

Error Exponents of the Dirty-Paper and Gel'fand-Pinsker Channels*

Ran Tamir[†] and Neri Merhav[‡]

May 14, 2022

Abstract

We derive various error exponents for communication channels with random states, which are available non-causally at the encoder only. For both the finite-alphabet Gel'fand-Pinsker channel and its Gaussian counterpart, the dirty-paper channel, we derive random coding exponents, error exponents of the typical random codes (TRCs), and error exponents of expurgated codes. For the two channel models, we analyze some sub-optimal bin-index decoders, which turn out to be asymptotically optimal, at least for the random coding error exponent. For the dirty-paper channel, we show explicitly via a numerical example, that both the error exponent of the TRC and the expurgated exponent strictly improve upon the random coding exponent, at relatively low coding rates, which is a known fact for discrete memoryless channels without random states. We also show that at rates below capacity, the optimal values of the dirty-paper design parameter α in the random coding sense and in the TRC exponent sense are different from one another, and they are both different from the optimal α that is required for attaining the channel capacity. For the Gel'fand-Pinsker channel, we allow for a variable-rate random binning code construction, and prove that the previously proposed maximum penalized mutual information decoder is asymptotically optimal within a given class of decoders, at least for the random coding error exponent.

Index Terms: Dirty-paper channel, error exponent, expurgated exponent, random states, side information, typical random code.

*This research was supported by the Israel Science Foundation (ISF) grant no. 137/18.

[†]R. Tamir is with the Department of Information Technology and Electrical Engineering, ETH Zurich, 8092 Zürich, Switzerland (e-mail: tamir@isi.ee.ethz.ch).

[‡]N. Merhav is with the Andrew & Erna Viterbi Faculty of Electrical and Computer Engineering, Technion – Israel Institute of Technology, Technion City, Haifa 32000, Israel (e-mail: merhav@ee.technion.ac.il).

1 Introduction

Channels with random states available as side information (SI) at the encoder have been studied for more than four decades. In 1980, Gel'fand and Pinsker [11] have derived the capacity formula for this channel model with discrete alphabets, and Costa has considered the Gaussian counterpart a few years later [6], which is widely known as the *dirty-paper channel* (DPC). Applications and extensions of their work include computer memories with defects [12], multiuser channel models [31, 32], joint source-channel coding [25], and information embedding in cover signals [26], just to name a few. Duality with source coding problems with SI was explored in [4, 7, 29]. For a tutorial on the subject, see [13].

Exponential error bounds have also been derived for channel models with random states as SI at the transmitter. Erez and Zamir [9] have derived random coding error exponents for the discrete memoryless additive noise channel. Later, Somekh-Baruch and Merhav [30] derived random coding error exponents for general discrete memoryless channels (DMCs) and for the multiple-access channel, both with channel SI at the transmitter. Error exponents for the DPC were studied by Lie, Moulin, and Koetter in [14]. Random coding error exponents for an extended channel model with available (but not necessary identical) SI versions at the encoder, the adversary, and the decoder sides subject to various cost constraints were developed by Moulin and Wang [27]. A strong converse result and a sphere-packing type bound for the Gel'fand-Pinsker channel were derived by Tyagi and Narayan [37].

Error exponents of typical random codes (TRCs) and expurgated codes for the DPC and the Gel'fand-Pinsker channel are the main theme of this work. The error exponent of the TRC [21] is defined as¹

$$E_{\text{trc}}(R) = \lim_{n \rightarrow \infty} \left\{ -\frac{1}{n} \mathbb{E} [\ln P_e(\mathcal{C}_n)] \right\}, \quad (1)$$

where R is the coding rate, $P_e(\mathcal{C}_n)$ is the error probability of a codebook \mathcal{C}_n , and the expectation is with respect to (w.r.t.) the randomness of \mathcal{C}_n across the ensemble of codes. As explained in [21], the error exponent of the TRC does not only strictly improve upon the random coding error exponent at low coding rates, but actually provides the exponent function around which the negative normalized logarithmic error probability concentrates.

¹Note that this definition is different from the ordinary random-coding exponent, which is given by $E_r(R) = \lim_{n \rightarrow \infty} \left\{ -\frac{1}{n} \ln \mathbb{E} [P_e(\mathcal{C}_n)] \right\}$.

In [3], Barg and Forney considered TRCs with independently and identically distributed codewords as well as typical linear codes, for the special case of the binary symmetric channel with maximum likelihood (ML) decoding. In [28] Nazari *et al.* provided bounds on the error exponents of TRCs for both DMCs (which coincide with one another for the optimal input distribution) and multiple-access channels. In a recent article by Merhav [21], an exact single-letter expression has been derived for the error exponent of typical, random, fixed-composition codes, over DMCs, and a wide class of (stochastic) decoders, collectively referred to as the generalized likelihood decoder. Later, Merhav has studied error exponents of TRCs for the colored Gaussian channel [22], typical random trellis codes [23], and has derived a Lagrange–dual lower bound to the TRC exponent [24]. Recently, Tamir *et al.* have studied the large deviations behavior around the TRC exponent [35], error exponents of typical random Slepian–Wolf codes [33], and universal decoding for the TRC exponent [34]. More interesting concentration results of the logarithmic error probability of random codes around the error exponent of the TRC have been reported in [36]. Finally, a dual-domain lower bound to the TRC error exponent for general channels and pairwise-independent random-coding ensembles appears in [5].

For the DPC, an ordinary random binning code is analyzed and various error exponents are derived. Specifically, we provide some relatively simple expressions for the exact random coding error exponent and for the error exponent of the TRC. As in the ordinary DMC (without random states), an improvement is achieved at relatively low coding rates by code expurgation. We show also that in the DPC, the TRC exponent and the expurgated exponent strictly improve upon the random coding error exponent at some ranges of low rates. Although we implement a simple sub-optimal decoder, which seeks the closest codeword to the channel output vector, and not the optimal bin-index decoder, we show that at least for the random coding exponent, our decoder is as good as the optimal decoder. We also show that at low rates, such as rate zero, the optimal values of the design parameter² α in the random coding sense and in the TRC exponent sense are different, and they both differ from the optimal α that is required for achieving the channel capacity.

Moving further, we turn to derive similar exponential error bounds for the Gel’fand–Pinsker channel. Also for the Gel’fand–Pinsker channel, we construct a random-binning code, but now

²Recall that in the DPC, the transmitted vector is $\mathbf{x} = \mathbf{u}(m, \mathbf{s}) - \alpha \mathbf{s}$, with \mathbf{s} being the SI vector and $\mathbf{u}(m, \mathbf{s})$ an auxiliary codeword that depends on both the SI vector and the transmitted message $m \in \{1, 2, \dots, M\}$, and where α is subject to optimization.

we allow for a slightly more sophisticated code construction, which is in the spirit of [27]. For every possible SI type, we draw a different random-binning code, and select the binning rate individually, thus allowing for more degrees of freedom to improve the code performance. For completeness, we also adopt the penalized maximum mutual information (MMI) decoder proposed in [27]. The DPC and the Gel'fand-Pinsker channel are very close in spirit, and one may even consider the DPC as a special case of the Gel'fand-Pinsker channel, but still, they differ significantly by the simple fact that in the Gel'fand-Pinsker channel, we allow for a different sub-code for each SI type³. As a consequence, the analyses in the two cases follow different lines and the resulting expressions in the DPC case are considerably simpler, considering the low number of parameters that should undergo optimization. In the Gel'fand-Pinsker case, on the other hand, the final expressions are given by optimization problems, the dimension of which grows with the alphabet sizes. As opposed to our analysis for the DPC, which is tight at all coding rates, here, when deriving the TRC exponent and the expurgated bound, we make a pairwise error analysis, thus providing exponent functions which are tight only at relatively low rates, which is the range where these exponent functions improve upon the random coding error exponent (and the latter is tight at the high rates). For the above described code construction of variable-rate binning (that depends on the empirical distribution of the SI), we prove that at least for the random coding error exponent, the penalized MMI decoder is actually optimal among all metrics that depend both on the joint empirical distribution of the codeword and the channel output sequence as well as on the SI possible type⁴. Due to recent findings in [34], we conjecture that the penalized MMI decoder is also optimal w.r.t. the error exponents of the TRC, but leave this question for future work.

The remaining part of the paper is organized as follows. In Section 2, we establish notation conventions. In Section 3, we consider the DPC; in Subsection 3.1, we formalize the model, review some preliminaries, and indicate the main objectives and in Subsection 3.2, we provide the main results and discuss them. Section 4 is devoted to the Gel'fand-Pinsker channel. In Subsection 4.1, we formalize the settings and in Subsection 4.2, we provide and discuss the results. In Section 5 we prove our results regarding the DPC and in the Appendixes, we prove

³Note that in the continuous case, the different types of \mathbf{s} are defined according to their norm, but $I(U; S)$ is independent of $\|\mathbf{s}\|$. In the Gel'fand-Pinsker channel, on the other hand, there is no such parallel property.

⁴Since the decoder has no access to the actual SI, it has to seek all codebooks pertaining to all possible SI types. Then, the penalized MMI decoder balances the fact that each codebook has a different binning rate.

more supplementary results concerning DPC, discuss optimal bin index decoding, and prove the results concerning the Gel'fand-Pinsker model.

2 Notation Conventions

Throughout the paper, random variables will be denoted by capital letters and specific values they may take will be denoted by the corresponding lower case 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. For example, the random vector $\mathbf{X} = (X_1, X_2, \dots, X_n)$, (n – positive integer) may take a specific vector value $\mathbf{x} = (x_1, x_2, \dots, x_n)$ in \mathbb{R}^n . When used in the linear-algebraic context, these vectors should be thought of as column vectors, and so, when they appear with superscript T , they will be transformed into row vectors by transposition. Thus, $\mathbf{x}^T \mathbf{y}$ is understood as the inner product of \mathbf{x} and \mathbf{y} . The notation $\|\mathbf{x}\|$ will stand for the Euclidean norm of vector \mathbf{x} . The n -dimensional hypersphere of radius \sqrt{nr} will be denoted by $\mathcal{S}(\sqrt{nr})$ and its surface area by $\text{Surf}\{\mathcal{S}(\sqrt{nr})\}$. As customary in probability theory, we write $\mathbf{X} = (X_1, \dots, X_n) \sim \mathcal{N}(0, \sigma^2 \cdot I_n)$ (I_n being the $n \times n$ identity matrix) to denote that the probability density function of \mathbf{X} is

$$P_{\mathbf{X}}(\mathbf{x}) = (2\pi\sigma^2)^{-n/2} \cdot \exp\left\{-\frac{1}{2\sigma^2}\|\mathbf{x}\|^2\right\}. \quad (2)$$

Logarithms, here and throughout the sequel, are taken to the natural base. The probability of an event \mathcal{E} will be denoted by $\mathbb{P}\{\mathcal{E}\}$, and the expectation operator will be denoted by $\mathbb{E}[\cdot]$. 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, $\lim_{n \rightarrow \infty} \frac{1}{n} \ln \frac{a_n}{b_n} = 0$. Similarly, $a_n \leq b_n$ means that $\limsup_{n \rightarrow \infty} (1/n) \ln (a_n/b_n) \leq 0$, and so on. The indicator function of an event \mathcal{E} will be denoted by $\mathbb{1}\{\mathcal{E}\}$. The notation $[x]_+$ will stand for $\max\{0, x\}$.

In the discrete case, alphabets of random variables and their realizations will be denoted by calligraphic letters. Accordingly, alphabets of random vectors and their realizations will be superscripted by their dimensions. For example, the random vector $\mathbf{X} = (X_1, \dots, X_n)$, may take a specific vector value $\mathbf{x} = (x_1, \dots, x_n)$ 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 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 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 information between X and Y , and similarly for other quantities. The weighted divergence between two conditional distributions (channels), say, $Q_{Y|X}$ and $W = \{W(y|x), x \in \mathcal{X}, y \in \mathcal{Y}\}$, with weighting Q_X is defined as

$$D(Q_{Y|X} || W | Q_X) = \sum_{x \in \mathcal{X}} Q_X(x) \sum_{y \in \mathcal{Y}} Q_{Y|X}(y|x) \ln \frac{Q_{Y|X}(y|x)}{W(y|x)}. \quad (3)$$

The empirical distribution of a sequence $\mathbf{x} \in \mathcal{X}^n$, which will be denoted by $\hat{P}_{\mathbf{x}}$, is the vector of relative frequencies, $\hat{P}_{\mathbf{x}}(x)$, of each symbol $x \in \mathcal{X}$ in \mathbf{x} . The type class of $\mathbf{x} \in \mathcal{X}^n$, denoted $\mathcal{T}^n(\mathbf{x})$, is the set of all vectors $\mathbf{x}' \in \mathcal{X}^n$ with $\hat{P}_{\mathbf{x}'} = \hat{P}_{\mathbf{x}}$. When we wish to emphasize the dependence of the type class on the empirical distribution \hat{P} , we will denote it by $\mathcal{T}^n(\hat{P})$. The set of all types of vectors of length n over \mathcal{X} will be denoted by $\mathcal{P}_n(\mathcal{X})$. Information measures associated with empirical distributions will be denoted with ‘hats’ and will be subscripted by the sequences from which they are induced. 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, $\hat{P}_{\mathbf{xy}}$ would be the joint empirical distribution of $(\mathbf{x}, \mathbf{y}) = \{(x_i, y_i)\}_{i=1}^n$, $\mathcal{T}^n(Q_{X|Y} | \mathbf{y})$ will stand for the conditional type class induced by a sequence \mathbf{y} and a relevant empirical conditional distribution $Q_{X|Y}$, which is the set of all vectors $\mathbf{x} \in \mathcal{X}^n$ with $\hat{P}_{\mathbf{xy}} = Q_{X|Y} \times \hat{P}_{\mathbf{y}}$, $\hat{I}_{\mathbf{xy}}(X; Y)$ will denote the empirical mutual information induced by \mathbf{x} and \mathbf{y} , and so on. Similar conventions will apply to triplets of sequences, say, $\{(\mathbf{x}, \mathbf{y}, \mathbf{z})\}$, 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 Error Exponents of Dirty–Paper Coding

3.1 Setup, Preliminaries, and Objectives

Consider the DPC,

$$\mathbf{Y} = \mathbf{X} + \mathbf{S} + \mathbf{Z}, \quad (4)$$

where $\mathbf{X} = (X_1, \dots, X_n)$ is the channel input vector, whose power is limited according to $\|\mathbf{X}\|^2 \leq nP$, $\mathbf{S} = (S_1, \dots, S_n) \sim \mathcal{N}(0, Q \cdot I_n)$, is the random interference signal vector, and $\mathbf{Z} = (Z_1, \dots, Z_n) \sim \mathcal{N}(0, \sigma_Z^2 \cdot I_n)$ is the additive Gaussian noise, which is independent of \mathbf{X} and \mathbf{S} . Here, $Q > 0$ and $\sigma_Z^2 > 0$ are the interference variance and the noise variance, respectively.

Consider the following mechanism of random codebook selection. Let the coding rate, $R \geq 0$, be given. Let $\alpha > 0$ be a design parameter (to be optimized later⁵), and define

$$\rho_0 \triangleq \sqrt{\frac{\alpha^2 Q}{P + \alpha^2 Q}} = \sqrt{\frac{\alpha^2 Q}{W}}, \quad (5)$$

where $W \triangleq P + \alpha^2 Q$. Next, define

$$I_{US} \triangleq \frac{1}{2} \ln \left(\frac{1}{1 - \rho_0^2} \right) = \frac{1}{2} \ln \left(\frac{W}{P} \right). \quad (6)$$

Generate a random codebook, \mathcal{C} , of $M = e^{n(R+I_{US}+\Delta)}$ ($\Delta > 0$ being arbitrarily small) codewords, \mathbf{u}_k , $k = 0, 1, \dots, M - 1$, by independent random selection of each codeword under the uniform distribution over the surface of an n -dimensional hypersphere of radius \sqrt{nW} , centered at the origin. Next, divide \mathcal{C} into $M_1 = e^{nR}$ bins, $\mathcal{C}_0, \mathcal{C}_1, \dots, \mathcal{C}_{M_1-1}$, each of size $M_2 = M/M_1 = e^{n(I_{US}+\Delta)}$.

Let $\epsilon > 0$ be arbitrarily small. Given a message $m \in \{0, 1, \dots, M_1 - 1\}$ and a realization, \mathbf{s} of \mathbf{S} , the encoder seeks, within bin number m , a codeword, \mathbf{u}_k , $k \in \{M_2m, M_2m + 1, \dots, M_2(m + 1) - 1\}$, such that

$$\alpha_{\mathbf{s}}(1 + \epsilon)\|\mathbf{s}\|^2 \geq \mathbf{u}_k^T \mathbf{s} \geq \alpha_{\mathbf{s}}\|\mathbf{s}\|^2. \quad (7)$$

The coefficient $\alpha_{\mathbf{s}}$ in (7) is defined as

$$\alpha_{\mathbf{s}} \triangleq \alpha \cdot \sqrt{\frac{nQ}{\|\mathbf{s}\|^2}}. \quad (8)$$

We denote

$$\mathcal{T}(\mathbf{U}|\mathbf{s}) = \{\mathbf{u} : \|\mathbf{u}\|^2 = nW, \alpha_{\mathbf{s}}(1 + \epsilon) \geq \mathbf{u}^T \mathbf{s} \geq \alpha_{\mathbf{s}}\|\mathbf{s}\|^2\}. \quad (9)$$

The criterion (7) is equivalent to seeking a codeword \mathbf{u}_k whose empirical correlation coefficient with \mathbf{s} , $\hat{\rho}(\mathbf{u}_k, \mathbf{s}) \triangleq \mathbf{u}_k^T \mathbf{s} / [\|\mathbf{u}_k\| \cdot \|\mathbf{s}\|]$, is nearly ρ_0 . Since the bin size, M_2 , is exponentially larger than $e^{nI_{US}}$, the probability of not finding even one codeword in bin number m , which satisfies this condition, decays double exponentially with n . We therefore safely neglect this event of

⁵Note that the optimal α here may not be the same as the optimal α that achieves the capacity [6].

encoding failure. We define the encoder, more precisely, as follows: suppose that for the given \mathbf{s} and m observed by the encoder, there are $K_n(\mathbf{s}, m) \geq 1$ codewords within the bin \mathcal{C}_m that satisfy (7). Then, the encoder randomly selects one of them under the uniform distribution, to be the transmitted codeword, \mathbf{u}_k , i.e.,

$$\mathbb{P}\{\mathbf{u}_k = \mathbf{u} | \mathbf{s}, m\} = \frac{1}{K_n(\mathbf{s}, m)}, \quad \forall \mathbf{u} \in \mathcal{C}_m \cap \mathcal{T}(\mathbf{U} | \mathbf{s}). \quad (10)$$

Upon randomly selecting \mathbf{u}_k , the encoder transmits⁶

$$\mathbf{x} = \mathbf{u}_k - \alpha_{\mathbf{s}} \cdot \mathbf{s}. \quad (12)$$

Note that

$$\begin{aligned} \|\mathbf{x}\|^2 &= \|\mathbf{u}_k\|^2 - 2\alpha_{\mathbf{s}} \mathbf{u}_k^T \mathbf{s} + \alpha_{\mathbf{s}}^2 \|\mathbf{s}\|^2 \\ &\leq nW - 2\alpha_{\mathbf{s}}^2 \|\mathbf{s}\|^2 + \alpha_{\mathbf{s}}^2 \|\mathbf{s}\|^2 \\ &= nW - \alpha_{\mathbf{s}}^2 \|\mathbf{s}\|^2 \\ &= nW - n\alpha^2 Q \\ &= nP, \end{aligned} \quad (13)$$

and so, the power constraint is met.

The receiver implements the MMI decoder, which in the Gaussian-quadratic case considered here, amounts to seeking the codeword, \mathbf{u}_k , $k \in \{0, 1, \dots, M-1\}$, that maximizes the squared (or, equivalently, the absolute) empirical correlation, $\hat{\rho}^2(\mathbf{u}_k, \mathbf{y})$, i.e.,

$$\hat{k} = \arg \max_k \hat{\rho}^2(\mathbf{u}_k, \mathbf{y}) = \arg \max_k \frac{(\mathbf{u}_k^T \mathbf{y})^2}{\|\mathbf{u}_k\|^2 \cdot \|\mathbf{y}\|^2} = \arg \max_k (\mathbf{u}_k^T \mathbf{y})^2, \quad (14)$$

and finally, decoding m according to the bin to which $\mathbf{u}_{\hat{k}}$ belongs, that is,

$$\hat{m} = \left\lfloor \frac{\hat{k}}{M_2} \right\rfloor. \quad (15)$$

⁶One may also consider a more general encoding scheme, where \mathbf{x} is randomly selected from the conditional type class

$$\mathcal{T}(\mathbf{x} | \mathbf{u}, \mathbf{s}) = \left\{ \mathbf{x} : \|\mathbf{x}\|^2 = nP, \mathbf{x}^T \mathbf{u} = n\sqrt{PW} \rho_{xu}, \mathbf{x}^T \mathbf{s} = n\sqrt{P} \hat{\sigma}_s \rho_{xs} \right\}, \quad (11)$$

where the parameters ρ_{xs} and ρ_{xu} are subjected to optimization. Note that this more general coding is much closer in spirit to the coding strategy for the Gel'fand-Pinsker channel, as given in Subsection 4.1, where the transmitted codeword is drawn from the conditional type class given \mathbf{u}, \mathbf{s} .

This two-stage decoding process is asymptotically optimal, at least in the random-coding sense, as it follows by a combination of two arguments. First, we argue by the end of Subsection 5.1 ahead that MMI decoding is asymptotically optimal, provided that one wants to fully decode \mathbf{u}_k (and not only the bin), and second, we prove in Appendix A that a simple ML decoder and the optimal bin index decoder are asymptotically equivalent, at least in the random coding sense.

For a given code, let $P_e(\mathcal{C}_n)$ be the probability of error in the bin index decoding. The random coding error exponent is defined as

$$\mathsf{E}_r(R) = \lim_{n \rightarrow \infty} -\frac{1}{n} \ln \mathbb{E} [P_e(\mathcal{C}_n)], \quad (16)$$

and the error exponent of the TRC is defined by

$$\mathsf{E}_{\text{trc}}(R) = \lim_{n \rightarrow \infty} -\frac{1}{n} \mathbb{E} [\ln P_e(\mathcal{C}_n)]. \quad (17)$$

Our first objective is to derive exact single-letter expressions for (16) and (17).

Another objective is to prove the existence of a sequence of codes $\mathcal{C} = \{\mathcal{C}_n\}_{n=1}^\infty$, whose error exponent is strictly higher than $\mathsf{E}_r(R)$ and $\mathsf{E}_{\text{trc}}(R)$, at least at low coding rates, and obtain a single-letter expression that lower bounds the following limit

$$\mathsf{E}_{\text{ex}}(\mathcal{C}) = \liminf_{n \rightarrow \infty} -\frac{1}{n} \ln \max_m P_{e|m}(\mathcal{C}_n), \quad (18)$$

where $P_{e|m}(\mathcal{C}_n)$ is the conditional error probability, given that message m was transmitted.

In this section, we analyze, study and discuss the random coding exponent, the typical code exponent and the expurgated exponent associated with this model, and we examine them, not only as functions of the rate R , but also as functions of α and of Q . In particular, we show that the optimal value of α for rates below capacity may be different from the optimal α that is needed to achieve capacity, namely, $\alpha^* = P/(P + \sigma_Z^2)$ [6, eq. (7)].

For the sake of convenience and simplicity, we initially assume that the random interference vector, \mathbf{S} , is distributed uniformly across the surface of the n -dimensional hypersphere of radius $\sqrt{n\hat{Q}}$ (that is, $\|\mathbf{S}\|^2 = n\hat{Q}$ with probability one) and return to the Gaussian model later (by weighing the various radii according to the Gaussian divergence between \hat{Q} and Q), as part of our main theorem in this section. Recall that the encoder depends on \mathbf{S} only via its empirical correlations with the various codewords, $\{\mathbf{u}_k\}$, and these empirical correlations are scale-invariant. The decoder, on the other hand, has no access to \mathbf{S} anyway.

3.2 Statement of the Main Results

Let P, Q, \hat{Q}, σ^2 and $\alpha \in [0, 1]$ be given. Define the following quantities:

$$z = 1 - e^{-2(R+I_{US})} = 1 - \frac{Pe^{-2R}}{W} \quad (19)$$

$$a = \alpha\sqrt{Q}(\sqrt{\hat{Q}} - \alpha\sqrt{Q}) + W, \quad (20)$$

and for two given reals, ρ and ϱ , both in $(-1, 1)$, define also

$$b = \sqrt{W}(\sqrt{\hat{Q}} - \alpha\sqrt{Q})\varrho + \rho W. \quad (21)$$

For two given positive reals, p and q ($p \leq q$), define

$$\mu(p, q) = 1 + (q - p)z \quad (22)$$

$$\Delta(p, q) = [\mu(p, q) + p] \cdot [\mu(p, q) - q] + \rho^2 pq. \quad (23)$$

Next, define

$$\begin{aligned} E(R, \hat{Q}, \alpha, \rho, \varrho, p, q) &= \frac{1}{2} \ln \mu(p, q) + \frac{1}{2\sigma^2 \mu(p, q)} \left[(q - p)z[W + \hat{Q} - \alpha^2 Q] + \right. \\ &\quad \left. \frac{\mu(p, q)(pa^2 - qb^2) - pq(a^2 - 2\rho ab + b^2)}{W \cdot \Delta(p, q)} \right] \end{aligned} \quad (24)$$

$$E(R, \hat{Q}, \alpha, \rho, \varrho) = \sup_{\{(p, q): 0 \leq p \leq q, \Delta(p, q) > 0\}} E(R, \hat{Q}, \alpha, \rho, \varrho, p, q). \quad (25)$$

Define also $\mathcal{P}(\rho, \rho_0)$ as the set of values of ϱ within $(-1, 1)$ such that the correlation matrix

$$\begin{pmatrix} 1 & \rho & \rho_0 \\ \rho & 1 & \varrho \\ \rho_0 & \varrho & 1 \end{pmatrix} \quad (26)$$

would be positive semi-definite, and let

$$E(R, \hat{Q}, \alpha, \rho) = \inf_{\varrho \in \mathcal{P}(\rho, \rho_0)} \left\{ E(R, \hat{Q}, \alpha, \rho, \varrho) + L(\rho, \varrho) \right\} + \frac{1}{2} \ln(1 - \rho^2) - \frac{1}{2} \ln \frac{W}{P}, \quad (27)$$

where

$$L(\rho, \varrho) = -\frac{1}{2} \ln(1 - \rho^2 - \varrho^2 - \rho_0^2 + 2\rho\varrho\rho_0). \quad (28)$$

Finally, letting

$$\begin{aligned} E_0(R, \hat{Q}, \alpha, \rho) &\triangleq E(R, \hat{Q}, \alpha, \rho) + \frac{1}{2} \ln \frac{1}{1 - \rho^2} - \frac{1}{2} \ln \frac{W}{P} - R \\ &= \inf_{\varrho \in \mathcal{P}(\rho, \rho_0)} \left\{ E(R, \hat{Q}, \alpha, \rho, \varrho) + L(\rho, \varrho) \right\} - \ln \frac{W}{P} - R, \end{aligned} \quad (29)$$

we have the following result, the proof of which is given in Section 5.

Theorem 1. Consider the setting described in Subsection 3.1. The error exponents $\mathsf{E}_r(R)$ and $\mathsf{E}_{trc}(R)$ associated with dirty-paper coding and MMI decoding are given by:

$$E_r(R, \hat{Q}, \alpha) = \inf_{\rho \in (-1, 1)} E_0(R, \hat{Q}, \alpha, \rho), \quad (30)$$

$$E_{trc}(R, \hat{Q}, \alpha) = \inf_{\rho^2 < 1 - (P/W)^2 e^{-4R}} E_0(R, \hat{Q}, \alpha, \rho), \quad (31)$$

respectively. In addition, there exists a sequence of codes, $\mathcal{C} = \{\mathcal{C}_n\}_{n=1}^{\infty}$, such that the error exponent $\mathsf{E}_{ex}(\mathcal{C})$ associated with dirty-paper coding and MMI decoding is lower-bounded by:

$$E_{ex}(R, \hat{Q}, \alpha) = \inf_{\rho^2 < 1 - (P/W)^2 e^{-2R}} E_0(R, \hat{Q}, \alpha, \rho). \quad (32)$$

If \mathbf{S} is distributed uniformly over the surface of a hypersphere of radius \sqrt{nQ} , take $\hat{Q} = Q$ in all above expressions, and then maximize over the design parameter $\alpha \in [0, 1]$ for each error exponent, to obtain optimal performance. Alternatively, if $\mathbf{S} \sim \mathcal{N}(0, Q \cdot I_n)$, first minimize over \hat{Q} each one of the corresponding error exponents plus the additional term

$$D(\hat{Q} \| Q) = \frac{1}{2} \left[\frac{\hat{Q}}{Q} - \ln \left(\frac{\hat{Q}}{Q} \right) - 1 \right], \quad (33)$$

and finally, maximize again over α .

We can simplify the bounds significantly by confining the inner-most optimization (25) to $p = q$, corresponding to a relatively simple union-bound analysis of pairwise error probabilities, which is tight at some range of low rates. This is relevant since the interesting range where the TRC error exponent differs from the random coding error exponent is the range of low rates anyway. Accordingly, the choice $p = q$ yields:

$$E(R, \hat{Q}, \alpha, \rho, \varrho, q, q) = \frac{q(a^2 - b^2) - q^2(a^2 - 2\rho ab + b^2)}{2W\sigma^2[1 - q^2(1 - \rho^2)]} \quad (34)$$

to be maximized over $q \in [0, 1/\sqrt{1 - \rho^2}]$ which can be carried out explicitly, yielding

$$E(R, \hat{Q}, \alpha, \rho, \varrho) \geq \frac{1}{2W\sigma^2\sqrt{1 - \rho^2}} \cdot T \left(a^2 - b^2, \frac{a^2 - 2\rho ab + b^2}{\sqrt{1 - \rho^2}} \right), \quad (35)$$

where the function $T(\cdot, \cdot)$ is defined as

$$T(g, h) \triangleq \sup_{0 \leq \tau < 1} \frac{g\tau - h\tau^2}{1 - \tau^2} = \begin{cases} 0 & g \leq 0 \\ \frac{g^2}{2(h + \sqrt{h^2 - g^2})} & h \geq g > 0 \\ \infty & g > h \geq 0 \end{cases}. \quad (36)$$

The random coding exponent, $E_r(R)$, the typical-code error exponent, $E_{\text{trc}}(R)$, and the expurgated error exponent, $E_{\text{ex}}(R)$, are presented in Figure 1. As can be seen in Figure 1, $E_{\text{trc}}(R)$ and $E_{\text{ex}}(R)$ coincide at $R = 0$, but $E_{\text{trc}}(R) < E_{\text{ex}}(R)$ at relatively positive low coding rates. At relatively high rates, the three exponent functions coincide. Figure 2 presents zero-rate error exponents as a function of Q for the DPC with the parameters $P = 10$ and $\sigma_Z^2 = 1$, and with optimized α in the interval $[0, 1]$. The two exponents $E_{\text{trc}}(0)$ and $E_{\text{ex}}(0)$ coincide. Note that the random coding exponent is almost a constant, independently of Q , in agreement with [15]. It turns out that for larger values of Q , $E_r(0)$ is slightly increasing with Q , which may seem counter-intuitive. However, note that for $Q > 0$, even if we select $\alpha = 1$ (which is sub-optimal), we completely cancel the interference (yielding $\mathbf{Y} = (\mathbf{U} - \mathbf{S}) + \mathbf{S} + \mathbf{Z} = \mathbf{U} + \mathbf{Z}$, yet the effective transmission power (the power of \mathbf{U}) is $P + Q$ (rather than P), although the transmission power (of $\mathbf{X} = \mathbf{U} - \mathbf{S}$) is still P . On the other hand, there is the effective rate reduction of $I(U; S) = \frac{1}{2} \ln(1 + \frac{Q}{P})$ (which does not exist when $Q = 0$). Still, the overall effect of increasing Q might be positive. Figure 3 presents zero-rate error exponents as a function of α for the parameters $P = 10$ and $Q = \sigma_Z^2 = 1$. The optimal values of α are different from each other: $\alpha_r^* \approx 0.90$, $\alpha_{\text{trc}}^* = \alpha_{\text{ex}}^* \approx 0.38$. The latter two are also different from the optimal, capacity-achieving α , which is $\alpha_{\text{capacity}}^* = P/(P + \sigma_Z^2) = 10/11 = 0.9091$.

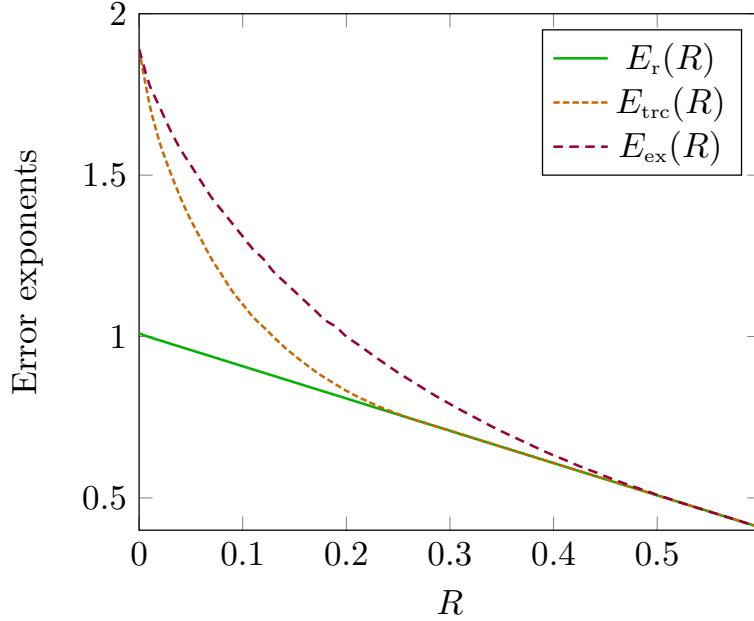


Figure 1: Low-rate error exponent functions for the DPC with the parameters, $P = 10$, $Q = \sigma_Z^2 = 1$, and with optimized α in the interval $[0, 1]$.

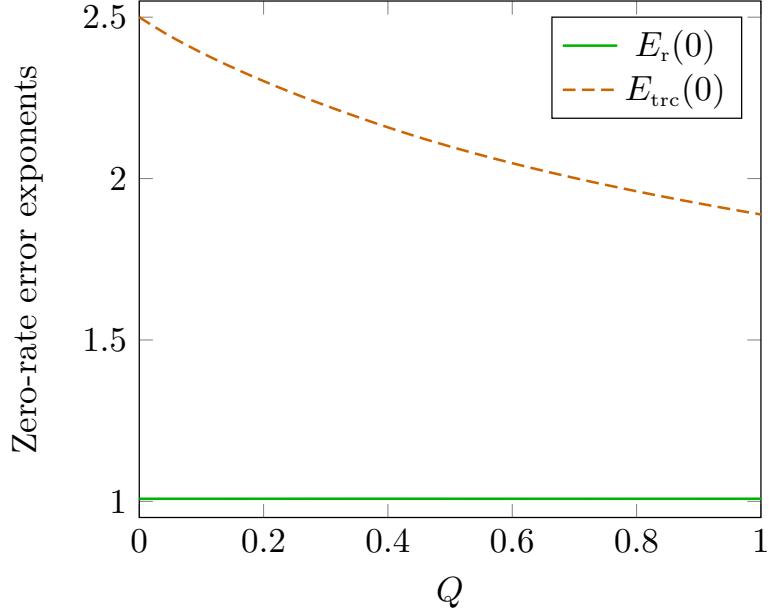


Figure 2: Zero-rate error exponents as functions of Q for the DPC with the parameters, $P = 10$, $\sigma_Z^2 = 1$, and with optimized α in the interval $[0, 1]$. The random coding exponent, $E_r(0)$ and the typical-code error exponent, $E_{trc}(0)$, are in solid and dashed lines, respectively. The exponents $E_{trc}(0)$ and $E_{ex}(0)$ coincide.

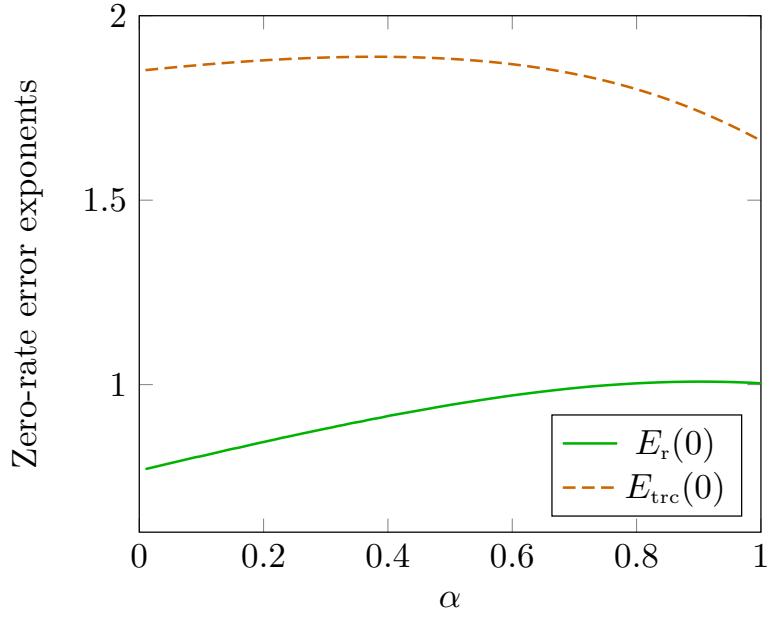


Figure 3: Zero-rate error exponents as functions of α for $P = 10$, $Q = \sigma_Z^2 = 1$. The random coding exponent, $E_r(0)$ and the typical-code error exponent, $E_{trc}(0)$, are in solid and dashed lines, respectively. The exponents $E_{trc}(0)$ and $E_{ex}(0)$ coincide.

4 Error Exponents of the Gel'fand-Pinsker Channel

4.1 Setting and Objectives

Consider a state dependent DMC $W : \mathcal{X} \times \mathcal{S} \rightarrow \mathcal{Y}$ with finite input, state and output alphabets \mathcal{X} , \mathcal{S} and \mathcal{Y} , respectively. The \mathcal{S} -valued state process $\{S_t\}_{t=1}^\infty$ is stationary and memoryless with known probability mass function P_S . The probability law of the DMC is specified by

$$W(\mathbf{y}|\mathbf{x}, \mathbf{s}) = \prod_{t=1}^n W(y_t|x_t, s_t), \quad (37)$$

where $\mathbf{x} \in \mathcal{X}^n$, $\mathbf{s} \in \mathcal{S}^n$, and $\mathbf{y} \in \mathcal{Y}^n$.

Let the coding rate R be given. Let \mathcal{U} be a finite auxiliary alphabet. For a given type $Q_S \in \mathcal{P}_n(\mathcal{S})$, let $Q_{U|S}(Q_S)$ be any conditional type (to be optimized for every Q_S). Furthermore, for any Q_S , let $Q_{X|SU}(Q_S)$ be another conditional type (to be optimized as well). Let $\varepsilon > 0$ be given. For $Q = Q_{U|S} \times Q_S$, let $R(Q_S) = I_Q(S; U) + \varepsilon$. For any $Q_S \in \mathcal{P}_n(\mathcal{S})$, draw $e^{n(R+R(Q_S))}$ independent n -vectors, uniformly over the type class $\mathcal{T}(Q_U)$, where Q_U is the U -marginal of $Q_{U|S} \times Q_S$. Partition these codewords into $M = e^{nR}$ bins, each one of size $M(Q_S) = e^{nR(Q_S)}$.

Let us denote those bins as

$$\mathcal{B}(Q_S, m) = \{\mathbf{u}_{Q_S, m, 1}, \mathbf{u}_{Q_S, m, 2}, \dots, \mathbf{u}_{Q_S, m, M(Q_S)}\}, \quad Q_S \in \mathcal{P}_n(\mathcal{S}), \quad m \in \{1, 2, \dots, M\}. \quad (38)$$

Note that this random-binning code construction is similar to the one in Subsection 3.1, but here, we allow the binning rate to depend on the SI type, thus allowing for more degrees of freedom to improve the overall performance.

For a given message $m \in \{1, 2, \dots, M\}$ and a state vector $\mathbf{s} \in \mathcal{S}^n$, we choose the vector \mathbf{u} from the set $\mathcal{C}(m, \mathbf{s}) \triangleq \mathcal{B}(\hat{P}_{\mathbf{s}}, m) \cap \mathcal{T}(Q_{U|S}|\mathbf{s})$ with equal probabilities. The probability that $\mathcal{C}(m, \mathbf{s})$ is empty decays double-exponentially fast⁷, hence we neglect this possible error event. For a given $\mathbf{s} \in \mathcal{S}^n$ and a selected vector \mathbf{u} , we draw the codeword \mathbf{x} according to the uniform distribution over the conditional type class $\mathcal{T}(Q_{X|SU}|\mathbf{s}, \mathbf{u})$ and transmit it over the channel.

Following the same rationale as in Subsection 3.1, also here we implement a sub-optimal two-stage decoder, which first decodes for the \mathbf{u} codeword according to some metric that depends on the joint empirical distribution with the received vector \mathbf{y} , and afterwards, provides only the

⁷This fact follows from Lemma 1 in Subsection 5.1.

bin index that corresponds to the decoded \mathbf{u} . More precisely, the decoder observes the received vector \mathbf{y} and decodes for a bin index using the following generalized deterministic decoder:

$$\hat{m}(\mathbf{y}) = \arg \max_{m \in \{1, 2, \dots, M\}} \left\{ \max_{Q_S \in \mathcal{P}_n(\mathcal{S})} \max_{\mathbf{u} \in \mathcal{B}(Q_S, m)} G(\hat{P}_{\mathbf{u}\mathbf{y}}, Q_S) \right\}, \quad (39)$$

where $\hat{P}_{\mathbf{u}\mathbf{y}}$ is the empirical distribution of (\mathbf{u}, \mathbf{y}) , and $G(\cdot, \cdot)$ is a given continuous, real-valued functional of this empirical distribution and of another distribution $Q_S \in \mathcal{P}_n(\mathcal{S})$.

For a given codebook, the probability of error is given by

$$P_e(\mathcal{C}_n) = \frac{1}{M} \sum_{m=1}^M \sum_{\mathbf{s} \in \mathcal{S}^n} P(\mathbf{s}) \sum_{\mathbf{y} \in \mathcal{Y}^n} W(\mathbf{y}|\mathbf{x}, \mathbf{s}) \cdot \mathbb{1}\{\hat{m}(\mathbf{y}) \neq m\}. \quad (40)$$

Our objectives here are identical to those defined in Subsection 3.1.

4.2 Main Results

In order to present the random coding error exponent, define the exponent function

$$E_r(R) = \min_{Q_S} \max_{Q_{UX|S}} \min_{Q_{Y|SUX}} \{D(Q_S||P_S) + D(Q_{Y|SUX}||W_{Y|XS}|Q_{UX|S} \times Q_S) + [I_Q(U; Y) - I_Q(U; S) - R]_+\}. \quad (41)$$

Then, we have the following result, which is proved in Appendix C.

Theorem 2. *Consider the setting described in Subsection 4.1.*

1. *It holds that*

$$\lim_{n \rightarrow \infty} -\frac{1}{n} \ln \mathbb{E}[P_e(\mathcal{C}_n)] = E_r(R). \quad (42)$$

2. *The universal decoder*

$$\hat{m} = \arg \max_{m \in \{1, 2, \dots, M\}} \left\{ \max_{Q_S \in \mathcal{P}_n(\mathcal{S})} \max_{\mathbf{u} \in \mathcal{B}(Q_S, m)} [\hat{I}_{\mathbf{u}\mathbf{y}}(U; Y) - R(Q_S)] \right\} \quad (43)$$

achieves $E_r(R)$.

Discussion An expression similar to (41) can be found in two previous works. First in [30], where the coding technique is slightly different than ours and composed by two steps. First, the empirical distribution of the state sequence is transmitted to the receiver, and only then,

the message is encoded similarly as in Subsection 4.1, by using a codebook, which is optimally designed for the empirical statistics of \mathbf{s} . Since the decoder knows in which codebook to look at, it uses an ordinary MMI decoder to decode for a bin index. The final expression in [30] is given by the minimum between (41) and another expression, which is related to the first decoding phase of transmitting the statistics of \mathbf{s} . Hence, our exponential error bound is at least as tight as the one in [30]. The expression in (41) appears also in [27], where a similar codebook generation has already been encountered. Although the universal decoder (43) has already been proposed in [27], its optimality has not been proved before.

We continue by presenting a numerical example of the exact error exponent given in Theorem 2. Let $\mathcal{S} = \mathcal{U} = \mathcal{X} = \mathcal{Y} = \{0, 1\}$ and $\mathbb{P}\{S = 0\} = 1 - \mathbb{P}\{S = 1\} = p \in [0, 1]$. It is important to note that choosing $|\mathcal{U}| = 2$ may not be optimal, but we make this choice in order to keep the computational complexity relatively low. Regarding the state-dependent channel, consider the following. If $S = 0$, then $Y = X$ with probability one, i.e., the channel is clean. Otherwise, if $S = 1$, the channel is stuck at 0: $\mathbb{P}\{Y = 0|X = 0\} = 1 - \mathbb{P}\{Y = 1|X = 0\} = 1$ and $\mathbb{P}\{Y = 0|X = 1\} = 1 - \mathbb{P}\{Y = 1|X = 1\} = 1$. The capacity of this channel is given by

$$C_{\text{GP}} = \max_{Q_{U|S}, X(U, S)} \{I(U; Y) - I(U; S)\} = p \text{ [bits]}, \quad (44)$$

which follows as a minor modification of [8, pp. 178-180, Example 7.3].

We plot the exponent function itself in Figure 4 and find that its functional behavior is similar to that of the random coding error exponent in a DMC without random states; it decreases in an affine fashion for relatively low coding rates, and in a strictly convex fashion at the high coding rates. The reliability of this state-dependent channel obviously depends on the probability of $S = 0$; the higher this probability is, the percentage of time the channel is clean is bigger, and the channel is more reliable, although the decoder is ignorant of the state realization. As can be seen in Figure 4, where we compare between $p = 0.7$, $p = 0.5$, and $p = 0.3$, the reliability of the channel is highest at $p = 0.7$ and lowest at $p = 0.3$.

Following the studies in [3, 21, 28] on TRCs in ordinary channel coding, we claim that also in the Gel'fand-Pinsker Channel, the random coding error exponent, whose exact value is given in Theorem 2, does not yield the true exponential behavior of the error probability of a randomly chosen code, since it is dominated by the relatively bad codes in the ensemble, rather than the channel noise, at least at low coding rates. Due to the definition of the TRC exponent, the

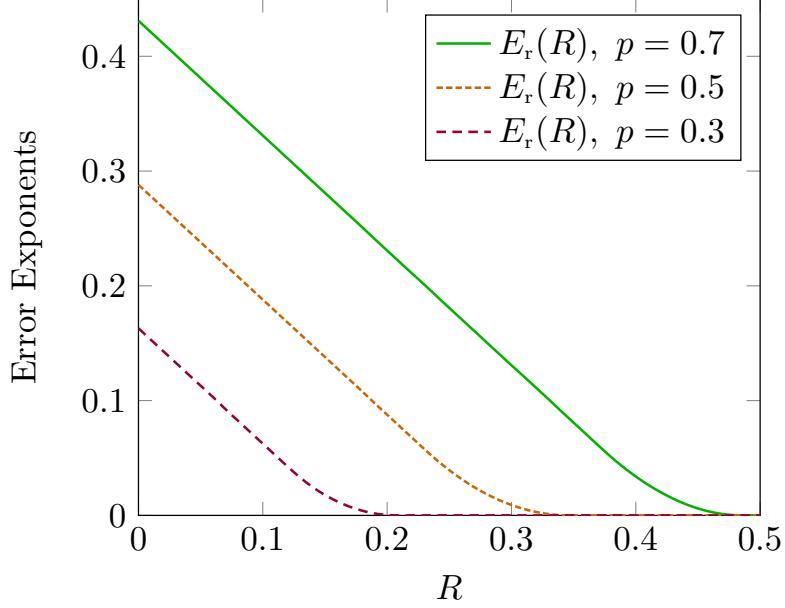


Figure 4: Random coding error exponents in the Gel'fand-Pinsker channel which is a clean channel when $S = 0$ and a ‘stuck at 0’ channel when $S = 1$, for three different values of $p = \mathbb{P}\{S = 0\}$. Not very surprising, the reliability of this channel is a monotone function of p .

derivation of a single-letter expression is not as easy as in ordinary random coding (for example, see the proof in [21, Section 5]), since the expectations over the randomness of the ensemble and over the randomness of the channel cannot be switched, which is one of the first steps in random coding analysis. Let us choose the universal decoding metric $g(Q_{UY}, Q_S) = I_Q(U; Y) - R(Q_S)$. In order to present a lower bound on the error exponent of the TRC, define the expressions

$$E_0(Q_{UU'SX}, Q_{S'}) = \min_{\{Q_{Y|UU'SX}: g(Q_{U'Y}, Q_{S'}) \geq g(Q_{UY}, Q_S)\}} D(Q_{Y|UU'SX} \| W_{Y|SX} | Q_{UU'SX}), \quad (45)$$

$$E_1(Q_{UU'S}, Q_{S'}) = \min_{\{\bar{Q}_{X|UU'S}: \bar{Q}_{X|US} = Q_{X|US}\}} [I_{\bar{Q}}(U'; X|US) + E_0(Q_{UU'S} \times \bar{Q}_{X|UU'S}, Q_{S'})], \quad (46)$$

and,

$$E_2(Q_{UU'}, Q_{S'}) = \min_{\{\tilde{Q}_{S|UU'}: Q_S = Q_{S'}\}} [I_{\tilde{Q}}(S; U'|U) + E_1(Q_{UU'} \times \tilde{Q}_{S|UU'}, Q_{S'})]. \quad (47)$$

Denote the set $\mathcal{Q}(Q_U, Q_{U'}) = \{\ddot{Q}_{UU'} : \ddot{Q}_U = Q_U, \ddot{Q}_{U'} = Q_{U'}\}$ and define the exponent function

$$E_{\text{trc}}(R) = \max_{\{Q_{UX|S}\}} \min_{Q_S, Q_{S'}} \min_{\{\ddot{Q}_{UU'} \in \mathcal{Q}(Q_U, Q_{U'}): I_{\ddot{Q}}(U; U') \leq 2R + R(Q_S) + R(Q_{S'})\}} [D(Q_S \| P_S) + E_2(\ddot{Q}_{UU'}, Q_{S'}) + I_{\ddot{Q}}(U; U') - R - R(Q_{S'})]. \quad (48)$$

Then, our second result is the following theorem, which is proved in Appendix D.

Theorem 3. Consider the setting described in Subsection 4.1. It holds that

$$\liminf_{n \rightarrow \infty} -\frac{1}{n} \mathbb{E}[\ln P_e(\mathcal{C}_n)] \geq E_{\text{trc}}(R). \quad (49)$$

Since our analysis in Appendix D amounts only to pairwise error events, the resulting exponent function is only a lower bound in general and is not tight at relatively high coding rates. Note that at high coding rates, the random coding error exponent of (41) provides the exact value of the error exponent of the TRC.

In ordinary channel coding, the random coding error exponent, and the error exponent of the TRC are both improved at relatively low coding rates by code expurgation. As we already seen in Figure 1 above, this fact is also true for the DPC. Upon using similar techniques as in [34, Appendix A], which is an error exponent derivation of an expurgated code in ordinary channel coding, we are able to derive a bound which is tighter than $E_r(R)$ and $E_{\text{trc}}(R)$, at least at low coding rates. Let us define the exponent function

$$E_{\text{ex}}(R) = \max_{\{Q_{UX|S}\}} \min_{Q_S, Q_{S'}} \min_{\{\ddot{Q}_{UU'} \in \mathcal{Q}(Q_U, Q_{U'}): I_{\ddot{Q}}(U; U') \leq R + R(Q_S) + R(Q_{S'})\}} [D(Q_S \| P_S) + E_2(\ddot{Q}_{UU'}, Q_{S'}) + I_{\ddot{Q}}(U; U') - R - R(Q_{S'})]. \quad (50)$$

Then, our third result is the following theorem, which is proved in Appendix E.

Theorem 4. Consider the setting described in Subsection 4.1. There exists a sequence of constant composition codes, $\{\mathcal{C}_n, n = 1, 2, \dots\}$, such that

$$\liminf_{n \rightarrow \infty} -\frac{1}{n} \ln \max_m P_{e|m}(\mathcal{C}_n) \geq E_{\text{ex}}(R). \quad (51)$$

5 Proof of Theorem 1

5.1 Preparatory Steps

Before moving on to the actual derivations of the various error exponent functions, two basic preparatory steps will prove useful. The first is associated with certain helpful properties that a randomly chosen code in the ensemble satisfies with an overwhelmingly high probability, and the second is associated with the structure of the joint distribution of the various variables in the coded communication system under discussion.

1. Two properties of good codes

There are two desired properties that are associated with a randomly chosen code in our ensemble, with an extremely high probability, and we henceforth refer to codes with those properties as *good codes*. Roughly speaking, a good code has the following two properties at the same time: (i) $K_n(s, m)$ is close to $e^{n\Delta}$ for all s and m , and (ii) For every given \mathbf{y} , there exists at least one codeword, \mathbf{u}_k , such that $\hat{\rho}^2(\mathbf{u}_k, \mathbf{y})$ is essentially at least as large as $1 - \exp[-2(R + I_{US})]$. These two features will be pivotal in our analysis.

To state properties (i) and (ii) more formally, we assert the two following corresponding lemmas, whose proofs appear in Appendix B.

Lemma 1. *Let $\epsilon > 0$ ($\epsilon \ll \Delta$) be arbitrarily small and let \mathcal{G}_1^n be the subset of all codes such that*

$$e^{n(\Delta-\epsilon)} \leq K_n(s, m) \leq e^{n(\Delta+\epsilon)} \quad (52)$$

for all $m \in \{0, 1, \dots, M-1\}$ and $s \in \mathcal{S}(\sqrt{n\hat{Q}}) \triangleq \{s : \|s\|^2 = n\hat{Q}\}$. Then, a randomly selected code falls in \mathcal{G}_1^n with probability that tends to unity double-exponentially as a function of n .

Lemma 2. *Let $\epsilon > 0$ be arbitrarily small and let \mathcal{G}_2^n be the subset of all codes such that for all $k, k' \in \{0, 1, \dots, M-1\}$, $k' \neq k$,*

$$\max_{\tilde{k} \neq k, k'} \hat{\rho}^2(\mathbf{u}_{\tilde{k}}, \mathbf{y}) \geq 1 - \exp[-2(R + I_{US} - \epsilon)], \quad (53)$$

for all $\mathbf{y} \in \mathbb{R}^n$. Then, a randomly selected code falls in \mathcal{G}_2^n with probability that tends to unity double-exponentially as a function of n .

Finally, a good code is in $\mathcal{G}^n = \mathcal{G}_1^n \cap \mathcal{G}_2^n$, which still holds a probability that tends to unity double-exponentially rapidly as n tends to infinity.

2. On the structure of the joint probability distribution of (k, s, \mathbf{y})

Since our decoder, first decodes the index k of the auxiliary codeword, \mathbf{u}_k ($0 \leq k \leq M-1$) and then decodes the message to be the index m of the bin to which k belongs (see eqs. (14), (15)), an obvious upper bound to the probability of error in estimating m is the probability of error in estimating k , since the latter also counts errors associated with incorrect values of k that still belong to the correct bin, m . But the gap is negligible since the number of incorrect

codewords in the correct bin is only $M_2 - 1$, which is of a smaller exponential order than $M - 1$. We therefore henceforth approach the error probability analysis in the same way as if we had to assess the probability of error in decoding k . To this end, it is instrumental to characterize the joint distribution of k with other entities that play a role in the coded communication system, namely, \mathbf{s} and \mathbf{y} .

We first observe that for a good code, the probability distribution of the index k is essentially uniform. To see why this is true, consider first the probability of k given the message m , where $m = \lfloor k/M_2 \rfloor$.

$$\begin{aligned} P(k|m) &= \int_{\mathbb{R}^n} P(\mathbf{s}) \cdot e^{-n\Delta} \mathbb{1}\{\mathbf{u}_k \in \mathcal{C}_m \cap \mathcal{T}(\mathbf{U}|\mathbf{s})\} \cdot d\mathbf{s} \\ &= \int_{\mathcal{T}(\mathbf{S}|\mathbf{u}_k)} P(\mathbf{s}) e^{-n\Delta} d\mathbf{s} \\ &= e^{-n\Delta} \int_{\mathcal{T}(\mathbf{S}|\mathbf{u}_k)} \frac{d\mathbf{s}}{\text{Surf}\{\mathcal{S}(\sqrt{n\hat{Q}})\}}, \end{aligned} \quad (54)$$

where $\mathcal{T}(\mathbf{S}|\mathbf{u}_k) = \{\mathbf{s} : \mathbf{u}_k \in \mathcal{T}(\mathbf{U}|\mathbf{s})\}$. Similarly as in the proof of Lemma 2, the last integral is easily seen to be of the exponential order of $\exp\{\frac{n}{2} \ln(1 - \rho_0^2)\} = e^{-nI_{US}}$, and so,

$$P(k|m) \doteq e^{-n(I_{US} + \Delta)} = \frac{1}{M_2}, \quad \text{whenever } m = \left\lfloor \frac{k}{M_2} \right\rfloor \quad (55)$$

and therefore,

$$P(k) \doteq \mathbb{P}\left\{m = \left\lfloor \frac{k}{M_2} \right\rfloor\right\} \cdot P(k|m) = \frac{1}{M_1} \cdot \frac{1}{M_2} = \frac{1}{M}, \quad k = 0, 1, \dots, M - 1 \quad (56)$$

where we have assumed that the prior distribution over the various messages, $\{m\}$, is uniform.

For a good code, the joint distribution of $(k, \mathbf{s}, \mathbf{y})$ is given by

$$\begin{aligned} P(k, \mathbf{s}, \mathbf{y}) &= P(k)P(\mathbf{s}|\mathbf{u}_k)P(\mathbf{y}|\mathbf{u}_k, \mathbf{s}) \\ &= \frac{1}{M} \cdot P(\mathbf{s}|\mathbf{u}_k)P(\mathbf{y}|\mathbf{u}_k, \mathbf{s}), \end{aligned} \quad (57)$$

where $P(\mathbf{y}|\mathbf{u}_k, \mathbf{s}) = \mathcal{N}(\mathbf{u}_k + (1 - \alpha_s)\mathbf{s}, \sigma_Z^2 I_n)$ is the additive white Gaussian noise channel, with input $\mathbf{x} + \mathbf{s} = \mathbf{u}_k + (1 - \alpha_s)\mathbf{s}$ and noise variance, σ_Z^2 , and

$$\begin{aligned} P(\mathbf{s}|\mathbf{u}_k) &= \frac{P(\mathbf{s}) \cdot P(\mathbf{u}_k|\mathbf{s})}{\int_{\mathbb{R}^n} P(\mathbf{s}') \cdot P(\mathbf{u}_k|\mathbf{s}') d\mathbf{s}'} \\ &= \frac{P(\mathbf{s}) \cdot e^{-n\Delta} \mathbb{1}\{\mathbf{u}_k \in \mathcal{C}_m \cap \mathcal{T}(\mathbf{U}|\mathbf{s})\}}{\int_{\mathbb{R}^n} P(\mathbf{s}') e^{-n\Delta} \mathbb{1}\{\mathbf{u}_k \in \mathcal{C}_m \cap \mathcal{T}(\mathbf{U}|\mathbf{s}')\} d\mathbf{s}'} \end{aligned}$$

$$\begin{aligned}
&= \frac{[1/\text{Surf}\{\mathcal{S}(\sqrt{n\hat{Q}})\}]\mathbb{1}\{\mathbf{u}_k \in \mathcal{C}_m \cap \mathcal{T}(\mathbf{U}|\mathbf{s})\}}{\int_{\mathcal{T}(\mathbf{S}|\mathbf{u}_k)}[1/\text{Surf}\{\mathcal{S}(\sqrt{n\hat{Q}})\}]\mathrm{d}\mathbf{s}'} \\
&= \frac{1}{\int_{\mathcal{T}(\mathbf{S}|\mathbf{u}_k)} \mathrm{d}\mathbf{s}'} \\
&\stackrel{.}{=} \frac{1}{\text{Vol}\{\mathcal{T}(\mathbf{S}|\mathbf{u}_k)\}}, \tag{58}
\end{aligned}$$

where $\text{Vol}\{\mathcal{T}(\mathbf{S}|\mathbf{u}_k)\}$ is the volume of $\mathcal{T}(\mathbf{S}|\mathbf{u}_k)$.

As a consequence of these relations, we can now present the error probability (in k) as follows.

$$\begin{aligned}
P_e(\mathcal{C}) &= \frac{1}{M} \sum_{k=0}^{M-1} \int_{\mathcal{T}(\mathbf{S}|\mathbf{u}_k)} \frac{\mathrm{d}\mathbf{s}}{\text{Vol}\{\mathcal{T}(\mathbf{s}|\mathbf{u}_k)\}} \int_{\Lambda_k^c} P(\mathbf{y}|\mathbf{u}_k, \mathbf{s}) \mathrm{d}\mathbf{y} \\
&= \frac{1}{M} \sum_{k=0}^{M-1} \int_{\Lambda_k^c} \left[\int_{\mathcal{T}(\mathbf{S}|\mathbf{u}_k)} \frac{P(\mathbf{y}|\mathbf{u}_k, \mathbf{s}) \mathrm{d}\mathbf{s}}{\text{Vol}\{\mathcal{T}(\mathbf{s}|\mathbf{u}_k)\}} \right] \mathrm{d}\mathbf{y} \\
&\stackrel{\triangle}{=} \frac{1}{M} \sum_{k=0}^{M-1} \int_{\Lambda_k^c} P(\mathbf{y}|\mathbf{u}_k) \mathrm{d}\mathbf{y}, \tag{59}
\end{aligned}$$

where Λ_k^c is the complement to the decision region in favor of \mathbf{u}_k . This is an ordinary expression of the probability of error, associated with a codebook $\mathcal{C} = \{\mathbf{u}_k\}$ over the effective channel

$$P(\mathbf{y}|\mathbf{u}_k) = \int_{\mathcal{T}(\mathbf{S}|\mathbf{u}_k)} \frac{P(\mathbf{y}|\mathbf{u}_k, \mathbf{s}) \mathrm{d}\mathbf{s}}{\text{Vol}\{\mathcal{T}(\mathbf{s}|\mathbf{u}_k)\}}. \tag{60}$$

According to this effective channel, \mathbf{y} depends on \mathbf{u}_k only via the empirical correlation coefficient, $\hat{\rho}(\mathbf{u}_k, \mathbf{y})$. Therefore, the optimal decoding metric also depends on $(\mathbf{u}_k, \mathbf{y})$ only via $\hat{\rho}(\mathbf{u}_k, \mathbf{y})$ (in other words, $\hat{\rho}(\mathbf{u}_k, \mathbf{y})$ serves as sufficient statistics). It follows from the results of [18] (see in particular, Example 2 therein) that at least for the random coding error exponent, the MMI decoder is asymptotically optimal in the sense of achieving the same error exponent as the maximum likelihood decoder.

5.2 Derivation

Considering the MMI decoder, which is equivalent to the maximum absolute correlation decoder, that chooses the index k with maximum $|\mathbf{u}_k^T \mathbf{y}|$, we have:

$$\begin{aligned}
P_e(\mathcal{C}_n) &\leq \frac{1}{M} \sum_{k=0}^{M-1} \sum_{k' \neq k} \int_{\mathbb{R}^n} P(\mathbf{s}) \mathrm{d}\mathbf{s} \int_{\mathbb{R}^n} P(\mathbf{y}|\mathbf{u}_k, \mathbf{s}) \times \\
&\quad \mathbb{1} \left\{ |\mathbf{u}_{k'}^T \mathbf{y}| \geq \max \left\{ |\mathbf{u}_k^T \mathbf{y}|, \max_{\tilde{k} \neq k, k'} |\mathbf{u}_{\tilde{k}}^T \mathbf{y}| \right\} \right\} \mathrm{d}\mathbf{y}. \tag{61}
\end{aligned}$$

Our good codes (in \mathcal{G}_n) satisfy

$$\forall k, k', \mathbf{y}, \max_{\tilde{k} \neq k, k'} |\mathbf{u}_{\tilde{k}}^T \mathbf{y}| \geq \sqrt{n(P + \alpha^2 Q) \|\mathbf{y}\|^2} \sqrt{1 - e^{-2(R_1 - \epsilon)}}, \quad (62)$$

where $R_1 = R + I_{US}$. Therefore, we can safely further bound the error probability of every $\mathcal{C}_n \in \mathcal{G}_n$ according to

$$\begin{aligned} P_e(\mathcal{C}_n) &\leq \frac{1}{M} \sum_{k=0}^{M-1} \sum_{k' \neq k} \int_{\mathbb{R}^n} P(\mathbf{s}) d\mathbf{s} \int_{\mathbb{R}^n} P(\mathbf{y} | \mathbf{u}_k, \mathbf{s}) \times \\ &\quad \mathbb{1} \left\{ |\mathbf{u}_{k'}^T \mathbf{y}| \geq \max\{|\mathbf{u}_k^T \mathbf{y}|, \sqrt{n(P + \alpha^2 Q) \|\mathbf{y}\|^2} \sqrt{1 - e^{-2(R_1 - \epsilon)}}\} \right\} d\mathbf{y} \end{aligned} \quad (63)$$

$$\begin{aligned} &= \frac{1}{M} \sum_{k=0}^{M-1} \sum_{k' \neq k} \int_{\mathbb{R}^n} P(\mathbf{s}) d\mathbf{s} \int_{\mathbb{R}^n} P(\mathbf{y} | \mathbf{u}_k, \mathbf{s}) \times \\ &\quad \mathbb{1} \left\{ |\mathbf{u}_{k'}^T \mathbf{y}| \geq |\mathbf{u}_k^T \mathbf{y}|, |\mathbf{u}_{k'}^T \mathbf{y}| \geq \sqrt{n(P + \alpha^2 Q) \|\mathbf{y}\|^2} \sqrt{1 - e^{-2(R_1 - \epsilon)}} \right\} d\mathbf{y}, \end{aligned} \quad (64)$$

where (64) is due to the simple identity $\mathbb{1}\{a \geq \max\{b, c\}\} = \mathbb{1}\{a \geq b, a \geq c\}$. For the sake of notational simplicity, we henceforth use the following alternative notation: $\mathbf{u} = \mathbf{u}_k$, $\mathbf{v} = \mathbf{u}_{k'}$, and $\mathbf{w} = \mathbf{u} + (1 - \alpha_s) \mathbf{s}$. Now,

$$I(\mathbf{s}) \triangleq (2\pi\sigma^2)^{-n/2} \int_{\mathbb{R}^n} d\mathbf{y} \cdot \exp \left\{ -\frac{1}{2\sigma^2} \|\mathbf{y} - \mathbf{w}\|^2 \right\} \cdot \mathbb{1} \left\{ |\mathbf{v}^T \mathbf{y}| \geq |\mathbf{u}^T \mathbf{y}|, |\mathbf{v}^T \mathbf{y}| \geq \sqrt{nW \|\mathbf{y}\|^2 z} \right\} \quad (65)$$

$$\begin{aligned} &\leq \frac{\exp\{-\|\mathbf{w}\|^2/2\sigma^2\}}{(2\pi\sigma^2)^{n/2}} \int_{\mathbb{R}^n} d\mathbf{y} \cdot \exp \left\{ \frac{\mathbf{y}^T \mathbf{w}}{\sigma^2} - \frac{\|\mathbf{y}\|^2}{2\sigma^2} \right\} \times \\ &\quad \exp \left\{ \frac{\theta}{2} \mathbf{y}^T (\mathbf{v} \mathbf{v}^T - \mathbf{u} \mathbf{u}^T) \mathbf{y} + \frac{\zeta}{2} \mathbf{y}^T (\mathbf{v} \mathbf{v}^T - nzW \cdot I_n) \mathbf{y} \right\} \end{aligned} \quad (66)$$

$$= \frac{\exp\{-\|\mathbf{w}\|^2/2\sigma^2\}}{(2\pi\sigma^2)^{n/2}} \int_{\mathbb{R}^n} d\mathbf{y} \cdot \exp \left\{ \frac{\mathbf{y}^T \mathbf{w}}{\sigma^2} - \frac{1}{2} \mathbf{y}^T \Gamma \mathbf{y} \right\}, \quad (67)$$

where (65) follows from the definitions of W and z , $\theta > 0$ and $\zeta > 0$ in (66) are Chernoff parameters, and Γ in (67) is defined by

$$\begin{aligned} \Gamma &= \left(\frac{1}{\sigma^2} + \zeta nzW \right) \cdot I_n + \theta \mathbf{u} \mathbf{u}^T - (\theta + \zeta) \mathbf{v} \mathbf{v}^T \\ &= \frac{1}{\sigma^2} [(1 + \zeta n\sigma^2 zW) \cdot I_n + \sigma^2 \theta \mathbf{u} \mathbf{u}^T - \sigma^2 (\theta + \zeta) \mathbf{v} \mathbf{v}^T]. \end{aligned} \quad (68)$$

We now use the following identity

$$\frac{1}{(2\pi)^{n/2} |\Lambda|^{1/2}} \int_{\mathbb{R}^n} d\mathbf{y} \exp \left\{ \mathbf{y}^T \boldsymbol{\omega} - \frac{1}{2} \mathbf{y}^T \Lambda^{-1} \mathbf{y} \right\} = \exp \left\{ \frac{1}{2} \boldsymbol{\omega}^T \Lambda \boldsymbol{\omega} \right\}, \quad (69)$$

and so, continuing from (67),

$$I(\mathbf{s}) \leq \frac{\exp\{-\|\mathbf{w}\|^2/2\sigma^2\}}{(2\pi\sigma^2)^{n/2}} \int_{\mathbb{R}^n} d\mathbf{y} \cdot \exp\left\{\frac{\mathbf{y}^T \mathbf{w}}{\sigma^2} - \frac{1}{2}\mathbf{y}^T \Gamma \mathbf{y}\right\} \quad (70)$$

$$= \frac{\exp\{-\|\mathbf{w}\|^2/2\sigma^2\}}{\sigma^n |\Gamma|^{1/2}} \exp\left\{\frac{1}{2\sigma^4} \mathbf{w}^T \Gamma^{-1} \mathbf{w}\right\} \quad (71)$$

$$= \frac{\exp\{-\|\mathbf{w}\|^2/2\sigma^2\}}{\sigma^n |\Gamma|^{1/2}} \exp\left\{\frac{1}{2\sigma^2} \mathbf{w}^T [(1 + \zeta n\sigma^2 zW)I_n + \sigma^2 \theta \mathbf{u} \mathbf{u}^T - \sigma^2(\theta + \zeta) \mathbf{v} \mathbf{v}^T]^{-1} \mathbf{w}\right\} \quad (72)$$

$$= \frac{\exp\{-\|\mathbf{w}\|^2/2\sigma^2\}}{|\mu I_n + t \mathbf{u} \mathbf{u}^T - r \mathbf{v} \mathbf{v}^T|^{1/2}} \exp\left\{\frac{1}{2\sigma^2} \mathbf{w}^T (\mu I_n + t \mathbf{u} \mathbf{u}^T - r \mathbf{v} \mathbf{v}^T)^{-1} \mathbf{w}\right\}, \quad (73)$$

where (72) follows by substituting (68), and in (73) we have denoted $\mu = 1 + \zeta n\sigma^2 zW$, $t = \sigma^2 \theta$, and $r = \sigma^2(\theta + \zeta)$. We now have to find both the inverse and the determinant of $\mu I_n + t \mathbf{u} \mathbf{u}^T - r \mathbf{v} \mathbf{v}^T$, where we use the fact that $\mathbf{u}^T \mathbf{u} = \mathbf{v}^T \mathbf{v} = nW$ and $\mathbf{u}^T \mathbf{v} = n\rho W$. Beginning from the inverse, we invoke the matrix inversion lemma, asserting that for given matrices, A , B , C , and D , of dimensions, $n \times n$, $n \times k$, $k \times k$, and $k \times n$, respectively ($k \leq n$),

$$(A + BCD)^{-1} = A^{-1} - A^{-1}B(C^{-1} + DA^{-1}B)^{-1}DA^{-1}. \quad (74)$$

Setting $k = 2$, $A = \mu I_n$, $B = [t \mathbf{u} \quad r \mathbf{v}]$, $C = I_2$, $D = [\mathbf{u} \quad -\mathbf{v}]^T$, $p = nWt$ and $q = nWr$, we arrive at

$$(\mu I_n + t \mathbf{u} \mathbf{u}^T - r \mathbf{v} \mathbf{v}^T)^{-1} = \frac{1}{\mu} I_n - \frac{t(\mu - q) \mathbf{u} \mathbf{u}^T - r(\mu + p) \mathbf{v} \mathbf{v}^T + \rho q t (\mathbf{u} \mathbf{v}^T + \mathbf{v} \mathbf{u}^T)}{\mu[(\mu + p)(\mu - q) + \rho^2 pq]} \quad (75)$$

$$= \frac{1}{\mu} I_n - \frac{\mu t \mathbf{u} \mathbf{u}^T - \mu r \mathbf{v} \mathbf{v}^T - q t [\mathbf{u} \mathbf{u}^T + \mathbf{v} \mathbf{v}^T - \rho (\mathbf{u} \mathbf{v}^T + \mathbf{v} \mathbf{u}^T)]}{\mu[(\mu + p)(\mu - q) + \rho^2 pq]}, \quad (76)$$

where we have used the fact that $pr = qt$. To find the determinant of $\mu I_n + t \mathbf{u} \mathbf{u}^T - r \mathbf{v} \mathbf{v}^T$, we find the eigenvalues and take their product. First, observe that all $n - 2$ linearly independent vectors that are orthogonal to both \mathbf{u} and \mathbf{v} are eigenvectors pertaining to the eigenvalue μ . The two remaining eigenvalues correspond to two linearly independent vectors that lie in the subspace spanned by \mathbf{u} and \mathbf{v} . Let us denote $\mathbf{r} = a \mathbf{u} + b \mathbf{v}$. Then for \mathbf{r} to be an eigenvector,

$$(\mu I_n + t \mathbf{u} \mathbf{u}^T - r \mathbf{v} \mathbf{v}^T) \mathbf{r} = (\mu I_n + t \mathbf{u} \mathbf{u}^T - r \mathbf{v} \mathbf{v}^T)(a \mathbf{u} + b \mathbf{v}) \quad (77)$$

$$= \mu a \mathbf{u} + \mu b \mathbf{v} + a p \mathbf{u} - a \rho q \mathbf{v} + b \rho p \mathbf{u} - b q \mathbf{v} \quad (78)$$

$$= [\mu a + p(a + \rho b)] \mathbf{u} + [\mu b - q(\rho a + b)] \mathbf{v}. \quad (79)$$

The resulting eigenvalues are therefore the eigenvalues of the 2×2 matrix

$$\begin{pmatrix} \mu + p & \rho p \\ -\rho q & \mu - q \end{pmatrix}, \quad (80)$$

which are readily found to be $\lambda = \mu + (p - q)/2 \pm \sqrt{(p + q)^2 - 4\rho^2 pq}/2$. Thus,

$$|\mu I_n + t\mathbf{u}\mathbf{u}^T - r\mathbf{v}\mathbf{v}^T|^{1/2} = \mu^{n/2-1} \sqrt{\mu^2 + \mu(p - q) - pq(1 - \rho^2)}. \quad (81)$$

Now, substituting (76) and (81) back into (73) yields that

$$\begin{aligned} I(\mathbf{s}) &\leq \frac{1}{\mu^{n/2-1} \sqrt{\mu^2 + \mu(p - q) - pq(1 - \rho^2)}} \times \\ &\quad \exp \left(-\frac{1}{2\sigma^2 \mu} \left[n(\mu - 1)[W + (1 - \alpha^2)Q] + \frac{\mu t A^2 - \mu r B^2 - qt(A^2 - 2\rho AB + B^2)}{(\mu + p)(\mu - q) + \rho^2 pq} \right] \right) \end{aligned} \quad (82)$$

$$\begin{aligned} &= \frac{1}{[1 + (q - p)z]^{n/2-1} \sqrt{[1 + (1 - z)p + qz][1 - pz - q(1 - z)] + \rho^2 pq}} \times \\ &\quad \exp \left(-\frac{1}{2\sigma^2 \mu} \left[n(q - p)z[W + (1 - \alpha^2)Q] \right. \right. \\ &\quad \left. \left. + \frac{[1 + (q - p)z](pA^2 - qB^2) - pq(A^2 - 2\rho AB + B^2)}{nW([1 + p(1 - z) + qz][1 - pz - q(1 - z)] + \rho^2 pq)} \right] \right), \end{aligned} \quad (83)$$

where we have used the relations, $t = p/nW$, $r = q/nW$, $\mu = 1 + (q - p)z$ ($q \geq p$), and where

$$A = \mathbf{w}^T \mathbf{u} \quad (84)$$

$$= (1 - \hat{\alpha}) \mathbf{s}^T \mathbf{u} + nW \quad (85)$$

$$= \hat{\alpha}(1 - \hat{\alpha}) \mathbf{s}^T \mathbf{s} + nW \quad (86)$$

$$= n[\alpha(\sqrt{\hat{Q}} - \alpha\sqrt{Q})\sqrt{Q} + W] \quad (87)$$

$$\stackrel{\triangle}{=} n \cdot a \quad (88)$$

and

$$B = \mathbf{w}^T \mathbf{v} \quad (89)$$

$$= (1 - \hat{\alpha}) \mathbf{s}^T \mathbf{v} + \rho nW \quad (90)$$

$$= (1 - \hat{\alpha}) \varrho \sqrt{nW} \|\mathbf{s}\| + \rho nW \quad (91)$$

$$= n[(\sqrt{\hat{Q}} - \alpha\sqrt{Q})\sqrt{W} \varrho + \rho W] \quad (92)$$

$$\stackrel{\triangle}{=} n \cdot b, \quad (93)$$

with ϱ designating the empirical correlation coefficient between \mathbf{s} and \mathbf{v} . Using both (88) and (93) in (83) and neglecting the factor in (83) that is independent of n , we have that

$$I(\mathbf{s}) \stackrel{.}{\leq} \exp \left\{ -n \left(\frac{1}{2} \ln[1 + (q - p)z] + \frac{1}{2\sigma^2[1 + (q - p)z]} \left[(q - p)z[W + (1 - \alpha^2)Q] + \right. \right. \right.$$

$$\frac{[1 + (q - p)z](pa^2 - qb^2) - pq(a^2 - 2\rho ab + b^2)}{W([1 + p(1 - z) + qz][1 - pz - q(1 - z)] + \rho^2 pq)} \Big] \Big) \Big\} \quad (94)$$

$$\triangleq e^{-nE(p, q, \hat{\sigma}_s^2, \rho, \varrho)}, \quad (95)$$

where the dependence of $E(p, q, \hat{\sigma}_s^2, \rho, \varrho)$ on ϱ is through b , and where $E(p, q, \hat{\sigma}_s^2, \rho, \varrho)$ should be maximized over the set

$$\mathcal{A} = \{(p, q) : q \geq p \geq 0, [1 + p(1 - z) + qz][1 - pz - q(1 - z)] + \rho^2 pq > 0\}, \quad (96)$$

resulting in

$$E(\hat{\sigma}_s^2, \rho, \varrho) = \sup_{(p, q) \in \mathcal{A}} E(p, q, \hat{\sigma}_s^2, \rho, \varrho). \quad (97)$$

As for the simpler bound in (34)-(36), we now choose $q = p$ (amounting to simple union-bound analysis), which simplifies to

$$E(q, q, \hat{\sigma}_s^2, \rho, \varrho) = \frac{q(a^2 - b^2) - q^2(a^2 - 2\rho ab + b^2)}{2\sigma^2 W[1 - q^2(1 - \rho^2)]}, \quad (98)$$

and the supremum over q should be taken in the range $q \in [0, 1/\sqrt{1 - \rho^2}]$. Alternatively, defining $\tau = q\sqrt{1 - \rho^2}$, then (98) is equivalent to

$$E(\tau, \hat{\sigma}_s^2, \rho, \varrho) = \frac{1}{2\sigma^2 W\sqrt{1 - \rho^2}} \cdot \frac{g\tau - h\tau^2}{1 - \tau^2}, \quad (99)$$

which should be maximized over $\tau \in [0, 1]$, where $g = a^2 - b^2$ and

$$h = \frac{a^2 - 2\rho ab + b^2}{\sqrt{1 - \rho^2}}. \quad (100)$$

Then,

$$\sup_{0 \leq \tau < 1} \frac{g\tau - h\tau^2}{1 - \tau^2} = T(g, h) \triangleq \begin{cases} 0 & g \leq 0 \\ \frac{g^2}{2(h + \sqrt{h^2 - g^2})} & h \geq g > 0 \\ \infty & g > h > 0 \end{cases} \quad (101)$$

It follows that

$$I(\mathbf{s}) \leq \exp \left\{ -\frac{n}{2W\sigma^2\sqrt{1 - \rho^2}} \cdot T \left(a^2 - b^2, \frac{a^2 - 2\rho ab + b^2}{\sqrt{1 - \rho^2}} \right) \right\}. \quad (102)$$

Note that for a given $\hat{Q} = \|\mathbf{s}\|^2/n$, and a given correlation coefficient, ρ , between \mathbf{u} and \mathbf{v} , the variable a is a deterministic constant and b depends only on the empirical correlation coefficient, ϱ . Let us then denote the simplified exponent for given $\hat{\sigma}_s^2$, ρ , and ϱ , by

$$E_{\text{sim}}(\hat{\sigma}_s^2, \rho, \varrho) = \frac{1}{2W\sigma^2\sqrt{1 - \rho^2}} \cdot T \left(a^2 - b^2, \frac{a^2 - 2\rho ab + b^2}{\sqrt{1 - \rho^2}} \right). \quad (103)$$

The probability that \mathbf{s} would have an empirical correlation coefficient, ϱ , with \mathbf{v} given that it has empirical correlation ρ_0 with \mathbf{u} is exponentially

$$P(\mathcal{T}(\mathbf{s}|\mathbf{u}, \mathbf{v}) | \mathbf{s} \in \mathcal{T}(\mathbf{s}|\mathbf{u})) = \frac{\text{Vol}\{\mathcal{T}(\mathbf{s}|\mathbf{u}, \mathbf{v})\}}{\text{Vol}\{\mathcal{T}(\mathbf{s}|\mathbf{u})\}} \quad (104)$$

$$\stackrel{\cdot}{=} \frac{(2\pi e \sigma_s^2 [1 - (\rho_0^2 + \varrho^2 - 2\rho\rho_0\varrho)/(1 - \rho^2)])^{n/2}}{(2\pi e \sigma_s^2 [1 - \rho_0^2])^{n/2}} \quad (105)$$

$$\stackrel{\triangle}{=} e^{-nZ(\rho, \varrho)}, \quad (106)$$

where (105) is obtained similarly as in [1] and

$$Z(\rho, \varrho) = \frac{1}{2} \ln \left[\frac{1 - \rho_0^2}{1 - (\rho_0^2 + \varrho^2 - 2\rho\rho_0\varrho)/(1 - \rho^2)} \right] \quad (107)$$

$$= \frac{1}{2} \ln \left[\frac{1}{1 - (\rho_0^2 + \varrho^2 - 2\rho\rho_0\varrho)/(1 - \rho^2)} \right] - \frac{1}{2} \ln \left(1 + \frac{\alpha^2 Q}{P} \right) \quad (108)$$

$$= \frac{1}{2} \ln \left[\frac{1}{1 - \rho^2 - \rho_0^2 - \varrho^2 + 2\rho\rho_0\varrho} \right] + \frac{1}{2} \ln(1 - \rho^2) - \frac{1}{2} \ln \left(1 + \frac{\alpha^2 Q}{P} \right) \quad (109)$$

$$\stackrel{\triangle}{=} L(\rho, \varrho) + \frac{1}{2} \ln(1 - \rho^2) - \frac{1}{2} \ln \left(1 + \frac{\alpha^2 Q}{P} \right), \quad (110)$$

where (108) follows from (5). Thus, the overall exponent of a pairwise error is

$$E(\hat{\sigma}_s^2, \rho) = \inf_{\{\varrho \in \mathcal{P}(\rho, \rho_0)\}} [E(\hat{\sigma}_s^2, \rho, \varrho) + Z(\rho, \varrho)] \quad (111)$$

$$= \inf_{\{\varrho \in \mathcal{P}(\rho, \rho_0)\}} [E(\hat{\sigma}_s^2, \rho, \varrho) + L(\rho, \varrho)] + \frac{1}{2} \ln(1 - \rho^2) - \frac{1}{2} \ln \left(1 + \frac{\alpha^2 Q}{P} \right) \quad (112)$$

$$\stackrel{\triangle}{=} \hat{E}(\hat{\sigma}_s^2, \rho) + \frac{1}{2} \ln(1 - \rho^2) - \frac{1}{2} \ln \left(1 + \frac{\alpha^2 Q}{P} \right), \quad (113)$$

where $\mathcal{P}(\rho, \rho_0)$ is the set of values of ϱ such that the matrix

$$\begin{pmatrix} 1 & \rho_0 & \rho \\ \rho_0 & 1 & \varrho \\ \rho & \varrho & 1 \end{pmatrix} \quad (114)$$

is non-negative definite. Finally, we have the following exponents

$$E_r(R, \hat{\sigma}_s^2) = \inf_{\{\rho: |\rho| < 1\}} \left[E(\hat{\sigma}_s^2, \rho) + \frac{1}{2} \ln \frac{1}{1 - \rho^2} \right] - \frac{1}{2} \ln \left(1 + \frac{\alpha^2 Q}{P} \right) - R \quad (115)$$

$$= \inf_{\{\rho: |\rho| < 1\}} \hat{E}(\hat{\sigma}_s^2, \rho) - \ln \left(1 + \frac{\alpha^2 Q}{P} \right) - R. \quad (116)$$

Similarly,

$$E_{\text{trc}}(R, \hat{\sigma}_s^2) = \inf_{\{\rho: \rho^2 < 1 - (P/W)^2 e^{-4R}\}} \hat{E}(\hat{\sigma}_s^2, \rho) - \ln \left(1 + \frac{\alpha^2 Q}{P} \right) - R \quad (117)$$

$$E_{\text{ex}}(R, \hat{\sigma}_s^2) = \inf_{\{\rho: \rho^2 < 1 - (P/W)^2 e^{-2R}\}} \hat{E}(\hat{\sigma}_s^2, \rho) - \ln \left(1 + \frac{\alpha^2 Q}{P} \right) - R. \quad (118)$$

In order to understand the constraint in (117), consider the following. The error probability is upper-bounded by

$$P_e(\mathcal{C}_n) \leq \frac{1}{M} \sum_{k=0}^{M-1} \sum_{k' \neq k} \exp \left\{ -nE(\hat{\sigma}_s^2, \rho_{\mathbf{u}_k \mathbf{u}_{k'}}) \right\} \quad (119)$$

$$\doteq \sum_{\rho_{UU'}} M(\rho_{UU'}) \exp \left\{ -n[E(\hat{\sigma}_s^2, \rho_{UU'}) + R] \right\}, \quad (120)$$

which is of the exponential order of

$$\max_{\rho_{UU'}} M(\rho_{UU'}) \exp \left\{ -n[E(\hat{\sigma}_s^2, \rho_{UU'}) + R] \right\}, \quad (121)$$

where $M(\rho_{UU'})$ is the typical number of codeword pairs $(\mathbf{u}_k, \mathbf{u}_{k'})$ whose empirical correlation coefficient is about $\rho_{UU'}$ and the sum is over a fine grid in $(-1, 1)$. Since there are about $e^{2n(R+I_{US})}$ codeword pairs in \mathcal{C}_n and since the probability of the event $\{\mathbf{u}_k^T \mathbf{u}_{k'}/(nW) \approx \rho_{UU'}\}$ is about $\exp\{-\frac{n}{2} \ln[1/(1-\rho_{UU'}^2)]\}$, the typical value of the number $M(\rho_{UU'})$ is of the exponential order of $\exp\{-n[2(R+I_{US}) - \frac{1}{2} \ln[1/(1-\rho_{UU'}^2)]]\}$, whenever $2(R+I_{US}) - \frac{1}{2} \ln[1/(1-\rho_{UU'}^2)] > 0$, and is zero otherwise. More details on this point can be found in [21, 22]. One can arrive at the constraint in (118) by performing a standard expurgation process (like the one provided in [34, Appendix A]) according to the conditional error probabilities.

Appendix A - Bin Index Decoding

In principle, both in the DPC and the GP channel models defined in Subsections 3.1 and 4.1, respectively, an optimal bin index decoder should be implemented, in order to minimize the probability of error. Such an optimal decoder compares between ‘metrics’ that depend on the whole set of \mathbf{u} ’s in each bin. Therefore, this optimal bin index decoder is relatively hard to implement, and moreover, it is quite complicated to analyze. Considering the papers [2] and [19], where it has been proved that specific sub-optimal bin index decoders attain the same random coding exponent as the optimal bin index decoder, it is reasonable to suspect that also in the current work, one may lose nothing, at least in the random coding exponent sense, when using a two-stage sub-optimal decoder, like the one in (14) and (15). In the lines to follow, we show by relatively simple arguments that this is indeed the case here.

Consider a random codebook of size $M_0 = e^{nR_0}$, partitioned into $M = e^{n(R_0 - R_B)}$ bins, each of size $M_B = e^{nR_B}$. Let $m \in \{0, 1, \dots, M_0 - 1\}$ be the index of the transmitted codeword,

and let $\mu = \lfloor m/M_B \rfloor \in \{0, 1, \dots, M-1\}$ be the index of its bin, \mathcal{C}_μ . Consider a sub-optimal, two-step decoder that decodes m by first decoding μ , using an optimal bin index decoder, and then decoding m by ML decoding within the sub-code pertaining to the decoded bin. Then, on the one hand,

$$\mathbb{P}\{\hat{m} \neq m\} \geq e^{-nE_r(R_0)}. \quad (\text{A.1})$$

On the other hand,

$$\mathbb{P}\{\hat{m} \neq m\} = \mathbb{P}\{\hat{m} \neq m, \hat{\mu} \neq \mu\} + \mathbb{P}\{\hat{m} \neq m, \hat{\mu} = \mu\} \quad (\text{A.2})$$

$$\leq \mathbb{P}\{\hat{\mu} \neq \mu\} + \mathbb{P}\left\{\arg \max_{\mathbf{u}_{m'} \in \mathcal{C}_\mu} P(\mathbf{y}|\mathbf{u}_{m'}) \neq m, \hat{\mu} = \mu\right\} \quad (\text{A.3})$$

$$\leq \mathbb{P}\{\hat{\mu} \neq \mu\} + \mathbb{P}\left\{\arg \max_{\mathbf{u}_{m'} \in \mathcal{C}_\mu} P(\mathbf{y}|\mathbf{u}_{m'}) \neq m\right\} \quad (\text{A.4})$$

$$\leq \mathbb{P}\{\hat{\mu} \neq \mu\} + e^{-nE_r(R_B)}, \quad (\text{A.5})$$

and so, it follows from (A.1) and (A.5) that

$$\mathbb{P}\{\hat{\mu} \neq \mu\} \geq e^{-nE_r(R_0)} - e^{-nE_r(R_B)} \quad (\text{A.6})$$

$$= e^{-nE_r(R_0)}. \quad (\text{A.7})$$

Now, let \tilde{m} be the ordinary ML-decoded version of m and let $\tilde{\mu} = \lfloor \tilde{m}/M_B \rfloor$ be a sub-optimal bin index decoder that relies simply on \tilde{m} . Then, as a matching upper bound to (A.7) we have

$$\mathbb{P}\{\hat{\mu} \neq \mu\} \leq \mathbb{P}\{\tilde{\mu} \neq \mu\} \quad (\text{A.8})$$

$$\leq \mathbb{P}\{\tilde{m} \neq m\} \quad (\text{A.9})$$

$$\leq e^{-nE_r(R_0)}. \quad (\text{A.10})$$

We conclude that

$$\mathbb{P}\{\tilde{\mu} \neq \mu\} = \mathbb{P}\{\hat{\mu} \neq \mu\}, \quad (\text{A.11})$$

i.e., at least in the random coding sense, the suggested sub-optimal bin index decoder is as good as the optimal bin index decoder.

Appendix B - Proofs of Lemmas 1 and 2

Proof of Lemma 1

Consider first a given m and $\mathbf{s} \in \mathcal{S}(\sqrt{n\hat{Q}})$. Observe that $K_n(\mathbf{s}, m) = |\mathcal{C}_m \cap \mathcal{T}(\mathbf{U}|\mathbf{s})|$ is a binomial random variable with $|\mathcal{C}_m| = M_2 = e^{n[I_{US} + \Delta]}$ trials and probability of success of the

exponential order of $e^{-nI_{US}}$, and therefore $K_n(m, s)$ concentrates double-exponentially rapidly around $e^{n\Delta}$. More precisely, similarly as in [20, Eqs. (24)–(25)], given $0 < \epsilon \ll \Delta$, we have:

$$\mathbb{P}\{K_n(s, m) > e^{n(\Delta+\epsilon)}\} \leq \exp\{-(n\epsilon - 1)e^{n\epsilon}\} \quad (\text{B.1})$$

$$\mathbb{P}\{K_n(s, m) < e^{n(\Delta-\epsilon)}\} \leq \exp\{-[1 - (n\epsilon + 1)e^{-n\epsilon}]e^{n\epsilon}\}. \quad (\text{B.2})$$

Let \mathcal{G}_1^n be the collection of codes for which $e^{n(\Delta-\epsilon)} \leq K_n(s, m) \leq e^{n(\Delta+\epsilon)}$ for all $m \in \{0, 1, \dots, M-1\}$ and $s \in \mathcal{S}(\sqrt{n\hat{Q}})$. We now show that a randomly selected code falls in \mathcal{G}_1^n with a probability that tends to one double-exponentially. To this end, consider a fine quantization of the vectors in $\mathcal{S}_n(\sqrt{n\hat{Q}})$ in the following manner: every $s \in \mathcal{S}_n(\sqrt{n\hat{Q}})$ can be represented as follows. Let $\theta_i \in [0, 2\pi)$, $i = 1, 2, \dots, n-1$, and let the components of s be given by

$$s_1 = \sqrt{n\hat{Q}} \sin \theta_1, \quad (\text{B.3})$$

$$s_2 = \sqrt{n\hat{Q}} \cos \theta_1 \sin \theta_2, \quad (\text{B.4})$$

$$s_3 = \sqrt{n\hat{Q}} \cos \theta_1 \cos \theta_2 \sin \theta_3, \quad (\text{B.5})$$

...

$$s_{n-1} = \sqrt{n\hat{Q}} \cos \theta_1 \cdots \cos \theta_{n-2} \sin \theta_{n-1}, \quad (\text{B.6})$$

$$s_n = \sqrt{n\hat{Q}} \cos \theta_1 \cdots \cos \theta_{n-2} \cos \theta_{n-1}. \quad (\text{B.7})$$

Now, let us quantize each θ_i uniformly using n^2 points with a quantization step-size of $2\pi/n^2$. Thus, the total number of quantization points within the hyprcube $[0, 2\pi)^{n-1}$ is $n^{2(n-1)}$. Given $s \in \mathcal{S}_n(\sqrt{n\hat{Q}})$, we extract $\theta_1, \dots, \theta_{n-1}$, and then quantize each θ_i to its nearest quantization value, $\hat{\theta}_i$. Note that $|\sin \hat{\theta}_i - \sin \theta_i| \leq |\hat{\theta}_i - \theta_i| \leq \pi/n^2$ since the absolute value of the derivative of the sinusoidal function is bounded by 1. The same comment applies also to $|\cos \hat{\theta}_i - \cos \theta_i|$. According to the above representation, we can think of each component s_k , $k = 1, 2, \dots, n$, as being given by $\sqrt{n\hat{Q}} \prod_{i=1}^n g_{i,k}(\theta_i)$, where each $g_{i,k}(\theta_i)$ is either $\sin \theta_i$, or $\cos \theta_i$, or it is identical to 1. Clearly, it is also true that $|g_i(\hat{\theta}_i) - g_i(\theta_i)| \leq |\hat{\theta}_i - \theta_i| \leq \pi/n^2$. and that $|g_i(\theta_i)|$ and $|g_i(\hat{\theta}_i)|$ are upper bounded by 1. The quantization error in s_ℓ , $\ell = 1, 2, \dots, n$, is therefore upper bounded by

$$|s_\ell - \hat{s}_\ell| = \sqrt{n\hat{Q}} \left| \prod_{i=1}^n g_i(\theta_i) - \prod_{i=1}^n g_i(\hat{\theta}_i) \right| \quad (\text{B.8})$$

$$= \sqrt{n\hat{Q}} \left| \sum_{j=1}^n \left[\prod_{i=1}^{j-1} g_i(\hat{\theta}_i) \prod_{i=j}^n g_i(\theta_i) - \prod_{i=1}^j g_i(\hat{\theta}_i) \prod_{i=j+1}^n g_i(\theta_i) \right] \right| \quad (\text{B.9})$$

$$\leq \sqrt{n\hat{Q}} \sum_{j=1}^n \left| \prod_{i=1}^{j-1} g_i(\hat{\theta}_i) \prod_{i=j}^n g_i(\theta_i) - \prod_{i=1}^j g_i(\hat{\theta}_i) \prod_{i=j+1}^n g_i(\theta_i) \right| \quad (\text{B.10})$$

$$\leq \sqrt{n\hat{Q}} \sum_{j=1}^n \left| \prod_{i=1}^{j-1} g_i(\hat{\theta}_i) \prod_{i=j+1}^n g_i(\theta_i) \cdot [g_j(\hat{\theta}_j) - g_j(\theta_j)] \right| \quad (\text{B.11})$$

$$\leq \sqrt{n\hat{Q}} \sum_{j=1}^n \left| \prod_{i=1}^{j-1} g_i(\hat{\theta}_i) \prod_{i=j+1}^n g_i(\theta_i) \right| \cdot \left| g_j(\hat{\theta}_j) - g_j(\theta_j) \right| \quad (\text{B.12})$$

$$\leq \sqrt{n\hat{Q}} \sum_{j=1}^n \frac{\pi}{n^2} \quad (\text{B.13})$$

$$= \frac{\pi\sqrt{\hat{Q}}}{\sqrt{n}}, \quad (\text{B.14})$$

and so, $\|\mathbf{s} - \hat{\mathbf{s}}\| \leq \pi\sqrt{\hat{Q}}$. Since the large-deviations bounds on $K_n(\mathbf{s}, m)$ (eqs. (B.1) and (B.2)), decay double-exponentially with n , while M is only exponential and the number of quantization points is only $n^{2(n-1)}$, it follows by the union bound that with probability that tends to one double-exponentially, these bounds hold simultaneously for all m and all quantization points on the hypersphere surface. Given that this happens, then for any point on the hypersphere surface, we have

$$\mathbf{u}^T \mathbf{s} = \mathbf{u}^T [\hat{\mathbf{s}} + (\mathbf{s} - \hat{\mathbf{s}})] \quad (\text{B.15})$$

$$= \mathbf{u}^T \hat{\mathbf{s}} + \mathbf{u}^T (\mathbf{s} - \hat{\mathbf{s}}) \quad (\text{B.16})$$

$$\geq \alpha_{\mathbf{s}} \hat{\mathbf{s}}^T \hat{\mathbf{s}} - \|\mathbf{u}\| \cdot \|\mathbf{s} - \hat{\mathbf{s}}\| \quad (\text{B.17})$$

$$\geq \alpha_{\mathbf{s}} \hat{\mathbf{s}}^T \hat{\mathbf{s}} - \sqrt{nW} \cdot \pi\sqrt{\hat{Q}} \quad (\text{B.18})$$

$$= n\alpha\sqrt{Q\hat{Q}} - \pi\sqrt{nW\hat{Q}}, \quad (\text{B.19})$$

where the second term, which scales with \sqrt{n} , is asymptotically negligible relative to the first one, which is linear in n . It follows that every codeword in $\mathcal{C}_m \cap \mathcal{T}(\mathbf{U}|\hat{\mathbf{s}})$ is also in $\mathcal{C}_m \cap \mathcal{T}(\mathbf{U}|\mathbf{s})$, provided that \mathbf{s} is quantized to $\hat{\mathbf{s}}$, and provided that $\mathcal{T}(\mathbf{U}|\mathbf{s})$ is slightly expanded by reducing the threshold, $\alpha_{\mathbf{s}}\|\mathbf{s}\|^2$, within a relative amount that vanishes as n grows without bound.

Proof of Lemma 2

For a given \mathbf{y} and \tilde{k} , consider first the probability

$$\mathbb{P}\left\{\hat{\rho}^2(\mathbf{U}_{\tilde{k}}, \mathbf{y}) \geq 1 - \exp[-2(R + I_{US} - \epsilon)]\right\}.$$

Since $\mathbf{U}_{\tilde{k}}$ is distributed uniformly over the surface of a hypersphere, this probability is equal to the relative area of an n -dimensional spherical cap with half-angle

$$\theta = \arccos(\sqrt{1 - \exp[-2(R + I_{US} - \epsilon)]}), \quad (\text{B.20})$$

which is of the exponential order of (see, e.g., [38]):

$$\begin{aligned} \sin^n(\theta) &= \exp\left\{\frac{n}{2} \ln \sin^2 \theta\right\} \\ &= \exp\left\{\frac{n}{2} \ln(1 - \cos^2 \theta)\right\} \\ &= \exp\left\{\frac{n}{2} \ln(1 - [1 - \exp\{-2(R + I_{US} - \epsilon)\}])\right\} \\ &= \exp\{-n(R + I_{US} - \epsilon)\}. \end{aligned} \quad (\text{B.21})$$

Therefore, for a given (k, k') and \mathbf{y} ,

$$\begin{aligned} &\mathbb{P}\left\{\max_{\tilde{k} \neq k, k'} \hat{\rho}^2(\mathbf{U}_{\tilde{k}}, \mathbf{y}) < 1 - \exp[-2(R + I_{US} - \epsilon)]\right\} \\ &\quad \doteq [1 - \exp\{-n(R + I_{US} - \epsilon)\}]^M \\ &\quad = [1 - \exp\{-n(R + I_{US} - \epsilon)\}]^{\exp\{n[R + I_{US} + \Delta]\}} \\ &\quad = \exp\{\exp\{n[R + I_{US} + \Delta]\} \ln [1 - \exp\{-n(R + I_{US} - \epsilon)\}]\} \\ &\quad \leq \exp\{-\exp\{n[R + I_{US} + \Delta]\} \exp\{-n(R + I_{US} - \epsilon)\}\} \\ &\quad = \exp\{-\exp\{n[\Delta + \epsilon]\}\}, \end{aligned} \quad (\text{B.22})$$

which decays double-exponentially as $n \rightarrow \infty$. Applying the union bound over all pairs (k, k') , introduces an exponential factor of the order of M^2 , which leaves the probability of the union double-exponentially small. As for the union over $\{\mathbf{y}\}$, it is sufficient to consider one hypersphere surface since the empirical correlation coefficient is invariant to scaling of \mathbf{y} . Consider again, quantization of the hypersphere of \mathbf{y} as in the proof of Lemma 1, with $n^{2(n-1)}$ quantization points. With very high probability, the same property applies to every quantization point at the same time, since the factor of $n^{2(n-1)}$ still leaves the probability of the union double-exponentially small. Finally, we pass to the continuum of $\{\mathbf{y}\}$ in the hypersphere, in the same

way as in the proof of Lemma 1, by using the fact that the quantization error is small and hence affects the empirical correlation coefficient by a vanishingly small amount as n grows without bound.

Appendix C - Proof of Theorem 2

Step 1: Error exponent for a general decoding metric

Given $m \in \{1, 2, \dots, M\}$, $\mathbf{S} = \mathbf{s}$, $\mathbf{U} = \mathbf{u} \in \mathcal{C}(m, \mathbf{s})$, $\mathbf{X} = \mathbf{x} \in \mathcal{T}(Q_{X|SU}|\mathbf{s}, \mathbf{u})$, and $\mathbf{Y} = \mathbf{y}$, the probability of error is given by

$$P_e(m, \mathbf{s}, \mathbf{u}, \mathbf{x}, \mathbf{y}) = \mathbb{P} \left\{ \bigcup_{Q_{S'}} \bigcup_{m' \neq m} \bigcup_{k=1}^{M(Q_{S'})} \{G(\hat{P}_{\mathbf{U}_{Q_{S'}, m', k} \mathbf{y}}, Q_{S'}) \geq G(\hat{P}_{\mathbf{u} \mathbf{y}}, \hat{P}_{\mathbf{s}})\} \right\} \quad (\text{C.1})$$

$$\doteq \min \left\{ 1, \sum_{Q_{S'}} \sum_{m' \neq m} \sum_{k=1}^{M(Q_{S'})} \mathbb{P}\{G(\hat{P}_{\mathbf{U}_{Q_{S'}, m', k} \mathbf{y}}, Q_{S'}) \geq G(\hat{P}_{\mathbf{u} \mathbf{y}}, \hat{P}_{\mathbf{s}})\} \right\}. \quad (\text{C.2})$$

For any $Q_{S'}$, $m' \neq m$, and $k \in \{1, 2, \dots, M(Q_{S'})\}$, let us denote $\mathbf{U}' = \mathbf{U}_{Q_{S'}, m', k}$. Then, the pairwise probability inside (C.2) can be assessed using the method of types as follows

$$\begin{aligned} & \mathbb{P}\{G(\hat{P}_{\mathbf{U}' \mathbf{y}}, Q_{S'}) \geq G(\hat{P}_{\mathbf{u} \mathbf{y}}, \hat{P}_{\mathbf{s}})\} \\ &= \sum_{\{\mathbf{u}': G(\hat{P}_{\mathbf{u}' \mathbf{y}}, Q_{S'}) \geq G(\hat{P}_{\mathbf{u} \mathbf{y}}, \hat{P}_{\mathbf{s}})\}} \frac{1}{|\mathcal{T}(Q_{U'})|} \end{aligned} \quad (\text{C.3})$$

$$= \sum_{\{Q_{U'|Y}: G(Q_{U'|Y} \times \hat{P}_{\mathbf{y}}, Q_{S'}) \geq G(\hat{P}_{\mathbf{u} \mathbf{y}}, \hat{P}_{\mathbf{s}})\}} \sum_{\mathbf{u}' \in \mathcal{T}(Q_{U'|Y}|\mathbf{y})} \frac{1}{|\mathcal{T}(Q_{U'})|} \quad (\text{C.4})$$

$$= \sum_{\{Q_{U'|Y}: G(Q_{U'|Y} \times \hat{P}_{\mathbf{y}}, Q_{S'}) \geq G(\hat{P}_{\mathbf{u} \mathbf{y}}, \hat{P}_{\mathbf{s}})\}} \frac{|\mathcal{T}(Q_{U'|Y}|\mathbf{y})|}{|\mathcal{T}(Q_{U'})|} \quad (\text{C.5})$$

$$\doteq \sum_{\{Q_{U'|Y}: G(Q_{U'|Y} \times \hat{P}_{\mathbf{y}}, Q_{S'}) \geq G(\hat{P}_{\mathbf{u} \mathbf{y}}, \hat{P}_{\mathbf{s}})\}} \exp\{-n I_Q(U'; Y)\} \quad (\text{C.6})$$

$$\doteq \exp \left\{ -n \min_{\{Q_{U'|Y}: G(Q_{U'|Y} \times \hat{P}_{\mathbf{y}}, Q_{S'}) \geq G(\hat{P}_{\mathbf{u} \mathbf{y}}, \hat{P}_{\mathbf{s}})\}} I_Q(U'; Y) \right\}. \quad (\text{C.7})$$

Note that the expression in (C.7) does not depend on $m' \neq m$ and $k \in \{1, 2, \dots, M(Q_{S'})\}$, hence, substituting (C.7) back into (C.2) yields that

$$\begin{aligned} & P_e(m, \mathbf{s}, \mathbf{u}, \mathbf{x}, \mathbf{y}) \\ & \doteq \min \left[1, \sum_{Q_{S'}} \sum_{m' \neq m} \sum_{k=1}^{M(Q_{S'})} \exp \left\{ -n \min_{\{Q_{U'|Y}: G(Q_{U'|Y} \times \hat{P}_{\mathbf{y}}, Q_{S'}) \geq G(\hat{P}_{\mathbf{u} \mathbf{y}}, \hat{P}_{\mathbf{s}})\}} I_Q(U'; Y) \right\} \right] \end{aligned} \quad (\text{C.8})$$

$$\doteq \exp \left\{ -n \min_{\{Q_{S'}, Q_{U'|Y}: G(Q_{U'|Y} \times \hat{P}_{\mathbf{y}}, Q_{S'}) \geq G(\hat{P}_{\mathbf{u}\mathbf{y}}, \hat{P}_{\mathbf{s}})\}} [I_Q(U'; Y) - R(Q_{S'}) - R - \varepsilon]_+ \right\} \quad (\text{C.9})$$

$$\triangleq \exp \left\{ -n E_0(R, \hat{P}_{\mathbf{s}}, \hat{P}_{\mathbf{u}\mathbf{y}}) \right\}. \quad (\text{C.10})$$

Next, given $m \in \{1, 2, \dots, M\}$, $\mathbf{S} = \mathbf{s}$, $\mathbf{U} = \mathbf{u} \in \mathcal{C}(m, \mathbf{s})$, and $\mathbf{X} = \mathbf{x} \in \mathcal{T}(Q_{X|SU}|\mathbf{s}, \mathbf{u})$, we average over the randomness of the channel output vector \mathbf{Y} :

$$P_e(m, \mathbf{s}, \mathbf{u}, \mathbf{x}) \doteq \sum_{\mathbf{y} \in \mathcal{Y}^n} W(\mathbf{y}|\mathbf{x}, \mathbf{s}) \exp \left\{ -n E_0(R, \hat{P}_{\mathbf{s}}, \hat{P}_{\mathbf{u}\mathbf{y}}) \right\} \quad (\text{C.11})$$

$$= \sum_{Q_{Y|SUX}} \sum_{\mathbf{y} \in \mathcal{T}(Q_{Y|SUX}|\mathbf{s}, \mathbf{u}, \mathbf{x})} W(\mathbf{y}|\mathbf{x}, \mathbf{s}) \exp \left\{ -n E_0(R, \hat{P}_{\mathbf{s}}, \hat{P}_{\mathbf{u}\mathbf{y}}) \right\} \quad (\text{C.12})$$

$$\doteq \sum_{Q_{Y|SUX}} \exp \{ -n D(Q_{Y|SUX} \| W_{Y|XS} | \hat{P}_{\mathbf{s}\mathbf{u}\mathbf{x}}) \} \exp \left\{ -n E_0(R, \hat{P}_{\mathbf{s}}, Q_{UY}) \right\} \quad (\text{C.13})$$

$$\doteq \exp \left\{ -n \cdot \min_{Q_{Y|SUX}} \{ D(Q_{Y|SUX} \| W_{Y|XS} | \hat{P}_{\mathbf{s}\mathbf{u}\mathbf{x}}) + E_0(R, \hat{P}_{\mathbf{s}}, Q_{UY}) \} \right\}. \quad (\text{C.14})$$

Note that (C.14) depends on $\mathbf{s}, \mathbf{u}, \mathbf{x}$ only via their joint empirical distribution, hence, averaging over the randomness of $\mathbf{U} \in \mathcal{B}(\hat{P}_{\mathbf{s}}, m) \cap \mathcal{T}(Q_{U|S}|\mathbf{s})$ and $\mathbf{X} \in \mathcal{T}(Q_{X|SU}|\mathbf{s}, \mathbf{u})$ yields

$$P_e(m, \mathbf{s}) \doteq \exp \left\{ -n \cdot \min_{Q_{Y|SUX}} \{ D(Q_{Y|SUX} \| W_{Y|XS} | Q_{UX|S} \times \hat{P}_{\mathbf{s}}) + E_0(R, \hat{P}_{\mathbf{s}}, Q_{UY}) \} \right\} \quad (\text{C.15})$$

$$\triangleq \exp \{ -n \cdot E_1(R, \hat{P}_{\mathbf{s}}, Q_{UX|S}) \}. \quad (\text{C.16})$$

The exponent function in (C.16) depends on $Q_{UX|S}$, which are design parameters of the system that can be chosen to minimize the average error probability. Thus, minimizing the average probability of error w.r.t. $Q_{UX|S}$, we arrive at

$$P_e(m, \mathbf{s}) \doteq \exp \left\{ -n \cdot \max_{Q_{UX|S}} E_1(R, \hat{P}_{\mathbf{s}}, Q_{UX|S}) \right\} \quad (\text{C.17})$$

$$\triangleq \exp \{ -n \cdot E_2(R, \hat{P}_{\mathbf{s}}) \}. \quad (\text{C.18})$$

Averaging w.r.t. the randomness of \mathbf{S} , we arrive at

$$P_e(m) \doteq \sum_{\mathbf{s} \in \mathcal{S}^n} P(\mathbf{s}) \exp \{ -n \cdot E_2(R, \hat{P}_{\mathbf{s}}) \} \quad (\text{C.19})$$

$$= \sum_{Q_S} \sum_{\mathbf{s} \in \mathcal{T}(Q_S)} P(\mathbf{s}) \exp \{ -n \cdot E_2(R, \hat{P}_{\mathbf{s}}) \} \quad (\text{C.20})$$

$$\doteq \exp \left\{ -n \cdot \min_{Q_S} [D(Q_S \| P_S) + E_2(R, Q_S)] \right\}, \quad (\text{C.21})$$

which does not depend on the specific value of m , hence,

$$P_e \doteq \exp \left\{ -n \cdot \min_{Q_S} [D(Q_S \| P_S) + E_2(R, Q_S)] \right\}. \quad (\text{C.22})$$

Finally, due to the arbitrariness of $\varepsilon > 0$, it follows that the exact random coding error exponent is given by

$$E(R) = \min_{Q_S} \max_{Q_{UX|S}} [D(Q_S \| P_S) + E_1(R, Q_S, Q_{UX|S})], \quad (\text{C.23})$$

where

$$E_1(R, Q_S, Q_{UX|S}) = \min_{Q_{Y|SUX}} \{D(Q_{Y|SUX} \| W_{Y|XS} | Q_{UX|S} \times Q_S) + E_0(R, Q_S, Q_{UY})\}, \quad (\text{C.24})$$

and

$$E_0(R, Q_S, Q_{UY}) = \min_{\{Q_{S'}, Q_{U'|Y}: G(Q_{U'|Y}, Q_{S'}) \geq G(Q_{UY}, Q_S)\}} [I_Q(U'; Y) - R(Q_{S'}) - R]_+. \quad (\text{C.25})$$

Step 2: An upper bound on the error exponent

Note that the minimum in (C.25) can be upper-bounded by choosing specific distributions in the feasible set. In (C.25), we take $Q_{U'|Y} = Q_{U|Y}$, $Q_{S'} = Q_S$, and then

$$E_0(R, Q_S, Q_{UY}) \leq [I_Q(U; Y) - R(Q_S) - R]_+. \quad (\text{C.26})$$

Hence, the overall error exponent is upper-bounded as

$$\begin{aligned} E(R) &\leq \min_{Q_S} \max_{Q_{UX|S}} \min_{Q_{Y|SUX}} \{D(Q_S \| P_S) + D(Q_{Y|SUX} \| W_{Y|XS} | Q_{UX|S} \times Q_S) \\ &\quad + [I_Q(U; Y) - R(Q_S) - R]_+\}. \end{aligned} \quad (\text{C.27})$$

Step 3: An optimal universal decoder

We prove that the upper bound of (C.27) is attainable by choosing the universal decoding metric $G(Q_{UY}, Q_S) = I_Q(U; Y) - R(Q_S)$. Now, we get for (C.25)

$$E_0(R, Q_S, Q_{UY}) = \min_{\{Q_{S'}, Q_{U'|Y}: G(Q_{U'|Y}, Q_{S'}) \geq G(Q_{UY}, Q_S)\}} [I_Q(U'; Y) - R(Q_{S'}) - R]_+ \quad (\text{C.28})$$

$$= \min_{\substack{Q_{S'}, Q_{U'|Y}: \\ \{I_Q(U'; Y) - R(Q_{S'}) \geq I_Q(U; Y) - R(Q_S)\}}} [I_Q(U'; Y) - R(Q_{S'}) - R]_+ \quad (\text{C.29})$$

$$= [I_Q(U; Y) - R(Q_S) - R]_+, \quad (\text{C.30})$$

which completes the proof of Theorem 2.

Appendix D - Proof of Theorem 3

Assume that the matrix $\{Q_{UX|S}\}$ is fixed. Let us choose the universal decoding metric $g(Q_{UY}, Q_S) = I_Q(U; Y) - R(Q_S)$. For a given codebook, the probability of error is given by

$$\begin{aligned} P_e(\mathcal{C}_n) &= \sum_{Q_S} \mathbb{P}[\mathbf{S} \in \mathcal{T}(Q_S)] \frac{1}{M \cdot M(Q_S)} \sum_{m=1}^M \sum_{\ell=1}^{M(Q_S)} \sum_{\mathbf{s} \in \mathcal{T}(Q_S)} P(\mathbf{s} | \mathbf{u}_{m,\ell}) \\ &\quad \times \sum_{\mathbf{x} \in \mathcal{T}(Q_{X|US} | \mathbf{u}_{m,\ell}, \mathbf{s})} \frac{1}{|\mathcal{T}(Q_{X|US} | \mathbf{u}_{m,\ell}, \mathbf{s})|} \\ &\quad \times \sum_{\mathbf{y} \in \mathcal{Y}^n} W(\mathbf{y} | \mathbf{x}, \mathbf{s}) \mathbb{1} \left\{ \bigcup_{Q_{S'}} \bigcup_{m' \neq m} \bigcup_{\ell'=1}^{M(Q_{S'})} \{g(\hat{P}_{\mathbf{u}_{m',\ell'} \mathbf{y}}, Q_{S'}) \geq g(\hat{P}_{\mathbf{u}_{m,\ell} \mathbf{y}}, Q_S)\} \right\}. \end{aligned} \quad (\text{D.1})$$

We upper-bound the inner-most summation over \mathbf{y} by⁸:

$$\begin{aligned} &\sum_{\mathbf{y} \in \mathcal{Y}^n} W(\mathbf{y} | \mathbf{x}, \mathbf{s}) \mathbb{1} \left\{ \bigcup_{Q_{S'}} \bigcup_{m' \neq m} \bigcup_{\ell'=1}^{M(Q_{S'})} \{g(\hat{P}_{\mathbf{u}_{m',\ell'} \mathbf{y}}, Q_{S'}) \geq g(\hat{P}_{\mathbf{u}_{m,\ell} \mathbf{y}}, Q_S)\} \right\} \\ &= \sum_{\mathbf{y} \in \mathcal{Y}^n} W(\mathbf{y} | \mathbf{x}, \mathbf{s}) \mathbb{1} \left\{ \bigcup_{Q_{S'}} \bigcup_{m' \neq m} \bigcup_{\ell'=1}^{M(Q_{S'})} \{\exp\{ng(\hat{P}_{\mathbf{u}_{m',\ell'} \mathbf{y}}, Q_{S'})\} \geq \exp\{ng(\hat{P}_{\mathbf{u}_{m,\ell} \mathbf{y}}, Q_S)\}\} \right\} \\ &\leq \sum_{\mathbf{y} \in \mathcal{Y}^n} W(\mathbf{y} | \mathbf{x}, \mathbf{s}) \sum_{Q_{S'}} \sum_{m' \neq m} \sum_{\ell'=1}^{M(Q_{S'})} \inf_{\mu \geq 0} \left[\frac{\exp\{ng(\hat{P}_{\mathbf{u}_{m',\ell'} \mathbf{y}}, Q_{S'})\}}{\exp\{ng(\hat{P}_{\mathbf{u}_{m,\ell} \mathbf{y}}, Q_S)\}} \right]^\mu \end{aligned} \quad (\text{D.3})$$

$$= \sum_{Q_{S'}} \sum_{m' \neq m} \sum_{\ell'=1}^{M(Q_{S'})} \sum_{\mathbf{y} \in \mathcal{Y}^n} W(\mathbf{y} | \mathbf{x}, \mathbf{s}) \inf_{\mu \geq 0} \left[\frac{\exp\{ng(\hat{P}_{\mathbf{u}_{m',\ell'} \mathbf{y}}, Q_{S'})\}}{\exp\{ng(\hat{P}_{\mathbf{u}_{m,\ell} \mathbf{y}}, Q_S)\}} \right]^\mu, \quad (\text{D.4})$$

where the inner-most sum over $\mathbf{y} \in \mathcal{Y}^n$ is assessed by the method of types as

$$\sum_{\mathbf{y} \in \mathcal{Y}^n} W(\mathbf{y} | \mathbf{x}, \mathbf{s}) \exp \left\{ -n \cdot \sup_{\mu \geq 0} \left\{ \mu \cdot [g(\hat{P}_{\mathbf{u}_{m,\ell} \mathbf{y}}, Q_S) - g(\hat{P}_{\mathbf{u}_{m',\ell'} \mathbf{y}}, Q_{S'})] \right\} \right\} \quad (\text{D.5})$$

$$= \sum_{Q_{Y|UU'SX}} \sum_{\mathbf{y} \in \mathcal{T}(Q_{Y|UU'SX} | \mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}, \mathbf{s}, \mathbf{x})} W(\mathbf{y} | \mathbf{x}, \mathbf{s}) \exp \left\{ -n \cdot \Psi(\hat{P}_{\mathbf{u}_{m,\ell} \mathbf{y}}, Q_S, \hat{P}_{\mathbf{u}_{m',\ell'} \mathbf{y}}, Q_{S'}) \right\} \quad (\text{D.6})$$

⁸A tighter upper bound in (D.3) can be obtained by using the inequality [10]

$$\mathbb{1} \left\{ \bigcup_k \{\exp\{ng(\hat{P}_{\mathbf{u}_k \mathbf{y}})\} \geq \exp\{ng(\hat{P}_{\mathbf{u} \mathbf{y}})\}\} \right\} \leq \left(\sum_k \inf_{\mu \geq 0} \left[\frac{\exp\{ng(\hat{P}_{\mathbf{u}_k \mathbf{y}})\}}{\exp\{ng(\hat{P}_{\mathbf{u} \mathbf{y}})\}} \right]^\mu \right)^\rho, \quad (\text{D.2})$$

where $\rho > 0$ is a parameter to be optimized. Using this inequality is expected to yield an exponent function which will be tighter at relatively high coding rates. Since the random coding error exponent given in Theorem 2 provides the true exponential behavior at the range of high coding rates, we refrain from applying (D.2) for two reasons: (i) simplicity and (ii) at low rates, the optimal value of ρ is expected to be 1 anyway (after limiting ρ to be less than 1 in order to apply Jensen's inequality), which corresponds to a simple union bound.

$$= \sum_{Q_{Y|UU'SX}} \sum_{\mathbf{y} \in \mathcal{T}(Q_{Y|UU'SX} | \mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}, \mathbf{s}, \mathbf{x})} e^{n\mathbb{E}_Q[\ln W(Y|X,S)]} \exp \{-n \cdot \Psi(Q_{UY}, Q_S, Q_{U'Y}, Q_{S'})\} \quad (\text{D.7})$$

$$\doteq \sum_{Q_{Y|UU'SX}} e^{-nD(Q_{Y|UU'SX} \| W_{Y|SX} | \hat{P}_{\mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}, \mathbf{s}, \mathbf{x}})} \exp \{-n \cdot \Psi(Q_{UY}, Q_S, Q_{U'Y}, Q_{S'})\} \quad (\text{D.8})$$

$$\triangleq \exp \{-nE_0(\hat{P}_{\mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}, \mathbf{s}, \mathbf{x}}, Q_{S'})\}. \quad (\text{D.9})$$

Substituting it back into (D.1) yields that

$$\begin{aligned} & P_e(\mathcal{C}_n) \\ & \leq \sum_{Q_S} \mathbb{P}[\mathbf{S} \in \mathcal{T}(Q_S)] \frac{1}{M \cdot M(Q_S)} \sum_{m=1}^M \sum_{\ell=1}^{M(Q_S)} \sum_{\mathbf{s} \in \mathcal{T}(Q_S)} P(\mathbf{s} | \mathbf{u}_{m,\ell}) \\ & \quad \times \sum_{\mathbf{x} \in \mathcal{T}(Q_{X|US} | \mathbf{u}_{m,\ell}, \mathbf{s})} \frac{1}{|\mathcal{T}(Q_{X|US} | \mathbf{u}_{m,\ell}, \mathbf{s})|} \sum_{Q_{S'}} \sum_{m' \neq m} \sum_{\ell'=1}^{M(Q_{S'})} \exp \{-nE_0(\hat{P}_{\mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}, \mathbf{s}, \mathbf{x}}, Q_{S'})\} \end{aligned} \quad (\text{D.10})$$

$$\begin{aligned} & = \sum_{Q_S} \mathbb{P}[\mathbf{S} \in \mathcal{T}(Q_S)] \frac{1}{M \cdot M(Q_S)} \sum_{m=1}^M \sum_{\ell=1}^{M(Q_S)} \sum_{\mathbf{s} \in \mathcal{T}(Q_S)} P(\mathbf{s} | \mathbf{u}_{m,\ell}) \\ & \quad \times \sum_{Q_{S'}} \sum_{m' \neq m} \sum_{\ell'=1}^{M(Q_{S'})} \sum_{\mathbf{x} \in \mathcal{T}(Q_{X|US} | \mathbf{u}_{m,\ell}, \mathbf{s})} \frac{1}{|\mathcal{T}(Q_{X|US} | \mathbf{u}_{m,\ell}, \mathbf{s})|} \exp \{-nE_0(\hat{P}_{\mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}, \mathbf{s}, \mathbf{x}}, Q_{S'})\}. \end{aligned} \quad (\text{D.11})$$

The inner-most sum over \mathbf{x} is assessed by the method of types as

$$\begin{aligned} & \sum_{\mathbf{x} \in \mathcal{T}(Q_{X|US} | \mathbf{u}_{m,\ell}, \mathbf{s})} \frac{1}{|\mathcal{T}(Q_{X|US} | \mathbf{u}_{m,\ell}, \mathbf{s})|} \exp \{-nE_0(\hat{P}_{\mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}, \mathbf{s}, \mathbf{x}}, Q_{S'})\} \\ & = \sum_{\{\bar{Q}_{X|UU'S} : \bar{Q}_{X|US} = Q_{X|US}\}} \sum_{\mathbf{x} \in \mathcal{T}(\bar{Q}_{X|UU'S} | \mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}, \mathbf{s})} \frac{1}{|\mathcal{T}(\bar{Q}_{X|UU'S} | \mathbf{u}_{m,\ell}, \mathbf{s})|} \exp \{-nE_0(\hat{P}_{\mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}, \mathbf{s}, \mathbf{x}}, Q_{S'})\} \end{aligned} \quad (\text{D.12})$$

$$= \sum_{\{\bar{Q}_{X|UU'S} : \bar{Q}_{X|US} = Q_{X|US}\}} \frac{|\mathcal{T}(\bar{Q}_{X|UU'S} | \mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}, \mathbf{s})|}{|\mathcal{T}(Q_{X|US} | \mathbf{u}_{m,\ell}, \mathbf{s})|} \exp \{-nE_0(\hat{P}_{\mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}, \mathbf{s}, \mathbf{x}}, Q_{S'})\} \quad (\text{D.13})$$

$$\doteq \sum_{\{\bar{Q}_{X|UU'S} : \bar{Q}_{X|US} = Q_{X|US}\}} \exp \{-nI_{\bar{Q}}(U'; X|US)\} \exp \{-nE_0(\hat{P}_{\mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}, \mathbf{s}, \mathbf{x}}, Q_{S'})\} \quad (\text{D.14})$$

$$\doteq \exp \left\{ -n \cdot \min_{\{\bar{Q}_{X|UU'S} : \bar{Q}_{X|US} = Q_{X|US}\}} [I_{\bar{Q}}(U'; X|US) + E_0(\hat{P}_{\mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}, \mathbf{s}, \mathbf{x}}, Q_{S'})] \right\} \quad (\text{D.15})$$

$$\triangleq \exp\{-nE_1(\hat{P}_{\mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}, \mathbf{s}}, Q_{S'})\}. \quad (\text{D.16})$$

Substituting it back into (D.11) yields that

$$\begin{aligned} P_e(\mathcal{C}_n) &\leq \sum_{Q_S} \mathbb{P}[\mathbf{S} \in \mathcal{T}(Q_S)] \frac{1}{M \cdot M(Q_S)} \sum_{m=1}^M \sum_{\ell=1}^{M(Q_S)} \sum_{\mathbf{s} \in \mathcal{T}(Q_S)} P(\mathbf{s} | \mathbf{u}_{m,\ell}) \\ &\quad \times \sum_{Q_{S'}} \sum_{m' \neq m} \sum_{\ell'=1}^{M(Q_{S'})} \exp\{-nE_1(\hat{P}_{\mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}, \mathbf{s}}, Q_{S'})\} \end{aligned} \quad (\text{D.17})$$

$$\begin{aligned} &= \sum_{Q_S} \mathbb{P}[\mathbf{S} \in \mathcal{T}(Q_S)] \frac{1}{M \cdot M(Q_S)} \sum_{m=1}^M \sum_{\ell=1}^{M(Q_S)} \\ &\quad \times \sum_{Q_{S'}} \sum_{m' \neq m} \sum_{\ell'=1}^{M(Q_{S'})} \sum_{\mathbf{s} \in \mathcal{T}(Q_S)} P(\mathbf{s} | \mathbf{u}_{m,\ell}) \exp\{-nE_1(\hat{P}_{\mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}, \mathbf{s}}, Q_{S'})\}. \end{aligned} \quad (\text{D.18})$$

Again, the inner-most sum is assessed by the method of types as

$$\begin{aligned} &\sum_{\mathbf{s} \in \mathcal{T}(Q_S)} P(\mathbf{s} | \mathbf{u}_{m,\ell}) \exp\{-nE_1(\hat{P}_{\mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}, \mathbf{s}}, Q_{S'})\} \\ &= \sum_{\{\tilde{Q}_{S|UU}: \tilde{Q}_S = Q_S\}} \sum_{\mathbf{s} \in \mathcal{T}(\tilde{Q}_{S|UU} | \mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'})} P(\mathbf{s} | \mathbf{u}_{m,\ell}) \exp\{-nE_1(\hat{P}_{\mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}, \mathbf{s}}, Q_{S'})\} \end{aligned} \quad (\text{D.19})$$

$$\begin{aligned} &= \sum_{\{\tilde{Q}_{S|UU}: \tilde{Q}_S = Q_S\}} \sum_{\mathbf{s} \in \mathcal{T}(\tilde{Q}_{S|UU} | \mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'})} \frac{1}{|\mathcal{T}(\tilde{Q}_{S|U} | \mathbf{u}_{m,\ell})|} \exp\{-nE_1(\hat{P}_{\mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}} \times \tilde{Q}_{S|UU}, Q_{S'})\} \end{aligned} \quad (\text{D.20})$$

$$= \sum_{\{\tilde{Q}_{S|UU}: \tilde{Q}_S = Q_S\}} \frac{|\mathcal{T}(\tilde{Q}_{S|UU} | \mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'})|}{|\mathcal{T}(\tilde{Q}_{S|U} | \mathbf{u}_{m,\ell})|} \exp\{-nE_1(\hat{P}_{\mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}} \times \tilde{Q}_{S|UU}, Q_{S'})\} \quad (\text{D.21})$$

$$\doteq \sum_{\{\tilde{Q}_{S|UU}: \tilde{Q}_S = Q_S\}} \exp\{-nI_{\tilde{Q}}(S; U' | U)\} \exp\{-nE_1(\hat{P}_{\mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}} \times \tilde{Q}_{S|UU}, Q_{S'})\} \quad (\text{D.22})$$

$$\doteq \exp \left\{ -n \cdot \min_{\{\tilde{Q}_{S|UU}: \tilde{Q}_S = Q_S\}} [I_{\tilde{Q}}(S; U' | U) + E_1(\hat{P}_{\mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}} \times \tilde{Q}_{S|UU}, Q_{S'})] \right\} \quad (\text{D.23})$$

$$\triangleq \exp\{-nE_2(\hat{P}_{\mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}}, Q_{S'})\}. \quad (\text{D.24})$$

Substituting it back into (D.18) yields that

$$\begin{aligned} &P_e(\mathcal{C}_n) \\ &\leq \sum_{Q_S} \sum_{Q_{S'}} \mathbb{P}[\mathbf{S} \in \mathcal{T}(Q_S)] \frac{1}{M \cdot M(Q_S)} \sum_{m=1}^M \sum_{\ell=1}^{M(Q_S)} \sum_{m' \neq m} \sum_{\ell'=1}^{M(Q_{S'})} \exp\{-nE_2(\hat{P}_{\mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}}, Q_{S'})\} \end{aligned} \quad (\text{D.25})$$

$$\doteq \sum_{Q_S} \sum_{Q_{S'}} e^{-nD(Q_S\|P_S)} e^{-n(R+R(Q_S))} \sum_{m=1}^M \sum_{\ell=1}^{M(Q_S)} \sum_{m' \neq m} \sum_{\ell'=1}^{M(Q_{S'})} \exp\{-nE_2(\hat{P}_{\mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}}, Q_{S'})\} \quad (\text{D.26})$$

$$= \sum_{Q_S} \sum_{Q_{S'}} e^{-nD(Q_S\|P_S)} e^{-n(R+R(Q_S))} \sum_{\ddot{Q}_{UU'} \in \mathcal{Q}(Q_U, Q_{U'})} N(\ddot{Q}_{UU'}) \exp\{-nE_2(\ddot{Q}_{UU'}, Q_{S'})\}, \quad (\text{D.27})$$

where $\mathcal{Q}(Q_U, Q_{U'}) = \{\ddot{Q}_{UU'} : \ddot{Q}_U = Q_U, \ddot{Q}_{U'} = Q_{U'}\}$ and

$$N(\ddot{Q}_{UU'}) \triangleq \sum_{m=1}^M \sum_{\ell=1}^{M(Q_S)} \sum_{m' \neq m} \sum_{\ell'=1}^{M(Q_{S'})} \mathbb{1} \left\{ (\mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}) \in \mathcal{T}(\ddot{Q}_{UU'}) \right\}. \quad (\text{D.28})$$

Now, for any $\rho > 1$,

$$\begin{aligned} \mathbb{E} \left[P_e(\mathcal{C}_n)^{1/\rho} \right] &\leq \sum_{Q_S} \sum_{Q_{S'}} e^{-nD(Q_S\|P_S)/\rho} e^{-n(R+R(Q_S))/\rho} \\ &\quad \sum_{\ddot{Q}_{UU'} \in \mathcal{Q}(Q_U, Q_{U'})} \mathbb{E} \left[N(\ddot{Q}_{UU'})^{1/\rho} \right] \exp\{-nE_2(\ddot{Q}_{UU'}, Q_{S'})/\rho\}. \end{aligned} \quad (\text{D.29})$$

The expectation in (D.29) is upper-bounded as [21]

$$\begin{aligned} &\mathbb{E} \left[N(\ddot{Q}_{UU'})^{1/\rho} \right] \\ &\leq \begin{cases} \exp\{n[2R + R(Q_S) + R(Q_{S'}) - I_{\ddot{Q}}(U; U')]/\rho\} & 2R + R(Q_S) + R(Q_{S'}) \geq I_{\ddot{Q}}(U; U') \\ \exp\{n[2R + R(Q_S) + R(Q_{S'}) - I_{\ddot{Q}}(U; U')]\} & 2R + R(Q_S) + R(Q_{S'}) < I_{\ddot{Q}}(U; U') \end{cases} \end{aligned} \quad (\text{D.30})$$

$$= \exp\{n([2R + R(Q_S) + R(Q_{S'}) - I_{\ddot{Q}}(U; U')]/\rho - [I_{\ddot{Q}}(U; U') - 2R - R(Q_S) - R(Q_{S'})]_+)\}, \quad (\text{D.31})$$

and so,

$$\begin{aligned} &\left(\mathbb{E} \left[N(\ddot{Q}_{UU'})^{1/\rho} \right] \right)^\rho \\ &\leq \exp\{n([2R + R(Q_S) + R(Q_{S'}) - I_{\ddot{Q}}(U; U')]/\rho - [I_{\ddot{Q}}(U; U') - 2R - R(Q_S) - R(Q_{S'})]_+)\} \end{aligned} \quad (\text{D.32})$$

$$\triangleq \exp\{nF(\ddot{Q}_{UU'}, R, R(Q_S), R(Q_{S'}), \rho)\}. \quad (\text{D.33})$$

Now, raising (D.29) to the power of ρ and substituting (D.33) back, we arrive at

$$\begin{aligned} &\left(\mathbb{E} \left[P_e(\mathcal{C}_n)^{1/\rho} \right] \right)^\rho \\ &\leq \sum_{Q_S} \sum_{Q_{S'}} e^{-nD(Q_S\|P_S)} e^{-n(R+R(Q_S))} \\ &\quad \sum_{\ddot{Q}_{UU'} \in \mathcal{Q}(Q_U, Q_{U'})} \exp\{nF(\ddot{Q}_{UU'}, R, R(Q_S), R(Q_{S'}), \rho)\} \exp\{-nE_2(\ddot{Q}_{UU'}, Q_{S'})\} \end{aligned} \quad (\text{D.34})$$

$$\doteq \exp \left\{ -n \cdot \min_{Q_S, Q_{S'}} \min_{\ddot{Q}_{UU'} \in \mathcal{Q}(Q_U, Q_{U'})} [E_2(\ddot{Q}_{UU'}, Q_{S'}) - F(\ddot{Q}_{UU'}, R, R(Q_S), R(Q_{S'}), \rho) + D(Q_S \| P_S) + R + R(Q_S)] \right\}. \quad (\text{D.35})$$

Hence, it follows from the inequality [33, Eq. (A35)]

$$\mathbb{E}[\ln P_e(\mathcal{C}_n)] \leq \ln \left(\mathbb{E} \left\{ [P_e(\mathcal{C}_n)]^{1/\rho} \right\} \right)^\rho, \quad (\text{D.36})$$

which holds for any $\rho > 0$, that

$$\begin{aligned} \liminf_{n \rightarrow \infty} -\frac{1}{n} \mathbb{E}[\ln P_e(\mathcal{C}_n)] &\geq \min_{Q_S, Q_{S'}} \min_{\ddot{Q}_{UU'} \in \mathcal{Q}(Q_U, Q_{U'})} [E_2(\ddot{Q}_{UU'}, Q_{S'}) - F(\ddot{Q}_{UU'}, R, R(Q_S), R(Q_{S'}), \rho) \\ &\quad + D(Q_S \| P_S) + R + R(Q_S)]. \end{aligned} \quad (\text{D.37})$$

Letting ρ grow without bound yields that

$$\begin{aligned} &\liminf_{n \rightarrow \infty} -\frac{1}{n} \mathbb{E}[\ln P_e(\mathcal{C}_n)] \\ &\geq \min_{Q_S, Q_{S'}} \min_{\{\ddot{Q}_{UU'} \in \mathcal{Q}(Q_U, Q_{U'}): I_{\ddot{Q}}(U; U') \leq 2R + R(Q_S) + R(Q_{S'})\}} \\ &\quad [E_2(\ddot{Q}_{UU'}, Q_{S'}) + I_{\ddot{Q}}(U; U') - 2R - R(Q_S) - R(Q_{S'}) + D(Q_S \| P_S) + R + R(Q_S)] \quad (\text{D.38}) \end{aligned}$$

$$\begin{aligned} &= \min_{Q_S, Q_{S'}} \min_{\{\ddot{Q}_{UU'} \in \mathcal{Q}(Q_U, Q_{U'}): I_{\ddot{Q}}(U; U') \leq 2R + R(Q_S) + R(Q_{S'})\}} \\ &\quad [D(Q_S \| P_S) + E_2(\ddot{Q}_{UU'}, Q_{S'}) + I_{\ddot{Q}}(U; U') - R - R(Q_{S'})]. \end{aligned} \quad (\text{D.39})$$

As a final step, we maximize the exponent function over the design parameters of the code:

$$\begin{aligned} \liminf_{n \rightarrow \infty} -\frac{1}{n} \mathbb{E}[\ln P_e(\mathcal{C}_n)] &\geq \max_{\{Q_{UX|S}\}} \min_{Q_S, Q_{S'}} \min_{\{\ddot{Q}_{UU'} \in \mathcal{Q}(Q_U, Q_{U'}): I_{\ddot{Q}}(U; U') \leq 2R + R(Q_S) + R(Q_{S'})\}} \\ &\quad [D(Q_S \| P_S) + E_2(\ddot{Q}_{UU'}, Q_{S'}) + I_{\ddot{Q}}(U; U') - R - R(Q_{S'})], \end{aligned} \quad (\text{D.40})$$

which completes the proof of Theorem 3.

Appendix E - Proof of Theorem 4

Assuming that message m was transmitted, the probability of error, for a given code \mathcal{C}_n , is given by

$$P_{e|m}(\mathcal{C}_n) = \sum_{Q_S} \mathbb{P}[\mathbf{S} \in \mathcal{T}(Q_S)] \frac{1}{M(Q_S)} \sum_{\ell=1}^{M(Q_S)} \sum_{\mathbf{s} \in \mathcal{T}(Q_S)} P(\mathbf{s} | \mathbf{u}_{m,\ell})$$

$$\begin{aligned}
& \times \sum_{\mathbf{x} \in \mathcal{T}(Q_{X|US} | \mathbf{u}_{m,\ell}, \mathbf{s})} \frac{1}{|\mathcal{T}(Q_{X|US} | \mathbf{u}_{m,\ell}, \mathbf{s})|} \\
& \times \sum_{\mathbf{y} \in \mathcal{Y}^n} W(\mathbf{y} | \mathbf{x}, \mathbf{s}) \mathbb{1} \left\{ \bigcup_{Q_{S'}} \bigcup_{m' \neq m} \bigcup_{\ell'=1}^{M(Q_{S'})} \{G(\hat{P}_{\mathbf{u}_{m',\ell'} \mathbf{y}}, Q_{S'}) \geq G(\hat{P}_{\mathbf{u}_{m,\ell} \mathbf{y}}, Q_S)\} \right\}. \quad (\text{E.1})
\end{aligned}$$

Since the whole difference relative to the total probability of error given in (D.1) is in the averaging over the set of bins (which is of size M), we may proceed using the same initial steps as in the proof of Theorem 3, and arrive at (upon using the result in (D.25))

$$\begin{aligned}
& P_{e|m}(\mathcal{C}_n) \\
& \stackrel{.}{\leq} \sum_{Q_S} \sum_{Q_{S'}} \mathbb{P}[\mathbf{S} \in \mathcal{T}(Q_S)] \frac{1}{M(Q_S)} \sum_{\ell=1}^{M(Q_S)} \sum_{m' \neq m} \sum_{\ell'=1}^{M(Q_{S'})} \exp\{-nE_2(\hat{P}_{\mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}}, Q_{S'})\} \quad (\text{E.2})
\end{aligned}$$

$$\stackrel{.}{=} \sum_{Q_S} \sum_{Q_{S'}} e^{-nD(Q_S \| P_S)} e^{-nR(Q_S)} \sum_{\ell=1}^{M(Q_S)} \sum_{m' \neq m} \sum_{\ell'=1}^{M(Q_{S'})} \exp\{-nE_2(\hat{P}_{\mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}}, Q_{S'})\} \quad (\text{E.3})$$

$$= \sum_{Q_S} \sum_{Q_{S'}} e^{-nD(Q_S \| P_S)} e^{-nR(Q_S)} \sum_{\ddot{Q}_{UU'} \in \mathcal{Q}(Q_U, Q_{U'})} \tilde{N}(\ddot{Q}_{UU'}) \exp\{-nE_2(\ddot{Q}_{UU'}, Q_{S'})\}, \quad (\text{E.4})$$

where $\mathcal{Q}(Q_U, Q_{U'}) = \{\ddot{Q}_{UU'} : \ddot{Q}_U = Q_U, \ddot{Q}_{U'} = Q_{U'}\}$ and

$$\tilde{N}(\ddot{Q}_{UU'}) \stackrel{\Delta}{=} \sum_{\ell=1}^{M(Q_S)} \sum_{m' \neq m} \sum_{\ell'=1}^{M(Q_{S'})} \mathbb{1} \left\{ (\mathbf{u}_{m,\ell}, \mathbf{u}_{m',\ell'}) \in \mathcal{T}(\ddot{Q}_{UU'}) \right\}. \quad (\text{E.5})$$

Now, for any $\rho > 1$,

$$\begin{aligned}
\mathbb{E} \left[P_{e|m}(\mathcal{C}_n)^{1/\rho} \right] & \stackrel{.}{\leq} \sum_{Q_S} \sum_{Q_{S'}} e^{-nD(Q_S \| P_S)/\rho} e^{-nR(Q_S)/\rho} \\
& \quad \sum_{\ddot{Q}_{UU'} \in \mathcal{Q}(Q_U, Q_{U'})} \mathbb{E} \left[\tilde{N}(\ddot{Q}_{UU'})^{1/\rho} \right] \exp\{-nE_2(\ddot{Q}_{UU'}, Q_{S'})/\rho\}. \quad (\text{E.6})
\end{aligned}$$

The expectation in (E.6) is upper-bounded as [21]

$$\begin{aligned}
& \mathbb{E} \left[\tilde{N}(\ddot{Q}_{UU'})^{1/\rho} \right] \\
& \stackrel{.}{\leq} \begin{cases} \exp\{n[R + R(Q_S) + R(Q_{S'}) - I_{\ddot{Q}}(U; U')]/\rho\} & R + R(Q_S) + R(Q_{S'}) \geq I_{\ddot{Q}}(U; U') \\ \exp\{n[R + R(Q_S) + R(Q_{S'}) - I_{\ddot{Q}}(U; U')]\} & R + R(Q_S) + R(Q_{S'}) < I_{\ddot{Q}}(U; U') \end{cases} \quad (\text{E.7})
\end{aligned}$$

$$= \exp\{n([R + R(Q_S) + R(Q_{S'}) - I_{\ddot{Q}}(U; U')]/\rho - [I_{\ddot{Q}}(U; U') - R - R(Q_S) - R(Q_{S'})]_+)\} \quad (\text{E.8})$$

$$\stackrel{\Delta}{=} \exp\{nG(\ddot{Q}_{UU'}, R, R(Q_S), R(Q_{S'}), \rho)\}. \quad (\text{E.9})$$

Substituting (E.9) back into (E.6) yields a bound which we shall shortly denote by $\Psi(R, \rho)$.

According to Markov's inequality, we get

$$\mathbb{P} \left\{ \frac{1}{M} \sum_{m=1}^M P_{e|m}(\mathcal{C}_n)^{1/\rho} > 2\Psi(R, \rho) \right\} \leq \frac{1}{2}, \quad (\text{E.10})$$

which means that there exists a code with

$$\frac{1}{M} \sum_{m=1}^M P_{e|m}(\mathcal{C}_n)^{1/\rho} \leq \Psi(R, \rho). \quad (\text{E.11})$$

We conclude that there exists a code \mathcal{C}'_n with $M/2$ bins for which

$$\max_m P_{e|m}(\mathcal{C}'_n)^{1/\rho} \leq 4\Psi(R, \rho), \quad (\text{E.12})$$

and so

$$\begin{aligned} & \max_m P_{e|m}(\mathcal{C}'_n) \\ & \stackrel{\cdot}{\leq} \left(\sum_{Q_S} \sum_{Q_{S'}} e^{-nD(Q_S\|P_S)/\rho} e^{-nR(Q_S)/\rho} \right. \\ & \quad \left. \sum_{\ddot{Q}_{UU'} \in \mathcal{Q}(Q_U, Q_{U'})} \exp\{nG(\ddot{Q}_{UU'}, R, R(Q_S), R(Q_{S'}), \rho)\} \exp\{-nE_2(\ddot{Q}_{UU'}, Q_{S'})/\rho\} \right)^\rho \quad (\text{E.13}) \end{aligned}$$

$$\begin{aligned} & \stackrel{\cdot}{=} \sum_{Q_S} \sum_{Q_{S'}} e^{-nD(Q_S\|P_S)} e^{-nR(Q_S)} \\ & \quad \sum_{\ddot{Q}_{UU'} \in \mathcal{Q}(Q_U, Q_{U'})} \exp\{n\rho G(\ddot{Q}_{UU'}, R, R(Q_S), R(Q_{S'}), \rho)\} \exp\{-nE_2(\ddot{Q}_{UU'}, Q_{S'})\} \quad (\text{E.14}) \end{aligned}$$

$$\begin{aligned} & \stackrel{\cdot}{=} \exp \left\{ -n \cdot \min_{Q_S, Q_{S'}} \min_{\ddot{Q}_{UU'} \in \mathcal{Q}(Q_U, Q_{U'})} [E_2(\ddot{Q}_{UU'}, Q_{S'}) - \rho G(\ddot{Q}_{UU'}, R, R(Q_S), R(Q_{S'}), \rho) \right. \\ & \quad \left. + D(Q_S\|P_S) + R(Q_S)] \right\}, \quad (\text{E.15}) \end{aligned}$$

thus,

$$\begin{aligned} & \liminf_{n \rightarrow \infty} -\frac{1}{n} \ln \max_m P_{e|m}(\mathcal{C}'_n) \\ & \geq \min_{Q_S, Q_{S'}} \min_{\ddot{Q}_{UU'} \in \mathcal{Q}(Q_U, Q_{U'})} [E_2(\ddot{Q}_{UU'}, Q_{S'}) - \rho G(\ddot{Q}_{UU'}, R, R(Q_S), R(Q_{S'}), \rho) \\ & \quad + D(Q_S\|P_S) + R(Q_S)]. \quad (\text{E.16}) \end{aligned}$$

Since the inequality in (E.16) holds for every $\rho \geq 1$, the negative exponential rate of the maximal

probability of error can be bounded as

$$\begin{aligned} & \liminf_{n \rightarrow \infty} -\frac{1}{n} \ln \max_m P_{e|m}(\mathcal{C}'_n) \\ & \geq \sup_{\rho \geq 1} \min_{Q_S, Q_{S'}} \min_{\ddot{Q}_{UU'} \in \mathcal{Q}(Q_U, Q_{U'})} [E_2(\ddot{Q}_{UU'}, Q_{S'}) - \rho G(\ddot{Q}_{UU'}, R, R(Q_S), R(Q_{S'}), \rho) \\ & \quad + D(Q_S \| P_S) + R(Q_S)] \end{aligned} \quad (\text{E.17})$$

$$\begin{aligned} & \geq \lim_{\rho \rightarrow \infty} \min_{Q_S, Q_{S'}} \min_{\ddot{Q}_{UU'} \in \mathcal{Q}(Q_U, Q_{U'})} [E_2(\ddot{Q}_{UU'}, Q_{S'}) - \rho G(\ddot{Q}_{UU'}, R, R(Q_S), R(Q_{S'}), \rho) \\ & \quad + D(Q_S \| P_S) + R(Q_S)]. \end{aligned} \quad (\text{E.18})$$

At this point, we shall proceed along the same steps as in [34, Eqs. (A.26)-(A.37)], and conclude that

$$\begin{aligned} & \liminf_{n \rightarrow \infty} -\frac{1}{n} \ln \max_m P_{e|m}(\mathcal{C}'_n) \\ & \geq \min_{Q_S, Q_{S'}} \min_{\{\ddot{Q}_{UU'} \in \mathcal{Q}(Q_U, Q_{U'}): I_{\ddot{Q}}(U; U') \leq R + R(Q_S) + R(Q_{S'})\}} \\ & \quad [E_2(\ddot{Q}_{UU'}, Q_{S'}) + I_{\ddot{Q}}(U; U') - R - R(Q_S) - R(Q_{S'}) + D(Q_S \| P_S) + R(Q_S)] \end{aligned} \quad (\text{E.19})$$

$$\begin{aligned} & = \min_{Q_S, Q_{S'}} \min_{\{\ddot{Q}_{UU'} \in \mathcal{Q}(Q_U, Q_{U'}): I_{\ddot{Q}}(U; U') \leq R + R(Q_S) + R(Q_{S'})\}} \\ & \quad [D(Q_S \| P_S) + E_2(\ddot{Q}_{UU'}, Q_{S'}) + I_{\ddot{Q}}(U; U') - R - R(Q_{S'})]. \end{aligned} \quad (\text{E.20})$$

As a final step, we maximize the exponent function over the design parameters of the code:

$$\begin{aligned} & \liminf_{n \rightarrow \infty} -\frac{1}{n} \ln \max_m P_{e|m}(\mathcal{C}'_n) \geq \max_{\{Q_{UX|S}\}} \min_{Q_S, Q_{S'}} \min_{\{\ddot{Q}_{UU'} \in \mathcal{Q}(Q_U, Q_{U'}): I_{\ddot{Q}}(U; U') \leq R + R(Q_S) + R(Q_{S'})\}} \\ & \quad [D(Q_S \| P_S) + E_2(\ddot{Q}_{UU'}, Q_{S'}) + I_{\ddot{Q}}(U; U') - R - R(Q_{S'})], \end{aligned} \quad (\text{E.21})$$

which completes the proof of Theorem 4.

References

- [1] E. Arikan and N. Merhav, “Guessing subject to distortion,” *IEEE Trans. Inf. Theory*, vol. 44, no. 3, pp. 1041–1056, May 1998.
- [2] R. Averbuch and N. Merhav, “Exact random coding exponents and universal decoders for the asymmetric broadcast channel,” *IEEE Trans. Inf. Theory*, vol. 64, no. 7, pp. 5070–5086, July 2018.

- [3] A. Barg and G. D. Forney, Jr., “Random codes: minimum distances and error exponents,” *IEEE Trans. Inf. Theory*, vol. 48, no. 9, pp. 2568–2573, September 2002.
- [4] R. J. Barron, B. Chen, and G. W. Wornell, “The duality between information embedding and source coding with side information and some applications,” *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1159–1180, May 2003.
- [5] G. Cocco, A. Guillén i Fàbregas, and J. Font-Segura, “Typical error exponents: a dual domain derivation,” 2022. [Online]. Available: <https://arxiv.org/abs/2203.15607>
- [6] M. Costa, “Writing on dirty paper,” *IEEE Trans. Inf. Theory*, vol. 29, no. 3, pp. 439–441, May 1983.
- [7] T. M. Cover and M. Chiang, “Duality between channel capacity and rate distortion with side information,” *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1629–1638, June 2002.
- [8] A. El Gamal and Y. H. Kim, *Network Information Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2011.
- [9] U. Erez and R. Zamir, “Error exponents of modulo-additive noise channels with side information at the transmitter,” *IEEE Trans. Inf. Theory*, vol. 47, no. 1, pp. 210–218, January 2001.
- [10] R. G. Gallager, *Information Theory and Reliable Communication*, New York, Wiley 1968.
- [11] S. I. Gel’fand and M. S. Pinsker, “Coding for channel with random parameters,” *Problem of Control and Information Theory*, vol. 9, no. 1, pp. 19–31, 1980.
- [12] C. Heegard and A. El Gamal, “On the capacity of computer memory with defects,” *IEEE Trans. Inf. Theory*, vol. 29, no. 5, pp. 731–739, September 1983.
- [13] G. Keshet, Y. Steinberg, and N. Merhav, “Channel coding in the presence of side information,” *Foundations and Trends in Communications and Information Theory*, vol. 4, nos. 6, pp. 1–136, 2007.
- [14] T. Liu, P. Moulin, and R. Koetter, “On error exponents of modulo lattice additive noise channels,” *IEEE Trans. Inf. Theory*, vol. 52, no. 2, pp. 454–471, February 2006.

- [15] T. Liu and P. Viswanath, “Opportunistic orthogonal writing on dirty paper,” *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 1828–1846, May 2006.
- [16] 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.
- [17] N. Merhav, “Statistical physics and information theory,” *Foundations and Trends in Communications and Information Theory*, vol. 6, nos. 1-2, pp. 1–212, 2009.
- [18] N. Merhav, “Universal decoding for arbitrary channels relative to a given class of decoding metrics,” *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5566–5576, September 2013.
- [19] N. Merhav, “Exact random coding error exponents of optimal bin index decoding,” *IEEE Trans. Inf. Theory*, vol. 60, no. 10, pp. 6024–6031, October 2014.
- [20] N. Merhav, “Reliability of universal decoding based on vector-quantized codewords,” *IEEE Trans. Inf. Theory*, vol. 63, no. 5, pp. 2696–2709, May 2017.
- [21] N. Merhav, “Error exponents of typical random codes,” *IEEE Trans. Inf. Theory*, vol. 64, no. 9, pp. 6223–6235, September 2018.
- [22] N. Merhav, “Error exponents of typical random codes for the colored Gaussian channel,” *IEEE Trans. Inf. Theory*, vol. 65, no. 12, pp. 8164–8179, December 2019.
- [23] N. Merhav, “Error exponents of typical random trellis codes,” *IEEE Trans. Inf. Theory*, vol. 66, no. 4, pp. 2067–2077, April 2020.
- [24] N. Merhav, “A Lagrange–dual lower bound to the error exponent of the typical random code,” *IEEE Trans. Inf. Theory*, vol. 66, no. 6, pp. 3456–3464, June 2020.
- [25] N. Merhav and S. Shamai, “On joint source-channel coding for the Wyner-Ziv source and the Gel’fand-Pinsker channel,” *IEEE Trans. Inf. Theory*, vol. 49, no. 11, pp. 2844–2855, November 2003.
- [26] P. Moulin and J. A. O’Sullivan, “Information-theoretic analysis of information hiding,” *IEEE Trans. Inf. Theory*, vol. 49, no. 3, pp. 563–593, March 2003.
- [27] P. Moulin and Y. Wang, “Capacity and random-coding exponents for channel coding with side information,” *IEEE Trans. Inf. Theory*, vol. 53, no. 4, pp. 1326–1347, April 2007.

- [28] A. Nazari, A. Anastasopoulos, and S. S. Pradhan, “Error exponent for multiple-access channels: lower bounds,” *IEEE Trans. Inf. Theory*, vol. 60, no. 9, pp. 5095–5115, September 2014.
- [29] S. S. Pradhan and J. C. Ramchandran, “Duality between source coding and channel coding and its extension to the side information case,” *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1181–1203, May 2003.
- [30] A. Somekh-Baruch and N. Merhav, “On the random coding error exponents of the single-user and the multiple-access Gel’fand–Pinsker channels,” in *Proc. IEEE Int. Symp. Information Theory*, Chicago, IL, June/July 2004, p. 448.
- [31] A. Somekh-Baruch, S. Shamai, and S. Verdú, “Cooperative multiple-access encoding with states available at one transmitter,” *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4448–4469, October 2008.
- [32] Y. Steinberg, “Coding for the degraded broadcast channel with random parameters, with causal and noncausal side information,” *IEEE Trans. Inf. Theory*, vol. 51, no. 8, pp. 2867–2877, August 2005.
- [33] R. Tamir and N. Merhav, “Trade-offs between error exponents and excess-rate exponents of typical Slepian–Wolf codes,” *Entropy* 2021, 23, 265. <http://doi.org/10.3390/e23030265>.
- [34] R. Tamir and N. Merhav, “Universal decoding for the typical random code and for the expurgated code,” *IEEE Trans. Inf. Theory*, vol. 68, no. 4, pp. 2156–2168, April 2022.
- [35] R. Tamir, N. Merhav, N. Weinberger, and A. Guillén i Fàbregas, “Large deviations behavior of the logarithmic error probability of random codes,” *IEEE Trans. Inf. Theory*, vol. 66, no. 11, pp. 6635–6659, November 2020.
- [36] L. V. Truong, G. Cocco, J. Font-Segura, and A. Guillén i Fàbregas, “Concentration properties of random codes,” 2022. [Online]. Available: <https://arxiv.org/abs/2203.07853>
- [37] H. Tyagi and P. Narayan, “The Gelfand–Pinsker channel: strong converse and upper bound for the reliability function,” in *Proc. IEEE Int. Symp. Information Theory*, Seoul, Korea, June/July 2009, pp. 1954–1957.

- [38] A. D. Wyner, “A bound on the number of distinguishable functions which are time-limited and approximately band-limited,” *SIAM Journal on Applied Mathematics*, vol. 24, no. 3, pp. 289–297, May 1973.