e^{n\Delta}$. In fact, this is true for the vast majority of rate–distortion codes. More precisely, let $0 < \epsilon \ll \Delta$ be given. Then, for every given Q_X with $H_Q(X) \geq \sqrt{\Delta}$, its associated $Q_{Y|X}$, and $\boldsymbol{x} \in \mathcal{T}(Q_X)$,

$$\Pr\left\{|\mathcal{C}_Q \cap \mathcal{T}(Q_{Y|X}|\boldsymbol{x})| \geq e^{n(\Delta+\epsilon)}\right\} \leq \exp\left\{-(n\epsilon - 1)e^{n\Delta}\right\} \tag{57}$$

and

$$\Pr\left\{|\mathcal{C}_Q \cap \mathcal{T}(Q_{Y|X}|\boldsymbol{x})| \leq e^{n(\Delta-\epsilon)}\right\} \leq \exp\left\{-[1 - (n\epsilon + 1)e^{-n\epsilon}]e^{n\Delta}\right\}. \tag{58}$$

From now on, suppose that $\mathcal{C}$ belongs to the vast majority of codes that satisfy

$$e^{n(\Delta-\epsilon)} \leq |\mathcal{C}_Q \cap \mathcal{T}(Q_{Y|X}|\boldsymbol{x})| \leq e^{n(\Delta+\epsilon)} \quad \forall \boldsymbol{x} \in \cup_{Q_X:\ H_Q(X)\geq\sqrt{\Delta}} \mathcal{T}(Q_X). \tag{59}$$

Next, for a given $\mathcal{C} = \cup_Q \mathcal{C}_Q$, since the various random ordering functions $\{M(\boldsymbol{x}, \cdot),\ \boldsymbol{x} \in \mathcal{T}(Q_{X|Y}|\boldsymbol{y})\}$ are independent, the quantity $|\mathcal{T}(Q_{X|Y}|\boldsymbol{y}) \cap f^{-1}(\boldsymbol{y})|$ is a binomial RV with exponentially $e^{nH_Q(X|Y)}$ trials and probability of success $1/|\mathcal{C}_Q \cap \mathcal{T}(Q_{Y|X}|\boldsymbol{x})| \doteq e^{-n(\Delta\pm\epsilon)}$. Therefore, since $H_Q(X|Y)$ is assumed at least as large as $\Delta + 3\epsilon$ whenever $H_Q(X) \geq \sqrt{\Delta}$ (by the code construction described in Section 3.2), then

$$\Pr\left\{|\mathcal{T}(Q_{X|Y}|\boldsymbol{y}) \cap f^{-1}(\boldsymbol{y})| \leq e^{n[H_Q(X|Y)-\Delta-2\epsilon]}\right\} \leq \exp\left\{-e^{n\epsilon} + n\epsilon + 1\right\}. \tag{60}$$

Let us define now the class $\mathcal{G}$ of codes $f = (\mathcal{C}, \mathcal{M})$ that satisfy (59) as well as the following two conditions. The first condition is that

$$|\mathcal{T}(Q_{X|Y}|\boldsymbol{y}) \cap f^{-1}(\boldsymbol{y})| \geq e^{n[H_Q(X|Y)-\Delta-2\epsilon]} \tag{61}$$

for every $\boldsymbol{y} \in \mathcal{C} \cap \mathcal{T}(Q_Y)$ with $H_Q(Y) \geq \sqrt{\Delta}$, and the second condition is that

$$|\mathcal{T}(Q_{X|YZ}|\boldsymbol{y}, \boldsymbol{z}) \cap f^{-1}(\boldsymbol{y})| \geq e^{n[H_Q(X|YZ)-\Delta-2\epsilon]} \tag{62}$$

for every $(\boldsymbol{y}, \boldsymbol{z}) \in \mathcal{T}(Q_{YZ})$ such that $\boldsymbol{y} \in \mathcal{C}$, $H_Q(Y) \geq \sqrt{\Delta}$, and with $Q_{X|YZ}$ such that $H_Q(X|Y, Z) \geq \Delta + 3\epsilon$. The double–exponential decay of the probabilities (57), (58) and (60) imply that the vast majority of codes $f = (\mathcal{C}, \mathcal{M})$ are in $\mathcal{G}$, in particular, $\mathcal{G}$ contains a fraction of the codes that tends to one double–exponentially.

Consider an arbitrary code $f = (\mathcal{C}, \mathcal{M}) \in \mathcal{G}$, and let $\boldsymbol{y} \in \mathcal{C} \cap \mathcal{T}(Q_Y)$ be given. Obviously, for Q_Y with $H_Q(Y) < \sqrt{\Delta}$, $P(\boldsymbol{y}) = G(\boldsymbol{y}) = \exp\{-n[H_Q(Y) + D(Q_Y\|G)]\}$ since $\boldsymbol{y} \equiv \boldsymbol{x}$. For $H_Q(Y) \geq \sqrt{\Delta}$,

since $|\mathcal{C}_Q \cap \mathcal{T}(Q_{Y|X}|\boldsymbol{x})| \geq e^{n(\Delta-\epsilon)}$, we have

$$\begin{aligned} P(\boldsymbol{y}) &= \sum_{\boldsymbol{x}} G(\boldsymbol{x})\mathcal{I}\{\boldsymbol{x} \in f^{-1}(\boldsymbol{y})\} && (63)\\ &= G(\boldsymbol{x})\Big|_{\boldsymbol{x}\in\mathcal{T}(Q_X)} \cdot |\mathcal{T}(Q_{X|Y}|\boldsymbol{y}) \cap f^{-1}(\boldsymbol{y})| && (64)\\ &\geq \exp\{-n[H_Q(X) + D(Q_X\|G) - H_Q(X|Y) + \Delta + 2\epsilon] - O_1(\log n)\} && (65)\\ &= \exp\{-n[A_Q(Y) + \Delta + 2\epsilon] - O_1(\log n)\}. && (66)\end{aligned}$$

Note that this lower bound to $P(\boldsymbol{y})$ applies also to Q_Y with $H_Q(Y) < \sqrt{\Delta}$, where $X \equiv Y$, since $A_Q(Y,Y) = I_Q(Y;Y) + D(Q_Y\|G) = H_Q(Y) + D(Q_Y\|G)$.

Next, consider a pair $(\boldsymbol{y},\boldsymbol{z}) \in \mathcal{T}(Q_{YZ})$ with $\boldsymbol{y} \in \mathcal{C}$. Again, if $H_Q(Y) < \sqrt{\Delta}$,

$$P(\boldsymbol{y},\boldsymbol{z}) = G(\boldsymbol{y})W(\boldsymbol{z}|\boldsymbol{y}) = \exp\{-n[H_Q(Y,Z) + D(Q_{YZ}\|G\times W)]\}. \quad (67)$$

For $H_Q(Y) \geq \sqrt{\Delta}$ (and hence also $H_Q(X) \geq \sqrt{\Delta}$), define the set

$$\begin{aligned}\mathcal{U}(Q_{X|Y},\Delta) &= \{Q_{X|YZ}:\ H_Q(X|Y,Z) \geq \Delta,\\ &\qquad \sum_z Q_{Z|Y}(z|y)Q_{X|YZ}(x|y,z) = Q_{X|Y}(x|y),\ \forall\ x,y\}, && (68)\end{aligned}$$

where, of course, $\mathcal{U}(Q_{X|Y},0)$ is identical to $\mathcal{U}(Q_{X|Y})$ defined before. Then, for $f \in \mathcal{G}$,

$$\begin{aligned} P(\boldsymbol{y},\boldsymbol{z}) &= \sum_{\boldsymbol{x}\in\mathcal{X}^n} G(\boldsymbol{x})W(\boldsymbol{z}|\boldsymbol{x})\mathcal{I}\{\boldsymbol{x} \in f^{-1}(\boldsymbol{y})\} && (69)\\ &= \sum_{\mathcal{T}(Q_{X|YZ}|\boldsymbol{y},\boldsymbol{z}):\ Q_{X|YZ}\in\mathcal{U}(Q_{X|Y},0)} [G(\boldsymbol{x})W(\boldsymbol{z}|\boldsymbol{x})]\Big|_{(\boldsymbol{x},\boldsymbol{z})\in\mathcal{T}(Q_{XZ})} \times\\ &\qquad \sum_{\boldsymbol{x}\in\mathcal{T}(Q_{X|YZ}|\boldsymbol{y},\boldsymbol{z})} \mathcal{I}\{\boldsymbol{x} \in f^{-1}(\boldsymbol{y})\} && (70)\\ &\geq \sum_{\{\mathcal{T}(Q_{X|YZ}|\boldsymbol{y},\boldsymbol{z}):\ Q_{X|YZ}\in\mathcal{U}(Q_{X|Y},\Delta+3\epsilon)\}} [G(\boldsymbol{x})W(\boldsymbol{z}|\boldsymbol{x})]\Big|_{(\boldsymbol{x},\boldsymbol{z})\in\mathcal{T}(Q_{XZ})} \times\\ &\qquad \sum_{\boldsymbol{x}\in\mathcal{T}(Q_{X|YZ}|\boldsymbol{y},\boldsymbol{z})} \mathcal{I}\{\boldsymbol{x} \in f^{-1}(\boldsymbol{y})\} && (71)\\ &\geq \sum_{\{\mathcal{T}(Q_{X|YZ}|\boldsymbol{y},\boldsymbol{z}):\ Q_{X|YZ}\in\mathcal{U}(Q_{X|Y},\Delta+3\epsilon)\}} [G(\boldsymbol{x})W(\boldsymbol{z}|\boldsymbol{x})]\Big|_{(\boldsymbol{x},\boldsymbol{z})\in\mathcal{T}(Q_{XZ})} \times\\ &\qquad \exp\{n[H_Q(X|Y,Z) - \Delta - 2\epsilon] - O_2(\log n)\} && (72)\\ &\geq e^{-n(\Delta+2\epsilon)-O_2(\log n)} \times\\ &\qquad \exp\left\{-n \min_{Q_{X|YZ}\in\mathcal{U}(Q_{X|Y},\Delta+3\epsilon)} \sum_{x,y,z} Q_{XYZ}(x,y,z)\log\frac{Q_{X|YZ}(x|y,z)}{G(x)W(z|x)}\right\} && (73)\end{aligned}$$

$$
\begin{aligned}
&\geq \exp\left\{-n\left[\Delta+2\epsilon+\left(\sqrt{\Delta}+\frac{3\epsilon}{\sqrt{\Delta}}\right)\max_{x,z}\log\frac{1}{G(x)W(z|x)}\right]-O_2(\log n)\right\}\times \\
&\quad \exp\left\{-n\min_{Q_{X|YZ}\in\mathcal{U}(Q_{X|Y})}\sum_{x,y,z}Q_{XYZ}(x,y,z)\log\frac{Q_{X|YZ}(x|y,z)}{G(x)W(z|x)}\right\} \qquad (74)\\
&\stackrel{\Delta}{=} \exp\{-n\theta(\Delta,\epsilon)-O_2(\log n)\}\cdot\exp\{-nB_Q(Y,Z)\}, \qquad (75)
\end{aligned}
$$

where $\lim_{\Delta\to 0}\lim_{\epsilon\to 0}\theta(\Delta,\epsilon)=0$, provided that $W(z|x)$ for every (x,z), and where the second to the last step follows from the following consideration. Let $Q^*_{X|YZ}$ minimize

$$\sum_{x,y,z}Q_{XYZ}(x,y,z)\log\frac{Q_{X|YZ}(x|y,z)}{G(x)W(z|x)}$$

over $\mathcal{U}(Q_{X|Y})$. Observe that

$$\tilde{Q}_{X|YZ}=\left(1-\sqrt{\Delta}-\frac{3\epsilon}{\sqrt{\Delta}}\right)Q^*_{X|YZ}+\left(\sqrt{\Delta}+\frac{3\epsilon}{\sqrt{\Delta}}\right)Q_X\in\mathcal{U}(Q_{X|Y},\Delta+3\epsilon) \qquad (76)$$

since

$$
\begin{aligned}
H_{\tilde{Q}}(X|Y,Z) &\geq \left(1-\sqrt{\Delta}-\frac{3\epsilon}{\sqrt{\Delta}}\right)H_{Q^*}(X|Y,Z)+\left(\sqrt{\Delta}+\frac{3\epsilon}{\sqrt{\Delta}}\right)H_Q(X) &(77)\\
&\geq \left(\sqrt{\Delta}+\frac{3\epsilon}{\sqrt{\Delta}}\right)\cdot\sqrt{\Delta} &(78)\\
&= \Delta+3\epsilon, &(79)
\end{aligned}
$$

and so,

$$
\begin{aligned}
&\min_{Q_{X|YZ}\in\mathcal{U}(Q_{X|Y},\Delta+3\epsilon)}\sum_{x,y,z}Q_{XYZ}(x,y,z)\log\frac{Q_{X|YZ}(x|y,z)}{G(x)W(z|x)} &(80)\\
\leq\ &\sum_{y,z}Q_{YZ}(y,z)\sum_x\tilde{Q}_{X|YZ}(x|y,z)\log\frac{\tilde{Q}_{X|YZ}(x|y,z)}{G(x)W(z|x)} &(81)\\
=\ &\sum_{y,z}Q_{YZ}(y,z)\sum_x\tilde{Q}_{X|YZ}(x|y,z)\log\frac{1}{G(x)W(z|x)}-H_{\tilde{Q}}(X|Y,Z) &(82)\\
\leq\ &\left(1-\sqrt{\Delta}-\frac{3\epsilon}{\sqrt{\Delta}}\right)\sum_{y,z}Q_{YZ}(y,z)\sum_x Q^*_{X|YZ}(x|y,z)\log\frac{1}{G(x)W(z|x)}+\\
&+\left(\sqrt{\Delta}+\frac{3\epsilon}{\sqrt{\Delta}}\right)\sum_{y,z}Q_{YZ}(y,z)\sum_x Q_X(x)\log\frac{1}{G(x)W(z|x)}-\\
&\left(1-\sqrt{\Delta}-\frac{3\epsilon}{\sqrt{\Delta}}\right)H_{Q^*}(X|Y,Z)-\left(\sqrt{\Delta}+\frac{3\epsilon}{\sqrt{\Delta}}\right)H_Q(X) &(83)\\
\leq\ &\left(1-\sqrt{\Delta}-\frac{3\epsilon}{\sqrt{\Delta}}\right)\sum_{y,z}Q_{YZ}(y,z)\sum_x Q^*_{X|YZ}(x|y,z)\log\frac{Q^*_{X|YZ}(x|y,z)}{G(x)W(z|x)}+
\end{aligned}
$$

$$\left(\sqrt{\Delta}+\frac{3\epsilon}{\sqrt{\Delta}}\right)\sum_{x,z}Q_X(x)Q_Z(z)\log\frac{1}{G(x)W(z|x)} \tag{84}$$

$$\leq \left(1-\sqrt{\Delta}-\frac{3\epsilon}{\sqrt{\Delta}}\right)\min_{Q_{X|YZ}\in\mathcal{U}(Q_{X|Y})}\sum_{x,y,z}Q_{XYZ}(x,y,z)\log\frac{Q_{X|YZ}(x|y,z)}{G(x)W(z|x)}+$$
$$\left(\sqrt{\Delta}+\frac{3\epsilon}{\sqrt{\Delta}}\right)\max_{x,z}\log\frac{1}{G(x)W(z|x)} \tag{85}$$

$$< \min_{Q_{X|YZ}\in\mathcal{U}(Q_{X|Y})}\sum_{x,y,z}Q_{XYZ}(x,y,z)\log\frac{Q_{X|YZ}(x|y,z)}{G(x)W(z|x)}+$$
$$\left(\sqrt{\Delta}+\frac{3\epsilon}{\sqrt{\Delta}}\right)\max_{x,z}\log\frac{1}{G(x)W(z|x)}. \tag{86}$$

Observe that the special case where $X\equiv Y$, $B_Q(Y,Z)=H_Q(Y,Z)+H_Q(Y|Y,Z)+D(Q_{YZ}\|G\times W)=H_Q(Y,Z)+D(Q_{YZ}\|G\times W)$, which is suitable also for the case where $H_Q(Y)<\sqrt{\Delta}$. Thus, to summarize, for $f\in\mathcal{G}$ and $\boldsymbol{y}\in\mathcal{C}$, when Δ (and hence also ϵ) is very small, then essentially, $P(\boldsymbol{y})\dot{\geq}e^{-nA_Q(Y)}$ and $P(\boldsymbol{y},\boldsymbol{z})\dot{\geq}e^{-nB_Q(Y,Z)}$. Earlier, we introduced the function $\alpha(\hat{P}_{\boldsymbol{y}})$ as an alternative notation that emphasizes the dependence on $\boldsymbol{y}$. By the same token, we now introduce the notation $\beta(\hat{P}_{\boldsymbol{yz}})$ and as alternative to $B_Q(Y,Z)$, for $(\boldsymbol{y},\boldsymbol{z})\in\mathcal{T}(Q_{YZ})$. Since we have already seen the matching[6] upper bounds, $P(\boldsymbol{y})\dot{\leq}e^{-nA_Q(Y)}$ and $P(\boldsymbol{y},\boldsymbol{z})\dot{\leq}e^{-nB_Q(Y,Z)}$, in the proof of Theorem 1, then we observe that for the vast majority of codes $\{f\}$, the likelihood function (4) can be approximated by

$$P(\boldsymbol{z}|\boldsymbol{y})\dot{=}\exp\{-n[\beta(\hat{P}_{\boldsymbol{yz}})-\alpha(\hat{P}_{\boldsymbol{y}})]\}\stackrel{\Delta}{=}e^{-n\gamma(\hat{P}_{\boldsymbol{yz}})}, \tag{87}$$

whenever $\boldsymbol{y}\in\mathcal{C}$. More precisely, in view of the above upper and lower bounds to $P(\boldsymbol{y})$ and $P(\boldsymbol{y},\boldsymbol{z})$, we have

$$P(\boldsymbol{z}|\boldsymbol{y})\geq\exp\{-n[\gamma(\hat{P}_{\boldsymbol{yz}})+\theta(\Delta,\epsilon)]-O_1(\log n)-O_2(\log n)\} \tag{88}$$

and

$$P(\boldsymbol{z}|\boldsymbol{y})\leq\exp\{-n[\gamma(\hat{P}_{\boldsymbol{yz}})-\Delta-2\epsilon]+O_1(\log n)+O_2(\log n)\}. \tag{89}$$

Thus, a good approximation to the ML decoder, which achieves the same exponent (in the limit $\epsilon\to0$ and $\Delta\to0$) is given by:

$$\hat{m}_{\mathrm{a}}=\arg\,\min_m\gamma(\hat{P}_{\boldsymbol{y}_m\boldsymbol{z}}). \tag{90}$$

We next derive a lower bound to the average[7] error probability of the optimal, ML decoder. As in [4] and [6], to obtain an efficient lower bound, we define a tie–breaking mechanism for the ML

[6]Matching – within infinitesimally small terms in the exponent.

[7]Averaging w.r.t. the randomness of $\{\boldsymbol{x}_m\}$ while $f\in\mathcal{G}$ is given.

decoder by means of a ranking function $M_{\mathrm{o}}(\boldsymbol{y},\boldsymbol{z})$, which for a given $\boldsymbol{z}$, is a one–to–one mapping from $\mathcal{C}$ to $\{1,2,\ldots,|\mathcal{C}|\}$, that satisfies the rule that $P(\boldsymbol{z}|\boldsymbol{y}) > P(\boldsymbol{z}|\boldsymbol{y}')$ implies $M_{\mathrm{o}}(\boldsymbol{y},\boldsymbol{z}) < M_{\mathrm{o}}(\boldsymbol{y}',\boldsymbol{z})$ for every $\boldsymbol{y},\boldsymbol{y}' \in \mathcal{C}$. Then, for $f \in \mathcal{G}$,

$$\begin{aligned}
\mathrm{P}_{\mathrm{e,o}}(f) &\geq \frac{1}{2}\sum_{\boldsymbol{y},\boldsymbol{z}} P(\boldsymbol{y},\boldsymbol{z}) \min\left\{1, e^{nR_{\mathrm{I}}} \cdot \sum_{\{\boldsymbol{y}':\ M_{\mathrm{o}}(\boldsymbol{y}',\boldsymbol{z}) \leq M_{\mathrm{o}}(\boldsymbol{y},\boldsymbol{z})\} \cap \mathcal{C}} P(\boldsymbol{y}')\right\} \\
&= \frac{1}{2}\sum_{\boldsymbol{z}} P(\boldsymbol{z}) \sum_{\boldsymbol{y}} P(\boldsymbol{y}|\boldsymbol{z}) \min\left\{1, e^{nR_{\mathrm{I}}} \cdot \sum_{\{\boldsymbol{y}':\ M_{\mathrm{o}}(\boldsymbol{y}',\boldsymbol{z}) \leq M_{\mathrm{o}}(\boldsymbol{y},\boldsymbol{z})\} \cap \mathcal{C}} P(\boldsymbol{y}')\right\} \\
&\triangleq \frac{1}{2}\sum_{\boldsymbol{z}} P(\boldsymbol{z}) \cdot \Pi(\boldsymbol{z}), \qquad (91)
\end{aligned}$$

where we have used Shulman's lower bound [10, Lemma A.2] on the probability of the union of pairwise independent events, relying on the fact that for a given f, the various quantized codewords $\{\boldsymbol{y}_m\}$ are independent due to the independence of $\{\boldsymbol{x}_m\}$. Let us also define

$$\tilde{\Pi}(\boldsymbol{z}) = \sum_{\boldsymbol{y}} P(\boldsymbol{y}|\boldsymbol{z}) \cdot \min\left\{1, e^{nR_{\mathrm{I}}} \cdot \sum_{\{\boldsymbol{y}':\ P(\boldsymbol{z}|\boldsymbol{y}') \geq e^{-n\delta_n(\Delta,\epsilon)} P(\boldsymbol{z}|\boldsymbol{y})\} \cap \mathcal{C}} P(\boldsymbol{y}')\right\}, \qquad (92)$$

where $\delta_n(\Delta,\epsilon) = \theta(\Delta,\epsilon) + \Delta + 2\epsilon + 2[O_1(\log n) + O_2(\log n)]$. We show in Subsection A.3 of the appendix (as an extension of [6, Lemma 2] and similarly to [9, Lemma 1]) that

$$\Pi(\boldsymbol{z}) \geq \left[1 + e^{n\delta_n(\Delta,\epsilon)}\left(1 + n\ln\frac{1}{G_{\min}}\right)\right]^{-1} \tilde{\Pi}(\boldsymbol{z}), \qquad \forall \boldsymbol{z} \in \mathcal{Z}^n \qquad (93)$$

where $G_{\min} \triangleq \min_{x\in\mathcal{X}} G(x)$, and so, it follows that

$$\begin{aligned}
\mathrm{P}_{\mathrm{e,o}}(f) &\geq \frac{1}{2}\sum_{\boldsymbol{z}} P(\boldsymbol{z}) \cdot \Pi(\boldsymbol{z}) \qquad (94) \\
&\geq \frac{1}{2}\left[1 + e^{n\delta_n(\Delta,\epsilon)}\left(1 + n\ln\frac{1}{G_{\min}}\right)\right]^{-1} \sum_{\boldsymbol{z}} P(\boldsymbol{z}) \cdot \tilde{\Pi}(\boldsymbol{z}) \qquad (95) \\
&= \frac{1}{2}\left[1 + e^{n\delta_n(\Delta,\epsilon)}\left(1 + n\ln\frac{1}{G_{\min}}\right)\right]^{-1} \sum_{\boldsymbol{z}} P(\boldsymbol{z}) \cdot \sum_{\boldsymbol{y}\in\mathcal{C}} P(\boldsymbol{y}|\boldsymbol{z}) \times \\
&\quad \min\left\{1, e^{nR_{\mathrm{I}}} \cdot \sum_{\{\boldsymbol{y}':\ P(\boldsymbol{z}|\boldsymbol{y}') \geq e^{-n\delta_n(\Delta,\epsilon)} P(\boldsymbol{z}|\boldsymbol{y})\} \cap \mathcal{C}} P(\boldsymbol{y}')\right\} \qquad (96) \\
&\geq \frac{1}{2}\left[1 + e^{n\delta_n(\Delta,\epsilon)}\left(1 + n\ln\frac{1}{G_{\min}}\right)\right]^{-1} \sum_{\boldsymbol{y}\in\mathcal{C}} \sum_{\boldsymbol{z}} P(\boldsymbol{y},\boldsymbol{z}) \times \\
&\quad \min\left\{1, e^{nR_{\mathrm{I}}} \cdot \sum_{\{\boldsymbol{y}':\ \gamma(\hat{P}_{\boldsymbol{y}'\boldsymbol{z}}) \leq \gamma(\hat{P}_{\boldsymbol{y}\boldsymbol{z}})\} \cap \mathcal{C}} P(\boldsymbol{y}')\right\} \qquad (97)
\end{aligned}$$

$$
\begin{aligned}
&\geq \frac{1}{2}\left[1+e^{n\delta_n(\Delta,\epsilon)}\left(1+n\ln\frac{1}{G_{\min}}\right)\right]^{-1}\sum_{\boldsymbol{y}\in\mathcal{C}}\sum_{\boldsymbol{z}}P(\boldsymbol{y},\boldsymbol{z})\times \\
&\quad \min\left\{1, e^{nR_{\mathrm{I}}}\cdot\sum_{\{\boldsymbol{y}'\in\mathcal{T}(\boldsymbol{y}|\boldsymbol{z})\cap\mathcal{C}\}}P(\boldsymbol{y}')\right\} \qquad (98)\\
&= \frac{1}{2}\left[1+e^{n\delta_n(\Delta,\epsilon)}\left(1+n\ln\frac{1}{G_{\min}}\right)\right]^{-1}\sum_{\boldsymbol{y}\in\mathcal{C}}\sum_{\boldsymbol{z}}P(\boldsymbol{y},\boldsymbol{z})\times \\
&\quad \min\Big\{1, e^{nR_{\mathrm{I}}}\cdot P[\mathcal{T}(\boldsymbol{y}|\boldsymbol{z})\cap\mathcal{C}]\Big\} \qquad (99)\\
&= \frac{1}{2}\left[1+e^{n\delta_n(\Delta,\epsilon)}\left(1+n\ln\frac{1}{G_{\min}}\right)\right]^{-1}\sum_{\boldsymbol{y}\in\mathcal{C}}\sum_{\boldsymbol{z}}P(\boldsymbol{y},\boldsymbol{z})\times \\
&\quad \min\Big\{1, e^{nR_{\mathrm{I}}}\cdot|\mathcal{T}(\boldsymbol{y}|\boldsymbol{z})\cap\mathcal{C}|\cdot P(\boldsymbol{y})\Big\} \qquad (100)\\
&= \frac{1}{2}\left[1+e^{n\delta_n(\Delta,\epsilon)}\left(1+n\ln\frac{1}{G_{\min}}\right)\right]^{-1}\sum_{\boldsymbol{y}\in\mathcal{C}}\sum_{\boldsymbol{z}}P(\boldsymbol{y},\boldsymbol{z})\times \\
&\quad \min\Big\{1, e^{nR_{\mathrm{I}}}\cdot N(\boldsymbol{y}|\boldsymbol{z})\cdot P(\boldsymbol{y})\Big\}, \qquad (101)
\end{aligned}
$$

where in the third inequality, we have used the fact that $\{\boldsymbol{y}':\ \gamma(\hat{P}_{\boldsymbol{y}'\boldsymbol{z}})\leq\gamma(\hat{P}_{\boldsymbol{y}\boldsymbol{z}})\}$ is a subset of $\{\boldsymbol{y}':\ P(\boldsymbol{z}|\boldsymbol{y}')\geq e^{-n\delta_n(\Delta,\epsilon)}P(\boldsymbol{z}|\boldsymbol{y})\}$, as implied by eqs. (88) and (89). Since the last expression is of the same exponential order as eq. (30), of the upper bound (after taking ϵ and Δ to zero) then so is its expectation[8] w.r.t. the randomness of f, where here the above derived (exponentially tight) lower bounds to $P(\boldsymbol{y})$ and $P(\boldsymbol{y},\boldsymbol{z})$ should be used. This would yield a lower bound to $\bar{\mathrm{P}}_{\mathrm{e,o}}$, which is of the exponential order of $e^{-nE(R_{\mathrm{I}})}$. This completes the proof of Theorem 2.

7 Summary and Conclusion

The main contributions of this work were as follows. We proposed a universal decoder, which is a variant of the MMI decoder, but is different in the sense that it takes into account the distribution of the quantized codewords (for a given lossy source encoder). We analyzed the error exponent of this decoder and have shown that it improves on the ordinary MMI decoder, analyzed in [2], and sometimes strictly so. We have also shown that our proposed decoder provides the same error exponent as that of the ML decoder, at least as long as all single–letter transition probabilities of

[8]There is a minor issue that has to be kept in mind when taking the expectation. The lower bound for a given f is applicable only for $f\in\mathcal{G}$, not for every f. But since $\mathcal{G}^c$ is an extremely small minority of the codes (i.e., a double–exponentially small fraction of them), then the contribution of codes outside $\mathcal{G}$ can safely be neglected in the exponential scale, and so, the expectation over all codes is exponentially the same as the expectation over all codes within $\mathcal{G}$.

the channel, $\{W(z|x)\}$ are strictly positive, and we speculate that this positivity constraint can be removed. Our decoder is also at least as good as any other decoder whose decoding metric depends on $(\boldsymbol{y}_m, \boldsymbol{z})$ only via the joint empirical distribution $\hat{P}_{\boldsymbol{y}_m \boldsymbol{z}}$. As a byproduct of our analysis, for a known channel W, we have also proposed a (non–universal) approximate ML decoder (90), which is easier to implement than the exact ML decoder, based on (4), yet it yields the same error exponent, $E(R_{\rm I})$.

Appendix

A.1 Modifying the Map $Q_X \to Q_Y$ To Be One–to–One

Let $Q^*_{Y|X} = U[Q_X]$ denote our favorite choice of $Q_{Y|X}$ as a functional of Q_X, and let $Q^*_Y = (Q_X \times Q^*_{Y|X})_Y \stackrel{\Delta}{=} V[Q_X]$. The mapping $V[\cdot]$ may not necessarily be one–to–one. We would like to perturb $Q^*_{Y|X}$ very slightly (so that performance would be degraded by a small amount only), to $\tilde{Q}_{Y|X}$, such that $\tilde{Q}_Y = (Q_X \times \tilde{Q}_{Y|X})_Y = \tilde{V}[Q_X]$ would be one–to–one. We next describe one concrete way to do this.

Without loss of generality, assume the alphabet $\mathcal{X}$ to be $\{0, 1, \ldots, K-1\}$, where $K = |\mathcal{X}|$. For convenience, we will also assume that $|\mathcal{Y}| = |\mathcal{X}|$, and so, $\mathcal{Y}$ will also be taken to be $\{0, 1, \ldots, K-1\}$ (the extension to the case $|\mathcal{Y}| > |\mathcal{X}|$ will be straightforward). We first form a fine partition of the simplex. One way of doing this is the following. Let $\epsilon > 0$ be arbitrarily small, chosen such that $1/\epsilon$ is integer, and consider the partition of the simplex $\mathcal{Q}(\mathcal{X})$, of probability distributions $\{Q_X(x)\}$ over $\mathcal{X}$, into cells of size ϵ such that in each cell, the letter probabilities are bounded by $i_x\epsilon \le Q_X(x) < (i_x+1)\epsilon$, $x = 1, 2, \ldots, K-1$, for some given non–negative integers, $\{i_x\}_{x=1}^{K-1}$, which will be denoted collectively by $\boldsymbol{i}$. Let $\mathcal{Q}_{\boldsymbol{i}}$ denote the cell pertaining to the index vector $\boldsymbol{i}$. Assuming that $U[\cdot]$ (and hence also $V[\cdot]$) is continuous at least within each cell (otherwise, form any other fine partition of $\mathcal{Q}(\mathcal{X})$ with this property), let $V[\mathcal{Q}_{\boldsymbol{i}}]$ denote the image of $\mathcal{Q}_{\boldsymbol{i}}$ under V and let $Q^{\boldsymbol{i}}_Y$ denote an arbitrary representative member of $V[\mathcal{Q}_{\boldsymbol{i}}]$, which is taken to have strictly positive letter probabilities (if this is not the case, then slightly perturb the zero–probabilities to small positive values). Thus, the number of distinct representatives, $\{Q^{\boldsymbol{i}}_{Y|X}\}$, cannot exceed the number of cells, which is finite. Let Q_0 be an arbitrary distribution over $\mathcal{Y}$. Now, consider the mapping $\tilde{V}$ that maps $Q_X \in \mathcal{Q}_{\boldsymbol{i}}$ to $\tilde{Q}_Y = Q^{\boldsymbol{i}}_Y + \delta \cdot (Q_X - Q_0)$, where $\delta > 0$ is small enough such that $0 \le \tilde{Q}_Y(y) \le 1$

for all y and that the sets $\{Q_Y^{\boldsymbol{i}} + \delta \cdot (Q_X - Q_0) : \ Q_X \in \mathcal{Q}(\mathcal{X})\}$ are disjoint for every two different index vectors $\{\boldsymbol{i}\}$ (in particular, δ should not exceed $\min_{\boldsymbol{i} \neq \boldsymbol{i}'} \max_y |Q_Y^{\boldsymbol{i}}(y) - Q_Y^{\boldsymbol{i}'}(y)|$). Then, this mapping from Q_X to $\tilde{Q}_Y$ is clearly one–to–one. Finally, one can always slightly perturb $Q_{Y|X}^*$ to obtain a new channel $\tilde{Q}_{Y|X}$ such that $(Q_X \times \tilde{Q}_{Y|X})_Y = \tilde{Q}_Y$, as there are as many as $K-1$ degrees of freedom to this end. The perturbations that take us from Q_Y^* to $Q_Y^{\boldsymbol{i}}$, and then to $\tilde{Q}_Y$, as well as the perturbation from $Q_{Y|X}^*$ to $\tilde{Q}_{Y|X}$, are arbitrarily small, and hence so is the loss of performance.

A.2 $D(Q_X^*\|G)$ Might Be Strictly Positive

For simplicity, let us consider the case where $\mathcal{X} = \mathcal{Y} = \{0, 1, \ldots, K-1\}$ and there is no compression constraint, so $Q_{Y|X}$ can be taken to be the identity matrix (clearly, this situation can be approached in our setting, in the limit where the compression constraints are sufficiently soft) and let $R_{\text{I}} = 0$. Suppose further that W is also the identity matrix, i.e., the clean channel (which again, can be thought of as a limit of very good channels). In this case, $E(0)$ simplifies to

$$E(0) = \min_{Q_X} [2D(Q_X\|G) + H_Q(X)], \tag{A.1}$$

which is easily shown to be achieved by

$$Q_X^*(x) = \frac{G^2(x)}{\sum_{x' \in \mathcal{X}} G^2(x')}, \tag{A.2}$$

that differs from G (except some special cases) and hence $D(Q_X^*\|G) > 0$. On substituting Q_X^* back into the expression of $E(0)$, we obtain

$$E(0) = -\log \left[\sum_x G^2(x) \right], \tag{A.3}$$

as expected. On the other hand, the error exponent of [2], in this case, becomes

$$E_{\text{DD}}(0) = \min_{Q_X} [D(Q_X\|G) + H_Q(X)] = \min_{Q_X} \sum_x Q(x) \log \frac{1}{G(x)} = -\log \left[\max_x G(x) \right], \tag{A.4}$$

which is always smaller, except for some special cases. The same gap continues to apply at least for a certain range of low rates, where $E(R_{\text{I}}) = E(0) - R_{\text{I}}$ and $E_{\text{DD}}(R_{\text{I}}) = E_{\text{DD}}(0) - R_{\text{I}}$.

A.3 Proof of Eq. (93)

The proof is very similar to the proof of Lemma 1 in [9], which in turn, is an extension of [6, Lemma 2], and it is given here for the sake of completeness. For brevity, let us denote $\alpha = e^{n\delta_n(\Delta,\epsilon)}$ and

define

$$\Delta(\boldsymbol{y},\boldsymbol{z}) \stackrel{\Delta}{=} \{\boldsymbol{y}' :\ M_{\mathrm{o}}(\boldsymbol{y}',\boldsymbol{z}) > M_{\mathrm{o}}(\boldsymbol{y},\boldsymbol{z}),\ P(\boldsymbol{z}|\boldsymbol{y}') \geq \alpha^{-1}P(\boldsymbol{z}|\boldsymbol{y})\} \cap \mathcal{C} \tag{A.5}$$

$$= \{\boldsymbol{y}' :\ M_{\mathrm{o}}(\boldsymbol{y}',\boldsymbol{z}) > M_{\mathrm{o}}(\boldsymbol{y},\boldsymbol{z}),\ P(\boldsymbol{y})P(\boldsymbol{y}'|\boldsymbol{z}) \geq \alpha^{-1}P(\boldsymbol{y}')P(\boldsymbol{y}|\boldsymbol{z})\} \cap \mathcal{C}, \tag{A.6}$$

so that

$$\mathcal{E}_{\mathrm{t}}(\boldsymbol{y},\boldsymbol{z}) \stackrel{\Delta}{=} \{\boldsymbol{y}' :\ P(\boldsymbol{z}|\boldsymbol{y}') \geq \alpha^{-1}P(\boldsymbol{z}|\boldsymbol{y})\} \cap \mathcal{C}$$

is given by the disjoint union of $\Delta(\boldsymbol{y},\boldsymbol{z})$ and

$$\mathcal{E}_{\mathrm{o}}(\boldsymbol{y},\boldsymbol{z}) \stackrel{\Delta}{=} \{\boldsymbol{y}' :\ M_{\mathrm{o}}(\boldsymbol{y}',\boldsymbol{z}) < M_{\mathrm{o}}(\boldsymbol{y},\boldsymbol{z})\} \cap \mathcal{C}.$$

Let us also define the function $\phi(t) = \min\{1, t \cdot e^{nR_{\mathrm{I}}}\}$ for $t \geq 0$, and observe that for $t \leq s$, $\phi(s) \leq \frac{s}{t} \cdot \phi(t)$, as can easily be seen from the concavity of $\phi(\cdot)$ and the fact that $\phi(0) = 0$. Thus,

$$\Pi(\boldsymbol{z}) = \sum_{\boldsymbol{y}} P(\boldsymbol{y}|\boldsymbol{z})\phi(P[\mathcal{E}_{\mathrm{o}}(\boldsymbol{y},\boldsymbol{z})]) \tag{A.7}$$

$$\tilde{\Pi}(\boldsymbol{z}) = \sum_{\boldsymbol{y}} P(\boldsymbol{y}|\boldsymbol{z})\phi(P[\mathcal{E}_{\mathrm{o}}(\boldsymbol{y},\boldsymbol{z})] + P[\Delta(\boldsymbol{y},\boldsymbol{z})]) \tag{A.8}$$

$$\leq \sum_{\boldsymbol{y}} P(\boldsymbol{y}|\boldsymbol{z}) \left(\frac{P[\mathcal{E}_{\mathrm{o}}(\boldsymbol{y},\boldsymbol{z})] + P[\Delta(\boldsymbol{y},\boldsymbol{z})]}{(P[\mathcal{E}_{\mathrm{o}}(\boldsymbol{y},\boldsymbol{z})]}\right) \phi(P[\mathcal{E}_{\mathrm{o}}(\boldsymbol{y},\boldsymbol{z})]), \tag{A.9}$$

where in the last inequality, we have used the above mentioned property of the function $\phi(\cdot)$. Now, let us define

$$r(\boldsymbol{y},\boldsymbol{z}) \stackrel{\Delta}{=} \sum_{\boldsymbol{y}' \in \mathcal{E}_{\mathrm{o}}(\boldsymbol{y},\boldsymbol{z})} P(\boldsymbol{y}'|\boldsymbol{z}). \tag{A.10}$$

Then, for $\boldsymbol{y} \in \mathcal{C}$,

$$P(\boldsymbol{y}) = \sum_{\boldsymbol{y}'} P(\boldsymbol{y})P(\boldsymbol{y}'|\boldsymbol{z}) \tag{A.11}$$

$$\geq \sum_{\boldsymbol{y}' \in \mathcal{E}_{\mathrm{o}}(\boldsymbol{y},\boldsymbol{z})} P(\boldsymbol{y})P(\boldsymbol{y}'|\boldsymbol{z}) + \sum_{\boldsymbol{y}' \in \Delta(\boldsymbol{y},\boldsymbol{z})} P(\boldsymbol{y})P(\boldsymbol{y}'|\boldsymbol{z}) \tag{A.12}$$

$$= P(\boldsymbol{y})r(\boldsymbol{y},\boldsymbol{z}) + \sum_{\boldsymbol{y}' \in \Delta(\boldsymbol{y},\boldsymbol{z})} P(\boldsymbol{y})P(\boldsymbol{y}'|\boldsymbol{z}) \tag{A.13}$$

$$\geq P(\boldsymbol{y})r(\boldsymbol{y},\boldsymbol{z}) + \frac{1}{\alpha} \sum_{\boldsymbol{y}' \in \Delta(\boldsymbol{y},\boldsymbol{z})} P(\boldsymbol{y}')P(\boldsymbol{y}|\boldsymbol{z}) \tag{A.14}$$

$$= P(\boldsymbol{y})r(\boldsymbol{y},\boldsymbol{z}) + \frac{P(\boldsymbol{y}|\boldsymbol{z})}{\alpha} P[\Delta(\boldsymbol{y},\boldsymbol{z})], \tag{A.15}$$

and so,

$$P(\boldsymbol{y}|\boldsymbol{z})P[\Delta(\boldsymbol{y},\boldsymbol{z})] \leq \alpha P(\boldsymbol{y})[1-r(\boldsymbol{y},\boldsymbol{z})]. \tag{A.16}$$

We then have

$$\begin{aligned}
& \tilde{\Pi}(\boldsymbol{z}) - \Pi(\boldsymbol{z}) && \text{(A.17)}\\
\leq\ & \sum_{\boldsymbol{y}\in\mathcal{C}} P(\boldsymbol{y}|\boldsymbol{z})\frac{P[\Delta(\boldsymbol{y},\boldsymbol{z})]}{P[\mathcal{E}_{\text{o}}(\boldsymbol{y},\boldsymbol{z})]}\phi(P[\mathcal{E}_{\text{o}}(\boldsymbol{y},\boldsymbol{z})]) && \text{(A.18)}\\
\leq\ & \alpha\cdot\sum_{\boldsymbol{y}\in\mathcal{C}} \frac{P(\boldsymbol{y})[1-r(\boldsymbol{y},\boldsymbol{z})]}{P[\mathcal{E}_{\text{o}}(\boldsymbol{y},\boldsymbol{z})]}\phi(P[\mathcal{E}_{\text{o}}(\boldsymbol{y},\boldsymbol{z})]) && \text{(A.19)}\\
=\ & \alpha\cdot\sum_{\boldsymbol{y}\in\mathcal{C}}\sum_{\{\boldsymbol{y}'\in\mathcal{C}:\ M_{\text{o}}(\boldsymbol{y}',\boldsymbol{z})>M_{\text{o}}(\boldsymbol{y},\boldsymbol{z})\}} \frac{P(\boldsymbol{y})P(\boldsymbol{y}'|\boldsymbol{z})}{P[\mathcal{E}_{\text{o}}(\boldsymbol{y},\boldsymbol{z})]}\phi(P[\mathcal{E}_{\text{o}}(\boldsymbol{y},\boldsymbol{z})]) && \text{(A.20)}\\
\overset{\text{(a)}}{=}\ & \alpha\cdot\sum_{\boldsymbol{y}'\in\mathcal{C}}\sum_{\{\boldsymbol{y}\in\mathcal{C}:\ M_{\text{o}}(\boldsymbol{y}',\boldsymbol{z})>M_{\text{o}}(\boldsymbol{y},\boldsymbol{z})\}} \frac{P(\boldsymbol{y})P(\boldsymbol{y}'|\boldsymbol{z})}{P[\mathcal{E}_{\text{o}}(\boldsymbol{y},\boldsymbol{z})]}\phi(P[\mathcal{E}_{\text{o}}(\boldsymbol{y},\boldsymbol{z})]) && \text{(A.21)}\\
\overset{\text{(b)}}{\leq}\ & \alpha\cdot\sum_{\boldsymbol{y}'\in\mathcal{C}}\sum_{\{\boldsymbol{y}\in\mathcal{C}:\ M_{\text{o}}(\boldsymbol{y}',\boldsymbol{z})>M_{\text{o}}(\boldsymbol{y},\boldsymbol{z})\}} \frac{P(\boldsymbol{y})P(\boldsymbol{y}'|\boldsymbol{z})}{P[\mathcal{E}_{\text{o}}(\boldsymbol{y},\boldsymbol{z})]}\phi(P[\mathcal{E}_{\text{o}}(\boldsymbol{y}',\boldsymbol{z})]) && \text{(A.22)}\\
\leq\ & \alpha\cdot\sum_{\boldsymbol{y}'\in\mathcal{C}} P(\boldsymbol{y}'|\boldsymbol{z})\phi(P[\mathcal{E}_{\text{o}}(\boldsymbol{y}',\boldsymbol{z})])\cdot\sum_{\boldsymbol{y}}\frac{P(\boldsymbol{y})}{P[\mathcal{E}_{\text{o}}(\boldsymbol{y},\boldsymbol{z})]} && \text{(A.23)}\\
=\ & \alpha\cdot\Pi(\boldsymbol{z})\cdot\sum_{\boldsymbol{y}\in\mathcal{C}}\frac{P(\boldsymbol{y})}{P[\mathcal{E}_{\text{o}}(\boldsymbol{y},\boldsymbol{z})]}, && \text{(A.24)}
\end{aligned}$$

where in (a) we have interchanged the order of the summation and in (b), we have used the monotonicity of $\phi(\cdot)$ together with the fact that $\mathcal{E}_{\text{o}}(\boldsymbol{y},\boldsymbol{z}) \subseteq \mathcal{E}_{\text{o}}(\boldsymbol{y}',\boldsymbol{z})$ whenever $M_{\text{o}}(\boldsymbol{y}',\boldsymbol{z}) > M_{\text{o}}(\boldsymbol{y},\boldsymbol{z})$. To complete the proof, it remains to show then that for any $\boldsymbol{z}$,

$$K_n(\boldsymbol{z}) \triangleq \sum_{\boldsymbol{y}\in\mathcal{C}}\frac{P(\boldsymbol{y})}{P[\mathcal{E}_{\text{o}}(\boldsymbol{y},\boldsymbol{z})]} = \sum_{\boldsymbol{y}\in\mathcal{C}}\frac{P(\boldsymbol{y})}{\sum_{\{\boldsymbol{y}':\ M_{\text{o}}(\boldsymbol{y}',\boldsymbol{z})\leq M_{\text{o}}(\boldsymbol{y},\boldsymbol{z})\}}P(\boldsymbol{y}')} \tag{A.25}$$

cannot exceed $1+n\ln(1/G_{\min})$. For the given $\boldsymbol{z}$, consider the ordering of all members of $\mathcal{C}$ according to the ranking function $M_{\text{o}}(\boldsymbol{y},\boldsymbol{z})$, i.e.,

$$P(\boldsymbol{z}|\boldsymbol{y}[1]) \geq P(\boldsymbol{z}|\boldsymbol{y}[2]) \geq \ldots \geq P(\boldsymbol{z}|\boldsymbol{y}[N]), \qquad N=|\mathcal{C}| \tag{A.26}$$

and let us denote $a_i = P(\boldsymbol{y}[i])$, $A_i = \sum_{j=1}^{i} a_j$, $i=1,\ldots,N$. Then, using the facts that $A_1 = a_1 = P(\boldsymbol{y}[1])$ and $A_N = 1$, as well as the inequality

$$\ln(1+u) \equiv -\ln\left(1-\frac{u}{1+u}\right) \geq \frac{u}{1+u}, \tag{A.27}$$

we have

$$
\begin{aligned}
K_n(\boldsymbol{z}) &= \sum_{i=1}^{N} \frac{a_i}{A_i} && \text{(A.28)}\\
&= 1 + \sum_{i=2}^{N} \frac{a_i}{A_{i-1} + a_i} && \text{(A.29)}\\
&= 1 + \sum_{i=2}^{N} \frac{a_i/A_{i-1}}{1 + a_i/A_{i-1}} && \text{(A.30)}\\
&\leq 1 + \sum_{i=2}^{N} \ln\left(1 + \frac{a_i}{A_{i-1}}\right) && \text{(A.31)}\\
&= 1 + \sum_{i=2}^{N} \ln\left(\frac{A_{i-1} + a_i}{A_{i-1}}\right) && \text{(A.32)}\\
&= 1 + \sum_{i=2}^{N} \ln\left(\frac{A_i}{A_{i-1}}\right) && \text{(A.33)}\\
&= 1 + \ln\left(\frac{A_N}{A_1}\right) && \text{(A.34)}\\
&= \ln\left[\frac{1}{P(\boldsymbol{y}[1])}\right] + 1 && \text{(A.35)}\\
&\leq \ln\left(\frac{1}{G_{\min}^n}\right) + 1 && \text{(A.36)}\\
&= n \ln\left(\frac{1}{G_{\min}}\right) + 1, && \text{(A.37)}
\end{aligned}
$$

where we have used the fact that for every code in $\mathcal{G}$, and $\boldsymbol{y} \in \mathcal{C}$, $P(\boldsymbol{y}) > 0$, and it is at least as large as $G(\boldsymbol{x})$ for some $\boldsymbol{x} \in f^{-1}(\boldsymbol{y})$, which in turn, cannot be less than $G_{\min}^n$. This completes the proof of eq. (93).

References

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

[2] G. Dasarathy and S. C. Draper, "On reliability of content identification from databases based on noisy queries," *The 2011 IEEE Proc. International Symposium on Information Theory (ISIT 2011)*, pp. 1066–1070, St. Petersburg, Russia, July–August 2011.

[3] G. Dasarathy and S. C. Draper, "Upper and lower bounds on the reliability of content identification," *Proc. International Zurich Seminar (IZS)*, pp. 100–103, February 2014.

[4] M. Feder and A. Lapidoth, "Universal decoding for channels with memory," *IEEE Trans. Inform. Theory*, vol. 44, no. 5, pp. 1726–1745, September 1998.

[5] T. Ignatenko and F. M. J. Willems, "Biometric security from an information–theoretical perspective," *Foundations and Trends in Communications and Information Theory*, vol. 7, nos. 2–3, pp. 135–316.

[6] A. Lapidoth and J. Ziv, "On the universality of the LZ–based noisy channels decoding algorithm," *IEEE Trans. Inform. Theory*, vol. 44, no. 5, pp. 1746–1755, September 1998.

[7] N. Merhav, "Statistical physics and information theory," (invited paper) *Foundations and Trends in Communications and Information Theory*, vol. 6, nos. 1–2, pp. 1–212, 2009.

[8] N. Merhav, "Universal decoding for arbitrary channels relative to a given family of decoding metrics," *IEEE Trans. Inform. Theory*, vol. 59, no. 9, pp. 5566–5576, September 2013.

[9] N. Merhav, "Universal decoding using a noisy codebook," submitted for publication and available on–line at: `http://arxiv.org/pdf/1609.00549.pdf`

[10] N. Shulman, *Communication over an Unknown Channel via Common Broadcasting*, Ph.D. dissertation, Department of Electrical Engineering – Systems, Tel Aviv University, July 2003. http://www.eng.tau.ac.il/∼shulman/papers/Nadav_PhD.pdf

[11] E. Tuncel, "Capacity/storage tradeoff in high–dimensional identification systems," *IEEE Trans. Inform. Theory*, vol. 55, no. 5, pp. 2097–2106, May 2009.

[12] A. L. Varna and M. Wu, "Modeling and analysis of content identification," *Proc. 2009 IEEE International Conference on Multimedia and Expo (ICME 2009)*, pp. 1528–1531, New York, U.S.A., June–July 2009.

[13] M. B. Westover and J. A. O'Sullivan, "Achievable rates for pattern recognition," *IEEE Trans. Inform. Theory*, vol. 54, no. 1, pp. 299–320, January 2008.

[14] F. Willems, T. Kalker, J. Goseling, and J.-P. Linnartz, "On the capacity of a biometrical identification system," *The 2003 IEEE Proc. International Symposium on Information Theory (ISIT 2003)*, p. 82, Yokohama, Japan, June–July 2003.

[15] F. Willems, T. Kalker, S. Baggen, and J.-P. Linnartz, "On the capacity of a biometrical identification system," (unknown year) available on–line at:
`http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.74.9512&rep=rep1&type=pdf`