MODERATE DEVIATIONS AND EXACT ASYMPTOTICS IN CHANNEL CODING

A Dissertation

Presented to the Faculty of the Graduate School

of Cornell University

in Partial Fulfillment of the Requirements for the Degree of

Doctor of Philosophy

by

Yücel Altuğ

August 2013

MODERATE DEVIATIONS AND EXACT ASYMPTOTICS IN CHANNEL CODING

Yücel Altuğ, Ph.D.

Cornell University 2013

Investigation of the data rate, blocklength and error probability interplay for the optimum block code(s) on a discrete memoryless channel is a fundamental problem of information theory. Because of the intricacy of the problem, it is ubiquitous to allow blocklength to grow unboundedly, which, in turn, gives informative optimality results. Although there are classical asymptotic regimes to investigate this interplay, they have certain limitations. This thesis is about two new asymptotics in channel coding, proposed to address these limitations.

In moderate deviations, we consider the optimal error performance of the sequence of codes with rates increasing to the capacity with a speed between the classical asymptotic regimes of error exponents and normal approximation and prove that error probability vanishes sub-exponentially fast with a rate related to the dispersion of the channel. This conclusion is in contrast with the classical asymptotic regimes, in which either error probability vanishes or rate increases to the capacity, but not *simultaneously*. We believe that this contrast makes moderate deviations more relevant to practical code design, since the goal of the channel coding is to attain a rate that is close to capacity *and* an error probability that is close to zero.

In exact asymptotics, we concentrate on the sub-exponential factors of the well-known exponentially decaying bounds on the error probability to improve their orders. The reason of this quest is the fact that the exponent of these bounds vanishes as rate approaches the capacity, which, in turn, makes the sub-exponential terms to play a sig-

nificant role in the approximation of the error probability for this range of rates. The sharpened orders of the sub-exponential factors of these refinements are close to each other in general, and are equal for symmetric channels. Moreover, we reveal a phase transition of the optimal order of the pre-factor for this class of channels.

BIOGRAPHICAL SKETCH

Yücel Altuğ received B.S. and M.S. degrees in electrical and electronics engineering from Boğaziçi University, Turkey, in 2006 and 2008, respectively. Since August 2008, he has been at Cornell University, pursuing the Ph.D. degree in electrical and computer engineering under the guidance of Aaron Wagner, where he received an M.S. degree in electrical and computer engineering in 2012. He spent some part of 2012 summer at ÉPFL, hosted by Emre Telatar, and was a visiting student research collaborator at Princeton University during 2012-2013 academic year, hosted by Paul Cuff.

His main research interest is information theory, in particular Shannon theory. He is also interested in large deviations theory and mechanism design.

He was a recipient of Irwin and Joan Jacobs Scholarship in 2008 and the Director's PhD Thesis Research Award, in 2013, both from the School of Electrical and Computer Engineering at Cornell University.

To my parents, my brother, and Seda.

ACKNOWLEDGEMENTS

First and foremost, I thank my advisor Aaron Wagner for being a *model advisor*, in the sense of being an excellent researcher, a superb teacher and an outstanding mentor. To put it succinctly, Aaron was always a source of inspiration during the years I had the privilege to work with him and I am sincerely grateful for the enormous effort he put into my education.

I thank Lang Tong and Gennady Samorodnitsky for agreeing to serve on my thesis committee and their valuable feedback on my research.

I thank Paul Cuff for hosting me at Princeton University for 2012-2013 academic year. I enjoyed the time I spent at Princeton and the weekly meetings of his research group were really fun. I would also like to thank Emre Telatar for hosting me at ÉPFL for one month during 2012 summer. It was always a pleasure to interact with him. I would like to thank Ioannis Kontoyiannis, Sergio Verdú, Serdar Yüksel and Tamás Linder for their keen interest in my career.

I thank Scott Coldren and Daniel Richter for flawlessly taking care of all the administrative stuff.

My heartfelt thanks go to the former members of our group, i.e., *Group 1.0*, Ebad Ahmed, Benjamin Kelly, Amine Laourine, and Md. Saifur Rahman for their friendship and support. I learnt a lot from them and am still fascinated how they could tolerate all the mess on my table! Also, I should especially acknowledge Ben for his patience while I was trying to explain him the things I feel excited about.

Throughout my years at Cornell, I had the good fortune of meeting wonderful people, whose existence made my life delightful. I really appreciate their company. An incomplete list of them includes: Rob Arbogast, Turan Birol, Shiyao Chen, Oliver Kosut, Sina Lashgari, Xin Luo, Enrique Mallada, Nithin Michael, Ilan Shomorony, Alireza Vahid, Meng Wang, Xiaohua Yang and Erdal Yılmaz.

I am indebted to my parents Ali and Sebahat Altuğ, and my brother Yılmaz Altuğ, for their unconditional love, support and understanding that started the day I was born. Without them, this thesis would not exist at all.

Finally, I thank my fiancée Seda Aktaş. Throughout the years this research has been conducted, she was always with me, always trusted me, and was my biggest[1] critic who motivated me to try harder. Although the results in this thesis are not even close to compensate all the things she gave up for us, in particular for my career, I still would like to devote it to her.

[1] Aaron was a close second, especially with the paper drafts!

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Channel coding

Information theory, which is founded by Shannon in his seminal paper [61], aims to characterize the fundamental limits of data compression and reliable communication, in its essence. Arguably the most important contribution of [61] is the mathematical abstraction of reliable communication problem, also known as channel coding. Despite (or perhaps thanks to) its simplicity, Shannon's model has stood the test of time and might justly be considered as the foundation of any modern communication system.

In channel coding, a transmitter wants to communicate a message, which takes values in a finite set $\mathcal{M}$, to a receiver through an unreliable medium, called *channel*. Typically, the statistics of the imperfection due to the channel, which is called *noise*, are assumed to be known to both transmitter and receiver. Instead of using the channel once, transmitter and receiver use it multiple times to reduce the error by exploiting their knowledge of the noise statistics. Moreover, in order to further reduce the error, transmitter (resp. receiver) uses specialized algorithms called *encoder* (resp. *decoder*). The number of channel uses is called *latency* or *blocklength*. Since the channel is used multiple times, one should scale the size of the message set, from which the transmitted message is drawn, with the latency, which is called *data rate* or simply *rate*. Because of the uncertainty introduced by the channel, there is a chance that receiver can not correctly recover the transmitted message, which is characterized by the *probability of error*.

There are various different channel models in the literature. In this thesis, we con-

sider *discrete memoryless* instance of channel coding, in which, the channel is assumed to be a stochastic matrix from a finite set, say $\mathcal{X}$, to another finite set, say $\mathcal{Y}$. $\mathcal{X}$ (resp. $\mathcal{Y}$) is called the *input* (resp. *output*) *alphabet* of the channel and the channel is usually denoted by $W(\cdot|\cdot)$. The set of discrete channels from a finite set $\mathcal{X}$ to another finite set $\mathcal{Y}$ will be denoted by $\mathcal{P}(\mathcal{Y}\,|\,\mathcal{X})$ in the sequel. Moreover, it is assumed that the transition probabilities at each time instance is independent from any past and future transitions, i.e., for all[1] $N \in \mathbb{Z}^+$ and[2] $(\mathbf{x}^N, \mathbf{y}^N) \in \mathcal{X}^N \times \mathcal{Y}^N$, $W(\mathbf{y}^N\,|\,\mathbf{x}^N) = \prod_{n=1}^{N} W(y_n\,|\,x_n)$. Given a discrete memoryless channel (DMC) W, an (N, R) code consists of a *message set*[3] $\mathcal{M} := \{1, \ldots, \lceil e^{NR} \rceil\}$, an *encoder* $f_N : \mathcal{M} \to \mathcal{X}^N$ and a decoder $\varphi_N : \mathcal{Y}^N \to \mathcal{M}$. Typically, it is assumed that the message is distributed uniformly over $\mathcal{M}$. In words, encoder maps a message m to a vector in the input space of the channel, which is called the *codeword* and typically denoted by $\mathbf{x}^N(m)$. The collection of all the codewords, i.e., $\{\mathbf{x}^N(m)\}_{m\in\mathcal{M}}$, is called the *codebook* and assumed to be available at transmitter and receiver. Upon receiving the channel output, receiver declares an estimate of the transmitted message by utilizing its knowledge of the channel statistics and the codebook. This operation is captured by decoder mapping. Given an (N, R) code (f_N, φ_N), its *maximal error probability*, $\mathrm{P_e}(f_N, \varphi_N)$, is defined by

$$\mathrm{P_e}(f_N, \varphi_N) := \max_{m\in\mathcal{M}} W\left\{\varphi_N(\mathbf{Y}^N) \neq m \,|\, \mathbf{x}^N(m)\right\}. \tag{1.1}$$

Similarly, *average error probability*, $\bar{\mathrm{P}}_\mathrm{e}(f_N, \varphi_N)$, is defined by

$$\bar{\mathrm{P}}_\mathrm{e}(f_N, \varphi_N) := \frac{1}{|\mathcal{M}|} \sum_{m\in\mathcal{M}} W\left\{\varphi_N(\mathbf{Y}^N) \neq m \,|\, \mathbf{x}^N(m)\right\}. \tag{1.2}$$

[1]Throughout the thesis, $\mathbb{Z}^+$, $\mathbb{R}$, $\mathbb{R}_+$ and $\mathbb{R}^+$ denotes the set of positive integers, the set of real numbers, non-negative real numbers and positive real numbers, respectively.

[2]In the sequel, boldface letters denote vectors, letters with subscripts denote individual components of vectors. Furthermore, capital letters represent random variables and lowercase letters denote individual realizations of the corresponding random variable.

[3]The base of the exponent determines the unit of information that can be communicated per channel use. For example, the unit associated with base-2 and the natural base is called *bit/channel use* and *nat/channel use*, respectively. Although bit is the standard unit for the most applications, working with natural base is more convenient for the purposes of this thesis and hence we opt for using nat as our unit of information.

Given any $N \in \mathbb{Z}^+$ and $R \in \mathbb{R}_+$, $\mathrm{P_e}(N,R)$ (resp. $\bar{\mathrm{P}}_\mathrm{e}(N,R)$) denotes the optimum (or minimum) average (resp. maximal) error probability attainable by any (N,R) code.

There is a fundamental interplay between blocklength, rate and the optimum error probability. Given the intricacy of determining the tradeoff for each value of these parameters, resorting to a relaxation is almost inevitable. A ubiquitous relaxation in information theory is to let some parameter grow unboundedly. Typically, blocklength is assumed to grow unboundedly[4]. Passing to this asymptotic, in turn, gives crisp, informative optimality results that serve as halting rules for the quest for designing optimal communication systems.

The most important instance of the aforementioned interplay is determining the maximum amount of rate that can be sustained such that error probability is arbitrarily small, as the blocklength grows. The answer is the *capacity* of the channel:

$$C := \max_{P \in \mathcal{P}(\mathcal{X})} \mathrm{I}(P;W), \tag{1.3}$$

where

$$\mathrm{I}(P;W) := \sum_{(x,y)\in\mathcal{X}\times\mathcal{Y}} P(x)W(y\,|\,x) \ln \frac{W(y\,|\,x)}{\sum_{z\in\mathcal{X}} P(z)W(y\,|\,z)}, \tag{1.4}$$

is the *mutual information* between input and output of the channel W when the input has the distribution P and the maximization[5] is over all probability measures on $\mathcal{X}$, denoted by $\mathcal{P}(\mathcal{X})$.

The following result of Shannon[6] shows that channel capacity constitutes the thresh-

[4]Because of the significance of the short to moderate blocklengths in practice, one can seek finite blocklength bounds on the error probability for a given rate. This can be done for a general class of channels (e.g., [52], [70], [71]) or particular channels (e.g., [52, Theorem 35], [52, Theorem 38]). Although these bounds are useful to assess the performance of practical codes, typically they are not conceptually illuminating. We shall adopt the asymptotic approach in this thesis.

[5]The maximum is well-defined since $\mathrm{I}(\cdot;W)$ is a concave function (e.g., [20, Lemma 1.3.5]).

[6]To be precise, Shannon has discovered the capacity formula in (1.3) and stated channel coding theorem, along with an outline of the proof for the direct part. The first published rigorous proof of the theorem is due to Feinstein [28] in which he attributes the proof of the converse part to Fano.

old for the maximum reliable rate.

Theorem (Channel coding theorem [61])**.** *Fix a DMC $W \in \mathcal{P}(\mathcal{Y}\,|\,\mathcal{X})$. For any $R < C$,* $\limsup_{N\to\infty} P_e(N,R) = 0$. *Conversely, for any $R > C$,* $\liminf_{N\to\infty} \bar{P}_e(N,R) > 0$. ♦

Although quite important, channel coding theorem provides a crude measure of the interplay between blocklength, rate and the error probability. For example, it does not address how fast error probability decays if rate is below the capacity or how fast rate can increase to the capacity as the blocklength increases for a given error probability. In order to address this type of refined questions, other asymptotical characterizations are devised, which we overview next.

1.1.1 Normal approximation

Given a DMC $W \in \mathcal{P}(\mathcal{Y}\,|\,\mathcal{X})$, for any $\epsilon \in (0,1)$ and $N \in \mathbb{Z}^+$, define the following[7]

$$R^*(N,\epsilon) := \max\{R \in \mathbb{R}_+ : \mathrm{P_e}(N,R) \le \epsilon\}. \tag{1.5}$$

In words, $R^*(N,\epsilon)$ characterizes the maximum rate possible given a blocklength and target error probability. Besides its mathematical importance, in the sense of being a refinement of the channel coding theorem, $R^*(N,\epsilon)$ has also practical significance, especially for modern applications that requires low latency, such as multimedia communications. For the practically interesting case $\epsilon \in (0, 1/2)$, Strassen's normal approximation result[8] gives an asymptotic characterization of $R^*(N,\epsilon)$.

[7] For the purposes of this section, it is immaterial whether we use average or maximal error probability.

[8] Recently, Polyanskiy *et al.* has discovered a small mistake in Strassen's arguments for a small class of channels when $\epsilon \in (1/2, 1)$ (cf., [52, Section IV.A]). Besides fixing this error, they also improve the third-order term and extend the result to different channel models, most notably additive white gaussian noise channel.

Theorem (Normal approximation [66]). *Fix a DMC $W \in \mathcal{P}(\mathcal{Y} \,|\, \mathcal{X})$ and $\epsilon \in (0, 1/2)$. Asymptotically,*

$$R^*(N, \epsilon) = C + \sqrt{\frac{V}{N}}\Phi^{-1}(\epsilon) + O\left(\frac{\ln n}{n}\right), \tag{1.6}$$

where

$$V := \min_{P \in \mathcal{P}(\mathcal{X}) \,:\, I(P;W)=C} \sum_{(x,y) \in \mathcal{X} \times \mathcal{Y}} P(x)W(y \,|\, x)\left[\ln \frac{W(y \,|\, x)}{\sum_{z \in \mathcal{X}} P(z)W(y \,|\, z)} - I(P; W)\right]^2, \tag{1.7}$$

is the dispersion *of the channel.* ♦

We shall refer to this asymptotic regime as the *large error probability regime* in the sequel.

1.1.2 Error Exponents

Given a DMC $W \in \mathcal{P}(\mathcal{Y} \,|\, \mathcal{X})$, for any $\epsilon \in (0, 1)$ and $N \in \mathbb{Z}^+$, define the following[9]

$$N^*(R, \epsilon) := \min\{N \in \mathbb{Z}^+ : \mathrm{P_e}(N, R) \leq \epsilon\}. \tag{1.8}$$

In words, $N^*(R, \epsilon)$ characterizes the minimum blocklength required to sustain a target error probability for a fixed rate. Intuitively, $N^*(R, \epsilon)$ can be thought as the "dual" of $R^*(N, \epsilon)$, defined in (1.6). Moreover, $N^*(R, \epsilon)$ is a fundamental performance metric of block codes.

A classical approach to approximate $N^*(R, \epsilon)$ is to fix a rate below the capacity and then to characterize $\mathrm{P_e}(N, R)$ asymptotically. From the early days of the field, it has been known that error probability decays exponentially fast in blocklength (e.g., [24], [27], [62]). Moreover, the best possible exponent, which is called *reliability function* of the

[9] One can either use average or maximal error probability in (1.8).

channel, has also been investigated thoroughly. The classical upper and lower bounds on the reliability function[10] by Gallager and Shannon *et al.* are the following:

Theorem (Random coding bound [34])**.** *Fix a DMC $W \in \mathcal{P}(\mathcal{Y} \mid \mathcal{X})$. For any $R \leq C$,*

$$P_e(N, R) \leq 4e^{-NE_r(R)}, \tag{1.9}$$

where the random coding exponent *of the channel is defined by*

$$E_r(R) := \max_{Q \in \mathcal{P}(\mathcal{X})} \max_{0 \leq \rho \leq 1} \{-\rho R + E_o(\rho, Q)\}, \tag{1.10}$$

with

$$E_o(\rho, Q) := -\ln \sum_{y \in \mathcal{Y}} \left(\sum_{x \in \mathcal{X}} Q(x) W(y \mid x)^{\frac{1}{1+\rho}} \right)^{1+\rho}. \tag{1.11}$$

♦

Theorem (Sphere–packing bound [63])**.** *Fix a DMC $W \in \mathcal{P}(\mathcal{Y} \mid \mathcal{X})$. For any $R \leq C$,*

$$P_e(N, R) \geq e^{-N[E_{SP}(R - o_1(N)) + o_2(N)]}, \tag{1.12}$$

where the sphere–packing exponent *of the channel is defined by*

$$E_{SP}(R) := \max_{Q \in \mathcal{P}(\mathcal{X})} \sup_{\rho \geq 0} \{-\rho R + E_o(\rho, Q)\}, \tag{1.13}$$

$$o_1(N) := \frac{\ln 8}{N} + \frac{|\mathcal{X}| \ln N}{N}, \tag{1.14}$$

$$o_2(N) := \frac{\ln 8}{N} + \sqrt{\frac{2}{N}} \ln \frac{e^2}{P_{\min}}, \tag{1.15}$$

and $P_{\min}$ is the minimum positive element of W. ♦

Remark 1. *Both $E_{SP}(\cdot)$ and $E_r(\cdot)$ are positive, non-increasing and convex functions on $(0, C)$ (e.g., [35, Theorem 5.6.4] and [35, pg. 158]). Moreover, sphere-packing and*

[10] There are low rate improvements of both the lower and upper bound (e.g., [35, Theorem 5.7.1] and [35, Theorem 5.8.2]). Unfortunately, none of these improvements give the reliability function for low rates, except $R = 0$, and it is a long-standing open problem to determine the reliability function for all rates. Since our focus in this thesis will be on high rates, for which random coding and sphere-packing exponents coincide to give the reliability function, we do not introduce the aforementioned low-rate improvements.

random coding exponents agree for high rates and hence giving the reliability function, denoted by $E(R)$. Specifically, the critical rate of the channel, denoted by R_{cr}, is defined as the minimum of such rates, i.e., $E_{SP}(R) = E_r(R)$ if and only if (iff) $R_{cr} \leq R$ (e.g., [35, pg. 160]). Further, $E_{SP}(R)$ can grow unboundedly below a certain rate. Specifically, R_∞ is defined as the minimum R such that for all $R > R_\infty$, $E_{SP}(R)$ is finite (e.g., [20, pg. 170]). See Figure 1.1 for a graphical representation of the aforementioned notions for a typical channel. $\diamond$

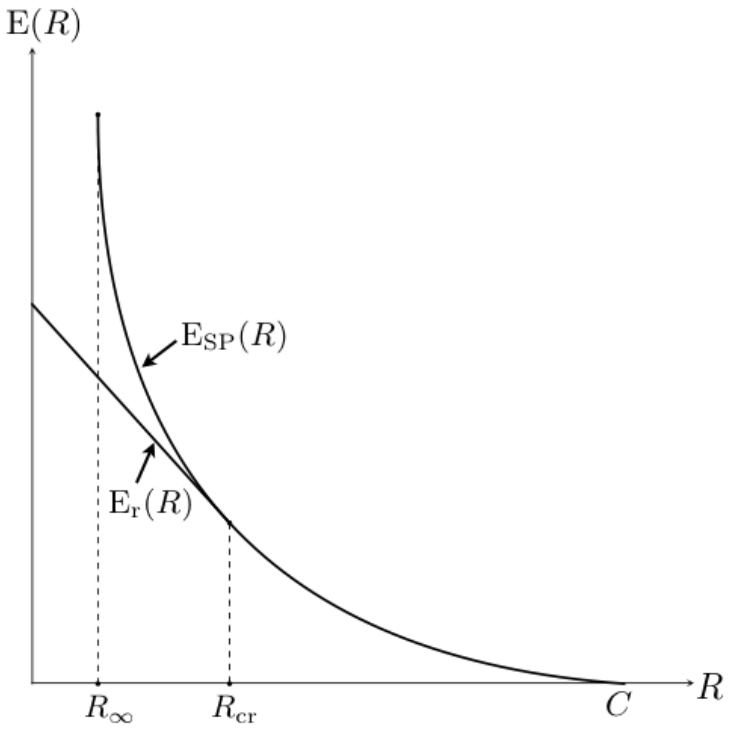

Figure 1.1: Random coding and sphere–packing exponents for a typical channel.

Remark 2. *Random coding bound was first discovered by Fano with a more involved proof (e.g., [27, pp. 324–331]). Also, Fano's exponent has a different algebraic form than the one given in* (1.10)*, which can be shown to be equal to Gallager's form. Fano's method of proving random coding bound is generally viewed as obsolete within information theory community, because of the simplicity of Gallager's proof.*

Sphere–packing bound was independently discovered by Haroutunian with a different proof [38]. Haroutunian's arguments give the following form of the sphere-packing exponent[11]

$$E_{SP}(R) := \max_{P\in\mathcal{P}(\mathcal{X})} \min_{V\in\mathcal{P}(\mathcal{Y}\,|\,\mathcal{X}):I(P;V)\leq R} D(V\|W|P), \tag{1.16}$$

where $D(V\|W|P) := \sum_{x\in\mathcal{X}} P(x)D(V(\cdot\,|\,x)\|W(\cdot\,|\,x))$ *and* $D(V(\cdot\,|\,x)\|W(\cdot\,|\,x))$ *is the* relative entropy *between probability distributions* $V(\cdot\,|\,x)$ *and* $W(\cdot\,|\,x)$ *(e.g., [18, pg. 19]). We call* (1.13) *(resp.* (1.16)*) Shannon-Gallager-Berlekamp (resp. Haroutunian) form of the sphere-packing exponent.* $\diamond$

We shall refer to this asymptotic regime as the *small error probability regime* in this thesis.

1.2 Motivation

Although small and large error probability regimes are deservedly celebrated, they have at least two limitations. The first limitation is about the nuisance factors in small error probability regime. Traditionally, these factors are ignored in the results that are considered to be conclusive for this regime, however they play a significant role in their practical usage. The second limitation is that neither small nor large error probability regime aims to explain the case where rate approaches the capacity and the error probability vanishes, *simultaneously*. However, this regime is arguably more relevant to practical code design than either small or large error probability regime, since the goal in channel coding is, after all, to attain a rate that is close to capacity *and* an error probability that is close to zero. Next, we discuss these two limitations and how to address them.

[11] It is well-known that the right sides of (1.13) and (1.16) are equal (e.g., [12]).

In order to demonstrate the first limitation, consider data storage, in which having an extremely small error probability, at the expense of working at rates strictly below the capacity, is crucial. However, the existing results only determine the exponent of error probability decay by washing out the sub-exponential factors. In particular, until recently, the tightest pre-factor for the upper bound on the error probability was $\Theta(1)$, due to Fano [27] and Gallager [34]. The best[12] pre-factor in the lower bound for constant composition codes[13] was $\Theta(N^{-|\mathcal{X}||\mathcal{Y}|})$, due to Haroutunian [38], where $|\mathcal{X}|$ and $|\mathcal{Y}|$ are the cardinalities of the input and output alphabets, respectively[14]. Clearly, there is a considerable gap between the orders of the pre-factors in the upper and lower bounds. This brings a sizable practical limitation, because the resulting bounds are not precise, especially for rates close to capacity, where the error exponent is close to zero, and hence sub-exponential term plays a significant role[15]. To address this limitation, one needs a more refined analysis to deduce a sharper characterization of the sub-exponential term associated with the small error probability results. We note that a by-product of this refined analysis is a more accurate characterization of the optimal error probability for small to moderate blocklength. As noted before, this regime of latency is becoming more important in contemporary applications, such as multimedia communications and control over imperfect channels, where having a small latency is vital.

[12]The version by Shannon *et al.*, which is mentioned in Section 1.1.2, has an $\Theta\left(e^{-\sqrt{N}}\right)$ pre-factor.

[13]A code is a constant composition code provided that all of the codewords has the same empirical distribution (e.g., [20, pg. 117]). It is well-known that (e.g., [63]) any (N, R) code includes a constant composition code with the same maximal error probability and rate not smaller than $R - \frac{|\mathcal{X}| \ln N}{N}$, where $|\mathcal{X}|$ is the cardinality of the input alphabet.

[14]There are recent attempts to improve the sphere-packing bound, most notably [70] and [71], for small to moderate blocklengths. In these works, the methodology is essentially the same with Shannon *et al.* [63], but the analysis is tightened at the expense of a more complicated bound. Further, it is computationally demonstrated that the derived bounds improve the sphere-packing bound of Shannon *et al.* for binary symmetric and binary erasure channels. However, neither of them give the order of the sub-exponential term explicitly and it appears that the order of the pre-factor for these improvements are the same as that of Shannon *et al.*

[15]For example, see [52, Section V] for a discussion on the inaccuracy of using the random coding bound to approximate $N^*(R, \epsilon)$ (cf., (1.8)) when R is close to C.

To demonstrate the second limitation, recall that although small error probability regime allows for vanishing error probabilities, rate is bounded away from the capacity. In large error probability regime, on the other hand, the rate approaches the capacity but error probability is bounded away from zero. Evidently, these two regimes correspond to two extreme ways of using available latency. Indeed, small (resp. large) error probability regime uses all the blocklength to minimize (resp. maximize) error probability (resp. rate) at the expense of fixing rate below the capacity (resp. having a non-vanishing error probability). However, none of the approaches is a balanced way of using the latency. To address this limitation, one needs to consider the asymptotic regime that lies between them, in which one requires the rate to approach the capacity and error probability to simultaneously tend to zero. Assessing the performance of codes in this regime, which we call *medium error probability regime* in the sequel, gives a more balanced (in terms of the latency usage) performance metric compared to the existing asymptotic regimes. Figure 1.2 provides a graphical representation of the small, medium and large error probability regimes.

The main goal of this study is to address the aforementioned two limitations of the existing asymptotic regimes. We give a summary of our main findings in Section 1.3. Before proceeding further, however, it is helpful to consider the more-elementary setup of the sum of independent and identically distributed (i.i.d.) random variables to place the aforementioned notions into context. If we scale the sum with $1/N$, it converges to the mean by the law of large numbers. Cramér's Theorem (e.g., [19], [21, Theorem 2.2.3]) characterizes the probability that the unnormalized sum makes an order-N deviation from its mean. This probability decays exponentially in N, and Cramér's characterization of the exponent is now termed a *large deviations* result. The central limit theorem, on the other hand, characterizes the probability that the unnormalized sum makes an order-$\sqrt{N}$ deviation. As N tends to infinity, this probability converges to a

positive constant that is governed by the Gaussian distribution. The small error probability regime in channel coding is analogous to large deviations for i.i.d. sums, in that they both characterize exponentially small probabilities using similar techniques. The large error probability regime is akin to the central limit theorem; as the term normal approximation already suggests.

Continuing the analogy with the i.i.d. sum of random variables, the medium error probability regime is analogous to the one in which the goal is to characterize the probability that the unnormalized sum makes a deviation whose size lies between two extremes of large deviations and the central limit theorem [21, Theorem 3.7.1], which is now called a *moderate deviations* result. Similarly, the refined analysis suggested to address the accuracy issue in small error probability regime resembles the *exact asymptotics* problem in large deviations (e.g., [7], [21, Theorem 3.7.4]). This problem aims to determine the pre-factor of the exponentially vanishing term in the large deviations theorem. Bahadur and Rao characterized this pre-factor, $\Theta(1/\sqrt{N})$, including the constant,

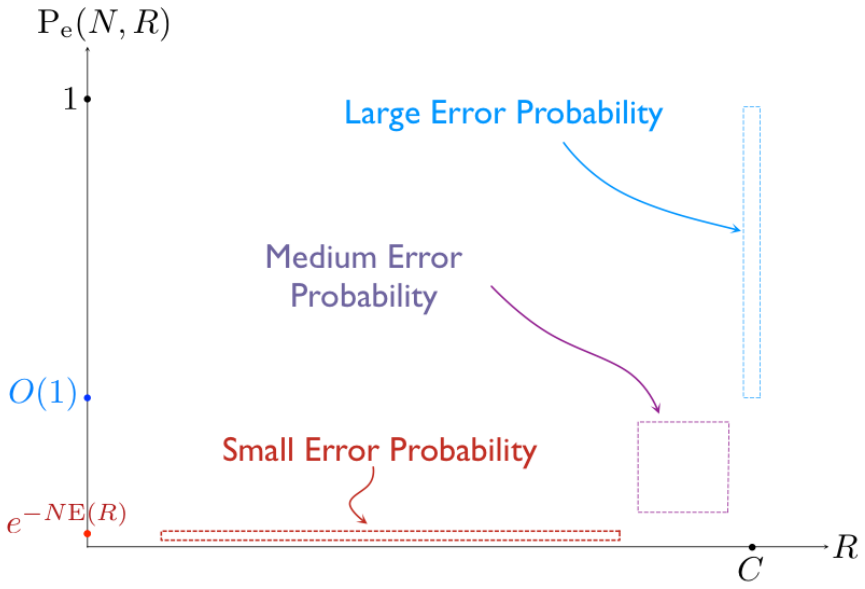

Figure 1.2: Graphical representation of small, medium and large probability regimes.

under some regularity conditions [7].

1.3 Summary of the results

In Chapter 2, we analyze the medium error probability regime. In particular, we characterize the optimal error probability when rate increases to the capacity, by proving that if this increase is slower than the one in large error probability regime, then the optimal error probability goes to zero sub-exponentially fast. Further, we show that the rate of this sub-exponential decay is inversely proportional to the dispersion of the channel, defined in (1.7), and hence giving another operational significance to this fundamental quantity.

The rest of the thesis is devoted to the more refined analysis in the small error probability regime, i.e., improvement of the sub-exponential term in the random coding and sphere-packing bounds.

In Chapter 3, we prove a lower bound for constant composition codes for rates between R_∞ and C with a pre-factor of $\Omega\left(N^{-\frac{1}{2}\left(1+\epsilon+\rho_R^*\right)}\right)$, for any $\epsilon > 0$, where ρ_R^* is the *maximum absolute-value subgradient* of $\mathrm{E_{SP}}(R)$.

Chapter 4 is devoted to prove the counterpart of the aforementioned result. Specifically, we prove the following:

1. If a positive dispersion DMC satisfies a certain regularity condition, then for rates between R_{cr} and C, there exists an (N, R) code with maximal error probability smaller than $\frac{K_1 e^{-N\mathrm{E_r}(R)}}{N^{\frac{1}{2}\left(1-\epsilon+\bar{\rho}_R^*\right)}}$, for any $\epsilon > 0$, where K_1 is a positive constant and $\bar{\rho}_R^*$ is related to the subdifferential of the random coding exponent $\mathrm{E_r}(R)$. Further, if the

channel is positive, then $\bar{\rho}_R^*$ is the *maximum absolute value subgradient* of $\mathrm{E_r}(R)$ and one can drop ϵ.

2. If a positive dispersion DMC does not satisfy the aforementioned regularity condition, then for rates between R_{cr} and C, there exists an (N, R) code with maximal error probability smaller than $\frac{K_2 e^{-N\mathrm{E_r}(R)}}{\sqrt{N}}$, where K_2 is a positive constant.

The order of the improved pre-factors are close to each other, but not exactly the same. However, when restricted to a specific class of channels, namely symmetric channels[16], we characterize the optimal order of the sub-exponential term, which constitutes Chapter 5. To be specific, for rates between R_{cr} and C, the optimal order of the pre-factor for the typical symmetric channels is $\Theta(N^{-0.5(1+|\mathrm{E}'(R)|)})$, where $\mathrm{E}'(R)$ is the slope of the reliability function at rate R, whereas for the remaining symmetric channels, $\Theta(N^{-0.5})$ is the optimal order of the pre-factor. This dichotomy of the sub-exponential term appears to be a noteworthy observation.

1.4 Notation

In the sequel, boldface letters denote vectors, letters with subscripts denote individual components of vectors. Capital letters represent random variables and lowercase letters denote individual realizations of the corresponding random variable. $\mathbb{Z}^+$, $\mathbb{R}$, $\mathbb{R}_+$ and $\mathbb{R}^+$ denotes the set of positive integers, the set of real, non-negative real and positive real numbers, respectively. Given two finite sets $\mathcal{X}$ and $\mathcal{Y}$, $\mathcal{P}(\mathcal{X})$ (resp. $\mathcal{P}(\mathcal{Y}|\mathcal{X})$) denotes the set of all probability measures on $\mathcal{X}$ (resp. the set of all stochastic matrices from $\mathcal{X}$ to $\mathcal{Y}$). Φ and ϕ denotes the distribution and density of the standard Gaussian random variable, respectively. Given a set $\mathcal{S}$, $\mathcal{S}^c$, $\mathrm{cl}(\mathcal{S})$, $\mathcal{S}^\circ$, $\mathrm{ri}(\mathcal{S})$ and $|\mathcal{S}|$ denotes the complementary set of

[16] See Definition 9 for the definition of symmetric channels.

$\mathcal{S}$, the closure of $\mathcal{S}$, the relative interior of $\mathcal{S}$ and the cardinality of $\mathcal{S}$, respectively. $\mathcal{S}(P)$ denotes the support of the probability distribution P. $\mathbb{1}\{\cdot\}$ denotes the standard indicator function. Given a matrix A, A^T (resp. $\det(A)$) denotes its transpose (resp. determinant).

CHAPTER 2

MODERATE DEVIATIONS IN CHANNEL CODING

Moderate deviations have been a fixture of probability theory for some time (e.g., [29], [30], [31, Sec. XVI.7], [45, Chapter 8], [49] and references therein). However, their appearance in information literature is recent. In particular, Slepian-Wolf problem, also known as *source coding with side information problem* (e.g., [65]), appears to be the first classical information theory setup investigated from moderate deviations perspective (cf., the work of He *et al.* [17], [39], [40], [41]). Altuğ and Wagner introduced moderate deviations in channel coding by proving the main result of this chapter for positive[1] discrete memoryless channels [1]. Polyanskiy and Verdú [53] extended the result in [1] by relaxing the positivity assumption for discrete memoryless channels and proving an analogous result for Gaussian channels. More recently, moderate deviations in lossy source coding and binary hypothesis testing problems have been investigated by Tan [67] and Sason [57], respectively.

The result provided here improves upon [1] by relaxing the positivity assumption and simplifying the argument. The proof is different from that of Polyanskiy and Verdú, who rely on methods from [52] and powerful results from probability theory. It is also different from that of He *et al.* and Tan, who use type theory. It is worth noting that standard finite block length bounds on the rate and error probability from small error probability regime are insufficient to obtain a conclusive moderate deviations result, so we develop new bounds that are tailored for the particular regime at hand.

[1] A discrete channel is positive if all of its transition probabilities are positive.

2.1 Statement of the results

Theorem 1. *For any DMC $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ with $V > 0$,*[2] *for any sequence of real numbers $\{\epsilon_N\}_{N\geq 1}$ satisfying*

$$\begin{aligned} &(i)\ \epsilon_N \to 0, \text{ as } N \to \infty, \\ &(ii)\ \epsilon_N \sqrt{N} \to \infty, \text{ as } N \to \infty, \end{aligned} \tag{2.1}$$

there exists a sequence of codes $\{(f_N, \varphi_N)\}_{N\geq 1}$ that satisfies $R_N := \frac{\ln|\varphi_N|}{N} \geq C - \epsilon_N$, for all $N \in \mathbb{Z}^+$ and

$$\limsup_{N\to\infty} \frac{1}{N\epsilon_N^2} \ln P_e(f_N, \varphi_N) \leq -\frac{1}{2V}, \tag{2.2}$$

where $P_e(f_N, \varphi_N)$ denotes the maximal error probability of (f_N, φ_N). ♦

Theorem 2. *For any DMC $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ with $V > 0$, for any sequence of real numbers $\{\epsilon_N\}_{N\geq 1}$ satisfying* (2.1) *and for any sequence of codes $\{(f_N, \varphi_N)\}_{N\geq 1}$ satisfying $R_N = \frac{\ln|\varphi_N|}{N} \geq C - \epsilon_N$, we have*

$$\liminf_{N\to\infty} \frac{1}{N\epsilon_N^2} \ln \bar{P}_e(f_N, \varphi_N) \geq -\frac{1}{2V}, \tag{2.3}$$

where $\bar{P}_e(f_N, \varphi_N)$ denotes the average error probability of (f_N, φ_N). ♦

Remark 3. *Polyanskiy and Verdú [52] show that the assumption $V > 0$ is necessary in order for $\frac{1}{N\epsilon_N^2} \ln P_e(f_N, \varphi_N)$ to have a finite limit. If $V = 0$, then it is tempting to conjecture that $\frac{1}{N\epsilon_N} \ln P_e(f_N, \varphi_N)$ has a finite limit (see [52, Theorem 4]).* ◇

Remark 4. *Our achievability proof follows from Gallager's random coding bound (e.g., [35, Corollary 2, pg. 140]), which states that for any rate R and block length N, there exists an (N, R) code (f_N, φ_N) such that*

$$P_e(f_N, \varphi_N) \leq 4e^{-NE_r(R)}. \tag{2.4}$$

[2] Since $V > 0$ implies that $C > R_\infty(W) \geq 0$ (e.g., [35, pg. 160]) we have $C > 0$.

Since N and R are arbitrary, we can let $R = C - \epsilon_N$ and approximate $E_r(\cdot)$ around C via a Taylor series to obtain Theorem 1. This line of reasoning is made rigorous in Section 2.2.1.

The achievability argument is deceptively simple in that it obscures issues that should be addressed to prove the converse. To prove the converse, we would like to show that for any ϵ_N satisfying the hypothesis of the theorem and any $\alpha > 1$, there exist sequences β_N and γ_N satisfying

$$\frac{\beta_N}{\epsilon_N} \to 0, \tag{2.5}$$

$$\frac{1}{N\epsilon_N^2} \ln \gamma_N \to 0, \tag{2.6}$$

such that for all sufficiently large N and all $(N, C - \epsilon_N)$ codes (f_N, φ_N), we have

$$P_e(f_N, \varphi_N) \geq \gamma_N e^{-N\alpha E_{SP}(C - \epsilon_N - \beta_N)}. \tag{2.7}$$

If one could prove such a bound, then she could obtain Theorem 2 by expanding $E_{SP}(\cdot)$ as a Taylor series around C and taking the appropriate limit.

But it is not clear whether a bound like (2.7) *holds. The refinement of the sphere–packing bound that is given in Chapter 3 (see also [5], [6]) states the following: for all $\epsilon > 0$, all fixed rates R below the capacity, and all sufficiently large N, any constant composition (N, R) code (f_N, φ_N) satisfies*[3]

$$P_e(f_N, \varphi_N) \geq \frac{K(R)}{\sqrt{N}} \exp\left\{-NE_{SP}\left(R - \frac{(1+\epsilon)\ln\sqrt{N}}{N}\right)\right\}. \tag{2.8}$$

Moreover, the N-dependence on the right side is essentially the best possible for a fixed R, owing to the refinement of the random coding bound given in Chapter 4 (see also [3]).

Although the rate backoff in this bound clearly satisfies (2.5), whether the pre-factor satisfies (2.6) hinges on R dependence of $K(R)$. This dependence is not currently known,

[3] Strictly speaking, (2.8) is not the same as the one given in Chapter 3. The latter is more involved than the former. The difference between them, however, is immaterial as far as the following discussion goes.

but it can be postulated via the following reasoning. In large error probability regime, in which the rate approaches the capacity at a speed of $1/\sqrt{N}$*, the error probability is asymptotically constant [66], and a Taylor series expansion of the sphere-packing exponent shows that the exponential factor in (2.8) is also asymptotically constant in this regime. If we assume that (2.8) holds in this regime, then it follows that the pre-factor must also be asymptotically constant, which suggests that* $K(R)$ *might behave as* $1/(C - R)$*. If this is true, then the pre-factor would satisfy (2.6), so (2.7) would hold.*

We show that (2.7) indeed holds, although our proof does not involve characterizing how $K(R)$ *varies with* R*.*[4] *Instead we prove (2.7) directly by using a particular set of classical information theory results, which do not appear to have been used in combination before, to prove a version of the sphere-packing exponent that is especially tight at finite block lengths and rates near capacity. The fact that our proof is similar to existing derivations of the sphere-packing exponent and uses well-known ingredients might give the impression that the result is routine. In fact, the required bounds are quite delicate, as the above discussion illustrates, and many conceptually-similar approaches to proving the sphere-packing exponent fail to give a conclusive moderate deviations result.* ◇

2.2 Proofs

Given any $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$, let

$$V(P) := \operatorname{Var}_{P\times W}\left[\ln \frac{W(Y|X)}{\sum_{z\in\mathcal{X}} P(z)W(Y|z)}\right], \tag{2.9}$$

where $(P \times W)(x, y) = P(x)W(y|x)$. Using (2.9), note that (1.7) can also be written as

$$V = \min_{P\in\mathcal{P}(\mathcal{X}):\, \mathrm{I}(P;W)=C} V(P), \tag{2.10}$$

[4] Determining how $K(R)$ varies with R is an interesting subject for future work.

and let $\tilde{P}$ denote some element of $\mathcal{P}(\mathcal{X})$ that achieves the minimum in (2.10).

We note a couple of auxiliary results[5] that will be used in the sequel.

Lemma 1. *Given any $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ with no all-zero column, $E_o(\rho, P)$ possesses the following properties:*

1) Given any $P \in \mathcal{P}(\mathcal{X})$, $E_o(\rho, P)$ is concave in $\rho \in \mathbb{R}_+$.

2) Given any $P \in \mathcal{P}(\mathcal{X})$,

$$\left.\frac{\partial E_o(\rho, P)}{\partial \rho}\right|_{\rho=0} = I(P; W). \tag{2.11}$$

3) Given any $P \in \mathcal{P}(\mathcal{X})$,

$$\left.\frac{\partial^2 E_o(\rho, P)}{\partial \rho^2}\right|_{\rho=0} = -V(P). \tag{2.12}$$

4) Given any $P \in \mathcal{P}(\mathcal{X})$,

$$\frac{\partial E_o(\rho, P)}{\partial \rho} \leq I(P; W), \ \forall\, \rho \in \mathbb{R}_+. \tag{2.13}$$

5) $\frac{\partial E_o(\rho,P)}{\partial \rho}$ is continuous over $(\rho, P) \in \mathbb{R}_+ \times \mathcal{P}(\mathcal{X})$.

6) $\frac{\partial^2 E_o(\rho,P)}{\partial \rho^2}$ is continuous over $(\rho, P) \in \mathbb{R}_+ \times \mathcal{P}(\mathcal{X})$.

7) $\frac{\partial^3 E_o(\rho,P)}{\partial \rho^3}$ is continuous over $(\rho, P) \in \mathbb{R}_+ \times \mathcal{P}(\mathcal{X})$. ♦

Proof. The proof is given in Appendix A.1. □

[5]The proof of the results are straightforward calculations. Further, items 1) through 4) have been noted before (e.g., [35, Theorem 5.6.3]). However, we have not encountered a proof for the remaining ones. Since the first four items directly follows from the calculations needed to deduce the last three, we opted to include them in Lemma 1 for the sake of reader's convenience.

2.2.1 Proof of Theorem 1

Let $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ be an arbitrary stochastic matrix satisfying the conditions stated in the theorem. Without loss of generality, suppose that W has no all-zero columns. Further, let $\{\epsilon_N\}_{N\geq 1}$ be an arbitrary sequence of real numbers, satisfying (2.1). By (2.1) and the fact that $C > 0$, we have

$$C - \epsilon_N > 0, \tag{2.14}$$

for all sufficiently large $N \in \mathbb{Z}^+$. Next, fix such an N. Gallager's random coding bound (e.g., [35, Corollary 2, pg. 140]) implies that there exists (f_N, φ_N), such that $\frac{\ln|\varphi_N|}{N} := R_N \geq C - \epsilon_N$ and

$$\mathrm{P_e}(f_N, \varphi_N) \leq 4\exp\left\{-N\left[\max_{0\leq\rho\leq 1}\{\mathrm{E_o}(\rho, P) - \rho R_N\}\right]\right\}, \tag{2.15}$$

for all $P \in \mathcal{P}(\mathcal{X})$. Therefore, (2.15) implies the existence of a sequence of codes $\{(f_N, \varphi_N)\}_{N\geq 1}$, s.t. for all $N \in \mathbb{Z}^+$, $R_N \geq C - \epsilon_N$ and

$$\frac{1}{N\epsilon_N^2}\ln \mathrm{P_e}(f_N, \varphi_N) \leq \frac{\ln 4}{N\epsilon_N^2} - \frac{1}{\epsilon_N^2}\max_{0\leq\rho\leq 1}\{\mathrm{E_o}(\rho, P) - \rho R_N\}, \tag{2.16}$$

for all sufficiently large N and any $P \in \mathcal{P}(\mathcal{X})$. Hence, it suffices to prove that (2.2) holds for this particular sequence of codes in order to conclude the result.

Using Taylor's Theorem, along with (2.11) and (2.12) (cf., items 2) and 3) of Lemma 1), for any $\rho \in \mathbb{R}_+$, we have

$$\mathrm{E_o}(\rho, \tilde{P}) = \rho C - \frac{\rho^2}{2}V + \frac{\rho^3}{6}\left.\frac{\partial^3 \mathrm{E_o}(\rho, \tilde{P})}{\partial\rho^3}\right|_{\rho=\bar{\rho}}, \tag{2.17}$$

for some $\bar{\rho} \in [0, \rho]$, where as noted before $\tilde{P}$ is some dispersion attaining input distribution. Next, let $\rho_N = \frac{\epsilon_N}{V}$, for all $N \in \mathbb{Z}^+$. Then, (2.17) yields,

$$\max_{0\leq\rho\leq 1}\left\{\mathrm{E_o}(\rho, \tilde{P}) - \rho R_N\right\} \geq \frac{\epsilon_N^2}{2V} - \frac{\epsilon_N^3}{6V^3}\left|\left.\frac{\partial^3 \mathrm{E_o}(\rho, \tilde{P})}{\partial\rho^3}\right|_{\rho=\bar{\rho}_N}\right|, \tag{2.18}$$

for all sufficiently large N and for some $\bar{\rho}_N \in [0, \rho_N]$.

Next, note that $\rho_N \leq 1$, for all sufficiently large N, since $\lim_{N\to\infty} \epsilon_N = 0$ (cf., (i) of (2.1)) and $V > 0$. We define

$$M := \max_{(\rho,P)\in[0,1]\times\mathcal{P}(\mathcal{X})} \left| \frac{\partial^3 \mathrm{E_o}(\rho, P)}{\partial \rho^3} \right|. \tag{2.19}$$

Owing to item 7) of Lemma 1, the maximum in (2.19) is well-defined and finite. Therefore, (2.18) and (2.19) imply that

$$\max_{0\leq\rho\leq 1} \left\{ \mathrm{E_o}(\rho, \tilde{P}) - \rho R_N \right\} \geq \frac{\epsilon_N^2}{2V} - \frac{\epsilon_N^3}{6V^3} M, \tag{2.20}$$

for all sufficiently large N.

Substituting (2.20) into (2.16) yields

$$\frac{1}{N\epsilon_N^2} \ln \mathrm{P_e}(f_N, \varphi_N) \leq \frac{\ln 4}{N\epsilon_N^2} - \frac{1}{2V}\left(1 - M\frac{\epsilon_N}{3V^2}\right), \tag{2.21}$$

which, in turn, implies (recall (2.1) and (2.19))

$$\limsup_{N\to\infty} \frac{1}{N\epsilon_N^2} \ln \mathrm{P_e}(f_N, \varphi_N) \leq -\frac{1}{2V}, \tag{2.22}$$

which is (2.2). □

2.2.2 Proof of Theorem 2

Let W and $\{\epsilon_N\}_{N\geq 1}$ be as in Section 2.2.1. Further, let $\{(f_N, \varphi_N)\}_{N\geq 1}$ be an arbitrary sequence of codes with $\frac{\ln|\varphi_N|}{N} := R_N \geq C - \epsilon_N$, for all $N \in \mathbb{Z}^+$. Observe that owing to standard arguments used to switch from the maximum to average error probability (e.g., [63, eq. (4.41)]), it is sufficient to show the conclusion for the maximum error probability, i.e.,

$$\liminf_{N\to\infty} \frac{1}{N\epsilon_N^2} \ln \mathrm{P_e}(f_N, \varphi_N) \geq -\frac{1}{2V}, \tag{2.23}$$

in order to prove (2.3). By similar reasoning [20, pg. 171], we can assume that the code is constant composition.

Next, we briefly outline the rest of the proof, which consists of three steps. The first step is to prove a strong converse theorem, Lemma 2, tailored to the particular situation at hand. The second step is to use Lemma 2 and "change of measure" to prove (2.7) (cf., Remark 4). The final step is to approximate the exponent in (2.7) via a Taylor series to conclude the result.

Remark 5. *Lemma 2, which could be of independent interest, is derived from Wolfowitz's converse to the channel coding theorem [72]. Although our version requires that the code be constant composition, an assumption not required by Wolfowitz, it shows that the error probability must be near unity if the rate exceeds the mutual information induced by the code. Wolfowitz requires the rate to exceed capacity.* $\diamond$

Remark 6. *One of the well-known change of measure arguments is Marton's [48, eq. (12)]. Although Marton originally applied it to rate distortion, the application to channel coding is obvious. It does not seem sufficient to prove* (2.7)*, however. Instead, we use a change of measure argument based on the log-sum inequality, given by Csiszár and Körner [20, pg. 167].* $\diamond$

Define the constant A as follows:

$$A := \max_{(P\times V)\,\in\,\mathcal{P}(\mathcal{X})\times\mathcal{P}(\mathcal{Y}|\mathcal{X})} \operatorname{Var}\left[\ln \frac{V(Y|X)}{Q(Y)}\right] + 1, \tag{2.24}$$

where $Q(y) := \sum_{x\in\mathcal{X}} P(x)V(y|x)$, $\forall y \in \mathcal{Y}$. Note that, since the cost function is continuous in the optimization variable and we work with finite alphabets, the maximum in (2.24) is well-defined and finite.

Lemma 2 (Strong Converse)**.** *Let (f, φ) be an arbitrary constant composition code with block length N, common type P, and rate $R > 0$. Let $V \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ be an arbitrary*

stochastic matrix satisfying $I(P;V) \leq R - 2\delta$, for some $\delta > 0$. Then, we have

$$\bar{P}_e(f,\varphi) \geq 1 - \frac{A}{N\delta^2} - e^{-N\delta}, \tag{2.25}$$

where A is defined in (2.24) *and the error probability is due to DMC V.* ♦

Proof. The proof follows similar steps to that of [35, Theorem 5.8.5]. Let (f,φ), $V \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ and $\delta > 0$ be as in the statement of the lemma. Define

$$G(m) := \left\{ \ln \frac{V(\mathbf{Y}^N|\mathbf{x}^N)}{Q(\mathbf{Y}^N)} > N\left[\mathrm{I}(P;V) + \delta\right] \right\}, \tag{2.26}$$

for any $m \in \mathcal{M} := \left\{1, \ldots, \lceil e^{NR} \rceil\right\}$, where $Q(\mathbf{y}^N) := \prod_{n=1}^{N} Q(y_n)$, $\forall \mathbf{y}^N \in \mathcal{Y}^N$ along with $Q(y) := \sum_{x\in\mathcal{X}} P(x)V(y|x)$. Also, for the sake of notational convenience, define $i(x,y) := \ln \frac{V(y|x)}{Q(y)}$, for any $(x,y) \in \mathcal{X} \times \mathcal{Y}$. Note that we have

$$\ln \frac{V(\mathbf{y}^N|\mathbf{x}^N(m))}{Q(\mathbf{y}^N)} = \sum_{n=1}^{N} \ln \frac{V(y_n|x_n(m))}{Q(y_n)} = \sum_{n=1}^{N} i(x_n(m); y_N), \tag{2.27}$$

for all $m \in \mathcal{M}$, where $\mathbf{x}^N(m)$ denotes the codeword of the code corresponding to the message m. Hence, for any $m \in \mathcal{M}$, we have

$$\begin{aligned}
\mathrm{E}_{V(\cdot|\mathbf{x}^N(m))}\left[i(\mathbf{x}^N(m), \mathbf{Y}^N) | \mathbf{x}^N(m) \right] &= \sum_{n=1}^{N} \mathrm{E}_{V(\cdot|x_n(m))}\left[i(x_n(m), Y_n) | x_n(m) \right] && (2.28)\\
&= \sum_{x\in\mathcal{X}} N(x|\mathbf{x}^N(m)) \sum_{y\in\mathcal{Y}} V(y|x) \ln \frac{V(y|x)}{Q(y)} && (2.29)\\
&= N \sum_{x\in\mathcal{X}} P(x) \sum_{y\in\mathcal{Y}} V(y|x) \ln \frac{V(y|x)}{Q(y)} && (2.30)\\
&= N\mathrm{I}(P;V), && (2.31)
\end{aligned}$$

where (2.28) follows from (2.27), (2.29) follows from the definition of $N(x|\mathbf{x}^N)$, which denotes the number of occurrences of the symbol $x \in \mathcal{X}$ in the string $\mathbf{x}^N$, and (2.30) follows from the definition of the type P.

Next, let $\varphi^{-1}(m) \subset \mathcal{Y}^N$ denote the decoding regions of (f, φ), $\forall m \in \mathcal{M}$. We have

$$1 - \bar{\mathrm{P}}_{\mathrm{e}}(f, \varphi) = \sum_{m \in \mathcal{M}} \frac{1}{|\mathcal{M}|} \sum_{\mathbf{y}^N \in \varphi^{-1}(m)} V(\mathbf{y}^N | \mathbf{x}^N(m)) \tag{2.32}$$

$$= \sum_{m \in \mathcal{M}} \frac{1}{|\mathcal{M}|} \sum_{\mathbf{y}^N \in \varphi^{-1}(m) \cap G(m)} V(\mathbf{y}^N | \mathbf{x}^N(m)) + \sum_{m \in \mathcal{M}} \frac{1}{|\mathcal{M}|} \sum_{\mathbf{y}^N \in \varphi^{-1}(m) \cap G(m)^c} V(\mathbf{y}^N | \mathbf{x}^N(m)), \tag{2.33}$$

Recalling (2.26), for any $\mathbf{y}^N \in G(m)^c$, we have

$$V(\mathbf{y}^N | \mathbf{x}^N(m)) \leq Q(\mathbf{y}^N) \exp\left\{N \left[\mathrm{I}(P; V) + \delta\right]\right\}, \tag{2.34}$$

which, in turn, implies that

$$\sum_{m \in \mathcal{M}} \frac{1}{|\mathcal{M}|} \sum_{\mathbf{y}^N \in \varphi^{-1}(m) \cap G(m)^c} V(\mathbf{y}^N | \mathbf{x}^N(m)) \leq \sum_{m \in \mathcal{M}} \frac{1}{|\mathcal{M}|} \sum_{\mathbf{y}^N \in \varphi^{-1}(m) \cap G(m)^c} Q(\mathbf{y}^N) e^{N[\mathrm{I}(P;V)+\delta]} \tag{2.35}$$

$$\leq \sum_{m \in \mathcal{M}} \frac{1}{|\mathcal{M}|} \sum_{\mathbf{y}^N \in \varphi^{-1}(m)} Q(\mathbf{y}^N) e^{N[\mathrm{I}(P;V)+\delta]} \tag{2.36}$$

$$= \frac{\exp\left\{N \left[\mathrm{I}(P; V) + \delta\right]\right\}}{\lceil e^{NR} \rceil} \sum_{m \in \mathcal{M}} \sum_{\mathbf{y}^N \in \varphi^{-1}(m)} Q(\mathbf{y}^N) \tag{2.37}$$

$$\leq \exp\left\{-N \left[R - \mathrm{I}(P; V) - \delta\right]\right\} \tag{2.38}$$

$$\leq e^{-N\delta}, \tag{2.39}$$

where (2.38) follows from the fact that the decoding regions are disjoint and Q is a probability measure on $\mathcal{Y}^N$ and (2.39) follows from $\mathrm{I}(P; V) \leq R - 2\delta$ assumption.

Next, note that for any $m \in \mathcal{M}$

$$\sum_{\mathbf{y}^N \in \varphi^{-1}(m) \cap G(m)} V(\mathbf{y}^N | \mathbf{x}^N(m)) \leq \sum_{\mathbf{y}^N \in G(m)} V(\mathbf{y}^N | \mathbf{x}^N(m)) \tag{2.40}$$

$$= V\left\{G(m) | \mathbf{x}^N(m)\right\}. \tag{2.41}$$

Further, using Chebyshev's inequality (recall (2.26), (2.27) and (2.31)), for any $m \in \mathcal{M}$

we have

$$V\left\{G(m)|\mathbf{x}^N(m)\right\} \leq \frac{\sum_{n=1}^N \mathrm{Var}\left[i(x_n(m);Y_n)|x_n(m)\right]}{N^2\delta^2} \tag{2.42}$$

$$= \frac{1}{N\delta^2}\left\{\frac{1}{N}\sum_{n=1}^N\sum_{y\in\mathcal{Y}} V(y|x_n(m))\ln^2\frac{V(y|x_n(m))}{Q(y)}\right.$$
$$\left.-\frac{1}{N}\sum_{n=1}^N\left(\sum_{y\in\mathcal{Y}} V(y|x_n(m))\ln\frac{V(y|x_n(m))}{Q(y)}\right)^2\right\} \tag{2.43}$$

$$\leq \frac{1}{N\delta^2}\left\{\frac{1}{N}\sum_{n=1}^N\sum_{y\in\mathcal{Y}} V(y|x_n(m))\ln^2\frac{V(y|x_n(m))}{Q(y)}\right.$$
$$\left.-\left(\frac{1}{N}\sum_{n=1}^N\sum_{y\in\mathcal{Y}} V(y|x_n(m))\ln\frac{V(y|x_n(m))}{Q(y)}\right)^2\right\} \tag{2.44}$$

$$= \frac{1}{N\delta^2}\left\{\sum_{x\in\mathcal{X}}P(x)\sum_{y\in\mathcal{Y}} V(y|x)\ln^2\frac{V(y|x)}{Q(y)}\right.$$
$$\left.-\left(\sum_{x\in\mathcal{X}}P(x)\sum_{y\in\mathcal{Y}} V(y|x)\ln\frac{V(y|x)}{Q(y)}\right)^2\right\} \tag{2.45}$$

$$= \frac{\mathrm{Var}\left[\ln\frac{V(Y|X)}{Q(Y)}\right]}{N\delta^2}, \tag{2.46}$$

where (2.44) follows from Jensen's inequality and (2.45) follows from the definition of P. Plugging (2.46) into (2.41) and recalling (2.24) yields

$$\forall m\in\mathcal{M}, \sum_{\mathbf{y}^N\in\varphi^{-1}(m)\cap G(m)} V(\mathbf{y}^N|\mathbf{x}^N(m)) \leq \frac{A}{N\delta^2}. \tag{2.47}$$

Plugging (2.39) and (2.47) into (2.33), we deduce that

$$\bar{\mathrm{P}}_{\mathrm{e}}(f,\varphi) \geq 1 - \frac{A}{N\delta^2} - e^{-N\delta}, \tag{2.48}$$

which is (2.25). □

Next, fix some $0<\gamma<1/2$. Let $\psi\in\mathbb{R}^+$ be defined as

$$\psi^2 := \frac{2A}{\gamma}. \tag{2.49}$$

Note that for all sufficiently large N,

$$0 < C - \left(\epsilon_N + \frac{2\psi}{\sqrt{N}}\right), \tag{2.50}$$

$$e^{-\psi\sqrt{N}} \leq \gamma/2. \tag{2.51}$$

As a direct consequence of the Strong Converse lemma (with the choice of $\delta = \psi/\sqrt{N}$), for any $V \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ satisfying $I(P_N; V) \leq R_N - \frac{2\psi}{\sqrt{N}}$, we have

$$\exists\, m \in \mathcal{M} = \left\{1, \ldots, \lceil e^{NR_N} \rceil\right\}, \text{ s.t. } 1 - V\left\{\varphi_N^{-1}(m)|\mathbf{x}^N(m)\right\} \geq 1 - \gamma, \tag{2.52}$$

for all sufficiently large $N \in \mathbb{Z}^+$, such that (2.50) and (2.51) hold. Here, P_N denotes the composition of the code. Note that N does not depend on the specific choice of V. Fix a sufficiently large N such that (2.50) and (2.51) hold.

Lemma 3 (Change of Measure)**.** *Let (f, φ) be an arbitrary constant composition code with block length N and composition P_N. Then*

$$P_e(f, \varphi) \geq \exp\left\{-N\left(\min_{V \in \mathcal{P}(\mathcal{Y}|\mathcal{X}):\, I(P_N;V) \leq R_N - \frac{2\psi}{\sqrt{N}}} \left\{\frac{D(V||W|P_N)}{1-\gamma} + \frac{h(1-\gamma)}{N(1-\gamma)}\right\}\right)\right\}, \tag{2.53}$$

for all sufficiently large $N \in \mathbb{Z}^+$ such that (2.50) *and* (2.51) *hold, where $h(\cdot)$ is the binary entropy function, i.e., $h(p) := p\ln(1/p) + (1-p)\ln(1/(1-p))$, $\forall\, p \in [0, 1]$, and the error probability is due to DMC W.* ♦

Proof. The argument is due to Csiszár and Körner (e.g., [20, pg. 167]), and we state it for the sake of completeness. Fix N and let V be any channel such that

$$\mathrm{I}(P_n; V) \leq R_n - \frac{2\psi}{\sqrt{n}}. \tag{2.54}$$

By the log-sum inequality (e.g., [20, pg. 48]), for any message m, we have

$$V(\varphi^{-1}(m)|\mathbf{x}^N(m)) \ln \frac{V(\varphi^{-1}(m)|\mathbf{x}^N(m))}{W(\varphi^{-1}(m)|\mathbf{x}^N(m))} + V((\varphi^{-1}(m))^c|\mathbf{x}^N(m)) \ln \frac{V((\varphi^{-1}(m))^c|\mathbf{x}^N(m))}{W((\varphi^{-1}(m))^c|\mathbf{x}^N(m))}$$
$$\leq \mathrm{D}(V||W|\mathbf{x}^N(m)), \tag{2.55}$$

where $\varphi^{-1}(m)$ denotes the decoding region for the m-th message and $(\varphi^{-1}(m))^c$ denotes its complement. This, in turn, implies that

$$V((\varphi^{-1}(m))^c|\mathbf{x}^N(m)) \ln \frac{1}{W(\varphi^{-1}(m)|\mathbf{x}^N(m))} \leq \mathrm{D}(V||W|\mathbf{x}^N(m)) + \mathrm{h}(V(\varphi^{-1}(m)|\mathbf{x}^N(m))). \tag{2.56}$$

Applying this inequality to a message satisfying (2.52) gives (2.53). □

By recalling the definition of Haroutunian form of the sphere-packing exponent (cf., (1.16)), (2.53) implies that

$$\mathrm{P_e}(f_N, \varphi_N) \geq e^{-\frac{\mathrm{h}(1-\gamma)}{(1-\gamma)}} \exp\left\{-N\left(\frac{\mathrm{E_{SP}}\left(C-\delta_N, W\right)}{1-\gamma}\right)\right\}, \tag{2.57}$$

where

$$\delta_N := \epsilon_N\left(1 + \frac{2\psi}{\sqrt{N\epsilon_N^2}}\right), \tag{2.58}$$

for all $N \in \mathbb{Z}^+$. Note that this establishes (2.7). We define

$$\alpha_N := 1 + \frac{2\psi}{\sqrt{N\epsilon_N^2}}, \ \forall\, N \in \mathbb{Z}^+, \tag{2.59}$$

and note that since $\epsilon_N \sqrt{N} \to \infty$ as $N \to \infty$ (cf., item (ii) of (2.1)), $\alpha_N \to 1$ as $N \to \infty$. Therefore, $\delta_N \to 0$ as $N \to \infty$ (cf., item (i) of (2.1)).

The third and final step of the proof is to approximate the exponent on the right side of (2.57). To this end, first note that if the rate is above the critical rate[6], i.e., $R \geq R_{\mathrm{cr}}$, then $\mathrm{E_{SP}}(R) = \mathrm{E_r}(R)$ (e.g., Remark 1), which, in turn, implies that

$$\mathrm{E_{SP}}\left(R\right) = \mathrm{E_r}(R) = \max_{P \in \mathcal{P}(\mathcal{X})} \max_{0 \leq \rho \leq 1} \left\{-\rho R + \mathrm{E_o}(\rho, P)\right\}, \tag{2.60}$$

by recalling the definition of the random coding exponent (e.g., (1.10)).

[6]See Remark 1 for the definition of R_{cr}.

Further, since $V > 0$, one can infer that (e.g., [35, pg. 160]) $R_{\rm cr} < \mathrm{C}$ and hence for all sufficiently large N, $C - \delta_N > R_{\rm cr}$. This observation, coupled with (2.60), ensures that for all sufficiently large N, we have

$$\mathrm{E_{SP}}\left(C - \delta_N\right) = \mathrm{E_r}\left(C - \delta_N\right) = \max_{P \in \mathcal{P}(\mathcal{X})} \max_{0 \le \rho \le 1} \left\{-\rho[C - \delta_N] + \mathrm{E_o}(\rho, P)\right\}. \tag{2.61}$$

Proposition 1. *(Sphere–packing exponent around C)*

$$\limsup_{n \to \infty} \frac{E_{SP}\left(C - \delta_N, W\right)}{\delta_N^2} \le \frac{1}{2\sigma^2(W)}. \tag{2.62}$$

♦

Proof. Let Q_N and ρ_N achieve the maxima in (2.60) at rate $C - \delta_N$, i.e.,

$$\mathrm{E_{SP}}(C - \delta_N) = -\rho_N(C - \delta_N) + \mathrm{E}_o(\rho_N, Q_N). \tag{2.63}$$

Now $\mathrm{E_{SP}}(C - \delta_N) > 0$ for all N, since the sphere-packing exponent is positive for all rates below the capacity (e.g., Remark 2). This implies that $\rho_N > 0$ for all N. Since $\mathrm{E_o}(\rho, P)$ is concave in ρ, it follows that

$$\mathrm{C} - \delta_N = \left.\frac{\partial \mathrm{E_o}(\rho, Q_N)}{\partial \rho}\right|_{\rho = \rho_N}, \tag{2.64}$$

for all N.

Our proof of Proposition 1 will use the following lemma.

Lemma 4.

(a) Any limit point of $\{Q_N\}$ *is capacity achieving.*

(b) $\lim_{N \to \infty} \rho_N = 0$.

(c) $\limsup_{N \to \infty} \frac{\rho_N}{\delta_N} \le \frac{1}{V}$. ♦

Proof. Consider arbitrary subsequences $\{Q_{N_n}\}_{n\geq 1}$ and $\{\rho_{N_n}\}_{n\geq 1}$ and note that, owing to the compactness of $\mathcal{P}(\mathcal{X})$ and $[0,1]$ (switching to a further subsequence, if necessary), we may assume that

$$\lim_{n\to\infty} Q_{N_n} = P_0, \quad \lim_{n\to\infty} \rho_{N_n} = \rho_0, \tag{2.65}$$

for some $P_0 \in \mathcal{P}(\mathcal{X})$ and $\rho_0 \in [0,1]$.

Now (2.64) and item 5) of Lemma 1 together imply that

$$C = \left.\frac{\partial \mathrm{E_o}(\rho, P_0)}{\partial \rho}\right|_{\rho=\rho_0}. \tag{2.66}$$

On the other hand, item 4) of Lemma 1 implies that

$$\left.\frac{\partial \mathrm{E_o}(\rho, P_0)}{\partial \rho}\right|_{\rho=\rho_0} \leq \mathrm{I}(P_0; W) \leq C. \tag{2.67}$$

It follows that P_0 is capacity achieving. Since the subsequence was arbitrary, this establishes (a).

Since P_0 is capacity achieving, the assumption that $V > 0$ implies that $\left.\frac{\partial^2 \mathrm{E_o}(\rho,P_0)}{\partial \rho^2}\right|_{\rho=0} < 0$ by part 3) of Lemma 1. Then, items 1) and 2) of Lemma 1 imply that the first inequality in (2.67) holds with equality if and only if $\rho_0 = 0$. Since the subsequence was arbitrary, this establishes (b).

Next consider $\frac{\partial \mathrm{E_o}(\rho,Q_{N_n})}{\partial \rho}$, viewed as a function of ρ. This function equals $\mathrm{I}(Q_{N_n}; W)$ at $\rho = 0$ by part 2) of Lemma 1, and it equals $C - \delta_{N_n}$ at ρ_{N_n} by (2.64). It is differentiable in ρ by item 6) of Lemma 1. Thus, by the mean value theorem, there must exist a $\hat{\rho}_{N_n}$ in $[0, \rho_{N_n}]$ such that

$$-\left.\frac{\partial^2 \mathrm{E_o}(\rho, Q_{N_n})}{\partial \rho^2}\right|_{\rho=\hat{\rho}_{N_n}} = \frac{\mathrm{I}(Q_{N_n}; W) - C + \delta_{N_n}}{\rho_{N_n}} \tag{2.68}$$

$$\leq \frac{\delta_{N_n}}{\rho_{N_n}}. \tag{2.69}$$

Now by items 3) and 6) of Lemma 1,

$$\lim_{n\to\infty} \left.\frac{\partial^2 \mathrm{E_o}(\rho, Q_{N_n})}{\partial \rho^2}\right|_{\rho=\hat{\rho}_{N_n}} = \left.\frac{\partial^2 \mathrm{E_o}(\rho, P_0)}{\partial \rho^2}\right|_{\rho=0} = -V(P_0) \leq -V. \tag{2.70}$$

Combining the last two inequalities gives

$$\limsup_{n\to\infty} \frac{\rho_{N_n}}{\delta_{N_n}} \leq \frac{1}{V}. \tag{2.71}$$

Since the subsequence was arbitrary, this establishes (c). □

We are now in a position to prove Proposition 1. For any sufficiently large N, Taylor's Theorem gives (recalling items 2) and 3) of Lemma 1)

$$\mathrm{E_{SP}}(C-\delta_N) = -\rho_N[C-\delta_N] + \mathrm{E_o}(\rho_N, Q_N) \tag{2.72}$$

$$= \rho_N\left[\mathrm{I}(Q_N;W) - C + \delta_N\right] - \frac{(\rho_N)^2}{2}V(Q_N) + \frac{(\rho_N)^3}{6}\left.\frac{\partial^3 \mathrm{E_o}(\rho, Q_N)}{\partial \rho^3}\right|_{\rho=\bar{\rho}_N}, \tag{2.73}$$

for some $\bar{\rho}_N \in [0, \rho_N]$. If we use the constant M defined in (2.19), then we eventually have

$$\mathrm{E_{SP}}(C-\delta_N) \leq \rho_N\left[\mathrm{I}(Q_N;W) - C + \delta_N\right] - \frac{(\rho_N)^2}{2}V(Q_N) + \frac{(\rho_N)^3 M}{6}. \tag{2.74}$$

Since we must have $\mathrm{I}(Q_N;W) \leq C$, this yields

$$\mathrm{E_{SP}}(C-\delta_N) \leq \rho_N\delta_N - \frac{(\rho_N)^2}{2}V(Q_N) + \frac{(\rho_N)^3 M}{6} \tag{2.75}$$

$$\leq \sup_{\rho\in\mathbb{R}_+}\left\{\rho\delta_N - \frac{\rho^2}{2}V(Q_N)\right\} + \frac{(\rho_N)^3 M}{6} \tag{2.76}$$

$$= \frac{\delta_N^2}{2V(P_N)} + \frac{(\rho_N)^3 M}{6}. \tag{2.77}$$

Using (2.77) and items (b) and (c) of Lemma 4, we deduce that

$$\limsup_{N\to\infty} \frac{\mathrm{E_{SP}}(\mathrm{C}-\delta_N)}{\delta_N^2} \leq \limsup_{N\to\infty} \frac{1}{2V(Q_N)} \tag{2.78}$$

$$\leq \frac{1}{2V}, \tag{2.79}$$

where (2.79) follows from the continuity of $V(\cdot)$ on $\mathcal{P}(\mathcal{X})$ (item 3) and 6) of Lemma 1), item (a) of Lemma 4 and the definition of V (cf., (2.9)). □

Equipped with Proposition 1, we conclude the proof as follows. Recall that $\delta_N = \epsilon_N \alpha_N$, where $\alpha_N > 0$, for all $N \in \mathbb{Z}^+$ and $\alpha_N \to 1$ as $N \to \infty$. Hence,

$$\limsup_{N\to\infty} \frac{\mathrm{E}_{\mathrm{SP}}\left(C - \delta_N\right)}{\delta_N^2} = \limsup_{N\to\infty} \frac{\mathrm{E}_{\mathrm{SP}}\left(C - \delta_N\right)}{\epsilon_N^2}. \tag{2.80}$$

Since $\lim_{N\to\infty} N\epsilon_N^2 = \infty$ (cf., item (ii) of (2.1)), (2.57), (2.61) and (2.80) imply that

$$\liminf_{N\to\infty} \frac{1}{N\epsilon_N^2} \ln \mathrm{P_e}(f_N, \varphi_N) \geq -\frac{1}{2V} \frac{1}{1-\gamma}. \tag{2.81}$$

Since $0 < \gamma < 1/2$ is arbitrary, letting $\gamma \to 0$ in the right side of (2.81) yields (2.23). □

CHAPTER 3

REFINEMENT OF THE SPHERE-PACKING BOUND

In this chapter, we improve the sub-exponential term in the sphere-packing lower bound. As noted before, this can be thought as the analogous of the *exact asymptotics* problem in large deviations (e.g., [7], [21, Theorem 3.7.4]) for channel coding. Exact asymptotics problem in large deviations aims to determine the pre-factor of the exponentially vanishing term in the large deviations theorem. Bahadur and Rao [7] characterized this pre-factor, $\Theta(1/\sqrt{N})$, including the constant, under some regularity conditions. Their result, in the form stated by Dembo and Zeitouni [21, Theorem 3.7.4], is the following:

Theorem (Bahadur-Rao)**.** *Let λ_N denote the law of $\hat{S}_N = \frac{1}{N}\sum_{i=1}^{N} Z_i$, where Z_i are i.i.d. real valued random variables with logarithmic moment generating function $\Lambda(\delta) := \ln E[e^{\delta Z_1}]$. Consider the set $A = [a, \infty)$, where $a = \Lambda'(\eta)$ for some positive $\eta \in \{\delta : \Lambda(\delta) < \infty\}^\circ$. If the law of X_1 is non-lattice*[1]*, then $\lim_{N\to\infty} J_N \lambda_N(A) = 1$, where*

$$J_N := e^{N\Lambda^*(a)}\eta\sqrt{\Lambda''(\eta)2\pi N}$$

and $\Lambda^*(\cdot)$ is the Fenchel-Legendre transform of $\Lambda(\cdot)$, i.e., $\Lambda^*(a) := \sup_{\delta\in\mathbb{R}}\{a\delta - \Lambda(\delta)\}$. ♦

If X_1 is a lattice random variable, then the order of the pre-factor is the same, but the constant is different.

In our analysis leading to improved pre-factors, the essential idea is to reduce the error event of a code to a sum of independent random variables. However, Bahadur-Rao theorem is not directly applicable, because after the aforementioned reduction, the threshold a must vary slightly with N, as will be evident in the sequel[2]. So, we need a

[1] X_1 is called *lattice random variable* if there exist constants d and $h \in \mathbb{R}^+$ such that $X_1 \in \{d + kh : k \in \mathbb{Z}\}$ – (a.s.) [23, pg. 129].

[2] We note that this slight variation is the reason to have the slope related term, in addition to $\Theta(N^{-\frac{1}{2}})$ factor, in the pre-factor of our result. For a concrete example regarding this, see the discussion at the end of Section 3.2.1.

varying threshold version of this result. Although there are extensions of this kind (e.g., [15]), these results also depend on the lattice nature of the random variables to deduce sharp constants. However, our focus in this study is on the order of the sub-exponential term, not the constants, so in order to prevent the technicalities associated with differentiating between lattice and non-lattice random variables, we prove the following result, that will be frequently used in the sequel.

Let $\{Z_i\}_{i\geq 1}$ be independent, real-valued random random variables with law λ_i and assume $\sum_{i=1}^n \mathrm{Var}[Z_i] > 0$. Define $\Lambda_i(\delta) := \ln \mathrm{E}\left[e^{\delta Z_i}\right]$ and assume the existence of a $q \in \mathbb{R}$ with a corresponding $\eta > 0$ satisfying

(i) There exists a neighborhood of η such that $\frac{1}{n}\sum_{i=1}^n \Lambda_i(\delta) < \infty$, for all δ in this neighborhood.

(ii) $\frac{1}{n}\sum_{i=1}^n \Lambda_i'(\eta) = q$.

Let $\Lambda_n^*(\cdot)$ denote the Fenchel-Legendre transform of $\frac{1}{n}\sum_{i=1}^n \Lambda_i(\cdot)$. Define $\frac{d\tilde{\lambda}_i}{d\lambda}(z) := e^{\eta z - \Lambda_i(\eta)}$, $T_i := Z_i - \mathrm{E}_{\tilde{\lambda}_i}[Z_i]$, $m_{2,n} := \sum_{i=1}^n \mathrm{Var}_{\tilde{\lambda}_i}[T_i]$, $m_{3,n} := \sum_{i=1}^n \mathrm{E}_{\tilde{\lambda}_i}[|T_i|^3]$. Define $\hat{S}_n := \frac{1}{n}\sum_{i=1}^n Z_i$ and let μ_n (resp. $\tilde{\mu}_n$) denote the law of $\hat{S}_n$ when Z_i are independent with laws λ_i (resp. $\tilde{\lambda}_i$). Set $K_n(q) := 2\sqrt{2\pi}\frac{m_{3,n}}{m_{2,n}}$ and $t_n(a,q) := a2\sqrt{2\pi}\eta\frac{m_{3,n}}{m_{2,n}}$ for any $a \geq 1$.

Lemma 5 (Concentration lemma)**.** *For any $n \in \mathbb{Z}^+$ and $a > 1$,*

$$\mu_n([q,\infty)) \leq \frac{e^{-n\Lambda_n^*(q)}[1 + \frac{t_n(a,q)}{a}]}{\eta\sqrt{2\pi m_{2,n}}}, \tag{3.1}$$

$$\mu_n([q,\infty)) \geq \frac{e^{-n\Lambda^*(q)}e^{-t_n(a,q)}\left(1-\frac{1}{a}\right)(1+t_n(a,q))}{\eta\sqrt{2\pi m_{2,n}}}\left\{1 - \frac{[1+(1+t_n(a,q))^2]}{(1+t_n(a,q))\eta\left(1-\frac{1}{a}\right)2\sqrt{em_{2,n}}}\right\}. \tag{3.2}$$

Moreover, if $\eta \leq 1$, then

$$\mu_n([q,\infty)) \geq \frac{e^{-K_n(\eta)}}{\sqrt{2\pi m_{2,n}}}\left(1 - \frac{1+(1+K_n(\eta))^2}{2\sqrt{m_{2,n}}}\right). \tag{3.3}$$

Further, if the random variables are also identically distributed, then (3.1) *still holds with* $t_n(a,q)$ *replaced with a* $\sqrt{2\pi}\eta\frac{m_{3,n}}{m_{2,n}}$. ♦

Proof. The proof is given in Appendix B.1. □

3.1 Definitions and statement of the result

Throughout the chapter, let W be a DMC satisfying $R_\infty < C$. For any $P \in \mathcal{P}(\mathcal{X})$, define

$$\mathrm{E_{SP}}(R,P) := \min_{V\in\mathcal{P}(\mathcal{Y}|\mathcal{X}):\,\mathrm{I}(P;V)\le R} \mathrm{D}(V\|W|P), \tag{3.4}$$

and note that $\mathrm{E_{SP}}(R) = \max_{P\in\mathcal{P}(\mathcal{X})} \mathrm{E_{SP}}(R,P)$.

The following can be shown[3] to be the *maximum absolute value subgradient* of the sphere packing exponent at point R

$$\rho_R^* := \max_{P\in\mathcal{P}(\mathcal{X}):\mathrm{E_{SP}}(R,P)=\mathrm{E_{SP}}(R)} \left|\mathrm{E'_{SP}}(R,P)\right|, \tag{3.5}$$

where $\mathrm{E'_{SP}}(R,P)$ denotes the slope[4] of $\mathrm{E_{SP}}(\cdot,P)$ at point R.

Given any (N,R) code (f,φ), let $e_m(f,\varphi)$ denotes the error probability of the m-th message.

Let $\mathcal{Z}$ be a finite set and $Q,\hat{Q}\in\mathcal{P}(\mathcal{Z})$. A *deterministic hypothesis test*, $T : \mathcal{Z}\to\{0,1\}$, over the set $\mathcal{Z}$ in which Q is the null hypothesis (H_0) and $\hat{Q}$ is the alternate

[3] Since $\mathrm{E_{SP}}(\cdot,P)$ is convex for all $P\in\mathcal{P}(\mathcal{X})$, $\mathrm{E_{SP}}(\cdot,\cdot)$ is continuous on $(R_\infty,\infty)\times\mathcal{P}(\mathcal{X})$ (cf., Lemma 30 in Appendix B.7) and $\mathcal{P}(\mathcal{X})$ is compact, one can invoke the characterization of the subdifferential of the maximum function (e.g., [56, Theorem 2.87]) to deduce that $\partial\mathrm{E_{SP}}(R) = \mathrm{conv}\,(\cup_{P:\mathrm{E_{SP}}(R,P)=\mathrm{E_{SP}}(R)}\{\partial\mathrm{E_{SP}}(\cdot,P)(R)\})$, where $\mathrm{conv}(\cdot)$, $\partial\mathrm{E_{SP}}(R)$ and $\partial\mathrm{E_{SP}}(\cdot,P)(R)$ denotes the *convex hull*, *subdifferential of* $E_{SP}(\cdot)$ *at point* R and *subdifferential of* $E_{SP}(\cdot,P)$ *at point* R, respectively. This observation, coupled with the differentiability of $\mathrm{E_{SP}}(\cdot,P)$, i.e., Proposition 4, and the continuity of $\mathrm{E'_{SP}}(R,\cdot)$, i.e., Proposition 5, suffices to conclude the claim.

[4] One can show that $\mathrm{E_{SP}}(R,P)$ is differentiable with respect to R, for given P, provided that $R_\infty < R < C$ and $\mathrm{E_{SP}}(R,P) > 0$, e.g., Proposition 4.

hypothesis (H_1) is defined as

$$T(z) = \begin{cases} 0, & \text{if } z \in \mathcal{U}_T, \\ 1, & \text{if } z \in \mathcal{U}_T^c, \end{cases} \tag{3.6}$$

where $\{\mathcal{U}_T, \mathcal{U}_T^c\}$ are called the *decision regions* of the test. Let $\mathcal{T}(Q, \hat{Q})$ denote the set of all deterministic tests between Q and $\hat{Q}$. The error probabilities associated with T are defined as $\alpha_T := Q\{\mathcal{U}_T^c\}$ and $\beta_T := \hat{Q}\{\mathcal{U}_T\}$. For any $r > 0$, define

$$\alpha^*_{Q,\hat{Q}}(r) := \min_{T \in \mathcal{T}(Q,\hat{Q}); \beta_T \leq e^{-r}} \alpha_T. \tag{3.7}$$

Theorem 3. *Consider any $R \in (R_\infty, C)$ and $\zeta \in \mathbb{R}^+$. Then, for any sufficiently large N, depending on R, W and ζ and any (N, R) constant composition code (f, φ),*

$$P_e(f, \varphi) \geq K \frac{e^{-NE_{SP}(R)}}{N^{\frac{1}{2}\left(1+(1+\zeta)\rho^*_R\right)}}, \tag{3.8}$$

where $K \in \mathbb{R}^+$ is a constant that depends on R, W and ζ. ♦

3.2 Proof of Theorem 3

3.2.1 Overview

There are at least three proofs of the sphere-packing bound in the literature: that of Shannon *et al.* [63], Haroutunian [38] and Blahut [12]. Of these, Blahut's argument seems to be the most natural starting point for obtaining improved pre-factors, as it allows one to convert the error event of a code into an event involving a sum of i.i.d. random variables, to which one can apply the Bahadur-Rao result. The Shannon *et al.* argument is similar to Blahut's in some ways, but it is less amenable to exact asymptotics. The Haroutunian argument is combinatorial and even farther removed from i.i.d. sums.

Blahut's argument proceeds as follows. Assume $R_\infty < R < C$ and let (f, φ) be an (N, R) code. Let $\{\mathcal{U}_m\}_{m\in\mathcal{M}}$ denote the decision regions of φ corresponding to each message $m \in \mathcal{M}$. Let $Q \in \mathcal{P}(\mathcal{Y})$ be an auxiliary output distribution. Let $W(\mathbf{y}^N|\mathbf{x}^N) := \prod_{n=1}^N W(y_n|x_n)$ and $Q(\mathbf{y}^N) := \prod_{n=1}^N Q(y_n)$. Since $\sum_{\mathbf{y}^N\in\mathcal{Y}^N} Q(\mathbf{y}^N) = 1$ and $|\mathcal{M}| \geq e^{NR}$, there must be a message $m \in \mathcal{M}$ such that $Q\{\mathcal{U}_m\} \leq e^{-NR}$. Let $\mathbf{x}^N := f(m)$ be the codeword for this message. It is clear that $\mathrm{P_e}(f, \varphi) \geq e_m(f, \varphi) = W\left\{\mathcal{U}_m^c|\mathbf{x}^N\right\}$.

Now consider the hypothesis test over the set $\mathcal{Y}^N$ in which $W(\cdot|\mathbf{x}^N)$ is the null hypothesis (H_0) and the i.i.d. output distribution Q is the alternate hypothesis (H_1). One feasible test is to accept H_0 on $\mathcal{U}_m$ and H_1 on $\mathcal{U}_m^c$, resulting in type-I and type-II error probabilities of $W(\mathcal{U}_m^c|\mathbf{x}^N) = e_m(f, \varphi)$ and $Q\{\mathcal{U}_m\}$, respectively. Since $\alpha^*_{W(\cdot|\mathbf{x}^N),Q}(NR)$ denotes the minimum type-I error probability, optimized over all tests, subject to the constraint that the type-II error probability does not exceed e^{-NR} (cf., (3.7)), we evidently must have

$$\mathrm{P_e}(f, \varphi) \geq \alpha^*_{W(\cdot|\mathbf{x}^N),Q}(NR). \tag{3.9}$$

The error exponent of this test can be expressed via the following definition. For any $V \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$, $P \in \mathcal{P}(\mathcal{X})$ and $Q \in \mathcal{P}(\mathcal{Y})$, define $\mathrm{D}(V||Q|P) := \sum_{x\in\mathcal{X}} P(x)\mathrm{D}(V(\cdot|x)||Q)$.

Definition 1. *For any $P \in \mathcal{P}(\mathcal{X})$ and $Q \in \mathcal{P}(\mathcal{Y})$*

$$e_{SP}(Q, P, r) := \inf_{V\in\mathcal{P}(\mathcal{Y}|\mathcal{X}):\, D(V||Q|P)\leq r} D(V||W|P). \tag{3.10}$$

for all $r \in \mathbb{R}_+$. $\lozenge$

Then the optimal type-I error exponent can be shown to be (e.g., [12, Section V]) $\mathrm{e_{SP}}(Q, P, R)$, where P is the empirical distribution of $\mathbf{x}^N$.

Note that this exponent depends on the output distribution Q, which is to be selected. This distribution can be chosen to depend on P, since it can depend on the code, although allowing such dependence necessitates a restriction to constant composition codes. In

the original argument [12, Section V], this freedom is not used, and Q depends on R (and the channel) but not P. Pre-factors aside, it is not clear that this choice yields the standard sphere-packing exponent when (3.10) is maximized over P. This is asserted to be the case in [12, Theorem 19] and [13, Theorem 10.1.4], but each of these proofs has a nontrivial gap[5]. Moreover, a numerical study indicates that for the Z-channel and for this choice of Q, $\mathrm{E_{SP}}(R) < \max_P \mathrm{e_{SP}}(Q, P, R)$, for a broad range of rates. For symmetric channels, Q can indeed be chosen independently of P [2], and so the code need not be constant composition. But in the general case, it appears that some dependence is necessary if one hopes to obtain the sphere-packing exponent.

Our choice of Q will depend on P and give the sphere-packing exponent. Thus, one of the ancillary contributions of this chapter is to give a complete proof that the hypothesis testing reduction described can be used to obtain the sphere-packing exponent. In fact, using the hypothesis testing reduction, we shall prove the stronger result that the exponent on the error probability of any constant-composition code with composition P is upper bounded by $\mathrm{E_{SP}}(R, P)$; previously, the only proof of this fact used combinatorial techniques.

It is worth noting that the Shannon *et al.* proof also involves the choice of an output distribution. Their choice of output distribution also depends on P, but it is defined differently from ours. Our choice yields the $\mathrm{E_{SP}}(R, P)$ exponent, whereas Shannon *et al.* only establish an exponent of $\mathrm{E_{SP}}(R)$.

Before concluding this section, it is instructive to consider a binary symmetric channel (BSC) with crossover probability $p \in (0, 1/2)$ in order to see why the slope related term arises in Theorem 3. One can check that the output distribution mentioned in [2,

[5]Specifically, the argument for [12, Theorem 19] seems to proceed as if Lagrange multipliers of $\max_P \mathrm{E_{SP}}(R, P)$ and $\max_P \mathrm{e_{SP}}(Q, P, R)$ are the same, which is not evident. For [13, Theorem 10.1.4], only $\mathrm{e_{SP}}(Q, P_R^*, R) = \max_P \mathrm{E_{SP}}(R, P)$ is shown, where P_R^* attains $\max_P \mathrm{E_{SP}}(R, P)$, which does not imply the claim.

Eq. 9] reduces to the uniform distribution and for these particular choices,

$$\alpha^*_{W(\cdot|\mathbf{x}^N),Q}(NR) \geq \sum_{n=n_R^*+1}^{N} \binom{N}{n} p^n (1-p)^{N-n} = \Pr\left\{ \frac{1}{N} \sum_{n=1}^{N} Z_n \geq \frac{n_R^*+1}{N} \right\}, \tag{3.11}$$

where $\{Z_n\}_{n=1}^N$ are i.i.d. Bernoulli random variables with parameter p and n_R^* is the largest $k \in \mathbb{Z}^+$ satisfying

$$e^{-NR} \geq \sum_{n=0}^{k} \binom{N}{n} 2^{-N} = \Pr\left\{ \frac{1}{N} \sum_{n=1}^{N} \tilde{Z}_n \leq \frac{k}{N} \right\}, \tag{3.12}$$

where $\{\tilde{Z}_n\}_{n=1}^N$ are i.i.d. Bernoulli random variables with parameter $1/2$. Provided that $k/N < 1/2$, one can apply Bahadur-Rao theorem to the right side of (3.12) to have

$$\Pr\left\{ \frac{1}{N} \sum_{n=1}^{N} \tilde{Z}_n \leq \frac{k}{N} \right\} \geq \frac{K_1}{\sqrt{N}} e^{-N\mathrm{D}\left(\frac{k}{N}\|\frac{1}{2}\right)}, \tag{3.13}$$

where $\mathrm{D}\left(k/n\|1/2\right) := k/n \ln \frac{k/n}{1/2} + (1-k/n) \ln \frac{1-k/n}{1/2}$ and K_1 is a positive constant. Plugging (3.13) into (3.12) and recalling the definition of n_R^*, one can verify that

$$\frac{n_R^*}{N} \leq \mathrm{h}^{-1}\left(\ln 2 - R + \frac{\ln \sqrt{N}}{N} - \frac{\ln K_1}{N} \right) \tag{3.14}$$

By plugging (3.14) into (3.11), applying Bahadur-Rao theorem on the right side of (3.11) and carrying out the algebra, one can verify that

$$\alpha^*_{W(\cdot|\mathbf{x}^N),Q}(NR) \geq \frac{K_2}{\sqrt{N}} e^{-N\mathrm{E_{SP}}\left(R - \frac{\ln \sqrt{N}}{N}\right)} \geq \frac{K_3}{N^{0.5(1+|\mathrm{E}'_{\mathrm{SP}}(R)|)}} e^{-N\mathrm{E_{SP}}(R)}, \tag{3.15}$$

where K_2, K_3 are positive constants and the last inequality follows by expanding $\mathrm{E_{SP}}(\cdot)$ as a power series about R. Note that if $\frac{n_R^*}{N}$ were constant in N, then applying Bahadur-Rao theorem to (3.11) would give a pre-factor with an order of $1/\sqrt{N}$. But Eq. (3.14) shows that $\frac{n_R^*}{N}$ increases with N at a rate of $\frac{\ln N}{N}$. While this increase is too slow to affect the exponent, it does affect the order of the pre-factor.

Finally, note that the arguments leading to (3.15) are nothing but the "packing of Hamming spheres". To be specific, one can check that (e.g., [24]) for this channel, the error probability of any (N, R) code is lower bounded by that of a hypothetical "sphere-packed code" with the same parameters. A sphere-packed code is a code such that

the decoding region of each codeword is an Hamming sphere of a certain radius, say $\lceil N\delta(R) \rceil$ with $\delta(R) > 0$, possibly excluding some strings in the outermost layer and the union of these spheres equals $\{0,1\}^N$. For the sphere-packed code, an error occurs when the noise pushes the received signal outside of the Hamming ball of radius n_R^* centered at the codeword, whose probability is precisely the right side of (3.11). By employing the upper bound given in (3.14), one can deduce (3.15).

By continuing this sphere-packing analogy, one can intuitively view the lower bound obtained via the hypothesis testing reduction as the error probability of a hypothetical sphere-packed (N, R) code on $\mathcal{Y}^N$ with $\ln \frac{Q(\cdot)}{W(\cdot|\mathbf{x}^N)}$ used instead of Hamming distance. Note that the extra term in the pre-factor essentially stems from the approximation of the "maximal packing radius" of the spheres under this metric.

3.2.2 Selecting the output distribution

In order to describe our output distribution, we require the following technical results.

For any $Q \in \mathcal{P}(\mathcal{Y})$ and $\lambda \in [0, 1)$, define

$$\Lambda_{Q,P}(\lambda) := \begin{cases} \mathrm{E}_P \left[\ln \mathrm{E}_{W(\cdot|X)} \left[\left(\frac{Q(Y)}{W(Y|X)} \right)^{\lambda} \right] \right], & \lambda \in (0,1), \\ 0, & \lambda = 0. \end{cases} \tag{3.16}$$

For any $R \in \mathbb{R}^+$, define

$$\mathcal{P}_R(\mathcal{X}) := \{P \in \mathcal{P}(\mathcal{X}) : \mathrm{E}_{\mathrm{SP}}(R, P) > 0\}, \tag{3.17}$$

$$\mathcal{P}_{P,W}(\mathcal{Y}) := \{Q \in \mathcal{P}(\mathcal{Y}) \ : \ \forall x \in \mathcal{S}(P),\ \mathcal{S}(Q) \cap \mathcal{S}(W(\cdot|x)) \neq \emptyset\}, \tag{3.18}$$

$$\tilde{\mathcal{P}}_{P,W}(\mathcal{Y}) := \{Q \in \mathcal{P}(\mathcal{Y}) \ : \ \forall x \in \mathcal{S}(P),\ Q \gg W(\cdot|x)\}. \tag{3.19}$$

Further, given any $R > R_\infty$ and $P \in \mathcal{P}(\mathcal{X})$,

$$K_{R,P} \ : \ \mathbb{R}_+ \times \mathcal{P}_{P,W}(\mathcal{Y}) \to \mathbb{R}, \text{ s.t. } K_{R,P}(\rho, Q) = -\rho R - (1+\rho)\Lambda_{Q,P}\left(\rho/(1+\rho)\right), \tag{3.20}$$

for all $(\rho, Q) \in \mathbb{R}_+ \times \mathcal{P}_{P,W}(\mathcal{Y})$.

Proposition 2 (Saddle-point)**.** *Consider any $R_\infty < R < C$ and $P \in \mathcal{P}_R(\mathcal{X})$.*

(i) $K_{R,P}(\cdot,\cdot)$ has a saddle-point with the saddle-value $E_{SP}(R,P)$.

(ii) Any saddle-point of $K_{R,P}(\cdot,\cdot)$, say (ρ^*, Q^*), satisfies $(\rho^*, Q^*) \in \mathbb{R}^+ \times \tilde{\mathcal{P}}_{P,W}(\mathcal{Y})$. ♦

Proof. The proof is provided in Appendix B.2. □

Let $S(R,P)$ denote the set of saddle-points of $K_{R,P}(\cdot,\cdot)$. Moreover,

$$S(R,P)|_{\mathbb{R}_+} := \{\rho \in \mathbb{R}_+ : \exists\, Q \in \mathcal{P}_{P,W}(\mathcal{Y}),\ \text{s.t. } (\rho, Q) \in S(R,P)\}, \tag{3.21}$$

$$S(R,P)|_{\mathcal{P}_{P,W}(\mathcal{Y})} := \{Q \in \mathcal{P}_{P,W}(\mathcal{Y}) : \exists \rho \in \mathbb{R}_+,\ \text{s.t. } (\rho, Q) \in S(R,P)\}. \tag{3.22}$$

Proposition 3 (Uniqueness of the saddle-point)**.** *For any $R_\infty < R < C$ and $P \in \mathcal{P}_R(\mathcal{X})$, $S(R,P)$ is a singleton.* ♦

Proof. The proof is given in Appendix B.3. □

Definition 2. *Fix any $R_\infty < R < C$.*

$$\rho^*_{R,\cdot} : \mathcal{P}_R(\mathcal{X}) \to \mathbb{R}_+,\ \textit{s.t. } \rho^*_{R,P} = S(R,P)|_{\mathbb{R}_+}, \tag{3.23}$$

$$Q^*_{R,\cdot} : \mathcal{P}_R(\mathcal{X}) \to \mathcal{P}_{P,W}(\mathcal{Y}),\ \textit{s.t. } Q^*_{R,P} = S(R,P)|_{\mathcal{P}_{P,W}(\mathcal{Y})}. \tag{3.24}$$

◊

Observe that owing to Proposition 3, both (3.23) and (3.24) are well-defined. The distribution $Q^*_{R,\cdot}$ in (3.24) will be our output distribution.

Proposition 4 (Differentiability of $\mathrm{E_{SP}}(\cdot, P)$)**.** *Consider any $R_\infty < R < C$ and $P \in \mathcal{P}_R(\mathcal{X})$. $E_{SP}(\cdot, P)$ is differentiable with $\rho^*_{R,P} = -\left.\frac{\partial E_{SP}(r,P)}{\partial r}\right|_{r=R}$.* ♦

Proof. The proof is given in Appendix B.4. □

Proposition 5 (Continuity of the saddle-point)**.** *Consider any $R_\infty < R < C$. Both $\rho^*_{R,\cdot}$ and $Q^*_{R,\cdot}$ are continuous on $\mathcal{P}_R(\mathcal{X})$.* ♦

Proof. The proof is provided in Appendix B.5. □

For any $R_\infty < R < C$ and $P \in \mathcal{P}_R(\mathcal{X})$, let $\mathrm{e_{SP}}(R, P, r) := \mathrm{e_{SP}}(Q^*_{P,R}, P, r)$ and $\mathrm{e_{SP}}(R, P) := \mathrm{e_{SP}}(R, P, R)$.

Proposition 6 (Equality of the exponents)**.** *For any $R_\infty < R < C$*

$$e_{SP}(R, P) = E_{SP}(R, P), \tag{3.25}$$

for all $P \in \mathcal{P}_R(\mathcal{X})$. ♦

Proof. The proof is given in Appendix B.6. □

Remark 7. *Recalling the discussion in the previous section, the equality of the exponents proposition, i.e., Proposition 6, ensures that the exponent of the lower bound on the error probability emerging as a result of binary hypothesis testing reduction in which $Q^*_{R,\cdot}$ is the alternate distribution matches the sphere-packing exponent.* ◇

3.2.3 Hypothesis testing reduction

For any $\nu, R \in \mathbb{R}^+$, define $\mathcal{P}_{R,\nu}(\mathcal{X}) := \{P \in \mathcal{P}(\mathcal{X}) : \mathrm{E_{SP}}(R, P) \geq \nu\}$. Fix some $R \in (R_\infty, C)$ and some sufficiently small $\nu > 0$ that only depends on W and R. Application of the hypothesis testing reduction of Section 3.2.1 to an (N, R) constant composition code

(f, φ) with common composition[6] $P \in \mathcal{P}_{R,\nu}(\mathcal{X})$ by using $Q^*_{R,P}$ as the auxiliary output distribution yields (recall (3.9))

$$\mathrm{P_e}(f, \varphi) \geq \alpha_N(R), \tag{3.26}$$

where $\alpha_N(R) := \alpha_{W(\cdot|\mathbf{x}^N), Q^*_{R,P}}(NR)$. On account of (3.26), in order to lower bound the maximal error probability of our code, it suffices to evaluate $\alpha_N(R)$.

However, since $Q^*_{R,P} \gg W(\cdot|\mathbf{x}^N)$ (cf., item (ii) of the saddle-point proposition, i.e., Proposition 2), but not necessarily[7] $Q^*_{R,P} \equiv W(\cdot|\mathbf{x}^N)$, we need to do little more work. To this end, we define

$$\tilde{\mathcal{T}}(Q, \hat{Q}) := \left\{ T \in \mathcal{T}(Q, \tilde{Q}) : \mathcal{U}_T \cap [\mathcal{S}(\hat{Q}) \backslash \mathcal{S}(Q, \hat{Q})] = \emptyset,\ \mathcal{U}_T^c \cap [\mathcal{S}(Q) \backslash \mathcal{S}(Q, \hat{Q})] = \emptyset \right\}, \tag{3.27}$$

where $\mathcal{S}(Q, \hat{Q}) := \mathcal{S}(Q) \cap \mathcal{S}(\hat{Q})$. Next, we note the following evident observations.

Claim 1. *For any $r \in \mathbb{R}^+$,*

$$\alpha^*_{Q,\hat{Q}}(r) = \min_{T \in \tilde{\mathcal{T}}(Q,\hat{Q}) : \beta_T \leq e^{-r}} \alpha_T. \tag{3.28}$$

♦

Claim 2. *For any $T \in \tilde{\mathcal{T}}(Q, \hat{Q})$, we have*

$$\alpha_T = Q\left\{\mathcal{S}(Q, \tilde{Q})\right\} Q\left\{\mathcal{U}_T^c \,|\, \mathcal{S}(Q, \hat{Q})\right\}, \quad \beta_T = \hat{Q}\left\{\mathcal{S}(Q, \hat{Q})\right\} \hat{Q}\left\{\mathcal{U}_T \,|\, \mathcal{S}(Q, \hat{Q})\right\}, \tag{3.29}$$

where the conditional probabilities are induced by Q and $\hat{Q}$, respectively. ♦

Observe that owing to (3.28) we have[8]

$$\alpha_N(R) = \min_{T \in \tilde{\mathcal{T}}(W(\cdot|\mathbf{x}^N), Q^*_{R,P}) : \beta_T \leq e^{-NR}} \alpha_T. \tag{3.30}$$

[6] If $P \in \mathcal{P}_{R,\nu}(\mathcal{X})^c$, then it is possible to prove that (3.8) is true. See Lemma 31 in Appendix B.7.

[7] We have this equivalence if we consider a positive channel, for example.

[8] $\tilde{\mathcal{T}}(W(\cdot|\mathbf{x}^N), Q^*_{R,P})$ is defined as in (3.27).

In order to apply Claims 1 and 2 to our particular case, we need the following definition.

Definition 3. *Given any $C > R > R_\infty$ and $P \in \mathcal{P}_R(\mathcal{X})$,*

$$W^-_{R,P}(\cdot|x) := \begin{cases} \tilde{W}_{1^-,Q^*_{R,P}}(\cdot|x), & \text{if } x \in \mathcal{S}(P), \\ W(\cdot|x), & \text{else}, \end{cases} \tag{3.31}$$

where

$$\tilde{W}_{1^-,Q^*_{R,P}}(\cdot|x) := \lim_{\lambda\uparrow 1} \tilde{W}_{\lambda,Q^*_{R,P}}(\cdot|x), \ \forall\, x \in \mathcal{S}(P). \tag{3.32}$$

and $\tilde{W}_{\lambda,Q^*_{R,P}}(\cdot|x)$ is the tilted distribution *as defined in* (B.51) *in Appendix B.2.* $\diamond$

Remark 8. *One can check that for any $x \in \mathcal{S}(P)$,*

$$\tilde{W}_{1^-,Q^*_{R,P}}(\cdot|x) = \begin{cases} \frac{Q^*_{R,P}(y)}{Q^*_{R,P}\{\mathcal{S}(W(\cdot|x))\}}, & \text{if } y \in \mathcal{S}(W(\cdot|x)), \\ 0, & \text{else}. \end{cases} \tag{3.33}$$

Equation (3.33) *and the fact that $Q^*_{R,P} \gg W(\cdot|x)$, for all $x \in \mathcal{S}(P)$, ensure that* (3.31) *is a well-defined stochastic matrix from $\mathcal{X}$ to $\mathcal{Y}$. Moreover, it is clear that $W^-_{R,P}(\cdot|x) \equiv W(\cdot|x)$, for all $x \in \mathcal{X}$.* $\diamond$

Returning to our application, since $Q^*_{R,P} \gg W(\cdot|\mathbf{x}^N)$, (3.29) implies that for any $\tilde{T} \in \tilde{\mathcal{T}}(W(\cdot|\mathbf{x}^N), Q^*_{R,P})$, we have

$$\alpha_{\tilde{T}} = W\left\{\mathcal{U}^c_{\tilde{T}}|\mathbf{x}^N\right\}, \quad \beta_{\tilde{T}} = Q^*_{R,P}\left\{\mathcal{S}(W(\cdot|\mathbf{x}^N))\right\} W^-_{R,P}\left\{\mathcal{U}_{\tilde{T}}|\mathbf{x}^N\right\}, \tag{3.34}$$

where $W^-_{R,P}(\mathbf{y}^N|\mathbf{x}^N) := \prod_{n=1}^N W^-_{R,P}(y_n|x_n)$ and $W^-_{R,P}$ is defined in (3.31).

Also,

$$\ln Q^*_{R,P}\left\{\mathcal{S}(W^N(\cdot|\mathbf{x}^N))\right\} = \sum_{n=1}^N \ln Q^*_{R,P}\left\{\mathcal{S}(W(\cdot|x_n))\right\} \tag{3.35}$$

$$= N \sum_{x\in\mathcal{S}(P)} P(x) \ln Q^*_{R,P}\left\{\mathcal{S}(W(\cdot|x))\right\} \tag{3.36}$$

$$= -N\mathrm{D}(W^-_{R,P}\|Q^*_{R,P}|P), \tag{3.37}$$

where (3.35) follows since $\mathcal{S}(W(\cdot|\mathbf{x}^N)) = \mathcal{S}(W(\cdot|x_1))\times\ldots\times\mathcal{S}(W(\cdot|x_N))$ and (3.37) follows by noting

$$\ln Q^*_{R,P}\left\{\mathcal{S}(W(\cdot|x))\right\} = -\mathrm{D}(W^-_{R,P}(\cdot|x)\|Q^*_{R,P}), \tag{3.38}$$

which is a direct consequence of (3.31).

Combining (3.34) and (3.37), we conclude that for any $\tilde{T} \in \tilde{\mathcal{T}}(W(\cdot|\mathbf{x}^N), Q^*_{R,P})$

$$\left[\beta_{\tilde{T}} \leq e^{-NR}\right] \Longleftrightarrow \left[W^-_{R,P}\left\{\mathcal{U}_{\tilde{T}}|\mathbf{x}^N\right\} \leq e^{-Nr(R,P)}\right], \tag{3.39}$$

where

$$r(R,P) := R - \mathrm{D}(W^-_{R,P}\|Q^*_{R,P}|P). \tag{3.40}$$

Observe that the right side of (3.39) defines a non-trivial constraint only if $r(R,P) > 0$, which we establish next. To this end, we first define the following set:

$$\tilde{\mathcal{P}}_{P,W}(\mathcal{Y}|\mathcal{X}) := \{V \in \mathcal{P}(\mathcal{Y}|\mathcal{X}) : \forall\, x \in \mathcal{S}(P),\ V(\cdot|x) \ll W(\cdot|x)\}. \tag{3.41}$$

Lemma 6 (Positivity of $r(R,P)$)). *Given any $R_\infty < R < C$ and $P \in \mathcal{P}_R(\mathcal{X})$,*

(i) $\forall\, V \in \tilde{\mathcal{P}}_{P,W}(\mathcal{Y}|\mathcal{X})$, $D(V\|Q^*_{R,P}|P) = D(V\|W^-_{R,P}|P) + D(W^-_{R,P}\|Q^*_{R,P}|P)$.

(ii) $r(R,P) > 0$. ♦

Proof. The proof is given in Appendix B.8. □

Now, consider a binary hypothesis testing setup with the null hypothesis (resp. alternate hypothesis) $W(\cdot|\mathbf{x}^N)$ (resp. $W^-_{R,P}(\cdot|\mathbf{x}^N)$). Owing to (3.26), (3.30), (3.34) and (3.39), we deduce that

$$e(f,\varphi) \geq \tilde{\alpha}_N(r(R,P)) := \min_{T' \in \tilde{T}(W(\cdot|\mathbf{x}^N), W^-_{R,P}(\cdot|\mathbf{x}^N)) : \beta_{T'} \leq e^{-Nr(R,P)}} \alpha_{T'}. \tag{3.42}$$

On account of (3.42), in order to lower bound the maximal error probability of our constant composition code, it suffices to evaluate $\tilde{\alpha}_N(r(R,P))$. Instead of directly characterizing $\tilde{\alpha}_N(r(R,P))$, we give a lower bound on it by means of a test that is easier to analyze. In order to define this test, we need the following "shifted exponent".

Definition 4. *Given any $C > R > R_\infty$, $r \in \mathbb{R}_+$ and $P \in \mathcal{P}_R(\mathcal{X})$,*

$$\tilde{e}_{SP}(R,P,r) := \inf_{V \in \mathcal{P}(\mathcal{Y}|\mathcal{X}) \,:\, D(V\|W^-_{R,P}|P) \le r} D(V\|W|P). \tag{3.43}$$

◊

Lemma 7. *(Shifted exponent) For any $R > R_\infty$ and $P \in \mathcal{P}_R(\mathcal{X})$ we have*

$$\tilde{e}_{SP}(R,P,r - D(W^-_{R,P}\|Q^*_{R,P}|P)) = e_{SP}(R,P,r), \tag{3.44}$$

for all $r > D(W^-_{R,P}\|Q^*_{R,P}|P)$. ♦

Proof. Fix an arbitrary $R > R_\infty$, $P \in \mathcal{P}_R(\mathcal{X})$ and $r > \mathrm{D}(W^-_{R,P}\|Q^*_{R,P}|P)$. Define $\tilde{r} := r - D(W^-_{R,P}\|Q^*_{R,P}|P)$. Clearly, $\tilde{r} \in \mathbb{R}^+$. On account of the fact that $\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,\tilde{r}) \le \tilde{e}_{\mathrm{SP}}(R,P,0) = \mathrm{D}(W^-_{R,P}\|W|P) < \infty$, it is easy to see that

$$\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,\tilde{r}) = \min_{V \in \tilde{\mathcal{P}}_{P,W}(\mathcal{Y}|\mathcal{X}) \,:\, \mathrm{D}(V\|W^-_{R,P}|P) \le \tilde{r}} \mathrm{D}(V\|W|P). \tag{3.45}$$

Similarly,

$$\mathrm{e}_{\mathrm{SP}}(R,P,r) = \min_{V \in \tilde{\mathcal{P}}_{P,W}(\mathcal{Y}|\mathcal{X}) \,:\, \mathrm{D}(V\|Q^*_{R,P}|P) \le r} \mathrm{D}(V\|W|P). \tag{3.46}$$

Item (i) of Lemma 6 ensures that the feasible regions of the right sides of (3.45) and (3.46) are the same. Since the cost functions of the two problems are the same, the lemma follows. □

Fix an arbitrary $\zeta \in \mathbb{R}^+$ and let $\epsilon_N := \left(\frac{1}{2} + \zeta\right)\frac{\ln N}{N}$ (resp. $\tilde{\epsilon}_N := \epsilon_N - \frac{1}{N}$) and define $R_N := R - \epsilon_N$ (resp. $\tilde{R}_N := R - \tilde{\epsilon}_N$). Note that for all sufficiently large $N \in \mathbb{Z}^+$,

$C > \tilde{R}_N > R_N > R_\infty$. Throughout, we consider such an $N \in \mathbb{Z}^+$. Further, similar to (3.40), define $r_N(P,R) := R_N - \mathrm{D}(W^-_{R,P}\|Q^*_{R,P}|P)$ (resp. $\tilde{r}_N(P,R) := \tilde{R}_N - \mathrm{D}(W^-_{R,P}\|Q^*_{R,P}|P)$). Also,

$$A_N := \left\{ \mathbf{y}^N \,:\, \frac{1}{N}\sum_{n=1}^{N} \ln \frac{W(y_n|x_n)}{W^-_{R,P}(y_n|x_n)} > r_N(R,P) - \tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r_N(R,P)) \right\}, \tag{3.47}$$

$$A^c_N = \left\{ \mathbf{y}^N \,:\, \frac{1}{N}\sum_{n=1}^{N} \ln \frac{W^-_{R,P}(y_n|x_n)}{W(y_n|x_n)} \geq \tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r_N(R,P)) - r_N(R,P) \right\}. \tag{3.48}$$

Equations (3.47) and (3.48) are the decision regions of the test, i.e., the test decides $W(\cdot|\mathbf{x}^N)$ if $\mathbf{y}^N \in A_N$ and $W^-_{R,P}(\cdot|\mathbf{x}^N)$ if $\mathbf{y}^N \in A^c_N$. Let

$$\alpha_N := W\left\{A^c_N|\mathbf{x}^N\right\}, \quad \beta_N := W^-_{R,P}\left\{A_N|\mathbf{x}^N\right\}, \tag{3.49}$$

denote the error probabilities of the aforementioned test.

Remark 9. *As noted before, the analysis of the events A_N and A^c_N would be direct applications of Bahadur-Rao theorem, but one major complication: the threshold in both events depends on N. One could define constant-threshold versions of these events by replacing $r_N(R,P)$ with $r(R,P)$. Applying exact asymptotics to the resulting events would yield a lower bound on α_N of the order $\frac{1}{\sqrt{N}}\exp(-NE_{SP}(R,P))$ and show that β_N is of the order $\frac{1}{\sqrt{N}}\exp(-Nr(R,P))$. The problem with this approach is that $P_e(f,\varphi)$ is lower bounded by the type-I error probability of the optimal test whose type-II probability does not exceed $e^{-Nr(R,P)}$. From the above expression of β_N, we see that the aforementioned test is not optimal because, although it is a likelihood ratio test, it is "undershooting" the type-II constraint due to the $1/\sqrt{N}$ pre-factor. By replacing $r(R,P)$ with $r_N(R,P)$, we ensure that β_N does not undershoot the constraint (in fact, it will violate it by a small amount). The $r_N(R,P)$ fluctuations will give rise to the slope term in the pre-factor of the probability of A_N.* $\diamond$

3.2.4 Analysis of the hypothesis test

In this section, we apply concentration lemma, i.e., Lemma 5, to lower bound α_N and β_N given in (3.49). To this end, we begin with the following technical results.

Definition 5. *Let $C > R > R_\infty$ and $P \in \mathcal{P}_R(\mathcal{X})$ be arbitrary but fixed. Let $\lambda \in \mathbb{R}$ be arbitrary.*

$$\Lambda_{0,P,x}(\lambda) := \ln E_{W(\cdot|x)}\left[e^{\lambda \ln \frac{W^-_{R,P}(Y|x)}{W(Y|x)}}\right], \tag{3.50}$$

$$\Lambda_{0,P}(\lambda) := \sum_{x\in\mathcal{X}} P(x)\Lambda_{0,P,x}(\lambda), \tag{3.51}$$

$$\Lambda_{1,P,x}(\lambda) := \ln E_{W^-_{R,P}(\cdot|x)}\left[e^{\lambda \ln \frac{W(Y|x)}{W^-_{R,P}(Y|x)}}\right], \tag{3.52}$$

$$\Lambda_{1,P}(\lambda) := \sum_{x\in\mathcal{X}} P(x)\Lambda_{1,P,x}(\lambda). \tag{3.53}$$

$\Diamond$

Remark 10. *We note the following:*

(i) Since $W^-_{R,P}(\cdot|x) \equiv W(\cdot|x)$ for all $x \in \mathcal{X}$, each quantity given in Definition 5 is well-defined. Also, one can check that $\Lambda_{1,P,x}(\lambda) = \Lambda_{0,P,x}(1-\lambda)$, which, in turn, implies that $\Lambda_{1,P}(\lambda) = \Lambda_{0,P}(1-\lambda)$.

(ii) The fact that $W^-_{R,P}(\cdot|x) \equiv W(\cdot|x)$ for all $x \in \mathcal{X}$ also ensures that $\Lambda_{0,P}(\lambda), \Lambda_{1,P}(\lambda) \in \mathbb{R}$ and hence both $\Lambda_{0,P}(\cdot)$ and $\Lambda_{1,P}(\cdot)$ are smooth functions over the real line, i.e., $\Lambda_{0,P}(\cdot), \Lambda_{1,P}(\cdot) \in C^\infty(\mathbb{R})$.

(iii) Consider any $\lambda \in \mathbb{R}$. It is easy to verify the following (for the sake of notational convenience, we denote partial derivatives with respect to λ as the ordinary ones):

$$\Lambda'_{0,P,x}(\lambda) = E_{\tilde{W}_{\lambda,P}(\cdot|x)}\left[\ln \frac{W^-_{R,P}(Y|x)}{W(Y|x)}\right], \tag{3.54}$$

$$\Lambda'_{0,P}(\lambda) = \sum_{x\in\mathcal{X}} P(x)\Lambda'_{0,P,x}(\lambda), \tag{3.55}$$

$$\Lambda''_{0,P,x}(\lambda) = Var_{\tilde{W}_{\lambda,P}(\cdot|x)}\left[\ln \frac{W^-_{R,P}(Y|x)}{W(Y|x)}\right], \tag{3.56}$$

$$\Lambda''_{0,P}(\lambda) = \sum_{x\in\mathcal{X}} P(x)\Lambda''_{0,P,x}(\lambda), \tag{3.57}$$

where $\tilde{W}_{\lambda,P}(\cdot|x) := \tilde{W}_{\lambda,W^-_{R,P}(\cdot|x)}$ *(cf.,* (B.51)*) for the sake of notational convenience.*

Further, item (ii) above ensures that

$$\Lambda'_{1,P,x}(\lambda) = -\Lambda'_{0,P,x}(1-\lambda), \quad \Lambda'_{1,P}(\lambda) = -\Lambda'_{0,P}(1-\lambda), \tag{3.58}$$

$$\Lambda''_{1,P,x}(\lambda) = \Lambda''_{0,P,x}(1-\lambda), \quad \Lambda''_{1,P}(\lambda) = \Lambda''_{0,P}(1-\lambda), \tag{3.59}$$

for any $\lambda \in \mathbb{R}$.

(iv) We have

$$\Lambda'_{0,P}(0) = -\Lambda'_{1,P}(1) = -D(W\|W^-_{R,P}|P), \tag{3.60}$$

$$\Lambda'_{0,P}(1) = -\Lambda'_{1,P}(0) = D(W^-_{R,P}\|W|P), \tag{3.61}$$

as a direct consequence of (3.55) *and* (3.58). ◇

Lemma 8 (Positive variance)**.** *Let* $C > R > R_\infty$ *and* $P \in \mathcal{P}_R(\mathcal{X})$ *be arbitrary. For all* $\lambda \in [0,1]$, $\Lambda''_{0,P}(\lambda) > 0$. ♦

Proof. Consider any $C > R > R_\infty$, $P \in \mathcal{P}_R(\mathcal{X})$ and recall that $r(R,P) = R - \mathrm{D}(W^-_{R,P}\|Q^*_{R,P}|P)$ (cf., (3.40)).

For contradiction, suppose there exists $\lambda \in [0,1]$ such that $\Lambda''_{0,P}(\lambda) = 0$. We have

$$\left[\Lambda''_{0,P}(\lambda) = 0\right] \iff \left[\forall x \in \mathcal{S}(P),\ \ln \frac{W^-_{R,P}(Y|x)}{W(Y|x)} = \Lambda'_{0,P,x}(\lambda),\ W(\cdot|x)\text{-(a.s.)}\right] \tag{3.62}$$

$$\iff \left[\forall x \in \mathcal{S}(P),\ W(Y|x) = W^-_{R,P}(Y|x)e^{-\Lambda'_{0,P,x}(\lambda)},\ W(\cdot|x)\text{-(a.s.)}\right], \tag{3.63}$$

where (3.62) follows from (3.54), (3.56) and (3.57). Summing the right side of (3.63) over $y \in \mathcal{S}(W(\cdot|x))$ yields

$$\forall x \in \mathcal{S}(P),\ \Lambda'_{0,P,x}(\lambda) = 0. \tag{3.64}$$

Combining (3.63) and (3.64) and recalling the definition of $W^-_{R,P}$ (cf., (3.31)), we deduce that

$$\left[\Lambda''_{0,P}(\lambda) = 0\right] \iff \left[\forall (x,y) \in \mathcal{X} \times \mathcal{Y},\ W(y|x) = W^-_{R,P}(y|x)\right]. \tag{3.65}$$

The right side of (3.65) implies that $\tilde{e}_{\mathrm{SP}}(R,P,r) = 0$ for all $r \in \mathbb{R}_+$ and in particular $\tilde{e}_{\mathrm{SP}}(R,P,r(R,P)) = 0$. This observation, coupled with the equality of the exponents proposition, i.e., Proposition 6, and the shifted exponent exponent lemma, i.e., Lemma 7, implies that $\mathrm{E}_{\mathrm{SP}}(R,P) = 0$ that contradicts the fact that $P \in \mathcal{P}_R(\mathcal{X})$. □

Definition 6. *Let $C > R > R_\infty$ be arbitrary. Define*

$$m_{0,3}(\lambda,P) := \sum_{x \in \mathcal{S}(P)} P(x) E_{\tilde{W}_{\lambda,P}(\cdot|x)}\left[\left|\ln \frac{W^-_{R,P}(Y|x)}{W(Y|x)} - \Lambda'_{0,P,x}(\lambda)\right|^3\right], \tag{3.66}$$

$$m_{1,3}(\lambda,P) := \sum_{x \in \mathcal{S}(P)} P(x) E_{\tilde{W}_{1-\lambda,P}(\cdot|x)}\left[\left|\ln \frac{W(Y|x)}{W^-_{R,P}(Y|x)} - \Lambda'_{1,P,x}(\lambda)\right|^3\right], \tag{3.67}$$

for any $(\lambda,P) \in [0,1] \times \mathcal{P}_R(\mathcal{X})$. ◊

Note that owing to (3.58), (3.66) and (3.67), one can verify that

$$\forall\, (\lambda,P) \in [0,1] \times \mathcal{P}_R(\mathcal{X}),\ m_{0,3}(\lambda,P) = m_{1,3}(1-\lambda,P). \tag{3.68}$$

Lemma 9 (Continuity)**.** *All of the following is true*

(i) $\Lambda'_{0,\cdot}(\cdot)$ *is continuous on* $(0,1] \times \mathcal{P}_R(\mathcal{X})$.

(ii) $\Lambda''_{0,\cdot}(\cdot)$ *is continuous on* $(0,1] \times \mathcal{P}_R(\mathcal{X})$.

(iii) $m_{0,3}(\cdot,\cdot)$ *is continuous on* $(0,1] \times \mathcal{P}_R(\mathcal{X})$.

(iv) $D(W^-_{R,\cdot}\|Q^*_{R,\cdot}|\cdot)$ *is continuous on* $\mathcal{P}_R(\mathcal{X})$. ♦

Proof. The proof is given in Appendix B.9. □

Lemma 10. *Fix arbitrary $C > R > R_\infty$ and $P \in \mathcal{P}_R(\mathcal{X})$. For any $r \in \mathbb{R}^+$, we have*

$$\tilde{e}_{SP}(R, P, r) = \max_{s \in \mathbb{R}_+} \{-sr + e_0(s, P)\}, \tag{3.69}$$

where

$$e_0(s, P) := -(1+s) \sum_{x \in \mathcal{S}(P)} P(x) \ln \sum_{y \in \mathcal{S}(W(\cdot|x))} W(y|x)^{1/(1+s)} W_{R,P}^-(y|x)^{s/(1+s)}, \tag{3.70}$$

for any $s \in \mathbb{R}_+$. ♦

Proof. We have,

$$\tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, r) = \inf_{V \in \mathcal{P}(\mathcal{Y}|\mathcal{X}) \,:\, \mathrm{D}(V\|W_{R,P}^-|P) \le r} \mathrm{D}(V\|W|P) \tag{3.71}$$

$$= \max_{s \in \mathbb{R}_+} \min_{V \in \mathcal{P}(\mathcal{Y}|\mathcal{X})} \Big\{ \mathrm{D}(V\|W|P) + s(\mathrm{D}(V\|W_{R,P}^-|P) - r) \Big\} \tag{3.72}$$

$$= \max_{s \in \mathbb{R}_+} \left\{ -sr + \sum_{x \in \mathcal{S}(P)} P(x) \min_{V(\cdot|x)} \Big[\mathrm{D}(V(\cdot|x)\|W(\cdot|x)) + s\mathrm{D}(V(\cdot|x)\|W_{R,P}^-(\cdot|x)) \Big] \right\} \tag{3.73}$$

$$= \max_{s \in \mathbb{R}_+} \{-sr + e_0(s, P)\}, \tag{3.74}$$

where (3.72) follows since Slater's condition holds (cf., [55, Corollary 28.2.1]), (3.74) follows by noting that

$$V_{P,s}^*(y|x) := \frac{W(y|x)^{1/(1+s)} W_{R,P}^-(y|x)^{s/(1+s)}}{\sum_{\tilde{y} \in \mathcal{Y}} W(\tilde{y}|x)^{1/(1+s)} W_{R,P}^-(\tilde{y}|x)^{s/(1+s)}}, \tag{3.75}$$

attains the minimum in (3.73) for any $x \in \mathcal{S}(P)$ and recalling (3.70). □

Corollary 1. *Consider any $C > R > R_\infty$, $P \in \mathcal{P}_R(\mathcal{X})$. For all $r \in \mathbb{R}^+$, the set of maximizers of* (3.69) *is exactly $\partial \tilde{e}_{SP}(R, P, \cdot)(r)$.* ♦

Proof. Proof follows exactly the same lines as that of Claim 14. □

Lemma 11 (Differentiability of the shifted exponent)**.** *Let $C > R > R_\infty$ and $r \in \mathbb{R}^+$ be given.*

$$s^*(R, \cdot, r) \,:\, \mathcal{P}_R(\mathcal{X}) \to \mathbb{R}_+,\ s.t.\ s^*(R, P, r) := -\frac{\partial \tilde{e}_{SP}(R, P, r)}{\partial r},\ \forall P \in \mathcal{P}_R(\mathcal{X}), \tag{3.76}$$

is a well-defined function. ♦

Proof. Consider any $P \in \mathcal{P}_R(\mathcal{X})$. For any $s \in \mathbb{R}_+$, (3.70), (3.50), (3.51), (3.55) and (3.57) imply that

$$\frac{\partial^2 e_o(s, P)}{\partial s^2} = -\frac{1}{(1+s)^3}\Lambda''_{0,P}\left(\frac{s}{1+s}\right) < 0. \tag{3.77}$$

where the inequality follows from the positive variance lemma, i.e., Lemma 8. Equation (3.77) ensures the strict concavity of the cost function of (3.69) and hence the uniqueness of the maximizer. Recalling Corollary 1, this implies that (3.76) is well-defined. □

The shifted exponent lemma, i.e., Lemma 7, and the differentiability of the shifted exponent, i.e., Lemma 11, immediately implies the following result.

Corollary 2. *Given any $C > R > R_\infty$ and $P \in \mathcal{P}_R(\mathcal{X})$ and ,*

$$\left.\frac{\partial e_{SP}(R, P, \tilde{r})}{\partial \tilde{r}}\right|_{\tilde{r}=r} = -s^*(R, P, r - D(W^-_{R,P}\|Q^*_{R,P}|P)), \tag{3.78}$$

for any $r > D(W^-_{R,P}\|Q^*_{R,P}|P)$. ♦

Throughout the rest, unless stated otherwise, suppose $C(W) > R > R_\infty$ and $P \in \mathcal{P}_R(\mathcal{X})$ be arbitrary and fixed.

Definition 7. *Consider any $C > R > R_\infty$ and $P \in \mathcal{P}_R(\mathcal{X})$. Given any $z \in \mathbb{R}$,*

$$\Lambda^*_{0,P}(z) := \sup_{\lambda \in \mathbb{R}} \{\lambda z - \Lambda_{0,P}(\lambda)\}, \tag{3.79}$$

$$\Lambda^*_{1,P}(z) := \sup_{\lambda \in \mathbb{R}} \{\lambda z - \Lambda_{1,P}(\lambda)\}. \tag{3.80}$$

◊

Lemma 12 (Regularity)**.** *Fix any $C > R > R_\infty$ and $P \in \mathcal{P}_R(\mathcal{X})$. For any $0 < r < D(W\|W^-_{R,P}|P)$,*

(i) $\Lambda^*_{0,P}(\tilde{e}_{SP}(R,P,r) - r) = \tilde{e}_{SP}(R,P,r)$.

(ii) $\Lambda^*_{1,P}(r - \tilde{e}_{SP}(R,P,r)) = r$.

(iii) There exists a unique $\eta(R,P,r) \in (0,1)$, such that $\Lambda'_{0,P}(\eta(R,P,r)) = \tilde{e}_{SP}(R,P,r) - r$. In particular, $\eta(R,P,r) = \frac{s^*(R,P,r)}{1+s^*(R,P,r)}$. ♦

Proof. The proof is given in Appendix B.10. □

Next, we claim that

$$0 < r(R,P) < \mathrm{I}(P;W) - \mathrm{D}(W^-_{R,P}\|Q^*_{R,P}|P) \le \mathrm{D}(W\|W^-_{R,P}|P). \tag{3.81}$$

The first inequality follows from the positivity of $r(R,P)$ lemma, i.e., Lemma 6. The second inequality is clear from the definition of $r(R,P)$ and the fact that $P \in \mathcal{P}_R(\mathcal{X})$. The last inequality follows by noting

$$\mathrm{D}(W^-_{R,P}\|Q^*_{R,P}|P) + \mathrm{D}(W\|W^-_{R,P}|P) = \mathrm{D}(W\|Q^*_{R,P}|P) \ge \min_{Q\in\mathcal{P}(\mathcal{Y})} \mathrm{D}(W\|Q|P) = \mathrm{I}(P;W), \tag{3.82}$$

where the first equality follows from the item (i) of Lemma 6 and the last one follows from (B.85). Hence, (3.81) follows.

Further, define

$$\Upsilon(W,R,\nu) := \max_{P\in\mathcal{P}_{R,\nu}(\mathcal{X})} \mathrm{D}(W\|Q^*_{R,P}|P), \quad H := \left[\frac{\frac{\nu}{2\Upsilon(W,R,\nu)}}{1+\frac{\nu}{2\Upsilon(W,R,\nu)}}, 1\right]. \tag{3.83}$$

Since $\mathrm{E_{SP}}(\cdot,\cdot)$ is continuous (cf., Lemma 30), $\mathcal{P}_{R,\nu}$ is closed and therefore, by noting the boundedness of $\mathcal{P}(\mathcal{X})$, is compact. Further, owing to the continuity of $\mathrm{D}(W\|Q^*_{R,\cdot}|\cdot)$ (cf., item (iv) of the continuity lemma, i.e., Lemma 9) and the compactness of $\mathcal{P}_{R,\nu}(\mathcal{X})$, $\Upsilon(W,R,\nu)$ is well-defined and finite.

Lemma 13. *For any* $P \in \mathcal{P}_{R,\nu}(\mathcal{X})$

$$\eta(R,P,r) \in H,\ \forall\, r \in (0, r(P,R)]. \tag{3.84}$$

♦

Proof. Let $P \in \mathcal{P}_{R,\nu}(\mathcal{X})$ be arbitrary. Owing to item (iii) of the regularity lemma, i.e., Lemma 12, it suffices to prove that for all $r \in (0, r(P,R)]$

$$\eta(R,P,r) \geq \frac{\frac{\nu}{2\Upsilon(W,R,\nu)}}{1+\frac{\nu}{2\Upsilon(W,R,\nu)}}. \tag{3.85}$$

Moreover, the fact that $\eta(R,P,r) = s^*(R,P,r)/(1+s^*(R,P,r))$ (cf., item (iii) of Lemma 12), (3.81), the convexity and the non-increasing property of $\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,\cdot)$, it suffices to show (3.85) for $r = r(R,P)$. The differentiability of the shifted exponent lemma, i.e., Lemma 11, and Corollary 2 imply that

$$s^*(R,P,r(R,P)) = -\left.\frac{\partial \tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r)}{\partial r}\right|_{r=r(R,P)} = -\left.\frac{\partial \mathrm{e}_{\mathrm{SP}}(R,P,r)}{\partial r}\right|_{r=R}. \tag{3.86}$$

Moreover, using the convexity and the non-increasing property of $\mathrm{e}_{\mathrm{SP}}(R,P,\cdot)$, one can see that

$$-\left.\frac{\partial \mathrm{e}_{\mathrm{SP}}(R,P,r)}{\partial r}\right|_{r=R} \geq \frac{\nu}{2(\mathrm{e}_{\mathrm{SP}}^{-1}(R,P,\cdot)(\nu/2)-R)} \geq \frac{\nu}{2\Upsilon(W,R,\nu)}, \tag{3.87}$$

where the last inequality follows by noting that $\mathrm{e}_{\mathrm{SP}}(R,P,r) = 0$ for all $r \geq \mathrm{D}(W\|Q^*_{R,P}|P)$. By combining (3.86) and (3.87), we deduce that

$$s^*(R,P,r(R,P)) \geq \frac{\nu}{2\Upsilon(W,R,\nu)}. \tag{3.88}$$

Since $\eta(R,P,r) = s^*(R,P,r)/(1+s^*(R,P,r))$, (3.88) implies (3.84). □

Finally, we define the following:

$$\overline{M}(\nu,W,R) := \max_{(\lambda,P)\in H\times\mathcal{P}_{R,\nu}} \frac{m_{0,3}(\lambda,P)}{\Lambda''_{0,P}(\lambda)}, \tag{3.89}$$

$$\overline{V}(\nu,W,R) := \max_{(\lambda,P)\in H\times\mathcal{P}_{R,\nu}} \Lambda''_{0,P}(\lambda), \tag{3.90}$$

$$\underline{V}(\nu,W,R) := \min_{(\lambda,P)\in H\times\mathcal{P}_{R,\nu}} \Lambda''_{0,P}(\lambda), \tag{3.91}$$

where H is as defined prior to Lemma 13. Recalling the compactness of H and $\mathcal{P}_{R,\nu}(\mathcal{X})$, the positive variance lemma, i.e., Lemma 8, and the continuity lemma, i.e., Lemma 9, ensure that (3.89), (3.90) and (3.91) are well-defined, positive and finite.

Define $K_{\max} := \overline{M}(\nu, W, R)2\sqrt{2\pi}$ and note that $K_{\max} \in \mathbb{R}^+$. Also, let $N \in \mathbb{Z}^+$ be sufficiently large, such that

$$\sqrt{N} \geq \frac{1 + (1 + K_{\max})^2}{\sqrt{\underline{V}(\nu, W, R)}}, \tag{3.92}$$

and consider such an N from now on.

Next, we apply the concentration lemma, i.e., Lemma 5, to α_N to deduce a lower bound. Observe that (3.56), (3.57) and the positive variance proposition, i.e., Proposition 8, and item (iii) of the regularity lemma, i.e., Lemma 12, ensures the fulfillment of the assumptions under which Lemma 5 is stated. Hence, we apply (3.3) to $W\left\{A_N^c|\mathbf{x}^N\right\}$ (cf., (3.48), (3.49) and (3.92)) to deduce

$$\alpha_N \geq \frac{K}{\sqrt{N}} \exp\{-N\Lambda_{0,P}^*(\tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, r_N(R, P)) - r_N(R, P))\}, \tag{3.93}$$

where we define

$$K := \frac{e^{-K_{\max}}}{2\sqrt{2\pi\overline{V}(\nu, W, R)}}. \tag{3.94}$$

Note that K only depends on W, R and ν.

Further, recalling the definition of β_N (cf., (3.47) and (3.49)) one can check that

$$\beta_N \geq W_{R,P}^- \left\{ \frac{1}{N} \sum_{n=1}^{N} \ln \frac{W(Y_n|x_n)}{W_{R,P}^-(Y_n|x_n)} \geq \tilde{r}_N(R, P) - \tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, \tilde{r}_N(R, P)) \mid \mathbf{x}^N \right\}. \tag{3.95}$$

Next, we apply the concentration lemma, i.e., Lemma 5, to the right side of (3.95) by noting the fact that the explanations provided prior to (3.93) are still valid (recall (3.58) and (3.59)) and infer the following

$$\beta_N \geq \frac{K}{\sqrt{N}} e^{-N\Lambda_{1,P}^*(\tilde{r}_N(R,P) - \tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,\tilde{r}_N(R,P)))} = \frac{K}{\sqrt{N}} e^{-N\tilde{r}_N(R,P)} = \frac{KN^{\zeta}}{e} e^{-Nr(R,P)}, \tag{3.96}$$

where the first equality follows from item (ii) of the regularity lemma, i.e., Lemma 12.

If we let $N \in \mathbb{Z}^+$ to be sufficiently large, so that

$$\frac{KN^{\zeta}}{e} > 1, \tag{3.97}$$

then (3.96) implies that $\beta_N > e^{-Nr(P,R)}$. Since our test is a likelihood ratio test, by violating the constraint we can only improve the optimal error performance, and hence (cf., (3.93))

$$\tilde{\alpha}_N(r(P,R)) \geq \alpha_N \geq \frac{K}{\sqrt{N}} e^{-N\Lambda^*_{0,P}(\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r_N(R,P))-r_N(R,P))}, \tag{3.98}$$

which, in turn, implies that (cf., (3.42))

$$\mathrm{P_e}(f,\varphi) \geq \frac{K}{\sqrt{N}} e^{-N\Lambda^*_{0,P}(\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r_N(R,P))-r_N(R,P))}. \tag{3.99}$$

3.2.5 Approximation of the exponent

In this final section of the chapter, we approximate the exponent in (3.99) to conclude the proof.

To begin with, we note that (e.g., [21, Exercise 2.2.24]) $\Lambda^*_{0,P}(\cdot)$ is a smooth function over $(-\mathrm{D}(W\|W^-_{R,P}|P), \mathrm{D}(W^-_{R,P}\|W|P))$, i.e., $\Lambda^*_{0,P}(\cdot) \in C^\infty(-\mathrm{D}(W\|W^-_{R,P}|P), \mathrm{D}(W^-_{R,P}\|W|P))$. Moreover, with the aid of the inverse function theorem and item (iii) of the regularity lemma, i.e., Lemma 12, one can check that for any $r \in (0, \mathrm{D}(W\|W^-_{R,P}|P))$,

$$\Lambda^{*\prime}_{0,P}(\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r) - r) = \eta(R,P,r), \quad \Lambda^{*\prime\prime}_{0,P}(\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r) - r) = \frac{1}{\Lambda^{\prime\prime}_{0,P}(\eta(R,P,r))}. \tag{3.100}$$

Define[9]

$$\delta(R,\nu,W) := R - \max_{P \in \mathcal{P}_{R,\nu}(\mathcal{X})} \mathrm{D}(W^-_{R,P}\|Q^*_{R,P}|P). \tag{3.101}$$

[9]Owing to item (iv) of the continuity lemma, i.e., Lemma 9, and the compactness of $\mathcal{P}_{R,\nu}(\mathcal{X})$, the maximum is well-defined.

Observe that owing to Lemma 6, $\delta(R, \nu, W) > 0$. Hence, one can choose $N \in \mathbb{Z}^+$ to be sufficiently large, such that $\epsilon_N \leq \delta(R, \nu, W)/2$. Consider such an N from now on.

Using Taylor's theorem, for some

$$\bar{x} \in (\tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, r(R, P)) - r(R, P), \tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, r_N(R, P)) - r_N(R, P)), \tag{3.102}$$

we have

$$\begin{aligned}
\Lambda^*_{0,P}(\tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, r_N(R, P)) - r_N(R, P)) = {} & \Lambda^*_{0,P}(\tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, r(R, P)) - r(R, P)) + \{r(R, P) \\
& + \tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, r_N(R, P)) - \tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, r(R, P)) \\
& - r_N(R, P)\} \Lambda^{*\prime}_{0,P}(\tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, r(R, P)) - r(R, P)) \\
& + \frac{\Lambda^{*\prime\prime}_{0,P}(\bar{x})}{2} \{[\tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, r_N(R, P)) - r_N(R, P)] - \\
& [\tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, r(R, P)) - r(R, P)]\}^2 \qquad (3.103) \\
= {} & \Lambda^*_{0,P}(\tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, r(R, P)) - r(R, P)) \\
& + \epsilon_N \Lambda^{*\prime}_{0,P}(\tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, r(R, P)) - r(R, P)) \\
& + \Lambda^{*\prime}_{0,P}(\tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, r(R, P)) - r(R, P)) \\
& [\tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, r_N(R, P)) - \tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, r(R, P))] \\
& + \frac{\Lambda^{*\prime\prime}_{0,P}(\bar{x})}{2} \{[\tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, r_N(R, P)) - r_N(R, P)] - \\
& [\tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, r(R, P)) - r(R, P)]\}^2 \qquad (3.104) \\
= {} & \Lambda^*_{0,P}(\tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, r(R, P)) - r(R, P)) + \eta(R, P, r(R, P)) \\
& \epsilon_N + \eta(R, P, r(R, P)) \\
& [\tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, r_N(R, P)) - \tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, r(R, P))] \\
& + \frac{\Lambda^{*\prime\prime}_{0,P}(\bar{x})}{2} \{[\tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, r_N(R, P)) - r_N(R, P)] - \\
& [\tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, r(R, P)) - r(R, P)]\}^2 , \qquad (3.105)
\end{aligned}$$

where (3.104) follows by recalling the fact that $r_N(R, P) = r(R, P) - \epsilon_N$ and (3.105) follows from (3.100) by recalling (3.81).

Recalling item (i) of the regularity lemma, i.e., Lemma 12, (3.105) implies that

$$\Lambda^*_{0,P}(\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r_N(R,P))-r_N(R,P))\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r_N(R,P))=\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r_N(R,P))$$
$$+\epsilon_N\frac{\eta(R,P,r(R,P))}{1-\eta(R,P,r(R,P))}+\frac{\Lambda^{*\prime\prime}_{0,P}(\bar{x})\epsilon_N^2}{2(1-\eta(R,P,r(R,P)))}$$
$$\left(1+\frac{\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r_N(R,P))-\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r(R,P))}{\epsilon_N}\right)^2, \tag{3.106}$$

for some $\bar{x}\in(\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r(R,P))-r(R,P),\ \tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r_N(R,P))-r_N(R,P))$.

Note that, since $\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,\cdot)-(\cdot)$ is strictly decreasing and continuous, there exists a unique $\bar{r}\in(r(R,P)-\delta(R,\nu,W)/2,r(R,P))$ such that[10] $\bar{x}=\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,\bar{r})-\bar{r}$ and hence (recall (3.100) and (3.81))

$$\Lambda^{*\prime\prime}_{0,P}(\bar{x})=1/\Lambda''_{0,P}(\eta(R,P,\bar{r})). \tag{3.107}$$

Moreover, item (iii) of the regularity lemma, i.e., Lemma 12, implies that

$$\frac{\eta(R,P,r(R,P))}{1-\eta(R,P,r(R,P))}=s^*(R,P,r(R,P)). \tag{3.108}$$

Plugging (3.107) and (3.108) into (3.106), we deduce that

$$\Lambda^*_{0,P}(\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r_N(R,P))-r_N(R,P))=\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r_N(R,P)) \tag{3.109}$$
$$=\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r(R,P))+s^*(R,P,r(R,P))\epsilon_N$$
$$+\frac{1+s^*(R,P,r(R,P))}{2\Lambda''_{0,P}(\eta(R,P,\bar{r}))}\epsilon_N^2$$
$$\left(1+\frac{\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r_N(R,P))-\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r(R,P))}{\epsilon_N}\right)^2, \tag{3.110}$$

Moreover, using exactly the same arguments as above, but this time with a first-order Taylor series, we infer that

$$\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r_N(R,P))=\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r(R,P))+\epsilon_N\frac{\eta(R,P,\tilde{r})}{1-\eta(R,P,\tilde{r})}, \tag{3.111}$$

[10] Actually, $\bar{r}\in(r_N(R,P),r(R,P))$.

for some $\tilde{r} \in (r_N(R,P), r(R,P))$.

On account of the convexity and the non-increasing property of $\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,\cdot)$, we have

$$\left|\frac{\partial \tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r')}{\partial r'}\right| \leq \frac{\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,0)}{\delta(R,\nu,W)/2}, \tag{3.112}$$

for any $r_N(R,P) \leq r' \leq r(R,P)$.

By noting that $\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,0) = \mathrm{D}(W^-_{R,P}\|W|P) = \Lambda'_{0,P}(1)$ and letting[11]

$$F := \max_{P\in\mathcal{P}_{R,\nu}(\mathcal{X})} \Lambda'_{0,P}(1) < \infty, \tag{3.113}$$

(3.112) further implies that

$$\frac{\eta(R,P,r')}{1-\eta(R,P,r')} = s^*(R,P,r') = \left|\frac{\partial \tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r')}{\partial r'}\right| \leq \frac{F}{\delta(R,\nu,W)/2} =: \tilde{s} < \infty, \tag{3.114}$$

for any $r_N(R,P) \leq r' \leq r(R,P)$.

Plugging (3.91), (3.111) and (3.114) into (3.110) yields

$$\begin{aligned}
\Lambda^*_{0,P}(\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r_N(R,P)) - r_N(R,P)) &= \tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r_N(R,P)) && (3.115)\\
&\leq \tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r(R,P)) + s^*(R,P,r(R,P))\epsilon_N \\
&\quad \left[1 + \epsilon_N \frac{(1+\tilde{s})^2[1+s^*(R,P,r(R,P))]}{2\underline{V}(\nu,W,R)s^*(R,P,r(R,P))}\right] && (3.116)\\
&= \mathrm{E}_{\mathrm{SP}}(R,P) + s^*(R,P,r(R,P))\epsilon_N \\
&\quad \left[1 + \epsilon_N \frac{(1+\tilde{s})^2[1+s^*(R,P,r(R,P))]}{2\underline{V}(\nu,W,R)s^*(R,P,r(R,P))}\right] && (3.117)\\
&\leq \mathrm{E}_{\mathrm{SP}}(R,P) + s^*(R,P,r(R,P))\epsilon_N \\
&\quad \left[1 + \epsilon_N \frac{(1+\tilde{s})^2}{2\underline{V}(\nu,W,R)}\left(1 + \frac{2\Upsilon(W,R,\nu)}{\nu}\right)\right], && (3.118)
\end{aligned}$$

where (3.117) follows from the equality of the exponents proposition, i.e., Proposition 6, and the shifted exponent lemma, i.e., Lemma 7, and (3.118) follows from (3.108) and Lemma 13.

[11] Owing to the continuity lemma, i.e., Lemma 9, the maximum is well-defined and finite.

Consider $\zeta \in \mathbb{R}^+$ that is fixed in the definition of ϵ_N. Since $\tilde{s}$ is bounded, $\underline{V}(\nu, W, R)$ and $\Upsilon(W, R, \nu)$ and the fact that $\nu > 0$, one can deduce that for all sufficiently large N,

$$\epsilon_N \frac{(1+\tilde{s})^2}{2\underline{V}(\nu, W, R)} \left(1 + \frac{2\Upsilon(W, R, \nu)}{\nu}\right) \leq \zeta, \tag{3.119}$$

and hence (3.118) reduces to the following, for all sufficiently large N,

$$\Lambda^*_{0,P}(\tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, r_N(R, P)) - r_N(R, P)) \leq \mathrm{E}_{\mathrm{SP}}(R, P) + s^*(R, P, r(R, P))\epsilon_N(1 + \zeta). \tag{3.120}$$

Next, we claim that

$$s^*(R, P, r(R, P)) = \rho^*_{R,P}. \tag{3.121}$$

To prove this, we first claim that $\rho^*_{R,P}$ is a Lagrange multiplier of $\mathrm{e}_{\mathrm{SP}}(R, P)$. To see this, first note that

$$\begin{aligned}
\mathrm{e}_{\mathrm{SP}}(R, P) &= \mathrm{E}_{\mathrm{SP}}(R, P) && (3.122)\\
&= K_{R,P}(\rho^*_{R,P}, Q^*_{R,P}) && (3.123)\\
&= \max_{\rho \in \mathbb{R}_+} K_{R,P}(\rho, Q^*_{R,P}) && (3.124)\\
&= \max_{\rho \in \mathbb{R}_+} \min_{V \in \mathcal{P}(\mathcal{Y}|\mathcal{X})} \left[\mathrm{D}(V\|W|P) + \rho(\mathrm{D}(V\|Q^*_{R,P}|P) - R)\right], && (3.125)
\end{aligned}$$

where (3.122) follows from the equality of the exponents proposition, i.e., Proposition 6, (3.123) follows from the saddle-point proposition, i.e., Proposition 2, and the uniqueness of the saddle-point proposition, i.e., Proposition 3, (3.124) follows by noting that $(\rho^*_{R,P}, Q^*_{R,P})$ is the unique saddle-point of $K_{R,P}(\cdot, \cdot)$ and (3.125) follows by solving the convex minimization problem. Hence, (3.125) gives the Lagrangian dual of $\mathrm{e}_{\mathrm{SP}}(R, P)$.

Further, one can also check that

$$\begin{aligned}
&\max_{\rho \in \mathbb{R}_+} \min_{V \in \mathcal{P}(\mathcal{Y}|\mathcal{X})} \left[\mathrm{D}(V\|W|P) + \rho(\mathrm{D}(V\|Q^*_{R,P}|P) - R)\right]\\
&= \min_{V \in \mathcal{P}(\mathcal{Y}|\mathcal{X})} \left[\mathrm{D}(V\|W|P) + \rho^*_{R,P}(\mathrm{D}(V\|Q^*_{R,P}|P) - R)\right]. && (3.126)
\end{aligned}$$

(3.125) and (3.126) implies that $\rho^*_{R,P}$ is a Lagrange multiplier of $\mathrm{e}_{\mathrm{SP}}(R,P)$. Moreover, the sub-differential characterization of the Lagrange multipliers (e.g., [55, Theorem 29.1]) along with the differentiability of the shifted exponent lemma, i.e., Lemma 11, and Corollary 2, implies (3.121).

Plugging (3.121) into (3.120), we deduce that

$$\Lambda^*_{0,P}(\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r_N(R,P))-r_N(R,P))\leq \mathrm{E}_{\mathrm{SP}}(R,P)+\rho^*_{R,P}\epsilon_N(1+\zeta). \tag{3.127}$$

Define $\mathcal{P}^*_R(\mathcal{X}):=\{P\in\mathcal{P}(\mathcal{X}):\mathrm{E}_{\mathrm{SP}}(R,P)=\mathrm{E}_{\mathrm{SP}}(R)\}\neq\emptyset$. Observe that $\mathcal{P}^*_R$ is a compact set. Also, for any $P\in\mathcal{P}(\mathcal{X})$, $|P-\mathcal{P}^*_R|:=\inf_{Q\in\mathcal{P}^*_R}\|Q-P\|_1$. For any $\theta\in\mathbb{R}^+$, $\mathcal{P}_\theta(\mathcal{X}):=\left\{P\in\mathcal{P}_{R,\nu}(\mathcal{X}):|P-\mathcal{P}^*_R(\mathcal{X})|\geq\theta\right\}$.

Observe that (recall (3.5) and the differentiability of $\mathrm{E}_{\mathrm{SP}}(\cdot,P)$ proposition, i.e., Proposition 4)

$$\rho^*_R=\max_{P\in\mathcal{P}^*_R(\mathcal{X})}\rho^*_{R,P}, \tag{3.128}$$

where owing to the compactness of $\mathcal{P}^*_R(\mathcal{X})$ and the continuity of $\rho^*_{R,\cdot}$, the maximum is well-defined and finite.

Since $\mathcal{P}_{R,\nu}(\mathcal{X})$ is compact, $\rho^*_{R,\cdot}$ is uniformly continuous on this set, equivalently

$$\forall\upsilon\in\mathbb{R}^+,\ \exists\, a(\upsilon)\in\mathbb{R}^+,\ \text{s.t. }\forall P,Q\in\mathcal{P}_{R,\nu}(\mathcal{X}),\ \|P-Q\|_1<a(\upsilon)\Rightarrow|\rho^*_{R,P}-\rho^*_{R,Q}|<\zeta. \tag{3.129}$$

Consider $\zeta\in\mathbb{R}^+$ that is fixed in the definition of ϵ_N and let $a(\zeta)\in\mathbb{R}^+$ be chosen such that (3.129) holds.

If $P\in\mathcal{P}_{R,\nu}(\mathcal{X})-\mathcal{P}_{a(\zeta)}(\mathcal{X})$, then (3.129) ensures that $\rho^*_{R,P}\leq\rho^*_R+\zeta$, which, in turn, implies that

$$\exp(-N\epsilon_N(1+\zeta)\rho^*_{R,P})\geq N^{-(1+\zeta)\left(\frac{1}{2}+\zeta\right)(\rho^*_R+\zeta)}. \tag{3.130}$$

Suppose $P \in \mathcal{P}_{a(\zeta)}(\mathcal{X})$. Since $\mathrm{E_{SP}}(R) - \max_{P \in \mathrm{cl}(\mathcal{P}_{a(\zeta)})} \mathrm{E_{SP}}(R, P) \in \mathbb{R}^+$, one can check that for all sufficiently large N, uniformly over $\mathcal{P}_{a(\zeta)}(\mathcal{X})$, we have

$$\exp\left(-N\left[\mathrm{E_{SP}}(R, P) + \epsilon_N(1+\zeta)\rho^*_{R,P}\right]\right) \geq \frac{e^{-N\mathrm{E_{SP}}(R)}}{N^{(1+\zeta)\left(\frac{1}{2}+\zeta\right)\rho^*_R}}. \tag{3.131}$$

Equations (3.99), (3.127), (3.130) and (3.131) imply (3.8). □

CHAPTER 4

REFINEMENT OF THE RANDOM CODING BOUND

In this chapter, we improve the sub-exponential term in the random coding bound. As noted before, the analysis in this chapter, as well as Chapter 3, can be considered to be the analogous of Bahadur-Rao theorem for i.i.d. sums of random variables within channel coding. In light of the analogies of the small, medium and large error probability regimes to large deviations, moderate deviations and central limit theorem in i.i.d. sums, which were pointed out in Section 1.2, one might expect the optimal order of the sub-exponential term for channel coding to be $\Theta(1/\sqrt{N})$, in conjunction with Bahadur-Rao theorem. However, the lower bound derived in Chapter 3 has an extra term related to the slope of $\mathrm{E_{SP}}(R)$ that suggests that $\Theta(1/\sqrt{N})$ is a pessimistic conjecture, provided that one can prove a matching upper bound.

The aim of this chapter is to supply such an upper bound. Specifically, for a large class of channels, we prove an upper bound on $\mathrm{P_e}(N, R)$ with a pre-factor having an extra term that is related to the slope of $\mathrm{E_r}(R)$, similar to the result in Chapter 3. However, our analysis necessitates us to distinguish a small class of channels, for which we prove an upper bound with $O(1/\sqrt{N})$ pre-factor. Although one might think that this is a deficiency of the analysis, binary erasures channel (BEC) is a concrete example against this thought, because in his classical paper [24], Elias has proved that for BEC the optimal order of the pre-factor is $\Theta(1/\sqrt{N})$. Hence, there is at least a dichotomy[1] of channels as far as the optimal order of the pre-factor goes.

The main idea to prove the results in this chapter is to reduce the problem of upper bounding the error probability of a random code to large deviations events involving

[1] In Chapter 5, we prove that for symmetric channels with positive dispersion, there are *exactly* two subclasses of channels, i.e., there *is* a dichotomy of channels with respect to the optimal order of the sub-exponential term.

sums of independent random variables and vectors. Exact asymptotics-type results will then be applied. This reduction is nontrivial and forms the main technical contribution of the chapter.

4.1 Definitions and statement of the results

Given a DMC $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$, $Q \in \mathcal{P}(\mathcal{X})$ and $R \in \mathbb{R}_+$,

$$\mathrm{E_r}(R, Q) := \max_{0 \le \rho \le 1} \{-\rho R + \mathrm{E_o}(\rho, Q)\}. \tag{4.1}$$

For any $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$, $Q \in \mathcal{P}(\mathcal{X})$, $N \in \mathbb{Z}^+$ and $R \in \mathbb{R}_+$ the *ensemble average error probability conditioned on the message m* (resp. *ensemble average error probability*) of an (N, R) random code with codewords generated by using Q along with a maximum likelihood decoder[2] is denoted by $\bar{\mathrm{P}}_{\mathrm{e},m}(Q, N, R)$ (resp. $\bar{\mathrm{P}}_{\mathrm{e}}(Q, N, R)$).

Further,

$$\mathcal{S}_Q := \{(x, y) \in \mathcal{X} \times \mathcal{Y} : Q(x)W(y|x) > 0\}, \tag{4.2}$$

$$\tilde{\mathcal{S}}_Q := \{(x, y, z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{X} : Q(x)W(y|x)Q(z)W(y|z) > 0\}, \tag{4.3}$$

$$\mathcal{X}_y := \{x \in \mathcal{X} : W(y|x) > 0\}. \tag{4.4}$$

Given a $(Q, W) \in \mathcal{P}(\mathcal{X}) \times \mathcal{P}(\mathcal{Y}|\mathcal{X})$ pair, the following property plays a crucial role in our analysis.

Definition 8 (Singularity[3])**.** *$W(y|x) = W(y|z)$, for all $(x, y, z) \in \tilde{\mathcal{S}}_Q$.* $\lozenge$

A $(Q, W) \in \mathcal{P}(\mathcal{X}) \times \mathcal{P}(\mathcal{Y}|\mathcal{X})$ pair is called nonsingular (resp. singular) provided that

[2] We assume that the ties are broken in such a way that always results in an error. However, this assumption increases the error probability by at most a factor of 2.

[3] We thank Alfred Hero for encouraging us to use the name singular.

Definition 8 does not hold (resp. holds). The set of all nonsingular (resp. singular) (Q, W) pairs is denoted by $\mathcal{P}_{\text{ns}}$ (resp. $\mathcal{P}_{\text{s}}$)

A channel W is called *nonsingular at rate R* provided that there exists $Q \in \mathcal{P}(\mathcal{X})$ with $\mathrm{E_r}(R, Q) = \mathrm{E_r}(R)$ such that (Q, W) pair is nonsingular. Similarly, a channel is called *singular at rate R* if for all $Q \in \mathcal{P}(\mathcal{X})$ with $\mathrm{E_r}(R, Q) = \mathrm{E_r}(R)$, (Q, W) pair is singular.

Remark 11. *Consider any $(Q, W) \in \mathcal{P}(\mathcal{X}) \times \mathcal{P}(\mathcal{Y}|\mathcal{X})$ pair.*

(i) Definition 8 can be viewed as a condition that ensures that when a random code with distribution Q is used for transmission through channel W, the optimal decoding algorithm, given the channel output, checks feasibility of the codewords.

(ii) In his investigation of the zero undetected error capacity[4] of discrete memoryless channels, Telatar uses a property similar to Definition 8. In particular, he proves that the zero undetected error capacity is equal to (Shannon) capacity for "channels for which the non-zero values of $W(y|x)$ depend only on y" [68, pg. 51]. This result supports the operational interpretation given in item (i) above.

(iii) Singularity also plays a role in the third-order term of the normal approximation for a DMC [51, Section 3.4.5]. Specifically, Polyanskiy defines [51, Eq. (3.296)]

$$V^r(Q, W) := \sum_{x,y} Q(x)W(y|x) \left[\ln \frac{W(y|x)}{q(y)} - \sum_{z} \frac{Q(z)W(y|z)}{q(y)} \ln \frac{W(y|z)}{q(y)} \right]^2, \quad (4.5)$$

where $q(y) := \sum_x Q(x)W(y|x)$, and proves that $\ln \sqrt{N}$ is an achievable third-order term in the normal approximation, provided that $V^r(Q, W) > 0$ [51, Theorem 53].

[4] For the definition of zero undetected error capacity, see [68, pg. 42].

By noticing

$$[V^r(Q,W)=0] \iff \left[\forall\, y\in\mathcal{Y},\ \ln W(y|x)=\sum_z \frac{Q(z)W(y|z)}{q(y)}\ln W(y|z),\ \forall\, x \text{ with } Q(x)W(y|x)>0\right], \tag{4.6}$$

it is easy to see that

$$[V^r(Q,W)=0] \iff \left[W(y|x)=W(y|z),\ \forall\,(x,y,z)\in\tilde{\mathcal{S}}_Q\right]. \tag{4.7}$$

From (4.7)*, it is evident that* $V^r(Q,W)=0$ *is equivalent to saying* (Q,W) *pair is singular. Moreover, in [51, Lemma 52], it is claimed that*

$$[V^r(Q,W)=0] \iff [\forall\,(x,y,y')\ :\ W(y|x)=W(y'|x) \text{ or } Q(x)W(y|x)=0]. \tag{4.8}$$

By choosing $Q=U_{\mathcal{X}}$ *and* W *as BEC with parameter* $\delta\in(0,1)$*, one can verify that* $V^r(Q,W)=0$*, via elementary calculation. Evidently, this* (Q,W) *pair does not satisfy the right side of* (4.8) *and hence* (4.8) *is incorrect.*

(iv) For an explanation of our reasoning for calling Definition 8 singular*, see Remark 15.* $\diamond$

Lastly, given $W\in\mathcal{P}(\mathcal{Y}|\mathcal{X})$ with $\mathrm{V}>0$,[5] $R\in(R_{\mathrm{cr}},C)$ and that W is nonsingular at rate R, we define[6]

$$\bar{\rho}^*_R := \sup_{Q:\mathrm{E_r}(R,Q)=\mathrm{E_r}(R) \text{ and } (Q,W)\in\mathcal{P}_{\mathrm{ns}}} -\left.\frac{\partial \mathrm{E_r}(r,Q)}{\partial r}\right|_{r=R}. \tag{4.9}$$

Theorem 4. *Let* $W\in\mathcal{P}(\mathcal{Y}|\mathcal{X})$ *be arbitrary with* $V>0$*.*

[5] Since $\mathrm{V}>0$ is equivalent to $R_{\mathrm{cr}}<C$ (e.g., [35, pg. 160]), (R_{cr},C) is nonempty.

[6] Differentiability of $\mathrm{E_r}(\cdot,Q)$ is proved in Lemma 14.

(i) If $Q \in \mathcal{P}(\mathcal{X})$ and $R \in \mathbb{R}_+$ are such that (Q, W) pair is singular and[7] *$R_{cr}(Q) < R < I(Q;W)$, then there exists $K_1 \in \mathbb{R}^+$ that depends on W, R and Q such that for any $m \in \{1, \ldots, \lceil e^{NR} \rceil\}$*

$$\bar{P}_{e,m}(Q, N, R) \leq \frac{K_1}{\sqrt{N}} e^{-NE_r(R,Q)}, \tag{4.10}$$

for all $N \in \mathbb{Z}^+$. Further, there exists an (N, R) code (f, φ) and $\tilde{K}_1 \in \mathbb{R}^+$ that depends on W, R and Q such that

$$P_e(f, \varphi) \leq \frac{\tilde{K}_1}{\sqrt{N}} e^{-NE_r(R,Q)}, \tag{4.11}$$

for all $N \in \mathbb{Z}^+$.

(ii) If $Q \in \mathcal{P}(\mathcal{X})$ and $R \in \mathbb{R}_+$ are such that (Q, W) pair is nonsingular and $R_{cr}(Q) < R < I(Q;W)$, then there exists $K_2 \in \mathbb{R}^+$ that depends on W, R and Q such that for any $m \in \{1, \ldots, \lceil e^{NR} \rceil\}$

$$\bar{P}_{e,m}(Q, N, R) \leq \frac{K_2}{N^{0.5(1+\rho_R^*(Q))}} e^{-NE_r(R,Q)}, \tag{4.12}$$

for all $N \in \mathbb{Z}^+$ where $\rho_R^*(Q) := -\frac{\partial E_r(r,Q)}{\partial r}\Big|_{r=R}$. Further, there exists an (N, R) code (f, φ) and $\tilde{K}_2 \in \mathbb{R}^+$ that depends on W, R and Q such that

$$P_e(f, \varphi) \leq \frac{\tilde{K}_2}{N^{0.5(1+\rho_R^*(Q))}} e^{-NE_r(R,Q)}, \tag{4.13}$$

for all $N \in \mathbb{Z}^+$. ♦

Theorem 4 is proved in Section 4.2 and immediately implies the following.

Corollary 3. *Let $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ be arbitrary with $V > 0$ and $R \in (R_{cr}, C)$.*

(i) If W is singular at rate R, then there exists an (N, R) code (f, φ) and $K_3 \in \mathbb{R}^+$ that depends on R and W such that

$$P_e(f, \varphi) \leq \frac{K_3}{\sqrt{N}} e^{-NE_r(R)}, \tag{4.14}$$

[7] $R_{\mathrm{cr}}(Q) := \frac{\partial \mathrm{E_o}(\rho,Q)}{\partial \rho}\Big|_{\rho=1}$ (e.g., [35, pg. 142]).

for all $N \in \mathbb{Z}^+$.

(ii) If W *is nonsingular at rate* R*, then for any* $\epsilon > 0$*, there exists an* (N, R) *code* (f, φ) *and* $K_4 \in \mathbb{R}^+$ *that depends on* R, W *and* ϵ *such that*

$$P_e(f, \varphi) \leq \frac{K_4}{N^{0.5(1+\bar{\rho}_R^* - \epsilon)}} e^{-NE_r(R)}, \tag{4.15}$$

for all $N \in \mathbb{Z}^+$. ♦

Theorem 5. *Let* $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ *be arbitrary with* $V > 0$ *and* $R \in (R_{cr}, C)$.

(i) The subdifferential of $E_r(\cdot)$ *at* R*, i.e.,* $\partial E_r(R)$*, satisfies*[8]

$$\partial E_r(R) = \operatorname{conv}\left(\left\{ \left.\frac{\partial E_r(r, Q)}{\partial r}\right|_{r=R} : E_r(R, Q) = E_r(R) \right\}\right). \tag{4.16}$$

(ii) Define $\rho_R^* := \max\{|a| : a \in \partial E_r(R)\}$*. If there exists* $Q \in \mathcal{P}(\mathcal{X})$ *such that* $E_r(R, Q) = E_r(R)$*,* (Q, W) *is nonsingular and* $-\left.\frac{\partial E_r(r,Q)}{\partial r}\right|_{r=R} = \rho_R^*$*, then there exists an* (N, R) *code* (f, φ) *and* $K_5 \in \mathbb{R}^+$ *that depends on* W, R *and* Q *such that*

$$P_e(f, \varphi) \leq \frac{K_5}{N^{0.5(1+\rho_R^*)}} e^{-NE_r(R)}, \tag{4.17}$$

for all $N \in \mathbb{Z}^+$*. Moreover,*

$$W(y|x) > 0, \text{ for all } (x, y) \in \mathcal{X} \times \mathcal{Y}, \tag{4.18}$$

is a sufficient condition for the existence of a $Q \in \mathcal{P}(\mathcal{X})$ *with the aforementioned properties.* ♦

Theorem 5 is proved in Section 4.3

[8] As usual, for a given set S, $\operatorname{conv}(S)$ denotes the *convex hull* of S.

Remark 12. *(i) It is evident that ρ_R^*, as defined in item (ii) of Theorem 5, is the absolute value of the left derivative of $E_r(\cdot)$ at R. Further, it is worth noting that in Theorem 3, we have proved that for any $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ with $\mathrm{V} > 0$ and $R_\infty < R < C$ and $\epsilon > 0$, the maximum error probability of any constant composition (N, R) code is lower bounded by*

$$\frac{K_5 e^{-NE_{SP}(R)}}{N^{\frac{1}{2}\left(1+\epsilon+\tilde{\rho}_R^*\right)}}, \tag{4.19}$$

for all sufficiently large N, where K_5 is a positive constant that depends on W, R and ϵ, and $\tilde{\rho}_R^*$ is the maximum absolute value subgradient of $E_{SP}(\cdot)$ at R, which also satisfies[9] *$\tilde{\rho}_R^* = \rho_R^*$, for all $R \in (R_{cr}, C)$.*

(ii) Item (ii) of Theorem 5 corrects an error[10] *of Dobrushin who claimed that for a strongly symmetric channel*[11] *with positive dispersion, for rates between R_{cr} and C, a pre-factor of $O(N^{-\frac{1}{2(1+|E_r'(R)|)}})$ is asymptotically tight [22, pg. 274, Theorem]. A lower bound of this order is evidently incorrect in light of item (ii) of Theorem 5. In fact, the invalidity of Dobrushin's claim can also be concluded by using the weaker achievable pre-factor of $O(1/\sqrt{N})$ that is reported in [4].* $\diamond$

Singularity is also crucial regarding the pre-factor of the ensemble average error probability for rates below the critical rate.

Theorem 6. *Let $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ be arbitrary with $C > 0$ and $R \leq R_{cr}$.*

(i) If for all $Q \in \mathcal{P}(\mathcal{X})$ with $E_o(1, Q) = \max_{P \in \mathcal{P}(\mathcal{X})} E_o(1, P)$, (Q, W) pair is singular,

[9] Since the non-increasing, convex curves $\mathrm{E_{SP}}(\cdot)$ and $\mathrm{E_r}(\cdot)$ agree on an interval around R, the maximum magnitude of their subdifferentials at R are also equal.

[10] We refer to the English translation of the work. We were not able to verify whether the mistake is present in the original Russian version. Moreover, the aforementioned work has other inaccuracies. For example, the conditional entropy term in [22, Eq. (1.16)] is off by a minus sign and the BSC result of Elias (e.g., [24, Theorem 1]) is mistakenly cited with a pre-factor of $\Theta(N^{-0.5})$, instead of the correct pre-factor of $\Theta(N^{-0.5(1+|\mathrm{E_r'}(R)|)})$.

[11] A channel is strongly symmetric if every row (resp. column) is a permutation of every other row (resp. column).

then for any such $Q \in \mathcal{P}(\mathcal{X})$, we have

$$K_6 e^{-NE_r(R)} \leq \bar{P}_e(Q, N, R) \leq e^{-NE_r(R)}, \tag{4.20}$$

for any $N \in \mathbb{Z}^+$ and for some $0 < K_6 < 1$ that depends on W, R and Q.

(ii) (Gallager [36]) If there exists $Q \in \mathcal{P}(\mathcal{X})$ with $E_o(1, Q) = \max_{P \in \mathcal{P}(\mathcal{X})} E_o(1, P)$ and (Q, W) pair is nonsingular, then

$$\bar{P}_e(Q, N, R) \sim \frac{g}{\sqrt{N}} e^{-NE_r(R)}, \tag{4.21}$$

where g is a positive constant that is explicitly characterized in [36]. ♦

Theorem 6 is proved in Section 4.4

Remark 13. *(i) Theorem 6 corrects a small oversight*[12] *by Gallager [37]. Specifically, in [36], item (ii) of Theorem 6 is claimed to be correct for any W with $C > 0$ and $R \leq R_{cr}$. It should be noted that the proof provided in [36] is valid under the nonsingularity assumption mentioned in item (ii) of Theorem 6.*

(ii) The abrupt drop in the order of the pre-factor at R_{cr} highlights a previously unreported role that the critical rate plays in the random coding bound. ◇

4.2 Proof of Theorem 4

4.2.1 Overview

From the well-known random coding arguments (e.g., [35, pg. 136]) one can deduce that for any message m

$$\bar{\mathrm{P}}_{\mathrm{e},m}(Q, N, R) \leq \sum_{\mathbf{x}_m, \mathbf{y}} Q(\mathbf{x}_m) W(\mathbf{y}|\mathbf{x}_m) \Pr\left\{ \bigcup_{m' \neq m} \left\{ \ln \frac{W(\mathbf{y}|\mathbf{x}_m)}{W(\mathbf{y}|\mathbf{X}_{m'})} \leq 0 \right\} \right\}. \tag{4.22}$$

[12] See Section C.1 for a particular example.

For the sake of notational convenience, let $\mathcal{E}_m := \bigcup_{m' \neq m} \left\{ \ln \frac{W(\mathbf{Y}|\mathbf{X}_m)}{W(\mathbf{Y}|\mathbf{X}_{m'})} \leq 0 \right\}$ denote the error event conditioned on message m.

One obvious way to relax the right side of (4.22) to make it more tractable is to use union bound. A straightforward application of the union bound is loose, however, because some realizations of $\mathbf{X}_m$ and $\mathbf{Y}$ are such that $\left\{ \ln \frac{W(\mathbf{Y}|\mathbf{X}_m)}{W(\mathbf{Y}|\mathbf{X}_{m'})} \leq 0 \right\}$ is likely to occur for many m'. One workaround is to define a set of "bad" $\mathbf{X}_m$ and $\mathbf{Y}$ realizations $\mathcal{D}_N \in \mathcal{X}^N \times \mathcal{Y}^N$ and proceed as follows

$$\bar{\mathrm{P}}_{\mathrm{e},m}(Q, N, R) \leq \Pr(\mathcal{E}_m \cap \mathcal{D}_N) + \Pr(\mathcal{E}_m \cap \mathcal{D}_N^c) \tag{4.23}$$

$$\leq \Pr(\mathcal{D}_N) + (\lceil e^{NR} \rceil - 1) \Pr\left\{ \mathcal{D}_N^c \cap \left\{ \ln \frac{W(\mathbf{Y}|\mathbf{X})}{W(\mathbf{Y}|\mathbf{Z})} \leq 0 \right\} \right\}. \tag{4.24}$$

Remark 14.

(i) Equation (4.24) *is Fano's [27, pg. 307, Theorem], valid for any auxiliary set $\mathcal{D}_N$, where X, Y and Z are distributed with $P_{X,Y,Z}(x, y, z) = Q(x)W(y|x)Q(z)$. Fano provides a choice of $\mathcal{D}_N$ for which a large deviations analysis of the right side of* (4.24) *yields the random coding exponent.*

(ii) It is evident that the introduction of an auxiliary set in Fano's bound is not limited to random code ensembles, but can also be employed to analyze error probability of a given block code under maximum likelihood decoding. In particular, Gallager used this idea in his analysis of low-density parity-check (LDPC) codes for the special case of binary input symmetric channels [33, Section 3.3]. After the invention of turbo codes [8] and the rediscovery of LDPC codes [47], there has been a considerable interest in deriving efficiently computable bounds on the performance of a given block code (e.g., [43], [58], [60], [64], [69] and references therein). Researching these bounds for possible refinements, in particular characterizing the pre-factors of the exponentially vanishing terms, is an interesting future research direction, which is not pursued in this paper.

(iii) There are other ways to control the aforementioned loss. One alternative is to use the following bound by Gallager (e.g., [35, eq. (5.6.7)])

$$\bar{P}_{e,m}(Q,N,R) \leq \sum_{\mathbf{x}_m,\mathbf{y}} Q(\mathbf{x}_m)W(\mathbf{y}|\mathbf{x}_m)\left(\sum_{m'\neq m} \Pr\left\{\ln\frac{W(\mathbf{y}|\mathbf{x}_m)}{W(\mathbf{y}|\mathbf{X}_{m'})} \leq 0\right\}\right)^{\rho}, \tag{4.25}$$

for any $\rho \in [0,1]$. Although the bound in (4.25) *is sufficient to obtain the random coding exponent, the bound in* (4.24) *seems to be better suited to obtaining improved pre-factors.*

A tighter alternative to (4.24) *is (e.g., [35, pg. 137], [52, Theorem 16])*

$$\bar{P}_{e,m}(Q,N,R) \leq \sum_{\mathbf{x},\mathbf{y}} Q(\mathbf{x})W(\mathbf{y}|\mathbf{x}) \min\left\{1, (\lceil e^{NR}\rceil - 1)\Pr\left\{\ln\frac{W(\mathbf{y}|\mathbf{x})}{W(\mathbf{y}|\mathbf{Z})} \leq 0\right\}\right\}. \tag{4.26}$$

Numerical evaluation of (4.26) *yields sharp bounds for the special cases of BSC and BEC [52]. Also, after we reported the results of this chapter in [3], Scarlett* et al. *[59] has recently given an alternative proof of Theorem 4 by starting from* (4.26)*. Although this derivation is simpler than the one based on* (4.24)*, the latter has the merit of being the starting point for possible refinements of the efficiently computable error probability bounds for a given block code, which is mentioned in item (ii) above.* $\diamond$

Next, one needs to choose an appropriate $\mathcal{D}_N$ and upper bound the terms on the right side of (4.24). Our choice will essentially be Fano's choice for $\mathcal{D}_N$ and our analysis will vary depending on whether (Q,W) pair is singular. Specifically, if (Q,W) pair is singular, then we use Fano's choice. However, if (Q,W) pair is nonsingular, then a perturbed version of Fano's $\mathcal{D}_N$ gives a better pre-factor and we will use such a perturbed version.

Before proceeding further, we note the following useful facts that will be used throughout the chapter.

Lemma 14. *Let $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ be arbitrary with $V > 0$.*

(i) For any $Q \in \mathcal{P}(\mathcal{X})$ such that $E_r(R, Q) > 0$ for some $R > R_\infty$, we have $\frac{\partial^2 E_o(\rho,Q)}{\partial \rho^2} < 0$ for all $\rho \in \mathbb{R}_+$.

(ii) Fix an arbitrary $Q \in \mathcal{P}(\mathcal{X})$ such that $E_r(R, Q) > 0$ for some $R > R_\infty$. For every r in the non-empty interval $\left(\frac{\partial E_o(\rho,Q)}{\partial \rho}\Big|_{\rho=1}, I(Q;W) \right)$, there exists a unique real number in $(0, 1)$, say $\rho_r^*(Q)$, such that

$$\frac{\partial E_o(\rho, Q)}{\partial \rho}\Big|_{\rho=\rho_r^*(Q)} = r. \tag{4.27}$$

Further, $\rho_{(\cdot)}^*(Q)$ is continuous over $\left(\frac{\partial E_o(\rho,Q)}{\partial \rho}\Big|_{\rho=1}, I(Q;W) \right)$ and satisfies

$$\rho_r^*(Q) = -\frac{\partial E_r(a, Q)}{\partial a}\Big|_{a=r}. \tag{4.28}$$

♦

Proof. The proof is given in Appendix C.2. □

To define the auxiliary set, we need the following definitions. First, fix some $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ with $V > 0$. Consider some $Q \in \mathcal{P}(\mathcal{X})$ and $R \in \mathbb{R}_+$ such that $R_{\text{cr}}(Q) < R < \text{I}(Q; W)$. Define

$$P_{X,Y,Z}(x, y, z) := Q(x)W(y|x)Q(z), \tag{4.29}$$

for all $(x, y, z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{X}$. Also, let

$$\tilde{P}_{X,Y,Z}(x, y, z) := \begin{cases} \frac{P_{X,Y,Z}(x,y,z)}{P_{X,Y,Z}\{\tilde{\mathcal{S}}_Q\}} & \text{if } (x, y, z) \in \tilde{\mathcal{S}}_Q, \\ 0 & \text{else.} \end{cases} \tag{4.30}$$

Let $P_{X,Y,Z}^N(\mathbf{x}, \mathbf{y}, \mathbf{z}) := \prod_{n=1}^N P_{X,Y,Z}(x_n, y_n, z_n)$ and $\mathcal{S}_Q^N$ (resp. $\tilde{S}_Q^N$) denote the N-fold cartesian product of $\mathcal{S}_Q$ (resp. $\tilde{\mathcal{S}}_Q$). Hence,

$$P_{X,Y,Z}^N \left\{ \mathbf{x}, \mathbf{y}, \mathbf{z} | \tilde{\mathcal{S}}_Q^N \right\} = \tilde{P}_{X,Y,Z}^N(\mathbf{x}, \mathbf{y}, \mathbf{z}) := \prod_{n=1}^N \tilde{P}_{X,Y,Z}(x_n, y_n, z_n). \tag{4.31}$$

For any $\rho \in [0,1]$, let[13]

$$f_\rho(y) := \frac{\left[\sum_{x\in\mathcal{X}} Q(x)W(y|x)^{1/(1+\rho)}\right]^{1+\rho}}{\sum_{b\in\mathcal{Y}}\left[\sum_{a\in\mathcal{X}} Q(a)W(b|a)^{1/(1+\rho)}\right]^{1+\rho}}, \forall\, y \in \mathcal{Y}, \tag{4.32}$$

$$\Lambda_\rho(\lambda) := \ln \mathrm{E}_{P_{X,Y}}\left[e^{\lambda \ln \frac{f_\rho(Y)}{W(Y|X)}}\right], \forall\, \lambda \in \mathbb{R}. \tag{4.33}$$

For any $\rho \in [0,1]$, $\ln \frac{f_\rho(y)}{W(y|x)} \in \mathbb{R}$ for all $(x,y) \in \mathcal{S}_Q$, hence $\Lambda_\rho(\cdot)$ is infinitely differentiable on $\mathbb{R}$. Thus, for any $\rho \in [0,1]$, the following is well-defined

$$D_{\mathrm{o}}(\rho) := \Lambda'_\rho\left(\frac{\rho}{1+\rho}\right). \tag{4.34}$$

Let $\{\epsilon_N\}_{N\geq 1}$ be a sequence of nonnegative real numbers such that $\lim_{N\to\infty}\epsilon_N = 0$ and define $R_N := R - \epsilon_N$. Let $N \in \mathbb{Z}^+$ be sufficiently large such that $R_N > R_{\mathrm{cr}}(Q)$. For the sake of notational convenience, let

$$\rho_N^* := \rho_{R_N}^*(Q) = -\left.\frac{\partial \mathrm{E_r}(r,Q)}{\partial r}\right|_{r=R_N}, \tag{4.35}$$

whose existence is ensured by (4.28).

We finally define the auxiliary set as follows:

$$\mathcal{D}_N(\epsilon_N) := \left\{\frac{1}{N}\sum_{n=1}^{N} \ln \frac{f_{\rho_N^*}(Y_n)}{W(Y_n|X_n)} > D_{\mathrm{o}}(\rho_N^*)\right\}. \tag{4.36}$$

Using the particular set defined in (4.36), equation (4.24) reads

$$\begin{aligned}\bar{\mathrm{P}}_{\mathrm{e},m}(Q,N,R) &\leq P_{X,Y}^N\{\mathcal{D}_N(\epsilon_N)\}\\ &+ (\lceil e^{NR}\rceil - 1)P_{X,Y,Z}^N\left\{\frac{1}{N}\sum_{n=1}^{N}\ln\frac{f_{\rho_N^*}(Y_n)}{W(Y_n|X_n)} \leq D_{\mathrm{o}}(\rho_N^*), \frac{1}{N}\sum_{n=1}^{N}\ln\frac{W(Y_n|X_n)}{W(Y_n|Z_n)} \leq 0\right\}.\end{aligned} \tag{4.37}$$

Remark 15. *(i) Setting $\epsilon_N = 0$ for all $N \in \mathbb{Z}^+$ gives Fano's choice of the auxiliary set. After this point, he proceeds with Chernoff bound arguments to upper bound the right side of* (4.37) *to deduce the random coding upper bound*[14] *with a pre-factor of $O(1)$ [27, pp. 324–331].*

[13]The following two quantities are defined for any $\rho \in \mathbb{R}_+$ in items (i) and (v) of Definition 12 in Appendix C.3, respectively. We reproduce them here for the reader's convenience.

[14]Fano's exponent, $\mathrm{E_F}(\cdot)$ (e.g., item (iv) of Definition 12 in Appendix C.3) has a different form than $\mathrm{E_r}(\cdot)$, yet they can be shown to be equal (e.g., Lemma 33 in Appendix C.3).

(ii) If (Q, W) is nonsingular, then the evident refinement of Fano's arguments is to use exact asymptotics result (e.g., [7], [21, Theorem 3.7.4]) instead of Chernoff bound. One can verify the conditions necessary to apply this result are satisfied and hence such a refinement gives a pre-factor of $O(1/\sqrt{N})$ [4]. Moreover, $O(1/\sqrt{N})$ is the tightest pre-factor possible if $\epsilon_N = 0$, because it can be shown that $P_{X,Y}^N\{\mathcal{D}_N(\epsilon_N)\} \sim \Theta(1/\sqrt{N})e^{-NE_r(R,Q)}$.

(iii) If (Q, W) is nonsingular, setting $\epsilon_N = 0$ for all $N \in \mathbb{Z}^+$ is not the best possible choice. With this choice, one can prove an upper bound of $O(1/N)e^{-NE_r(R,Q)}$ on the second term of (4.37)*, provided that the random vector*

$$\left[\ln \frac{f_{\rho_N^*}(Y)}{W(Y|X)}, \ln \frac{W(Y|X)}{W(Y|Z)}\right]^T, \tag{4.38}$$

is nonsingular when it is distributed with $\tilde{P}_{X,Y,Z}$, i.e., the covariance matrix of this random vector under $\tilde{P}_{X,Y,Z}$ is nonsingular. The nonsingularity of this random vector follows from the nonsingularity of (Q, W). Thus, by appropriately choosing $\epsilon_N > 0$, one can equalize the orders of the pre-factors for both terms of (4.37) *to deduce a tighter pre-factor. This intuition will be made rigorous in Section 4.2.3.*

(iv) If (Q, W) is singular, $\ln \frac{W(Y|X)}{W(Y|Z)} = 0$, $\tilde{P}_{X,Y,Z}-$(a.s.). Hence, the random vector given in (4.38) *is singular when it is distributed with $\tilde{P}_{X,Y,Z}$, i.e., the covariance matrix of this random vector under $\tilde{P}_{X,Y,Z}$ is singular. Therefore, we cannot expect to have an upper bound on the second term of* (4.37) *with an $O(1/N)$ pre-factor and hence we will set $\epsilon_N = 0$ for all $N \in \mathbb{Z}^+$ for this case. The details of the derivation is given in Section 4.2.2.*

(v) As it is evident from items (iii) and (iv) above, whether (Q, W) satisfies Definition 8 is closely related to the singularity of the covariance matrix of the random vector in (4.38) *under $\tilde{P}_{X,Y,Z}$. This relation is our rationale for calling Definition 8* singular. $\diamond$

Before proceeding further, we define the following quantities

For any $\rho \in [0,1]$, $\lambda \in \mathbb{R}$ and $\mathbf{v} \in \mathbb{R}^2$,

$$\tilde{P}^{\lambda,\rho}_{X,Y}(x,y) := \begin{cases} \frac{Q(x)W(y|x)^{1-\lambda} f_\rho(y)^\lambda}{\sum_{(a,b)\in\mathcal{S}_Q} Q(a)W(b|a)^{1-\lambda} f_\rho(b)^\lambda}, & \text{if } (x,y) \in \mathcal{S}_Q, \\ 0, & \text{else.} \end{cases} \tag{4.39}$$

$$\Lambda_{1,\rho}(\mathbf{v}) := \ln \mathrm{E}_{\tilde{P}_{X,Y,Z}} \left[e^{\mathbf{v}_1 \ln \frac{W(Y|X)}{f_\rho(Y)} + \mathbf{v}_2 \ln \frac{W(Y|Z)}{W(Y|X)}} \right]. \tag{4.40}$$

Clearly, $\tilde{P}^{\lambda,\rho}_{X,Y}$ is a well-defined probability measure and $\Lambda_{1,\rho}(\cdot)$ is infinitely differentiable on $\mathbb{R}^2$. Further,

Lemma 15. *Fix an arbitrary $r \in (R_{cr}(Q), I(Q;W))$. Let $\rho := -\left.\frac{\partial E_r(a,Q)}{\partial a}\right|_{a=r} \in (0,1)$ and $\tilde{\mathbf{v}} := \left[\frac{1-\rho}{1+\rho}, \frac{1}{1+\rho}\right]^T$. We have*

(i)

$$\left[\left.\frac{\partial \Lambda_{1,\rho}(\mathbf{v}_1, \tilde{\mathbf{v}}_2)}{\partial \mathbf{v}_1}\right|_{\mathbf{v}_1=\tilde{\mathbf{v}}_1}, \left.\frac{\partial \Lambda_{1,\rho}(\tilde{\mathbf{v}}_1, \mathbf{v}_2)}{\partial \mathbf{v}_2}\right|_{\mathbf{v}_2=\tilde{\mathbf{v}}_2} \right]^T = [-\Lambda'_\rho(\rho/(1+\rho)), 0]^T. \tag{4.41}$$

(ii)

$$\Lambda_{1,\rho}(\tilde{\mathbf{v}}) = -\ln P_{X,Y,Z}\left\{\tilde{\mathcal{S}}_Q\right\} + 2\Lambda_\rho\left(\frac{\rho}{1+\rho}\right). \tag{4.42}$$

♦

Proof. The proof is given in Appendix C.4. □

4.2.2 Proof of item (i) of Theorem 4

Assume (Q,W) pair is singular. As pointed out in item (iii) of Remark 15, we use the quantities given in Section 4.2.1 with $\epsilon_N = 0$ for all $N \in \mathbb{Z}^+$. Specifically, define

$$\rho^* := -\left.\frac{\partial \mathrm{E_r}(r,Q)}{\partial r}\right|_{r=R}. \tag{4.43}$$

Let f^*, $\Lambda(\cdot)$ and D_{o} denote the quantities defined in (4.32), (4.33) and (4.34), respectively, by choosing $\rho = \rho^*$. For convenience, let $\mathcal{D}_N$ denote the set defined in (4.36) with the aforementioned choices. Particularizing (4.24), we have

$$\begin{aligned}\bar{\mathrm{P}}_{\mathrm{e},m}(Q,N,R) &\leq P_{X,Y}^N\{\mathcal{D}_N\} \\ &\quad + (\lceil e^{NR}\rceil - 1)P_{X,Y,Z}^N\left\{\frac{1}{N}\sum_{n=1}^N \ln\frac{f^*(Y_n)}{W(Y_n|X_n)} \leq D_{\mathrm{o}}, \frac{1}{N}\sum_{n=1}^N \ln\frac{W(Y_n|X_n)}{W(Y_n|Z_n)} \leq 0\right\}.\end{aligned} \tag{4.44}$$

We begin by deriving an upper bound on the first term in the right side of (4.44).

Lemma 16. *$\Lambda''(\lambda) > 0$, for all $\lambda \in \mathbb{R}$.* ♦

Proof. The proof goes by contradiction. One can check that

$$[\exists\, \lambda \in \mathbb{R} \text{ with } \Lambda''(\lambda) = 0] \iff \left[\ln\frac{f^*(Y)}{W(Y|X)} = \Lambda'(\lambda),\ P_{X,Y}-\text{(a.s.)}\right]. \tag{4.45}$$

Further, define $\tilde{\mathcal{Y}} := \{y \in \mathcal{Y} : \mathcal{X}_y \neq \emptyset\}$. Note that $\tilde{\mathcal{Y}} \neq \emptyset$. Since (Q, W) pair is singular, for some $\delta_y \in \mathbb{R}^+$

$$W(y|x) = \delta_y,\ \forall x \in \mathcal{X}_y, \tag{4.46}$$

which, in turn, implies that

$$f^*(y) = \frac{\delta_y Q\left\{\mathcal{X}_y\right\}^{1+\rho^*}}{\sum_{b\in\tilde{\mathcal{Y}}}\delta_b Q\left\{\mathcal{X}_b\right\}^{1+\rho^*}}. \tag{4.47}$$

Equations (4.46) and (4.47) imply that

$$\ln\frac{f^*(y)}{W(y|x)} = \ln\frac{Q\left\{\mathcal{X}_y\right\}^{1+\rho^*}}{\sum_{b\in\tilde{\mathcal{Y}}}\delta_b Q\left\{\mathcal{X}_b\right\}^{1+\rho^*}},\ \forall\,(x,y) \in \tilde{\mathcal{S}}_Q. \tag{4.48}$$

Due to (4.48), one can check that the right side of (4.45) is equivalent to saying that $Q\left\{\mathcal{X}_y\right\}$ is constant for all $y \in \tilde{\mathcal{Y}}$. This last observation, coupled with the singularity of the pair (Q, W), further implies that

$$\mathrm{E}_{\mathrm{o}}(\rho, Q) = -(1+\rho)\ln Q\left\{\mathcal{X}_y\right\} - \ln\sum_y \delta_y, \tag{4.49}$$

for all $\rho \in \mathbb{R}_+$. Evidently, (4.49) implies that $\frac{\partial^2 \mathrm{E_o}(\rho,Q)}{\partial \rho^2} = 0$, for all $\rho \in \mathbb{R}_+$, which contradicts item (i) of Lemma 14. □

Equipped with Lemma 16, we can apply the concentration lemma, i.e., Lemma 5. Specifically, (3.1) implies[15] that (recall that our random variables are i.i.d.)

$$P_{X,Y}^N \{\mathcal{D}_N\} \leq e^{-N\Lambda^*(D_\mathrm{o})} \frac{1}{\sqrt{N}} \left\{ \frac{m_3}{\Lambda''(\eta)^{3/2}} + \frac{1}{\sqrt{2\pi\Lambda''(\eta)\eta}} \right\}, \tag{4.50}$$

where $\eta := \frac{\rho^*}{1+\rho^*}$, $m_3 := \mathrm{E}_{\tilde{P}_{X,Y}^{\eta,\rho^*}} \left[\left| \ln \frac{f^*(Y)}{W(Y|X)} - \Lambda'(\eta) \right|^3 \right]$ with $\tilde{P}_{X,Y}^{\eta,\rho^*}$ as defined in (4.39), and $\Lambda^*(D_\mathrm{o})$ is the Fenchel-Legendre transform of $\Lambda(\cdot)$ at D_o, i.e.,

$$\Lambda^*(D_\mathrm{o}) := \sup_{\lambda \in \mathbb{R}} \{D_\mathrm{o}\lambda - \Lambda(\lambda)\}. \tag{4.51}$$

Since $\Lambda(\cdot)$ is convex, the definition of D_o and (3.80) imply that

$$\Lambda^*(D_\mathrm{o}) = \eta\Lambda'(\eta) - \Lambda(\eta). \tag{4.52}$$

Moreover, Lemma 33 and (C.42) in Appendix C.3 imply that

$$\mathrm{E_r}(R, Q) = \eta\Lambda'(\eta) - \Lambda(\eta). \tag{4.53}$$

By plugging (4.53) into (4.52), we deduce that

$$\Lambda^*(D_\mathrm{o}) = \mathrm{E_r}(R, Q), \tag{4.54}$$

which, in turn, implies that

$$P_{X,Y}^N \{\mathcal{D}_N\} \leq e^{-N\mathrm{E_r}(R,Q)} \frac{1}{\sqrt{N}} \left\{ \frac{m_3}{\Lambda''(\eta)^{3/2}} + \frac{1}{\sqrt{2\pi\Lambda''(\eta)\eta}} \right\}. \tag{4.55}$$

[15] In the conference paper that we have reported the results of this chapter, the second term in the braces of (4.50) (resp. (4.66)) is incorrectly written as $\frac{1}{\sqrt{2\pi\eta}}$ [3, Eq. (66)] (resp. $\frac{1}{\sqrt{2\pi\tilde{\eta}}}$ [3, Eq. (69)]). The correct form is $\frac{1}{\sqrt{2\pi\Lambda''(\eta)\eta}}$ (resp. $\frac{1}{\sqrt{2\pi\Lambda_o''(\tilde{\eta})\tilde{\eta}}}$), as given in (4.50) (resp. (4.66)).

In order to upper bound the remaining term in the right side of (4.44), we first note that

$$\beta_N := P_{X,Y,Z}^N \left\{ \frac{1}{N} \sum_{n=1}^N \ln \frac{f^*(Y_n)}{W(Y_n|X_n)} \le D_{\mathrm{o}}, \frac{1}{N} \sum_{n=1}^N \ln \frac{W(Y_n|X_n)}{W(Y_n|Z_n)} \le 0 \right\} \tag{4.56}$$

$$= P_{X,Y,Z}^N \left\{ \tilde{S}_Q^N \right\} \tilde{P}_{X,Y,Z}^N \left\{ \frac{1}{N} \sum_{n=1}^N \ln \frac{W(Y_n|X_n)}{f^*(Y_n)} \ge -D_{\mathrm{o}}, \frac{1}{N} \sum_{n=1}^N \ln \frac{W(Y_n|Z_n)}{W(Y_n|X_n)} \ge 0 \right\} \tag{4.57}$$

$$= P_{X,Y,Z}^N \left\{ \tilde{S}_Q^N \right\} \tilde{P}_{X,Y,Z}^N \left\{ \frac{1}{N} \sum_{n=1}^N \ln \frac{W(Y_n|X_n)}{f^*(Y_n)} \ge -D_{\mathrm{o}} \right\}, \tag{4.58}$$

where (4.58) follows by noting $\ln \frac{W(y|z)}{W(y|x)} = 0$ for all $(x, y, z) \in \tilde{S}_Q$, which is a direct consequence of the singularity of (Q, W) pair.

Next, define

$$\forall\, \lambda \in \mathbb{R},\ \Lambda_{\mathrm{o}}(\lambda) := \ln \mathrm{E}_{\tilde{P}_{X,Y,Z}} \left[e^{\lambda \ln \frac{W(Y|X)}{f^*(Y)}} \right], \tag{4.59}$$

and note that $\Lambda_{\mathrm{o}}(\cdot)$ is infinitely differentiable on $\mathbb{R}$. Moreover, one can check that

$$\forall\, \mathbf{v} \in \mathbb{R}^2,\ \Lambda_{\mathrm{o}}(\mathbf{v}_1) = \Lambda_1(\mathbf{v}), \tag{4.60}$$

where $\Lambda_1(\cdot)$ denotes $\Lambda_{1,\rho^*}(\cdot)$ (e.g., (4.40)) for notational convenience. Further, for any $\lambda \in \mathbb{R}$, define

$$\tilde{Q}_{X,Y,Z}^{\lambda}(x, y, z) := \begin{cases} \frac{\tilde{P}_{X,Y,Z}(x,y,z) W(y|x)^{\lambda} f^*(y)^{-\lambda}}{\sum_{(a,b,c) \in \tilde{S}_Q} \tilde{P}_{X,Y,Z}(a,b,c) W(b|a)^{\lambda} f^*(b)^{-\lambda}} & \text{if } (x, y, z) \in \tilde{S}_Q, \\ 0 & \text{else.} \end{cases} \tag{4.61}$$

It is evident that $\tilde{Q}_{X,Y,Z}^{\lambda}$ is a well-defined probability measure and equivalent to $\tilde{P}_{X,Y,Z}$.

Lemma 17. *$\Lambda_o''(\lambda) > 0$ for all $\lambda \in \mathbb{R}$.* ♦

Proof. One can check that

$$\Lambda_{\mathrm{o}}'(\lambda) = \mathrm{E}_{\tilde{Q}_{X,Y,Z}^{\lambda}} \left[\ln \frac{W(Y|X)}{f^*(Y)} \right], \quad \Lambda_{\mathrm{o}}''(\lambda) = \mathrm{Var}_{\tilde{Q}_{X,Y,Z}^{\lambda}} \left[\ln \frac{W(Y|X)}{f^*(Y)} \right]. \tag{4.62}$$

For contradiction, assume there exists $\lambda \in \mathbb{R}$ with $\Lambda_{\mathrm{o}}''(\lambda) = 0$. We have

$$[\exists\, \lambda \in \mathbb{R} \text{ with } \Lambda_{\mathrm{o}}''(\lambda) = 0] \iff \left[\ln \frac{W(y|x)}{f^*(y)} = \Lambda_{\mathrm{o}}'(\lambda),\ \forall\, (x, y, z) \in \tilde{S}_Q \right] \tag{4.63}$$

$$\implies \left[\ln \frac{W(y|x)}{f^*(y)} = \Lambda_{\mathrm{o}}'(\lambda),\ \forall\, (x, y) \in \mathcal{S}_Q \right]. \tag{4.64}$$

Using exactly the same arguments as in the proof of Lemma 16, one can show that (4.64) contradicts item (i) of Lemma 14. □

From item (i) of Lemma 15 and (4.60), we deduce that

$$\Lambda_{\mathrm{o}}'\left(\frac{1-\rho^*}{1+\rho^*}\right) = -D_{\mathrm{o}}. \tag{4.65}$$

Lemma 17 and (4.65) enable us to apply the concentration lemma, i.e., Lemma 5, to obtain

$$\tilde{P}_{X,Y,Z}^N\left\{\frac{1}{N}\sum_{n=1}^{N}\ln\frac{W(Y_n|X_n)}{f^*(Y_N)} \geq -D_{\mathrm{o}}\right\} \leq e^{-N\Lambda_{\mathrm{o}}^*(-D_{\mathrm{o}})}\frac{1}{\sqrt{N}}\left\{\frac{\tilde{m}_3}{\Lambda_{\mathrm{o}}''(\tilde{\eta})^{3/2}} + \frac{1}{\sqrt{2\pi\Lambda_{\mathrm{o}}''(\tilde{\eta})\tilde{\eta}}}\right\}, \tag{4.66}$$

where $\tilde{\eta} := \frac{1-\rho^*}{1+\rho^*}$, $\tilde{m}_3 := \mathrm{E}_{\tilde{Q}_{X,Y,Z}^{\tilde{\eta}}}\left[\left|\ln\frac{W(Y|X)}{f^*(Y)} - \Lambda_{\mathrm{o}}'(\tilde{\eta})\right|^3\right]$ with $\tilde{Q}_{X,Y,Z}^{\tilde{\eta}}$ as defined in (4.61), and

$$\Lambda_{\mathrm{o}}^*(-D_{\mathrm{o}}) = \sup_{\lambda\in\mathbb{R}}\left\{-D_{\mathrm{o}}\lambda - \Lambda_{\mathrm{o}}(\lambda)\right\}. \tag{4.67}$$

Since $\Lambda_{\mathrm{o}}(\cdot)$ is convex, (4.65) and (4.67) imply that

$$\Lambda_{\mathrm{o}}^*(-D_{\mathrm{o}}) = -\tilde{\eta}D_{\mathrm{o}} - \Lambda_{\mathrm{o}}\left(\tilde{\eta}\right) \tag{4.68}$$

$$= -\tilde{\eta}D_{\mathrm{o}} - \Lambda_1([\tilde{\eta}, 1/(1+\rho^*)]^T), \tag{4.69}$$

where (4.69) follows from (4.60). Item (ii) of Lemma 15 yields

$$\Lambda_1([\tilde{\eta}, 1/(1+\rho^*)]^T) = -\ln P_{X,Y,Z}\left\{\tilde{\mathcal{S}}_Q\right\} + 2\Lambda\left(\frac{\rho^*}{1+\rho^*}\right). \tag{4.70}$$

Equations (4.69) and (4.70) imply that

$$\Lambda_{\mathrm{o}}^*(-D_{\mathrm{o}}) = \ln P_{X,Y,Z}\left\{\tilde{\mathcal{S}}_Q\right\} + \left[\left(\frac{\rho^*}{1+\rho^*}\right)\Lambda'\left(\frac{\rho^*}{1+\rho^*}\right) - \Lambda\left(\frac{\rho^*}{1+\rho^*}\right)\right] \tag{4.71}$$

$$- \left[\frac{1}{1+\rho^*}\Lambda'\left(\frac{\rho^*}{1+\rho^*}\right) + \Lambda\left(\frac{\rho^*}{1+\rho^*}\right)\right] \tag{4.72}$$

$$= \ln P_{X,Y,Z}\left\{\tilde{\mathcal{S}}_Q\right\} + \mathrm{E}_r(R,Q) - \left[\frac{1}{1+\rho^*}\Lambda'\left(\frac{\rho^*}{1+\rho^*}\right) + \Lambda\left(\frac{\rho^*}{1+\rho^*}\right)\right] \tag{4.73}$$

$$= \ln P_{X,Y,Z}\left\{\tilde{\mathcal{S}}_Q\right\} + \mathrm{E}_r(R,Q) + R, \tag{4.74}$$

where (4.73) follows from (4.52) and (4.54), and (4.74) follows since

$$-R = \frac{1}{1+\rho^*}\Lambda'\left(\frac{\rho^*}{1+\rho^*}\right) + \Lambda\left(\frac{\rho^*}{1+\rho^*}\right), \tag{4.75}$$

which is (C.43) in Appendix C.3.

Equations (4.58), (4.66) and (4.74) imply that

$$\beta_N \leq e^{-N(\mathrm{E_r}(R,Q)+R)}\frac{1}{\sqrt{N}}\left\{\frac{\tilde{m}_3}{\Lambda_{\mathrm{o}}''(\tilde{\eta})^{3/2}} + \frac{1}{\sqrt{2\pi\Lambda_{\mathrm{o}}''(\tilde{\eta})}\tilde{\eta}}\right\}, \tag{4.76}$$

which, in turn, implies that

$$\begin{aligned}(\lceil e^{NR}\rceil - 1)P_{X,Y,Z}^N\left\{\frac{1}{N}\sum_{n=1}^N \ln\frac{f^*(Y_n)}{W(Y_n|X_n)} \leq D_{\mathrm{o}}, \frac{1}{N}\sum_{n=1}^N \ln\frac{W(Y_n|X_n)}{W(Y_n|Z_n)} \leq 0\right\} \leq \\ \frac{e^{-N\mathrm{E_r}(R,Q)}}{\sqrt{N}}\left\{\frac{\tilde{m}_3}{\Lambda_{\mathrm{o}}''(\tilde{\eta})^{3/2}} + \frac{1}{\sqrt{2\pi\Lambda_{\mathrm{o}}''(\tilde{\eta})}\tilde{\eta}}\right\}.\end{aligned} \tag{4.77}$$

Plugging (4.55) and (4.77) into (4.44) implies (4.10).

The proof of (4.11) follows from the well-known expurgation idea (e.g., [35, pg. 140]) and is included for completeness. To this end, generate a random code with $2\lceil e^{NR}\rceil$ codewords using Q as specified in the beginning of this section. Using exactly the same arguments leading to the proof of (4.10), one can verify that for any message m

$$\begin{aligned}\bar{\mathrm{P}}_{\mathrm{e},m}\left(Q, N, R + \frac{\ln 2}{N}\right) \leq \frac{e^{-N\mathrm{E_r}(R,Q)}}{\sqrt{N}}\left\{\frac{m_3}{\Lambda''(\eta)^{3/2}} + \frac{1}{\sqrt{2\pi\Lambda''(\eta)}\eta}\right\} \\ + \frac{e^{-N\mathrm{E_r}(R,Q)}}{\sqrt{N}}\left\{\frac{2\tilde{m}_3}{\Lambda_{\mathrm{o}}''(\tilde{\eta})^{3/2}} + \frac{2}{\sqrt{2\pi\Lambda_{\mathrm{o}}''(\tilde{\eta})}\tilde{\eta}}\right\}\left\{1 + \frac{e^{-NR}}{2}\right\}.\end{aligned} \tag{4.78}$$

Clearly, (4.78) guarantees the existence of a code, say $(\tilde{f}, \tilde{\varphi})$, with blocklength N, $2\lceil e^{NR}\rceil$ messages, and average error probability upper bounded by the right side of (4.78). Now, if we throw out the worst (in terms of the corresponding conditional error probability) half of the codewords of this code, the resulting expurgated code, say (f, φ), becomes an (N, R) code with $\mathrm{P_e}(f, \varphi)$ not exceeding twice the right side of (4.78), which, in turn, implies (4.11). □

4.2.3 Proof of item (ii) of Theorem 4

Assume (Q, W) pair is nonsingular. Let $\{\epsilon_N\}_{N\geq 1}$ be such that $\epsilon_N = \frac{\ln \sqrt{N}}{N}$ for all $N \in \mathbb{Z}^+$ and $R_N := R - \epsilon_N$. Consider a sufficiently large N such that $R_N > R_{\mathrm{cr}}(Q)$. For notational convenience, let

$$\rho^* := -\left.\frac{\partial \mathrm{E_r}(r, Q)}{\partial r}\right|_{r=R}, \quad \rho_N^* := -\left.\frac{\partial \mathrm{E_r}(r, Q)}{\partial r}\right|_{r=R_N}. \tag{4.79}$$

Let $f^*, \Lambda(\cdot)$ and D_{o} denote the quantities defined in (4.32), (4.33) and (4.34), respectively, by choosing $\rho = \rho^*$. Similarly, let f_N^*, $\Lambda_N(\cdot)$ and $D_{\mathrm{o}}(N)$ denote the quantities defined in (4.32), (4.33) and (4.34), respectively, by choosing $\rho = \rho_N^*$. Let $\mathcal{D}_N$ denote the set defined in (4.36). Using these choices, (4.37) reads

$$\begin{aligned}
&\bar{\mathrm{P}}_{\mathrm{e},m}(Q, N, R) \leq P_{X,Y}^N\{\mathcal{D}_N\} \\
&+ (\lceil e^{NR} \rceil - 1) P_{X,Y,Z}^N \left\{ \frac{1}{N}\sum_{n=1}^N \ln \frac{f_N^*(Y_n)}{W(Y_n|X_n)} \leq D_{\mathrm{o}}(N), \frac{1}{N}\sum_{n=1}^N \ln \frac{W(Y_n|X_n)}{W(Y_n|Z_n)} \leq 0 \right\}.
\end{aligned} \tag{4.80}$$

In order to conclude the proof, we must upper bound the two terms on the right side of (4.80). We begin with the first term.

Let $\eta_N := \frac{\rho_N^*}{1+\rho_N^*}$ and $\eta := \frac{\rho^*}{1+\rho^*}$. Item (ii) of Lemma 14 ensures that $\rho_{(\cdot)}^*(Q)$ is continuous over $(R_{\mathrm{cr}}(Q), \mathrm{I}(Q; W))$ and hence, we have

$$\lim_{N\to\infty} \rho_N^* = \rho^*. \tag{4.81}$$

$$\lim_{N\to\infty} \eta_N = \eta. \tag{4.82}$$

$$\lim_{N\to\infty} f_N^*(y) = f^*(y). \tag{4.83}$$

$$\lim_{N\to\infty} \tilde{P}_{X,Y}^{\eta_N, \rho_N^*} = \tilde{P}_{X,Y}^{\eta, \rho^*}. \tag{4.84}$$

Lemma 18. *Fix an arbitrary $\rho \in [0, 1]$. For any $\lambda \in \mathbb{R}$, we have $\Lambda_\rho''(\lambda) \in \mathbb{R}^+$.* ♦

Proof. Via elementary calculation, one can check that

$$\Lambda'_\rho(\lambda) = \mathrm{E}_{\tilde{P}^{\lambda,\rho}_{X,Y}}\left[\ln \frac{f_\rho(Y)}{W(Y|X)}\right], \quad \Lambda''_\rho(\lambda) = \mathrm{Var}_{\tilde{P}^{\lambda,\rho}_{X,Y}}\left[\ln \frac{f_\rho(Y)}{W(Y|X)}\right] \geq 0, \tag{4.85}$$

where $\tilde{P}^{\lambda,\rho}_{X,Y}$ is defined in (4.39). The inequality in (4.85) ensures that it suffices to prove $\Lambda''_\rho(\cdot) \neq 0$. For contradiction, assume this is not the case. Then,

$$\left[\exists\, \lambda \in \mathbb{R} \text{ s.t. } \Lambda''_\rho(\lambda) = 0\right] \Longleftrightarrow \left[\ln \frac{f_\rho(Y)}{W(Y|X)} = \Lambda'_\rho(\lambda),\ \forall (x,y) \in \mathcal{S}_Q\right] \tag{4.86}$$

$$\Longrightarrow \left[W(y|x) = W(y|z),\ \forall (x,y,z) \in \tilde{\mathcal{S}}_Q\right]. \tag{4.87}$$

The right side of (4.87) is equivalent to saying (Q, W) pair is singular, which is a contradiction. Hence, we conclude that $\Lambda''_\rho(\lambda) > 0$. □

Lemma 18 ensures that $\Lambda''(\cdot), \Lambda''_N(\cdot) \in \mathbb{R}^+$, thus we can apply the concentration lemma, i.e., Lemma 5, to obtain[16]

$$P^N_{X,Y}\{\mathcal{D}_N\} \leq e^{-N\Lambda^*_N(D_\mathrm{o}(N))} \frac{1}{\sqrt{N}} \left\{ \frac{m_{3,N}}{\Lambda''_N(\eta_N)^{3/2}} + \frac{1}{\sqrt{2\pi\Lambda''_N(\eta_N)}\eta_N} \right\}, \tag{4.88}$$

where $m_{3,N} := \mathrm{E}_{\tilde{P}^{\eta_N,\rho^*_N}_{X,Y}}\left[\left|\ln \frac{f^*_N(Y)}{W(Y|X)} - \Lambda'_N(\eta_N)\right|^3\right]$ and $\Lambda^*_N(D_\mathrm{o}(N))$ is the Fenchel-Legendre transform of $\Lambda_N(\cdot)$ at $D_\mathrm{o}(N)$.

Since $\Lambda_N(\cdot)$ is convex, one can verify that

$$\Lambda^*_N(D_\mathrm{o}(N)) = \eta_N \Lambda'_N(\eta_N) - \Lambda_N(\eta_N). \tag{4.89}$$

Lemma 33 and (C.42) in Appendix C.3 imply that

$$\mathrm{E_r}(R_N, Q) = \eta_N \Lambda'_N(\eta_N) - \Lambda_N(\eta_N). \tag{4.90}$$

By plugging (4.90) into (4.89), we deduce that

$$\Lambda^*_N(D_\mathrm{o}(N)) = \mathrm{E_r}(R_N, Q). \tag{4.91}$$

[16] In the conference paper that we have reported the results of this chapter, the second term in the braces of (4.88) is incorrectly written as $\frac{1}{\sqrt{2\pi}\eta_N}$ [3, Eq. (29)]. The correct form is $\frac{1}{\sqrt{2\pi\Lambda''_N(\eta_N)}\eta_N}$, as given in (4.88).

By using (4.81)–(4.85), along with the continuity of $|\cdot|^3$ and $(\cdot)^2$, and the fact that $\mathcal{X}, \mathcal{Y}$ are finite sets, we conclude that

$$\lim_{N\to\infty} \Lambda_N''(\eta_N) = \Lambda''(\eta), \tag{4.92}$$

$$\lim_{N\to\infty} m_{3,N} = m_3 := \mathrm{E}_{\tilde{P}^{\eta,\rho^*}_{X,Y}}\left[\left|\ln \frac{f^*(Y)}{W(Y|X)} - \Lambda'(\eta)\right|^3\right]. \tag{4.93}$$

Due to (4.82), (4.92) and (4.93), one can choose a sufficiently large N with

$$\frac{m_{3,N}}{\Lambda_N''(\eta_N)^{3/2}} + \frac{1}{\sqrt{2\pi\Lambda_N''(\eta_N)}\eta_N} \le 2\left(\frac{m_3}{\Lambda''(\eta)^{3/2}} + \frac{1}{\sqrt{2\pi\Lambda''(\eta)}\eta}\right). \tag{4.94}$$

By plugging (4.91) and (4.94) into (4.88), we deduce that

$$P^N_{X,Y}\{\mathcal{D}_N\} \le \frac{2}{\sqrt{N}}\left(\frac{m_3}{\Lambda''(\eta)^{3/2}} + \frac{1}{\sqrt{2\pi\Lambda''(\eta)}\eta}\right) e^{-N\mathrm{E_r}(R_N,Q)}. \tag{4.95}$$

Next, we upper bound the second term on the right side of (4.37). To begin with, note that for any (x, y, z) with $Q(x)W(y|x)Q(z) > 0$, if $(x, y, z) \notin \tilde{\mathcal{S}}_Q$, then $\ln \frac{W(y|x)}{W(y|z)} = \infty$, which, in turn, implies that

$$\alpha_N := P^N_{X,Y,Z}\left\{\frac{1}{N}\sum_{n=1}^N \ln \frac{f^*_N(Y_n)}{W(Y_n|X_n)} \le D_{\mathrm{o}}(N), \frac{1}{N}\sum_{n=1}^N \ln \frac{W(Y_n|X_n)}{W(Y_n|Z_n)} \le 0\right\} \tag{4.96}$$

$$= P^N_{X,Y,Z}\left\{\tilde{\mathcal{S}}^N_Q\right\}\tilde{\alpha}_N, \tag{4.97}$$

where, in (4.97) we define

$$\tilde{\alpha}_N := \tilde{P}^N_{X,Y,Z}\left\{\frac{1}{N}\sum_{n=1}^N \ln \frac{W(Y_n|X_n)}{f^*_N(Y_n)} \ge -D_{\mathrm{o}}(N), \frac{1}{N}\sum_{n=1}^N \ln \frac{W(Y_n|Z_n)}{W(Y_n|X_n)} \ge 0\right\}. \tag{4.98}$$

Given any $\mathbf{v} \in \mathbb{R}^2$ let $\Lambda_{1,N}(\mathbf{v})$ and $\Lambda_1(\mathbf{v})$ denote $\Lambda_{1,\rho^*_N}(\mathbf{v})$ and $\Lambda_{1,\rho^*}(\mathbf{v})$, respectively, where $\Lambda_{1,\rho}(\mathbf{v})$ is defined in (4.40). Further, define

$$\mathbf{v}^*(N) := \left[\frac{1-\rho^*_N}{1+\rho^*_N}, \frac{1}{1+\rho^*_N}\right]^T, \quad \mathbf{v}^* := \left[\frac{1-\rho^*}{1+\rho^*}, \frac{1}{1+\rho^*}\right]^T. \tag{4.99}$$

Note that $\mathbf{v}_1^*, \mathbf{v}_1^*(N) \in (0,1)$ and $\mathbf{v}_2^*, \mathbf{v}_2^*(N) \in (1/2,1)$. Also, by using (4.81)–(4.83), one can verify that

$$\lim_{N\to\infty} \mathbf{v}^*(N) = \mathbf{v}^*, \tag{4.100}$$

$$\lim_{N\to\infty} \Lambda_{1,N}(\mathbf{v}^*(N)) = \Lambda_1(\mathbf{v}^*). \tag{4.101}$$

Given any $\rho \in [0,1]$ and $\mathbf{v} \in \mathbb{R}^2$, define

$$\tilde{Q}^{\mathbf{v},\rho}_{X,Y,Z}(x,y,z) := \begin{cases} \frac{\tilde{P}_{X,Y,Z}(x,y,z)W(y|x)^{\mathbf{v}_1-\mathbf{v}_2} f_\rho(y)^{-\mathbf{v}_1} W(y|z)^{\mathbf{v}_2}}{\sum_{(a,b,c)\in\tilde{S}_Q} \tilde{P}_{X,Y,Z}(a,b,c)W(b|a)^{\mathbf{v}_1-\mathbf{v}_2} f_\rho(b)^{-\mathbf{v}_1} W(b|c)^{\mathbf{v}_2}} & \text{if } (x,y,z) \in \tilde{S}_Q \\ 0 & \text{else.} \end{cases} \tag{4.102}$$

Note that $\tilde{Q}^{\mathbf{v},\rho}_{X,Y,Z}$ is a well-defined probability measure and equivalent to $\tilde{P}_{X,Y,Z}$. For notational convenience, let $\tilde{Q}^{\mathbf{v}^*(N)}_{X,Y,Z}$ and $\tilde{Q}^{\mathbf{v}^*}_{X,Y,Z}$ denote $\tilde{Q}^{\mathbf{v}^*(N),\rho^*_N}_{X,Y,Z}$ and $\tilde{Q}^{\mathbf{v}^*,\rho^*}_{X,Y,Z}$, respectively.

From (4.83), (4.100) and (4.102), we deduce that

$$\lim_{N\to\infty} \tilde{Q}^{\mathbf{v}^*(N)}_{X,Y,Z} = \tilde{Q}^{\mathbf{v}^*}_{X,Y,Z}. \tag{4.103}$$

In the remaining part of the proof, we need the following result whose validity heavily depends on the nonsingularity of the pair (Q,W).

Lemma 19. *Fix an arbitrary $r \in (R_{cr}(Q), I(Q;W))$. Let $\rho := -\frac{\partial E_r(a,Q)}{\partial a}\big|_{a=r} \in (0,1)$ and $\tilde{\mathbf{v}} := \left[\frac{1-\rho}{1+\rho}, \frac{1}{1+\rho}\right]^T$. We have*

$$\det\left(cov_{\tilde{Q}^{\tilde{\mathbf{v}},\rho}_{X,Y,Z},\rho}\left(\left[\ln\frac{W(Y|X)}{f_\rho(Y)}, \ln\frac{W(Y|Z)}{W(Y|X)} \right]^T \right) \right) > 0. \tag{4.104}$$

♦

Proof. The proof is given in Appendix C.5. □

Define

$$\mathbf{b}(N) := [-D_o(N), 0]^T, \quad \mathbf{b} := [-D_o, 0]^T, \quad \mathcal{B}(N) := [-D_o(N), \infty) \times [0, \infty). \tag{4.105}$$

$$\Lambda^*_{1,N}(\mathbf{d}) := \sup_{\mathbf{v}\in\mathbb{R}^2} \{\langle \mathbf{v}, \mathbf{d}\rangle - \Lambda_{1,N}(\mathbf{v})\}, \tag{4.106}$$

for any $\mathbf{d} \in \mathbb{R}^2$.

For notational convenience, let

$$\mathbf{S}_N := \mathrm{cov}_{\tilde{Q}_{X,Y,Z}^{\mathbf{v}^*(N)}}\left(\left[\ln \frac{W(Y|X)}{f_N^*(Y)}, \ln \frac{W(Y|Z)}{W(Y|X)}\right]^T\right), \mathbf{S} := \mathrm{cov}_{\tilde{Q}_{X,Y,Z}^{\mathbf{v}^*}}\left(\left[\ln \frac{W(Y|X)}{f^*(Y)}, \ln \frac{W(Y|Z)}{W(Y|X)}\right]^T\right), \tag{4.107}$$

and note that (4.104) ensures that $\lambda_{\min}(\mathbf{S}_N), \lambda_{\min}(\mathbf{S}) \in \mathbb{R}^+$, where $\lambda_{\min}(\mathbf{S}_N)$ (resp. $\lambda_{\min}(\mathbf{S})$) denotes the minimum eigenvalue of $\mathbf{S}_N$ (resp. $\mathbf{S}$).

Lemma 20. *For all sufficiently large N that depends on Q, W and R,*

$$\tilde{\alpha}_N \leq e^{-N\Lambda_{1,N}^*(\mathbf{b}(N))} \frac{c}{2\lambda_{\min}(\mathbf{\Sigma}_N)N}\left(k(R,W,Q)^2 + \frac{2}{\mathbf{v}_1^*(N)^2} + \frac{2}{\mathbf{v}_2^*(N)^2}\right), \tag{4.108}$$

where $c \in \mathbb{R}^+$ is a universal constant and $k(R,W,Q) \in \mathbb{R}^+$ is a constant that depends on R, W and Q. ♦

Proof. The proof is given in Appendix C.6. □

Remark 16. *Although we state Lemma 20 for our particular case, its extension to i.i.d. random vectors satisfying usual regularity conditions associated with strong large deviations results is evident. Moreover, it gives a more general upper bound than the existing vector exact asymptotics results of Chaganty and Sethuraman [16] and Petrovskii [50]. In particular, [16] and [50] handles strongly non-lattice random vectors*[17] *and lattice random vectors*[18]*, respectively. As opposed to random variables, however, these two cases don't exhaust all random vectors, and we are not aware of a result in the spirit of Lemma 20 that would give an upper bound of $O(1/N)$ for our case.* ◇

The following is a consequence of elementary linear algebra, whose proof is given in Appendix C.7 for completeness.

[17] A random vector is strongly non-lattice if the magnitude of its characteristic function is bounded away from 1 everywhere, except the origin.

[18] A random vector is lattice if it only takes values on a lattice.

Lemma 21. *For all sufficiently large N,*

$$\lambda_{min}(\mathbf{S}_N) \geq \frac{\lambda_{min}(\mathbf{S})}{2\sqrt{2}}. \tag{4.109}$$

♦

Further, due to (4.100) and $\mathbf{v}_1^*, \mathbf{v}_2^* \in \mathbb{R}^+$, we have

$$\frac{1}{\mathbf{v}_1^*(N)^2} + \frac{1}{\mathbf{v}_2^*(N)^2} \leq \frac{2}{(\mathbf{v}_1^*)^2} + \frac{2}{(\mathbf{v}_2^*)^2}, \tag{4.110}$$

for all sufficiently large N.

Plugging (4.109) and (4.110) into (4.108), we finally deduce that

$$\tilde{\alpha}_N \leq e^{-N\Lambda_{1,N}^*(\mathbf{b}(N))} \frac{4\sqrt{2}c}{\lambda_{\min}(\mathbf{\Sigma})N} \left(\frac{k(R,W,Q)^2}{4} + \frac{1}{(\mathbf{v}_1^*)^2} + \frac{1}{(\mathbf{v}_2^*)^2} \right), \tag{4.111}$$

for all sufficiently large N.

Next, we deal with the exponent in (4.111). First of all, owing to the convexity of $\Lambda_{1,N}(\cdot)$ and item (i) of Lemma 15, one can show that

$$\Lambda_{1,N}^*(\mathbf{b}(N)) = -\mathbf{v}_1^*(N) D_{\mathrm{o}}(N) - \Lambda_{1,N}(\mathbf{v}^*(N)). \tag{4.112}$$

Item (ii) of Lemma 15 and (4.112), along with the definitions of $D_{\mathrm{o}}(N)$ and $\mathbf{v}^*(N)$, imply that

$$\begin{aligned}
\Lambda_{1,N}^*(\mathbf{b}(N)) &= \ln P_{X,Y,Z}\left\{\tilde{\mathcal{S}}_Q\right\} + \left[\left(\frac{\rho_N^*}{1+\rho_N^*}\right)\Lambda_N'\left(\frac{\rho_N^*}{1+\rho_N^*}\right) - \Lambda_N\left(\frac{\rho_N^*}{1+\rho_N^*}\right)\right] \\
&\quad - \left[\frac{1}{1+\rho_N^*}\Lambda_N'\left(\frac{\rho_N^*}{1+\rho_N^*}\right) + \Lambda_N\left(\frac{\rho_N^*}{1+\rho_N^*}\right)\right] \qquad (4.113) \\
&= \ln P_{X,Y,Z}\left\{\tilde{\mathcal{S}}_Q\right\} + \mathrm{E}_r(R_N, Q) - \left[\frac{1}{1+\rho_N^*}\Lambda_N'\left(\frac{\rho_N^*}{1+\rho_N^*}\right) + \Lambda_N\left(\frac{\rho_N^*}{1+\rho_N^*}\right)\right] \qquad (4.114) \\
&= \ln P_{X,Y,Z}\left\{\tilde{\mathcal{S}}_Q\right\} + \mathrm{E}_r(R_N, Q) + R_N, \qquad (4.115)
\end{aligned}$$

where (4.114) follows from (4.89) and (4.91), and (4.115) follows from (C.43) in Appendix C.3.

By using (4.111), (4.115) and the fact that $\epsilon_N = \frac{\ln N}{2N}$, we have

$$\tilde{\alpha}_N \leq P_{X,Y,Z}\left\{\tilde{\mathcal{S}}_Q\right\}^{-N} \frac{4\sqrt{2}c}{\lambda_{\min}(\mathbf{\Sigma})\sqrt{N}}\left(\frac{k(R,W,Q)^2}{4} + \frac{1}{(\mathbf{v}_1^*)^2} + \frac{1}{(\mathbf{v}_2^*)^2}\right)e^{-N(\mathrm{E_r}(R_N,Q)+R)}. \quad (4.116)$$

Since $P_{X,Y,Z}^N\left\{\tilde{\mathcal{S}}_Q^N\right\} = P_{X,Y,Z}\left\{\tilde{\mathcal{S}}_Q\right\}^N$, (4.97) and (4.116) imply that

$$\alpha_N \leq \frac{4\sqrt{2}c}{\lambda_{\min}(\mathbf{\Sigma})\sqrt{N}}\left(\frac{k(R,W,Q)^2}{4} + \frac{1}{(\mathbf{v}_1^*)^2} + \frac{1}{(\mathbf{v}_2^*)^2}\right)e^{-N(\mathrm{E_r}(R_N,Q)+R)}. \quad (4.117)$$

Equation (4.117) finally implies that

$$\begin{aligned}&(\lceil e^{NR}\rceil - 1)P_{X,Y,Z}^N\left\{\frac{1}{N}\sum_{n=1}^N \ln\frac{f_N^*(Y_n)}{W(Y_n|X_n)} \leq D_{\mathrm{o}}(N), \frac{1}{N}\sum_{n=1}^N \ln\frac{W(Y_n|X_n)}{W(Y_n|Z_n)} \leq 0\right\}\\ &= (\lceil e^{NR}\rceil - 1)\alpha_N \leq \frac{4\sqrt{2}c}{\lambda_{\min}(\mathbf{\Sigma})\sqrt{N}}\left(\frac{k(R,W,Q)^2}{4} + \frac{1}{(\mathbf{v}_1^*)^2} + \frac{1}{(\mathbf{v}_2^*)^2}\right)e^{-N\mathrm{E_r}(R_N,Q)}. \quad (4.118)\end{aligned}$$

Plugging (4.95) and (4.118) into (4.37) yields,

$$\begin{aligned}\bar{\mathrm{P}}_{\mathrm{e},m}(Q,N,R) \leq{}& \frac{2}{\sqrt{N}}\left\{\frac{m_3}{\Lambda''(\eta)^{3/2}} + \frac{1}{\sqrt{2\pi\Lambda''(\eta)}\eta}\right\}e^{-N\mathrm{E_r}(R_N,Q)}\\ &+ \frac{4\sqrt{2}c}{\lambda_{\min}(\mathbf{\Sigma})\sqrt{N}}\left(\frac{k(R,W,Q)^2}{4} + \frac{1}{(\mathbf{v}_1^*)^2} + \frac{1}{(\mathbf{v}_2^*)^2}\right)e^{-N\mathrm{E_r}(R_N,Q)}. \quad (4.119)\end{aligned}$$

Evident convexity of $\mathrm{E_r}(\cdot, Q)$, along with its continuous differentiability over $[R_N, R]$, which is ensured by item (ii) of Lemma 14, enables us to deduce that (e.g., [14, eq. (3.2)])

$$\mathrm{E_r}(R_N,Q) \geq \mathrm{E_r}(R,Q) - \frac{\ln N}{2N}\left.\frac{\partial \mathrm{E_r}(r,Q)}{\partial r}\right|_{r=R}. \quad (4.120)$$

Equations (4.119) and (4.120) imply (4.12).

The proof of (4.13) follows from the same arguments leading to the proof of (4.11), which are given below for completeness. First, generate a random code with $2\lceil e^{NR}\rceil$

codewords using Q as specified in the beginning of this section. Using exactly the same arguments leading to the proof of (4.12), one can verify that for any message m

$$\bar{\mathrm{P}}_{\mathrm{e},m}\left(Q,N,R+\frac{\ln 2}{N}\right)\leq\frac{2}{\sqrt{N}}\left\{\frac{m_3}{\Lambda''(\eta)^{3/2}}+\frac{1}{\sqrt{2\pi\Lambda''(\eta)}\eta}\right\}e^{-N\mathrm{E_r}(R_N,Q)}+\frac{8\sqrt{2}c}{\lambda_{\min}(\mathbf{\Sigma})\sqrt{N}}$$
$$\times\left(\frac{k(R,W,Q)^2}{4}+\frac{1}{(\mathbf{v}_1^*)^2}+\frac{1}{(\mathbf{v}_2^*)^2}\right)\left(1+\frac{e^{-NR}}{2}\right)e^{-N\mathrm{E_r}(R_N,Q)}. \quad (4.121)$$

Clearly, (4.121) guarantees the existence of a code, say $(\tilde{f},\tilde{\varphi})$, with blocklength N, $2\lceil e^{NR}\rceil$ messages and average error probability upper bounded by the right side of (4.121). Now, if we throw out the worst (in terms of the corresponding conditional error probability) half of the codewords of this code, the resulting expurgated code, say (f,φ), becomes an (N,R) code with $\mathrm{P_e}\,(f,\varphi)$ not exceeding twice the right side of (4.121), which, in turn, implies (4.13). □

4.3 Proof of Theorem 5

Let $W\in\mathcal{P}(\mathcal{Y}|\mathcal{X})$ be arbitrary with $V>0$ and $R\in(R_{\mathrm{cr}},C)$.

(i) Write $\mathrm{E_r}(R)$ as

$$\mathrm{E_r}(R)=\max_{(\rho,Q)\in[0,1]\times\mathcal{P}(\mathcal{X})}\{-\rho R+\mathrm{E_o}(\rho,Q)\}. \quad (4.122)$$

Since the cost function of (4.122) is linear in R, continuous in (ρ,Q) (e.g., Lemma 1) and $[0,1]\times\mathcal{P}(\mathcal{X})$ is compact, we can apply a well-known result from convex analysis, namely subdifferential of the maximum function (e.g., [56, Theorem 2.87]), to deduce that

$$\partial\mathrm{E_r}(R)=\mathrm{conv}\left(\cup_{Q:\mathrm{E_r}(R,Q)=\mathrm{E_r}(R)}\partial\mathrm{E_r}(\cdot,Q)(R)\right) \quad (4.123)$$
$$=\mathrm{conv}\left(\left\{\left.\frac{\partial\mathrm{E_r}(r,Q)}{\partial r}\right|_{r=R}:\mathrm{E_r}(R,Q)=\mathrm{E_r}(R)\right\}\right), \quad (4.124)$$

where (4.124) follows from item (ii) of Lemma 14. Equation (4.124) implies (4.16).

(ii) Since $\mathrm{E_r}(\cdot)$ is a real-valued, convex function over $[R_{\mathrm{cr}}, C]$ and $R \in (R_{\mathrm{cr}}, C)$, its subdifferential at R, i.e., $\partial \mathrm{E_r}(R)$, is a nonempty, convex and compact set (e.g., [56, Theorem 2.74]), thus ρ_R^* is well-defined. Equation (4.17) is an evident consequence of item (ii) of Theorem 4 by invoking it with the $Q \in \mathcal{P}(\mathcal{X})$ whose existence is assumed in the statement of the theorem. The proof of the claim that (4.18) is a sufficient condition for the existence of a Q with the stated properties follows by contradiction. To this end, let $Q \in \mathcal{P}(\mathcal{X})$ be such that $\mathrm{E_r}(R, Q) = \mathrm{E_r}(R)$, $\rho_R^* = -\frac{\partial \mathrm{E_r}(r,Q)}{\partial r}\Big|_{r=R}$ and (Q, W) pair is singular. Owing to these assumptions, along with the positivity of the channel, one can check that there exists $\delta_y \in \mathbb{R}^+$ such that $W(y|x) = \delta_y$ for all $y \in \mathcal{Y}$ and $x \in \mathcal{X}$ with $Q(x) > 0$. This observation, coupled with the positivity of the channel, implies that $\mathrm{E_o}(\rho, Q) = -\ln \sum_y \delta_y$ for all $\rho \in \mathbb{R}_+$, which contradicts item (i) of Lemma 14. Hence, we conclude that (Q, W) pair should be nonsingular, which suffices to conclude the proof. □

4.4 Proof of Theorem 6

As pointed out in the statement of the theorem, item (ii) is due to Gallager and hence we only prove item (i). Let $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ with $C > 0$ and $R \leq R_{\mathrm{cr}}$ be arbitrary. Assume that for all $Q \in \mathcal{P}(\mathcal{X})$ with $\mathrm{E_o}(1, Q) = \max_{P \in \mathcal{P}(\mathcal{X})} \mathrm{E_o}(1, P)$, the (Q, W) pair is singular. Consider any such $Q \in \mathcal{P}(\mathcal{X})$. For this (Q, W) pair, let $P_{X,Y,Z}$ and $\tilde{P}_{X,Y,Z}$ be as given in (4.29) and (4.30), respectively. Let $\tilde{\mathcal{S}}_Q$ and $\mathcal{X}_y$ be as in (4.3) and (4.4), respectively, for this choice of (Q, W).

First, we show that

$$\ln P_{X,Y,Z}\left\{\tilde{\mathcal{S}}_Q\right\} = -\mathrm{E_o}(1, Q). \tag{4.125}$$

To see this, note that

$$\begin{aligned}
\ln P_{X,Y,Z}\left\{\tilde{\mathcal{S}}_Q\right\} &= \ln \sum_{(x,y,z)\in\tilde{\mathcal{S}}_Q} Q(x)W(y|x)Q(z) && (4.126)\\
&= \ln \sum_{(x,y,z)\in\tilde{\mathcal{S}}_Q} Q(x)W(y|x)^{1/2}Q(z)W(y|z)^{1/2} && (4.127)\\
&= \ln \sum_{y} \left[\sum_{x\in\mathcal{S}(Q)\cap\mathcal{X}_y} Q(x)W(y|x)^{1/2}\right]\left[\sum_{z\in\mathcal{S}(Q)\cap\mathcal{X}_y} Q(z)W(y|z)^{1/2}\right] && (4.128)\\
&= -\mathrm{E_o}(1, Q), && (4.129)
\end{aligned}$$

where (4.127) follows from the singularity of (Q, W).

Further, for any message m

$$\begin{aligned}
\bar{\mathrm{P}}_{\mathrm{e},m}(Q, N, R) &\le \left(\lceil e^{NR}\rceil - 1\right) P_{X,Y,Z}^N \left\{\frac{1}{N}\sum_{n=1}^{N} \ln\frac{W(Y_n|X_n)}{W(Y_n|Z_n)} \le 0\right\} && (4.130)\\
&= \left(\lceil e^{NR}\rceil - 1\right) P_{X,Y,Z}\left\{\tilde{\mathcal{S}}_Q\right\}^N \tilde{P}_{X,Y,Z}^N \left\{\frac{1}{N}\sum_{n=1}^{N} \ln\frac{W(Y_n|X_n)}{W(Y_n|Z_n)} \le 0\right\} && (4.131)\\
&= \left(\lceil e^{NR}\rceil - 1\right) P_{X,Y,Z}\left\{\tilde{\mathcal{S}}_Q\right\}^N && (4.132)\\
&\le e^{-N(-R+\mathrm{E_o}(1,Q))} && (4.133)\\
&= e^{-N\mathrm{E_r}(R)}, && (4.134)
\end{aligned}$$

where (4.131) follows from the fact that for any (x, y, z) with $Q(x)W(y|x)Q(z) > 0$, if $(x, y, z) \notin \tilde{\mathcal{S}}_Q$, then $\ln\frac{W(y|x)}{W(y|z)} = \infty$, (4.132) follows from the singularity of (Q, W), (4.133) follows from (4.125) and (4.134) is true because of the choice of $Q \in \mathcal{P}(\mathcal{X})$ and the fact that $R \le R_{\mathrm{cr}}$ (e.g., [36, pg. 245]). Hence, the upper bound of (4.20) follows.

In order to establish the lower bound of (4.20), one can use Gallager's arguments

[36, pg. 245-246] by noting

$$P_{X,Y,Z}^{N}\left\{\frac{1}{N}\sum_{n=1}^{N}\ln\frac{W(Y_n|X_n)}{W(Y_n|Z_n)}\leq 0\right\}=e^{-N\mathrm{E_o}(1,Q)}. \tag{4.135}$$

□

CHAPTER 5

EXACT ASYMPTOTICS OF THE ERROR PROBABILITY IN CHANNEL CODING: SYMMETRIC CHANNELS

In this chapter, we restrict our attention to an important special class of channels, namely symmetric channels[1].

As pointed out before, in his classical paper [24], Elias has proved that the optimal pre-factor for BSC (resp. BEC) is $\Theta(N^{-0.5(1+|\mathrm{E}'_{\mathrm{SP}}(R)|)})$ (resp. $\Theta(N^{-0.5})$), hence implying that there is at least a dichotomy of symmetric channels with respect to their pre-factors.

Our findings in this chapter establishes that this is indeed the case. In particular, for rates between the critical rate and capacity, we prove that for the typical[2] symmetric channel, $\Theta(N^{-0.5(1+|\mathrm{E}'_{\mathrm{SP}}(R)|)})$ is the pre-factor of the error probability of the optimal (N, R) code, whereas for a small class of channels, $\Theta(N^{-0.5})$ is the order of the pre-factor.

The main technical contribution of this chapter is the converse result for this small class of channels. Moreover, the method we employ to handle this type of channels can be modified to analyze any symmetric channel. Via this methodology, it is possible to prove converse results for the average error probability directly, *without* explicitly reducing the channel coding problem to a binary hypothesis testing problem, as our proof of the converse result for the typical case illustrates.

[1] For the definition symmetric channels, see Definition 9 below.

[2] Precise definition of the property that defines aforementioned dichotomy is given in Definition 10 below.

5.1 Definitions and statement of the results

Throughout this chapter $U_{\mathcal{X}}$ denotes the uniform input distribution over $\mathcal{X}$. For convenience, we recall the two forms[3] of the sphere-packing exponent and the random coding exponent

$$\mathrm{E_{SP}}(R, Q) := \min_{V:\mathrm{I}(Q;V)\leq R} \mathrm{D}(V\|W|Q),\ \mathrm{E_{SP}}(R) := \max_{Q\in\mathcal{P}(\mathcal{X})} \mathrm{E_{SP}}(R, Q), \tag{5.1}$$

$$\tilde{\mathrm{E}}_{\mathrm{SP}}(R, Q) := \sup_{\rho\geq 0} \{-\rho R + \mathrm{E_o}(\rho, Q)\},\ \tilde{\mathrm{E}}_{\mathrm{SP}}(R) := \max_{Q\in\mathcal{P}(\mathcal{X})} \tilde{\mathrm{E}}_{\mathrm{SP}}(R, Q), \tag{5.2}$$

$$\mathrm{E_r}(R, Q) := \max_{0\leq\rho\leq 1} \{-\rho R + \mathrm{E_o}(\rho, Q)\},\ \mathrm{E_r}(R) := \max_{Q\in\mathcal{P}(\mathcal{X})} \mathrm{E_r}(R, Q), \tag{5.3}$$

where

$$\mathrm{E_o}(\rho, Q) := -\ln \sum_{y\in\mathcal{Y}} \left(\sum_{x\in\mathcal{X}} Q(x) W(y|x)^{1/(1+\rho)} \right)^{1+\rho}. \tag{5.4}$$

It is well-known that (e.g., [20, Ex. 2.5.23]) $\mathrm{E_{SP}}(R, P) \geq \tilde{\mathrm{E}}_{\mathrm{SP}}(R, P)$ for any $P \in \mathcal{P}(\mathcal{X})$.

Definition 9 (Gallager [35])**.** *A discrete channel is* symmetric *if the channel outputs can be partitioned into subsets such that within each subset, the matrix of transition probabilities satisfies the following: each row (resp. column) is a permutation of each other row (resp. column).* ◊

Definition 10. *A channel $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ is* singular*, provided that*

$$\forall\, (x, y, z) \text{ s.t. } W(y|x)W(y|z) > 0,\ W(y|x) = W(y|z). \tag{5.5}$$

A channel that is not singular is called nonsingular. ◊

Remark 17. *Definition 10 might be thought as a special case of the one given in the previous chapter by using uniform input distribution.* ◇

[3] As noted before, the Haroutunian form and the Shannon-Gallager-Berlekamp form of the sphere-packing exponent are equal to each other, i.e., $\mathrm{E_{SP}}(R) = \tilde{\mathrm{E}}_{\mathrm{SP}}(R)$. However, for our purposes in this chapter, it is appropriate to distinguish them hence we denote the latter with $\tilde{\mathrm{E}}_{\mathrm{SP}}(R)$.

Theorem 7. *Let W be a symmetric and nonsingular channel with positive dispersion*[4]*.*

(i) For any $R_{cr} < R < C$,

$$P_e(N,R) \leq \frac{K_1}{N^{0.5(1+|E_r'(R)|)}} e^{-NE_r(R)}, \tag{5.6}$$

where K_1 is a positive constant that depends on W and R.

(ii) For any $R_\infty < R < C$ and for all sufficiently large N,

$$\bar{P}_e(N,R) \geq \frac{\tilde{K}_1}{N^{0.5(1+|E_{SP}'(R)|)}} e^{-NE_{SP}(R)}, \tag{5.7}$$

where $\tilde{K}_1$ is a positive constant that depends on W and R. ♦

Theorem 7 is proved in Section 5.2.1.

Theorem 8. *Let W be a symmetric and singular channel with positive dispersion.*

(i) For any $R_{cr} < R < C$,

$$P_e(N,R) \leq \frac{K_2}{\sqrt{N}} e^{-NE_r(R)}, \tag{5.8}$$

where K_2 is a positive constant that depends on W and R.

(ii) For any $R_\infty < R < C$ and for all sufficiently large N,

$$\bar{P}_e(N,R) \geq \frac{\tilde{K}_2}{\sqrt{N}} e^{-NE_{SP}(R)}, \tag{5.9}$$

where $\tilde{K}_2$ is a positive constant that depends on W and R. ♦

Theorem 8 is proved in Section 5.2.2.

[4]Positive dispersion assumption ensures that $R_\infty \leq R_{\text{cr}} < C$ (e.g., [35, pg. 160]).

5.2 Proofs

First, we provide the main idea behind the proof of the converse results. Consider any (N, R) code (f, φ), and let $\mathcal{S}_{R,N} \in \mathcal{Y}^N$ denote an arbitrary set to be chosen later. One can write $\bar{\mathrm{P}}_{\mathrm{e}}(f, \varphi)$ as

$$\bar{\mathrm{P}}_{\mathrm{e}}(f, \varphi) = \Pr\{\mathcal{S}_{R,N}\}\, \bar{\mathrm{P}}_{\mathrm{e}}(f, \varphi | \mathcal{S}_{R,N}), \tag{5.10}$$

where $\bar{\mathrm{P}}_{\mathrm{e}}(f, \varphi | \mathcal{S}_{R,N})$ denotes the average error probability of the code (f, φ) conditioned on $\mathcal{S}_{R,N}$. If one can choose $\mathcal{S}_{R,N}$, potentially by using an auxiliary output distribution, such that its probability is a good approximation[5] of the probability of error event of the code and can prove that $\bar{\mathrm{P}}_{\mathrm{e}}(f, \varphi | \mathcal{S}_{R,N}) = \Theta(1)$, then (5.10) will give sphere-packing lower bound. The last step might intuitively be thought similar to the (strong) converse to the channel coding theorem (e.g., [72]), but an appropriate choice of $\mathcal{S}_{R,N}$ in the first step is not evident.

If the channel is nonsingular, then we might expect to benefit from our analysis in Chapter 3, because the sought-after optimal order of the pre-factor has the slope-related term and Theorem 3 basically give the result if the restriction of constant composition codes can be dropped. We will do so, by choosing $\mathcal{S}_{R,N}$ similar to (3.48) and exploiting the symmetry of the channel[6].

It should be noted that the threshold of the aforementioned choice of $\mathcal{S}_{R,N}$ varies with a speed of $O\left(\frac{\ln \sqrt{N}}{N}\right)$. Hence, using this particular choice cannot give a pre-factor of $\Theta(N^{-0.5})$, which is the one we would like to prove for singular channels. By exploiting the singularity and the symmetry of the channel, which gives it a special structure, we choose a set $\mathcal{S}_{R,N}$ that involves deviations of a certain scaled sum of independent random

[5] For example, a prerequisite of a good approximation is vanishing exponentially fast with an exponent not larger than $\mathrm{E}_{\mathrm{SP}}(R)$.

[6] The fact that for symmetric channels it is possible to drop the constant composition step in the original derivations of the sphere-packing exponent has been observed in [71].

variables from a constant threshold[7] and prove that its probability vanishes exponentially fast with the exponent $\mathrm{E_{SP}}(R)$. Recalling Bahadur-Rao result, it will not be surprising to have an $\Theta(N^{-0.5})$ sub-exponential term for the probability of such a set, although how to choose a set with these properties is not evident.

In the rest of the chapter, we make the aforementioned intuition rigorous. To this end, we begin with a result that will be used in the proofs of both Theorem 7 and 8.

Lemma 22. *Fix a symmetric channel $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ with positive dispersion. Consider any $R_\infty < R < C$.*

(i) $E_{SP}(R) = E_{SP}(R, U_\mathcal{X}) = \tilde{E}_{SP}(R, U_\mathcal{X}) = \tilde{E}_{SP}(R)$.

(ii) For any $\rho \in \mathbb{R}_+$,

$$\sum_{y\in\mathcal{Y}} W(y|x)^{\frac{1}{1+\rho}} \left(\sum_{z\in\mathcal{X}} U_\mathcal{X}(z) W(y|z)^{\frac{1}{1+\rho}}\right)^{\rho} = \sum_{y\in\mathcal{Y}} \left(\sum_{z\in\mathcal{X}} U_\mathcal{X}(z) W(y|z)^{\frac{1}{1+\rho}}\right)^{1+\rho}, \tag{5.11}$$

for all $x \in \mathcal{X}$.

(iii) $\rho_R(U_\mathcal{X}) := -\left.\frac{\partial E_{SP}(r,U_\mathcal{X})}{\partial r}\right|_{r=R} \in \mathbb{R}^+$ *is well-defined and attains the supremum in the definition of $\tilde{E}_{SP}(R, U_\mathcal{X})$ (cf.,* (5.2)*).*

(iv) $q_R(y) := \dfrac{\left(\sum_{x\in\mathcal{X}} U_\mathcal{X}(x) W(y|x)^{\frac{1}{1+\rho_R(U_\mathcal{X})}}\right)^{1+\rho_R(U_\mathcal{X})}}{\sum_{b\in\mathcal{Y}}\left(\sum_{a\in\mathcal{X}} U_\mathcal{X}(a) W(b|a)^{\frac{1}{1+\rho_R(U_\mathcal{X})}}\right)^{1+\rho_R(U_\mathcal{X})}}$ *is a minimizer of the following optimization problem*

$$\min_{q\in\mathcal{P}(\mathcal{Y})} \left\{ -\rho_R(U_\mathcal{X})R - (1+\rho_R(U_\mathcal{X})) \sum_{x\in\mathcal{X}} U_\mathcal{X}(x) \ln \sum_{y\in\mathcal{Y}} W(y|x)^{\frac{1}{1+\rho_R(U_\mathcal{X})}} q(y)^{\frac{\rho_R(U_\mathcal{X})}{1+\rho_R(U_\mathcal{X})}} \right\}. \tag{5.12}$$

♦

Proof. The proof is given in Appendix D.1. □

[7] To be specific, threshold varies with a speed of $O(1/N)$. However, this variation only changes the constant in the final bound.

5.2.1 Proof of Theorem 7

We begin with the proof of (5.6). Owing to the symmetry of the channel, $\mathrm{E_r}(\cdot, U_{\mathcal{X}}) = \mathrm{E_r}(\cdot)$ on (R_{cr}, C) (e.g., [35, pg. 145]). Since $\mathrm{E_r}(\cdot, U_{\mathcal{X}})$ is continuously differentiable over (R_{cr}, C) (e.g., item (ii) of Lemma 14) and $(U_{\mathcal{X}}, W)$ pair is non-singular (e.g., Definition 8), (5.6) is a direct consequence of item (ii) of Theorem 5.

To prove (5.7), let q_R and $\rho_R(U_{\mathcal{X}})$ be as defined in Lemma 22. For convenience, we drop[8] $U_{\mathcal{X}}$ dependence in $\rho_R(U_{\mathcal{X}})$ from now on. Evidently[9], $q_R(y) > 0$ for all $y \in \mathcal{Y}$.

For any $R_\infty < r \leq R$, we define

$$\mathrm{e_{SP}}(r, R) := \inf_{V \in \mathcal{P}(\mathcal{Y}|\mathcal{X}) : \mathrm{D}(V\|q_R|U_{\mathcal{X}}) \leq r} \mathrm{D}(V\|W|U_{\mathcal{X}}). \tag{5.13}$$

For any $\mathbf{x}^N$ and $r \in \mathbb{R}_+$, let

$$\mathcal{S}\left(\mathbf{x}^N, r\right) := \left\{ \frac{1}{N} \sum_{n=1}^{N} \ln \frac{W(Y_n|x_n)}{q_R(Y_n)} \leq r - \mathrm{e_{SP}}(r, R) \right\}. \tag{5.14}$$

Lemma 23. *For any $\lambda \in \mathbb{R}$, $M_x(\lambda) := \sum_{y: W(y|x)>0} W(y|x)^{1-\lambda} q_R(y)^{\lambda}$ is finite and constant in $x \in \mathcal{X}$.* ♦

Proof. $M_x(\lambda) \in \mathbb{R}$ is an evident consequence of the fact that $W(\cdot|x) \ll q_R$ for any $x \in \mathcal{X}$, which is a direct consequence of the fact that $\mathcal{S}(q_R) = \mathcal{Y}$. Let $\{\mathcal{Y}_l\}_{l=1}^{L}$ be a partition[10] of the columns of W mentioned in Definition 9. Since each column is a permutation of any other column within the partition, $\left(\sum_{x \in \mathcal{X}} U_{\mathcal{X}}(x) W(y|x)^{1/(1+\rho_R)}\right)^{1+\rho_R}$ has the same value for any $y \in \mathcal{Y}_l$. This observation, coupled with the fact that all rows are permutations of each other row, suffices to conclude the proof of the second assertion. □

[8] Since $\frac{\partial \mathrm{E_{SP}}(a, U_{\mathcal{X}})}{\partial a}\Big|_{a=R} = -\frac{\partial \mathrm{E_{SP}}(a)}{\partial a}\Big|_{a=R}$, which is a direct consequence of items (i) and (iii) of Lemma 22, this dependence is redundant, indeed.

[9] Without loss of generality, we assume that W has no all-zero column.

[10] The choice of the partition is immaterial in what follows.

Remark 18. *The fact that we can lower bound error probability of an arbitrary code, as opposed to an arbitrary constant composition code, is essentially due to Lemma 23. However, its proof heavily depends on the symmetry of the channel and an analogous result for asymmetric channels is not evident to us.* $\diamond$

Using Lemma 23, along with the uniqueness theorem for moment generating functions (e.g., [11, Ex. 26.7]), we deduce that for any $\mathbf{x}^N$ and $r \in \mathbb{R}_+$,

$$W\left\{\mathcal{S}\left(\mathbf{x}^N, r\right) \mid \mathbf{x}^N\right\} = W\left\{\frac{1}{N}\sum_{n=1}^{N} \ln \frac{W(Y_n|x_{\mathrm{o}})}{q_R(Y_n)} \leq r - \mathrm{e}_{\mathrm{SP}}(r,R) \mid \mathbf{x}_{\mathrm{o}}^N\right\}, \tag{5.15}$$

where $\mathbf{x}_{\mathrm{o}}^N$ is an N-tuple consisting of all $x_{\mathrm{o}} \in \mathcal{X}$ and the choice of x_{o} is immaterial. For any $\lambda \in \mathbb{R}$, we define

$$\Lambda(\lambda) := \ln \mathrm{E}_{W(\cdot|x_{\mathrm{o}})}\left[e^{\lambda \ln \frac{q_R(Y)}{W(Y|x_{\mathrm{o}})}}\right]. \tag{5.16}$$

As a direct consequence of Lemma 23, $\Lambda(\cdot) \in \mathbb{R}$ over the real line, which, in turn, ensures that $\Lambda(\cdot)$ is smooth on $\mathbb{R}$.

For any $x \in \mathcal{X}$, define

$$W_R(y|x) := \begin{cases} \frac{q_R(y)}{q_R(\mathcal{S}(W(\cdot|x)))}, & \text{if } y \in \mathcal{S}(W(\cdot|x)), \\ 0, & \text{else.} \end{cases} \tag{5.17}$$

Evidently, $W_R(\cdot|x) \equiv W(\cdot|x)$, for all $x \in \mathcal{X}$.

Lemma 24. *(i)* $R > D(W_R\|q_R|U_{\mathcal{X}})$.

(ii) For any $r \in (D(W_R\|q_R|U_{\mathcal{X}}), R]$, $e_{SP}(r,R) = \max_{\rho\in\mathbb{R}_+}\left\{-\rho r - (1+\rho)\Lambda\left(\frac{\rho}{1+\rho}\right)\right\}$.

(iii) $e_{SP}(R,R) = E_{SP}(R)$. $\blacklozenge$

Proof. The proof is given in Appendix D.2. $\square$

For any $x \in \mathcal{X}$ and $\lambda \in [0,1)$, we define

$$\tilde{W}_\lambda(y|x) := \frac{W(y|x)^{1-\lambda} q_R(y)^\lambda}{\sum_{b:W(b|x)>0} W(b|x)^{1-\lambda} q_R(b)^\lambda}. \tag{5.18}$$

By elementary calculation, one can verify that

$$\Lambda'(\lambda) = \mathrm{E}_{\tilde{W}_\lambda(\cdot|x_0)}\left[\ln \frac{q_R(Y)}{W(Y|x_0)}\right],\ \Lambda''(\lambda) = \mathrm{Var}_{\tilde{W}_\lambda(\cdot|x_0)}\left[\ln \frac{q_R(Y)}{W(Y|x_0)}\right]. \tag{5.19}$$

Similarly, for any $\lambda \in [0,1)$, we define

$$m_3(\lambda) := \mathrm{E}_{\tilde{W}_\lambda(\cdot|x_0)}\left[\left|\ln \frac{q_R(Y)}{W(Y|x_0)} - \Lambda'(\lambda)\right|^3\right]. \tag{5.20}$$

From (5.18), (5.19) and (5.20), one can verify that $\Lambda'(\cdot)$, $\Lambda''(\cdot)$ and $m_3(\cdot)$ are continuous over $[0,1)$.

For any $b \in \mathbb{R}$, let $\Lambda^*(b)$ denote the Fenchel-Legendre transform of $\Lambda(\cdot)$ at b, i.e.,

$$\Lambda^*(b) := \sup_{\lambda \in \mathbb{R}} \{\lambda b - \Lambda(\lambda)\}. \tag{5.21}$$

Lemma 25. *(i)* $\Lambda''(\lambda) > 0$, *for any* $\lambda \in [0,1)$.

(ii) For any $r \in (D(W_R\|q_R|U_X), R]$, $s_r := -\frac{\partial e_{SP}(a,R)}{\partial a}\Big|_{a=r}$ *is a well-defined, continuous, positive and strictly decreasing function.*

(iii) Fix some $D(W_R\|q_R|U_X) < r \le R$. $\Lambda^*(e_{SP}(r,R) - r) = e_{SP}(r,R)$. *Moreover, there exists a unique* $\eta_r \in (0,1)$ *such that* $\Lambda'(\eta_r) = e_{SP}(r,R) - r$ *and* $\eta_r = s_r/(1+s_r)$. ♦

Proof. The proof is given in Appendix D.3. □

Define

$$\bar{R} := (R + \mathrm{D}(W_R\|q_R|U_X))/2. \tag{5.22}$$

Due to item (i) of Lemma 24, $\bar{R} \in (\mathrm{D}(W_R\|q_R|U_X), R)$. Moreover, as a direct consequence of items (ii) and (iii) of Lemma 25,

$$0 < \eta_R < \eta_r < \eta_{\bar{R}} < 1, \tag{5.23}$$

for any $r \in (\bar{R}, R)$. Fix an arbitrary $a > 1$ and define

$$t_{\max} := a2\sqrt{2\pi}\eta_{\bar{R}} \max_{\lambda\in[0,\eta_{\bar{R}}]} \frac{m_3(\lambda)}{\Lambda''(\lambda)}, \tag{5.24}$$

$$m_{2,\min} := \min_{\lambda\in[0,\eta_{\bar{R}}]} \Lambda''(\lambda), \tag{5.25}$$

$$m_{2,\max} := \max_{\lambda\in[0,\eta_{\bar{R}}]} \Lambda''(\lambda). \tag{5.26}$$

Evidently, all of the aforementioned quantities are well-defined and $t_{\max}, m_{2,\min}, m_{2,\max} \in \mathbb{R}^+$. Finally, define

$$k_{\mathrm{o}} := \frac{e^{-t_{\max}}\left(1-\frac{1}{a}\right)}{\eta_{\bar{R}} 2\sqrt{2\pi m_{2,\max}}} \in \mathbb{R}^+. \tag{5.27}$$

Fix $k_1, k_2 \in \mathbb{R}^+$ that satisfy $k_2 - k_1 = \ln k_{\mathrm{o}}$. For any $N \in \mathbb{Z}^+$, define $R_N := R - \frac{\ln\sqrt{N}}{N} - \frac{k_1}{N}$. Consider a sufficiently large N, such that

$$R_N \geq \bar{R} \quad \text{and} \quad \frac{[1+(1+t_{\max})^2]}{\eta_R\left(1-\frac{1}{a}\right)2\sqrt{eNm_{2,\min}}} \leq \frac{1}{2}. \tag{5.28}$$

Consider any (N, R) code, say (f_N, φ_N), with decoding regions $\{\mathcal{A}_m\}_{m=1}^{|\mathcal{M}|}$ and codewords $\left\{\mathbf{x}^N(m)\right\}_{m=1}^{|\mathcal{M}|}$, where $\mathcal{M} := \{1, \ldots, \lceil e^{NR}\rceil\}$ denotes the set of messages. Let $\bar{\mathrm{P}}_{\mathrm{e}}(f_N, \varphi_N)$ denote the average error probability of (f_N, φ_N). We have

$$\bar{\mathrm{P}}_{\mathrm{e}}(f_N, \varphi_N) = \frac{1}{|\mathcal{M}|}\sum_{m\in\mathcal{M}}\sum_{\mathbf{y}^N\in\mathcal{A}_m^c} W(\mathbf{y}^N|\mathbf{x}^N(m)). \tag{5.29}$$

For any $m \in \mathcal{M}$, we have

$$W\left\{\mathcal{S}(\mathbf{x}^N(m), R_N)|\mathbf{x}^N(m)\right\} = W\left\{\mathcal{S}(\mathbf{x}_{\mathrm{o}}^N, R_N)|\mathbf{x}_{\mathrm{o}}^N\right\} \tag{5.30}$$

$$\geq \frac{k_{\mathrm{o}}\left(1 + a2\sqrt{2\pi}\eta_{R_N}\frac{m_3(\eta_{R_N})}{\Lambda''(\eta_{R_N})}\right)}{\sqrt{N}} e^{-N\mathrm{e_{SP}}(R_N,R)} \tag{5.31}$$

$$\geq \frac{k_{\mathrm{o}}}{\sqrt{N}} e^{-N\mathrm{e_{SP}}(R_N,R)} \tag{5.32}$$

$$> 0, \tag{5.33}$$

where (5.30) follows from (5.15), along with the definition of $\mathcal{S}(\mathbf{x}_{\mathrm{o}}^N, R_N)$, i.e., (5.14), (5.31) follows from the concentration lemma, i.e. Lemma 5, whose applicability is ensured by items (i) and (iii) of Lemma 25, coupled with (5.28).

Continuing from (5.29), we have

$$\bar{\mathrm{P}}_{\mathrm{e}}(f_N, \varphi_N) \geq \sum_{m\in\mathcal{M}} \frac{W\left\{\mathcal{S}(\mathbf{x}^N(m), R_N)|\mathbf{x}^N(m)\right\}}{|\mathcal{M}|} \sum_{\mathbf{y}^N\in\mathcal{A}_m^c\cap\mathcal{S}(\mathbf{x}^N(m),R_N)} \frac{W(\mathbf{y}^N|\mathbf{x}^N(m))}{W\left\{\mathcal{S}(\mathbf{x}^N(m), R_N)|\mathbf{x}^N(m)\right\}} \tag{5.34}$$

$$\geq \frac{k_{\mathrm{o}}}{\sqrt{N}} e^{-N\mathrm{e}_{\mathrm{SP}}(R_N,R)} \frac{1}{|\mathcal{M}|} \sum_{m\in\mathcal{M}} \sum_{\mathbf{y}^N\in\mathcal{A}_m^c\cap\mathcal{S}(\mathbf{x}^N(m),R_N)} \frac{W(\mathbf{y}^N|\mathbf{x}^N(m))}{W\left\{\mathcal{S}(\mathbf{x}^N(m), R_N)|\mathbf{x}^N(m)\right\}}, \tag{5.35}$$

where (5.35) follows from (5.33).

For all $m \in \mathcal{M}$, define[11]

$$P_{Y|X,\mathcal{S}(\mathbf{x}^N(m),R_N)}(\mathbf{y}^N|\mathbf{x}^N(m)) := \begin{cases} \frac{W(\mathbf{y}^N|\mathbf{x}^N(m))}{W\left\{\mathcal{S}(\mathbf{x}^N(m),R_N)|\mathbf{x}^N(m)\right\}}, & \text{if } \mathbf{y}^N \in \mathcal{S}(\mathbf{x}^N(m), R_N), \\ 0, & \text{else.} \end{cases} \tag{5.36}$$

$$P_{Y|\mathcal{S}(\mathbf{x}^N(m),R_N)}(\mathbf{y}^N) := \begin{cases} \frac{q_R(\mathbf{y}^N)}{q_R\left\{\mathcal{S}(\mathbf{x}^N(m),R_N)\right\}}, & \text{if } \mathbf{y}^N \in \mathcal{S}(\mathbf{x}^N(m), R_N), \\ 0, & \text{else.} \end{cases} \tag{5.37}$$

Using (5.36) in (5.35), we have

$$\bar{\mathrm{P}}_{\mathrm{e}}(f_N, \varphi_N) \geq \frac{k_{\mathrm{o}}}{\sqrt{N}} e^{-N\mathrm{e}_{\mathrm{SP}}(R_N,R)} \frac{1}{|\mathcal{M}|} \sum_{m\in\mathcal{M}} \sum_{\mathbf{y}^N\in\mathcal{A}_m^c} P_{Y|X,\mathcal{S}(\mathbf{x}^N(m),R_N)}(\mathbf{y}^N|\mathbf{x}^N(m)) \tag{5.38}$$

$$= \frac{k_{\mathrm{o}}}{\sqrt{N}} e^{-N\mathrm{e}_{\mathrm{SP}}(R_N,R)} \left(1 - \frac{1}{|\mathcal{M}|} \sum_{m\in\mathcal{M}} \sum_{\mathbf{y}^N\in\mathcal{A}_m} P_{Y|X,\mathcal{S}(\mathbf{x}^N(m),R_N)}(\mathbf{y}^N|\mathbf{x}^N(m))\right). \tag{5.39}$$

Lemma 26. *For any $m \in \mathcal{M}$,*

$$\frac{1}{N} \ln \frac{P_{Y|X,\mathcal{S}(\mathbf{x}^N(m),R_N)}(\mathbf{y}^N|\mathbf{x}^N(m))}{P_{Y|\mathcal{S}(\mathbf{x}^N(m),R_N)}(\mathbf{y}^N)} \leq R - \frac{k_2}{N}, \tag{5.40}$$

for all $\mathbf{y}^N$ with $P_{Y|X,\mathcal{S}(\mathbf{x}^N(m),R_N)}(\mathbf{y}^N|\mathbf{x}^N(m)) > 0$. ♦

[11] Since $q_R \gg W(\cdot|x)$, (5.33) ensures that both of the following are well-defined probability measures.

Proof. Fix any $m \in \mathcal{M}$ and $\mathbf{y}^N \in \mathcal{S}\left(\mathbf{x}^N(m), R_N\right)$ with $W(\mathbf{y}^N|\mathbf{x}^N(m)) > 0$. We have

$$\frac{1}{N}\ln\frac{P_{Y|X,\mathcal{S}(\mathbf{x}^N(m),R_N)}(\mathbf{y}^N|\mathbf{x}^N(m))}{P_{Y|\mathcal{S}(\mathbf{x}^N(m),R_N)}(\mathbf{y}^N)} = \frac{1}{N}\ln\frac{W(\mathbf{y}^N|\mathbf{x}^N(m))}{q_R(\mathbf{y}^N)} + \frac{1}{N}\ln\frac{q_R\left\{\mathcal{S}(\mathbf{x}^N(m),R_N)\right\}}{W\left\{\mathcal{S}(\mathbf{x}^N(m),R_N)|\mathbf{x}^N(m)\right\}} \tag{5.41}$$

$$\leq \frac{1}{N}\ln\frac{W(\mathbf{y}^N|\mathbf{x}^N(m))}{q_R(\mathbf{y}^N)} + \mathrm{e}_{\mathrm{SP}}(R_N,R) + \frac{\ln\sqrt{N}}{N} - \frac{\ln k_{\mathrm{o}}}{N} \tag{5.42}$$

$$\leq R - \frac{k_2}{N}, \tag{5.43}$$

where (5.41) follows from the definitions of $P_{Y|X,\mathcal{S}(\mathbf{x}^N(m),R_N)}$ and $P_{Y|\mathcal{S}(\mathbf{x}^N(m),R_N)}$, i.e., (5.36) and (5.37), (5.42) follows from (5.32) and (5.43) follows from the definition of $\mathcal{S}\left(\mathbf{x}^N(m),R_N\right)$, i.e., (5.14), along with the fact that $k_2 - k_1 = \ln k_{\mathrm{o}}$. □

By using Lemma 26, along with the fact that decoding regions are disjoint and $P_{Y|\mathcal{S}(\mathbf{x}^N(m),R_N)}$ is a probability measure, (5.39) further implies that

$$\bar{\mathrm{P}}_{\mathrm{e}}(f_N,\varphi_N) \geq \frac{\left(1-e^{-k_2}\right)k_{\mathrm{o}}}{\sqrt{N}}e^{-N\mathrm{e}_{\mathrm{SP}}(R_N,R)}. \tag{5.44}$$

Lemma 27. *Let* $\epsilon_N := \frac{\ln\sqrt{N}}{N} + \frac{k_1}{N}$. *We have*

$$e_{SP}(R_N,R) \leq E_{SP}(R) + \epsilon_N|E'_{SP}(R)| + \epsilon_N^2\frac{(1+|E'_{SP}(R)|)}{2m_{2,\min}}(1+s_{\bar{R}})^2. \tag{5.45}$$

♦

Proof. The proof is given in Appendix D.4. □

Let $N \in \mathbb{Z}^+$ be sufficiently large such that $e^{-N\epsilon_N^2\frac{(1+|\mathrm{E}'_{\mathrm{SP}}(R)|)}{2m_{2,\min}}(1+s_{\bar{R}})^2} \geq 1/2$. Then, Lemma 27 and (5.44) imply that

$$\bar{\mathrm{P}}_{\mathrm{e}}(f_N,\varphi_N) \geq \frac{k_{\mathrm{o}}(1-e^{-k_2})e^{-k_1|\mathrm{E}'_{\mathrm{SP}}(R)|}}{2}\frac{e^{-N\mathrm{E}_{\mathrm{SP}}(R)}}{N^{0.5(1+|\mathrm{E}'_{\mathrm{SP}}(R)|)}}. \tag{5.46}$$

Since the code is arbitrary, (5.46) implies (5.7). □

5.2.2 Proof of Theorem 8

Due to the symmetry of the channel, $\mathrm{E_r}(\cdot, U_{\mathcal{X}}) = \mathrm{E_r}(\cdot)$ on (R_{cr}, C) (e.g., [35, pg. 145]). Since $(U_{\mathcal{X}}, W)$ is singular (e.g., Definition 8), (5.8) is a direct consequence of item (i) of Corollary 3.

To prove item (ii), define $q(y) := \sum_{x\in\mathcal{X}} U_{\mathcal{X}}(x)W(y|x)$. Due to the singularity of W, given any $y \in \mathcal{Y}$, $W(y|\cdot)$ is either zero or a positive constant that depends on y, say δ_y. Hence,

$$q(y) = \delta_y \alpha_y \text{ with } \alpha_y := \sum_{x:W(y|x)>0} U_{\mathcal{X}}(x). \tag{5.47}$$

Evidently,[12] $q(y) > 0$ for all $y \in \mathcal{Y}$ and hence $q \gg W(\cdot|x)$ for any $x \in \mathcal{X}$.

For any $r \in \mathbb{R}_+$, define

$$\mathcal{S}(r) := \left\{ \mathbf{y}^N : \frac{1}{N}\sum_{n=1}^{N} \ln \frac{1}{\alpha_{y_n}} \le r \right\}. \tag{5.48}$$

Let $\bar{R} := \frac{R+R_\infty}{2}$. Fix some $k \in \mathbb{R}^+$ and define $R_N := R - \frac{k}{N}$. Consider a sufficiently large N, such that $R_N \ge \bar{R}$.

Lemma 28. *(i) For any* $\mathbf{x}^N$*,*

$$W\left\{\mathcal{S}(R_N)|\mathbf{x}^N\right\} = W\left\{\mathcal{S}(R_N)|\mathbf{x}_o^N\right\}, \tag{5.49}$$

where $\mathbf{x}_o^N$ *is an N-tuple consisting of all* x_o*, for some* $x_o \in \mathcal{X}$*.*

(ii) For some $\tilde{K} \in \mathbb{R}^+$ *that depends on* $R, \bar{R}$ *and* W*,*

$$W\left\{\mathcal{S}(R_N)|\mathbf{x}_o^N\right\} \ge \frac{\tilde{K}}{\sqrt{N}} e^{-NE_{SP}(R)} > 0, \tag{5.50}$$

for all sufficiently large N*.* ♦

Proof. The proof is given in Appendix D.5. □

[12] Without loss of generality, we assume that W has no all-zero column.

Remark 19. *Similar to the nonsingular case, item (i) of Lemma 28 enables us to directly bound error probability of any code instead of restricting the analysis to the constant composition codes.* $\diamond$

Consider any (N, R) code, say (f_N, φ_N), with decoding regions $\{\mathcal{A}_m\}_{m=1}^{|\mathcal{M}|}$ and codewords $\{\mathbf{x}^N(m)\}_{m=1}^{|\mathcal{M}|}$, where $\mathcal{M}$ denotes the set of messages. Let $\bar{\mathrm{P}}_{\mathrm{e}}(f_N, \varphi_N)$ denote the average error probability of this code. We have

$$\bar{\mathrm{P}}_{\mathrm{e}}(f_N, \varphi_N) = \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \sum_{\mathbf{y}^N \in \mathcal{A}_m^c} W(\mathbf{y}^N | \mathbf{x}^N(m)) \tag{5.51}$$

$$\geq \frac{\tilde{K}}{\sqrt{N}} e^{-N \mathrm{E}_{\mathrm{SP}}(R)} \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \sum_{\mathbf{y}^N \in \mathcal{A}_m^c \cap \mathcal{S}(R_N)} \frac{W(\mathbf{y}^N | \mathbf{x}^N(m))}{W\{\mathcal{S}(R_N) | \mathbf{x}^N(m)\}}, \tag{5.52}$$

where (5.52) follows from Lemma 28.

For all $m \in \mathcal{M}$, define[13]

$$P_{Y|X,\mathcal{S}(R_N)}(\mathbf{y}^N | \mathbf{x}^N(m)) := \begin{cases} \frac{W(\mathbf{y}^N | \mathbf{x}^N(m))}{W\{\mathcal{S}(R_N) | \mathbf{x}^N(m)\}}, & \text{if } \mathbf{y}^N \in \mathcal{S}(R_N), \\ 0, & \text{else.} \end{cases} \tag{5.53}$$

$$P_{Y|\mathcal{S}(R_N)}(\mathbf{y}^N) := \begin{cases} \frac{q_R(\mathbf{y}^N)}{q_R\{\mathcal{S}(R_N)\}}, & \text{if } \mathbf{y}^N \in \mathcal{S}(R_N), \\ 0, & \text{else.} \end{cases} \tag{5.54}$$

Using (5.53) in (5.52), we deduce that

$$\bar{\mathrm{P}}_{\mathrm{e}}(f_N, \varphi_N) \geq \frac{\tilde{K}}{\sqrt{N}} e^{-N \mathrm{E}_{\mathrm{SP}}(R)} \left(1 - \frac{1}{|\mathcal{M}|} \sum_{m \in \mathcal{M}} \sum_{\mathbf{y}^N \in \mathcal{A}_m} P_{Y|X,\mathcal{S}(R_N)}(\mathbf{y}^N | \mathbf{x}^N(m)) \right). \tag{5.55}$$

Lemma 29. *For any $m \in \mathcal{M}$,*

$$\frac{1}{N} \ln \frac{P_{Y|X,\mathcal{S}(R_N)}(\mathbf{y}^N | \mathbf{x}^N(m))}{P_{Y|\mathcal{S}(R_N)}(\mathbf{y}^N)} \leq R - \frac{k}{N}, \tag{5.56}$$

for all $\mathbf{y}^N$ with $P_{Y|X,\mathcal{S}(R_N)}(\mathbf{y}^N | \mathbf{x}^N(m)) > 0$. $\blacklozenge$

[13] From item (ii) of Lemma 28 and the fact that $q \gg W(\cdot|x)$, both of the following are well-defined probability measures.

Proof. Fix any $m \in \mathcal{M}$ and $\mathbf{y}^N \in \mathcal{S}(R_N)$ with $W(\mathbf{y}^N|\mathbf{x}^N(m)) > 0$. First, we claim that

$$q(\mathcal{S}(R_N)) = W\left\{\mathcal{S}(R_N)|\mathbf{x}^N(m)\right\}. \tag{5.57}$$

To see this,

$$\begin{aligned} q(\mathcal{S}(R_N)) &= \sum_{\mathbf{x}^N} U_{\mathcal{X}^N}(\mathbf{x}^N) \sum_{\mathbf{y}^N} W(\mathbf{y}^N|\mathbf{x}^N) \mathbb{1}\left\{\mathbf{y}^N : \frac{1}{N}\sum_{n=1} \ln \frac{1}{\alpha_{y_n}} \leq R_N\right\} \\ &= \sum_{\mathbf{x}^N} U_{\mathcal{X}^N}(\mathbf{x}^N) W\left\{\mathcal{S}(R_N)|\mathbf{x}^N\right\} \\ &= \sum_{\mathbf{x}^N} U_{\mathcal{X}^N}(\mathbf{x}^N) W\left\{\mathcal{S}(R_N)|\mathbf{x}_{\mathrm{o}}^N\right\} \qquad (5.58) \\ &= W\left\{\mathcal{S}(R_N)|\mathbf{x}^N(m)\right\}, \qquad (5.59) \end{aligned}$$

where both (5.58) and (5.59) follow from item (i) of Lemma 28. Hence,

$$\frac{1}{N} \ln \frac{P_{Y|X,\mathcal{S}(R_N)}(\mathbf{y}^N|\mathbf{x}^N(m))}{P_{Y|\mathcal{S}(R_N)}(\mathbf{y}^N)} = \frac{1}{N} \ln \frac{W(\mathbf{y}^N|\mathbf{x}^N(m))}{q(\mathbf{y}^N)} = \frac{1}{N}\sum_{n=1}^{N} \ln \frac{1}{\alpha_{y_n}} \leq R - \frac{k}{N}, \tag{5.60}$$

where the first equality follows from (5.57), the second equality follows from the fact that whenever $W(y|x) > 0$, $\frac{W(y|x)}{q(y)} = \frac{1}{\alpha_y}$, which is a direct consequence of the singularity of the channel, and the inequality follows from the definition of $\mathcal{S}(R_N)$, i.e., (5.48). □

By using Lemma 29, along with the fact that decoding regions are disjoint and $P_{Y|\mathcal{S}(R_N)}$ is a probability measure, (5.55) implies that

$$\bar{\mathrm{P}}_{\mathrm{e}}(f_N, \varphi_N) \geq \frac{\tilde{K}\left(1 - e^{-k}\right)}{\sqrt{N}} e^{-N\mathrm{E}_{\mathrm{SP}}(R)}. \tag{5.61}$$

Since the code is arbitrary, (5.61) implies (5.9). □

CHAPTER 6

CONCLUSION AND FUTURE WORK

In this thesis, we considered two asymptotic setups regarding the blocklength, rate and error probability interplay of the optimum block code(s) on a discrete memoryless channel.

In the first setup, we introduced moderate deviations (medium error probability regime) in channel coding, as a more balanced way of using available blocklength compared to the classical small and large error probability regimes. We proved that when the rate increases to the capacity with a slower speed than the large error probability regime, error probability decays sub-exponentially fast and showed that the rate of this decay is inversely proportional to the channel dispersion.

In the second setup, we took a closer look at the small error probability regime to improve the sub-exponential terms in the classical error probability bounds, to address the accuracy issue of the error exponent results that limits their practical usage, especially for rates around the capacity. Our improved pre-factor orders are close to each other and coincide for symmetric channels. Further, for symmetric channels with positive dispersion, we discovered a phase transition of the optimal pre-factor order.

Before we conclude, we present a list[1] of possible research directions related to the results in this thesis:

1. In Chapter 2, our focus was on the leading order term in the error probability decay. An analysis similar to the remaining chapters to improve the lower-order terms might be an interesting topic for future work.

[1]The following list is not meant to be exhaustive and the ordering is not with respect to significance or elegance.

2. In Chapter 2, we proved a moderate deviations result for positive dispersion channels. Extending the analysis to zero-dispersion channels might be interesting from a theoretical perspective, since the order of the sub-exponential decay is likely to be different.

3. Dropping the constant composition code restriction in Theorem 3 appears to be a compelling, yet challenging direction to research.

4. The main result of Chapter 3 does not distinguish between singular and non-singular channels. In light of the results of Chapter 4 and 5, one would expect that a lower bound with a pre-factor of $\Theta(1/\sqrt{N})$ holds (at least for constant composition codes) for singular, asymmetric channels.

5. Researching the role of singularity on the third-order term in the normal approximation regime is an interesting topic to investigate.

6. Extending the refined analysis for the small error probability regime in channel coding to other information theory problems is an evident avenue to research. Lossy source coding seems to be a tempting starting point for such a study.

APPENDIX A

APPENDIX OF CHAPTER 2

A.1 Proof of Lemma 1

Consider any $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$. For all $y \in \mathcal{Y}$, define

$$\mathcal{X}_y := \{x \in \mathcal{X} : W(y|x) > 0\}. \tag{A.1}$$

Observe that owing to the no all-zero column assumption on W and (A.1), for all $y \in \mathcal{Y}$, $\mathcal{X}_y \neq \emptyset$. Moreover, for any $P \in \mathcal{P}(\mathcal{X})$, there exists $y \in \mathcal{Y}$ with $\mathcal{X}_y \cap \mathcal{S}(P) \neq \emptyset$.

For all $y \in \mathcal{Y}$, define

$$f_y \,:\, \mathbb{R}_+ \times \mathcal{P}(\mathcal{X}) \to \mathbb{R}_+, \text{ s.t. } f_y(\rho, P) := \sum_{x \in \mathcal{X}} P(x) W(y|x)^{\frac{1}{(1+\rho)}}, \; \forall\, (\rho, P) \in \mathbb{R}_+ \times \mathcal{P}(\mathcal{X}). \tag{A.2}$$

Evidently $f_y(\cdot, \cdot)$ is continuous on $\mathbb{R}_+ \times \mathcal{P}(\mathcal{X})$. Also, straightforward calculation reveals that

$$\frac{\partial f_y(\rho, P)}{\partial \rho} = -\frac{1}{(1+\rho)^2} \sum_{x \in \mathcal{X}_y} P(x) W(y|x)^{\frac{1}{(1+\rho)}} \ln W(y|x), \tag{A.3}$$

$$\frac{\partial^2 f_y(\rho, P)}{\partial \rho^2} = \frac{1}{(1+\rho)^3} \sum_{x \in \mathcal{X}_y} P(x) W(y|x)^{\frac{1}{(1+\rho)}} \ln W(y|x) \left[2 + \frac{\ln W(y|x)}{(1+\rho)}\right], \tag{A.4}$$

$$\frac{\partial^3 f_y(\rho, P)}{\partial \rho^3} = -\frac{1}{(1+\rho)^4} \sum_{x \in \mathcal{X}_y} P(x) W(y|x)^{\frac{1}{(1+\rho)}} \ln W(y|x) \left[6 + \frac{6 \ln W(y|x)}{(1+\rho)} + \frac{(\ln W(y|x))^2}{(1+\rho)^2}\right]. \tag{A.5}$$

Further,

$$\forall\, P \in \mathcal{P}(\mathcal{X}), \text{ s.t. } \mathcal{S}(P) \cap \mathcal{X}_y = \emptyset, \; f_y(\cdot, P) = 0. \tag{A.6}$$

Equation (A.6), coupled with (A.3), (A.4) and (A.5), implies that $\frac{\partial f_y(\rho,P)}{\partial \rho}$, $\frac{\partial^2 f_y(\rho,P)}{\partial \rho^2}$ and $\frac{\partial^3 f_y(\rho,P)}{\partial \rho^3}$ are continuous for all $(\rho, P) \in \mathbb{R}_+ \times \mathcal{P}(\mathcal{X})$.

For all $y \in \mathcal{Y}$, define

$$g_y : \mathbb{R}_+ \times \mathcal{P}(\mathcal{X}) \to \mathbb{R}_+, \text{ s.t. } g_y(\rho, P) := f_y(\rho, P)^{(1+\rho)}, \tag{A.7}$$

where $f_y(\cdot,\cdot)$ is defined in (A.2). It follows that $g_y(\cdot,\cdot)$ is continuous on $\mathbb{R}_+ \times \mathcal{P}(\mathcal{X})$.

Note that

$$\forall\, P \in \mathcal{P}(\mathcal{X}), \text{ s.t. } \mathcal{S}(P) \cap \mathcal{X}_y = \emptyset,\ g_y(\cdot, P) = 0. \tag{A.8}$$

Consider any $P \in \mathcal{P}(\mathcal{X})$ with $\mathcal{S}(P) \cap \mathcal{X}_y \neq \emptyset$. By noting $g_y(\rho, P) = e^{(1+\rho)\ln f_y(\rho,P)}$, one can check that

$$\frac{\partial g_y(\rho,P)}{\partial \rho} = g_y(\rho,P)\left[(1+\rho)\frac{\frac{\partial f_y(\rho,P)}{\partial \rho}}{f_y(\rho,P)} + \ln f_y(\rho,P)\right], \tag{A.9}$$

$$\begin{aligned}\frac{\partial^2 g_y(\rho,P)}{\partial \rho^2} = {} & \frac{\partial g_y(\rho,P)}{\partial \rho}\left[(1+\rho)\frac{\frac{\partial f_y(\rho,P)}{\partial \rho}}{f_y(\rho,P)} + \ln f_y(\rho,P)\right] + \\ & g_y(\rho,P)\left[2\frac{\frac{\partial f_y(\rho,P)}{\partial \rho}}{f_y(\rho,P)} + (1+\rho)\left\{\frac{\frac{\partial^2 f_y(\rho,P)}{\partial \rho^2}}{f_y(\rho,P)} - \left(\frac{\frac{\partial f_y(\rho,P)}{\partial \rho}}{f_y(\rho,P)}\right)^2\right\}\right],\end{aligned} \tag{A.10}$$

$$\begin{aligned}\frac{\partial^3 g_y(\rho,P)}{\partial \rho^3} = {} & \frac{\partial^2 g_y(\rho,P)}{\partial \rho^2}\left[(1+\rho)\frac{\frac{\partial f_y(\rho,P)}{\partial \rho}}{f_y(\rho,P)} + \ln f_y(\rho,P)\right] + \frac{\partial g_y(\rho,P)}{\partial \rho}\left[4\frac{\frac{\partial f_y(\rho,P)}{\partial \rho}}{f_y(\rho,P)} + \right. \\ & \left. 2(1+\rho)\left\{\frac{\frac{\partial^2 f_y(\rho,P)}{\partial \rho^2}}{f_y(\rho,P)} - 2\left(\frac{\frac{\partial f_y(\rho,P)}{\partial \rho}}{f_y(\rho,P)}\right)^2\right\}\right] + g_y(\rho,P)\left[\left\{\frac{\frac{\partial^2 f_y(\rho,P)}{\partial \rho^2}}{f_y(\rho,P)} - \left(\frac{\frac{\partial f_y(\rho,P)}{\partial \rho}}{f_y(\rho,P)}\right)^2\right\}\times \right. \\ & \left. \left\{3 - 2\frac{\frac{\partial f_y(\rho,P)}{\partial \rho}}{f_y(\rho,P)}\right\} + (1+\rho)\left\{\frac{\frac{\partial^3 f_y(\rho,P)}{\partial \rho^3}}{f_y(\rho,P)} - \frac{\frac{\partial^2 f_y(\rho,P)}{\partial \rho^2}\frac{\partial f_y(\rho,P)}{\partial \rho}}{f_y(\rho,P)^2}\right\}\right].\end{aligned} \tag{A.11}$$

For any $y \in \mathcal{Y}$, define

$$\omega_{\min}(y) := \min_{y \in \mathcal{Y}} \min_{x \in \mathcal{X}_y} W(y|x), \tag{A.12}$$

$$\omega_{\max}(y) := \max_{y \in \mathcal{Y}} \max_{x \in \mathcal{X}_y} W(y|x). \tag{A.13}$$

From (A.3), by using (A.12) and (A.13), we infer that

$$\frac{\partial f_y(\rho,P)}{\partial \rho} \leq \frac{f_y(\rho,P)}{(1+\rho)^2} \ln \frac{1}{\omega_{\min}(y)}, \tag{A.14}$$

$$\frac{\partial f_y(\rho,P)}{\partial \rho} \geq \frac{f_y(\rho,P)}{(1+\rho)^2} \ln \frac{1}{\omega_{\max}(y)}. \tag{A.15}$$

Consider any sequence $\{(\rho_k, P_k)\}_{k\geq 1}$ in $\mathbb{R}_+ \times \mathcal{P}(\mathcal{X})$ with $\mathcal{S}(P_k) \cap \mathcal{X}_y \neq \emptyset$ for all $k \in \mathbb{Z}^+$ and $(\rho_k, P_k) \to (\rho_o, P_o)$ for some $(\rho_o, P_o) \in \mathbb{R}_+ \times \mathcal{P}(\mathcal{X})$ with $\mathcal{S}(P_o) \cap \mathcal{X}_y = \emptyset$. Using (A.14) and (A.15), we deduce that

$$\begin{aligned}\mathbb{R}_+ \ni \frac{1}{(1+\rho_o)^2} \ln \frac{1}{\omega_{\max}(y)} &\leq \liminf_{k\to\infty} \frac{\frac{\partial f_y(\rho,P_k)}{\partial \rho}\Big|_{\rho=\rho_k}}{f_y(\rho_k,P_k)} \\ &\leq \limsup_{k\to\infty} \frac{\frac{\partial f_y(\rho,P_k)}{\partial \rho}\Big|_{\rho=\rho_k}}{f_y(\rho_k,P_k)} \leq \frac{1}{(1+\rho_o)^2} \ln \frac{1}{\omega_{\min}(y)} \in \mathbb{R}^+. \end{aligned} \tag{A.16}$$

Note that (A.16) is evident if $\mathcal{S}(P_o) \cap \mathcal{X}_y \neq \emptyset$.

Claim 3. *Given any $y \in \mathcal{Y}$, $\frac{\partial g_y(\rho,P)}{\partial \rho}$ is continuous for all $(\rho, P) \in \mathbb{R}_+ \times \mathcal{P}(\mathcal{X})$.* ♦

Proof. Fix any $y \in \mathcal{Y}$. Consider any $(\rho_o, P_o) \in \mathbb{R}_+ \times \mathcal{P}(\mathcal{X})$.

Note that if $\mathcal{S}(P_o) \cap \mathcal{X}_y \neq \emptyset$, then by recalling the continuity of $f_y(\cdot,\cdot)$, $\frac{\partial f_y(\rho,P)}{\partial \rho}$ and $g_y(\cdot,\cdot)$, (A.9) ensures that $\frac{\partial g_y(\rho,\cdot)}{\partial \rho}$ is continuous at (ρ_o, P_o). Hence, suppose $\mathcal{S}(P_o) \cap \mathcal{X}_y = \emptyset$.

Let $\{(\rho_k, P_k)\}_{k\geq 1}$ be arbitrary with $\lim_{k\to\infty}(\rho_k, P_k) = (\rho_o, P_o)$. Observe that (A.8), along with (A.2) and (A.7), ensures that

$$\frac{\partial g_y(\rho,P_k)}{\partial \rho}\Big|_{\rho=\rho_k} = 0, \text{ if } \mathcal{S}(P_k) \cap \mathcal{X}_y = \emptyset. \tag{A.17}$$

Consider any subsequence $\{(\rho_{k_n}, P_{k_n})\}_{n\geq 1}$. Now, if all but a finite number of P_{k_n} satisfy $\mathcal{S}(P_{k_n}) \cap \mathcal{X}_y = \emptyset$, then

$$\lim_{n\to\infty} \frac{\partial g_y(\rho,P_{k_n})}{\partial \rho}\Big|_{\rho=\rho_{k_n}} = 0, \tag{A.18}$$

owing to (A.17). Suppose this is not the case. One can verify[1] that

$$\lim_{n\to\infty} \frac{\partial g_y(\rho, P_{k_n})}{\partial \rho}\bigg|_{\rho=\rho_{k_n}} = 0, \tag{A.19}$$

by using the continuity of $f_y(\cdot,\cdot)$ and $g_y(\cdot,\cdot)$, along with (A.6), (A.8), (A.9) and (A.16).

Combining (A.18) and (A.19), we conclude that

$$\lim_{k\to\infty} \frac{\partial g_y(\rho, P_k)}{\partial \rho}\bigg|_{\rho=\rho_k} = 0 = \frac{\partial g_y(\rho, P_o)}{\partial \rho}\bigg|_{\rho=\rho_o}, \tag{A.20}$$

that implies the continuity if $\mathcal{S}(P_o) \cap \mathcal{X}_y = \emptyset$. □

For any $y \in \mathcal{Y}$, define

$$\overline{\omega}(y) := \max\{|\ln \omega_{\min}(y)|, |\ln \omega_{\max}(y)|\} \in \mathbb{R}^+, \tag{A.21}$$

where $\omega_{\min}(y)$ and $\omega_{\max}(y)$ are as defined in (A.12) and (A.13), respectively.

From (A.4), by using (A.21), we infer that

$$\frac{\partial^2 f_y(\rho, P)}{\partial \rho^2} \le \frac{2 f_y(\rho, P) \ln \omega_{\max}(y)}{(1+\rho)^3} + \frac{f_y(\rho, P)\overline{\omega}(y)^2}{(1+\rho)^4}, \tag{A.22}$$

$$\frac{\partial^2 f_y(\rho, P)}{\partial \rho^2} \ge \frac{2 f_y(\rho, P) \ln \omega_{\min}(y)}{(1+\rho)^3}. \tag{A.23}$$

Consider any sequence $\{(\rho_k, P_k)\}_{k\ge1}$ in $\mathbb{R}_+ \times \mathcal{P}(\mathcal{X})$ with $\mathcal{S}(P_k) \cap \mathcal{X}_y \neq \emptyset$ for all $k \in \mathbb{R}^+$ and $(\rho_k, P_k) \to (\rho_o, P_o)$ for some $(\rho_o, P_o) \in \mathbb{R}_+ \times \mathcal{P}(\mathcal{X})$ with $\mathcal{S}(P_o) \cap \mathcal{X}_y = \emptyset$. Using (A.22) and (A.23), we deduce that

$$\begin{aligned}\mathbb{R} \ni \frac{2}{(1+\rho_o)^3} \ln \omega_{\min} &\le \liminf_{k\to\infty} \frac{\frac{\partial^2 f_y(\rho, P_k)}{\partial \rho^2}\Big|_{\rho=\rho_k}}{f_y(\rho_k, P_k)} \\ &\le \limsup_{k\to\infty} \frac{\frac{\partial^2 f_y(\rho, P_k)}{\partial \rho^2}\Big|_{\rho=\rho_k}}{f_y(\rho_k, P_k)} \le \frac{2 \ln \omega_{\max}(y)}{(1+\rho_o)^3} + \frac{\overline{\omega}(y)^2}{(1+\rho_o)^4} \in \mathbb{R}^+. \end{aligned} \tag{A.24}$$

Note that (A.24) is evident if $\mathcal{S}(P_o) \cap \mathcal{X}_y \neq \emptyset$.

[1] Passing to a further subsequence $\{P_{k_{n_m}}\}_{m\ge1}$ such that $\mathcal{S}(P_{k_{n_m}}) \cap \mathcal{X}_y \neq \emptyset$, for all $m \in \mathbb{Z}^+$, if necessary.

Claim 4. *Given any $y \in \mathcal{Y}$, $\frac{\partial^2 g_y(\rho,P)}{\partial \rho^2}$ is continuous for all $(\rho, P) \in \mathbb{R}_+ \times \mathcal{P}(\mathcal{X})$.* ♦

Proof. Fix any $y \in \mathcal{Y}$. Consider any $(\rho_o, P_o) \in \mathbb{R}_+ \times \mathcal{P}(\mathcal{X})$.

Note that if $\mathcal{S}(P_o) \cap \mathcal{X}_y \neq \emptyset$, then, by using the continuity of $f_y(\cdot,\cdot)$, $\frac{\partial f_y(\rho,\cdot)}{\partial \rho}$, $\frac{\partial^2 f_y(\rho,\cdot)}{\partial \rho^2}$, $g_y(\cdot,\cdot)$ and $\frac{\partial g_y(\rho,\cdot)}{\partial \rho}$, (A.10) implies the continuity of $\frac{\partial^2 g_y(\rho,\cdot)}{\partial \rho^2}$ at the point (ρ_o, P_o). Hence, suppose $\mathcal{S}(P_o) \cap \mathcal{X}_y = \emptyset$.

Let $\{(\rho_k, P_k)\}_{k\geq 1}$ be arbitrary with $\lim_{k\to\infty}(\rho_k, P_k) = (\rho_o, P_o)$. Observe that (A.8), along with (A.2) and (A.7), ensures that

$$\left.\frac{\partial^2 g_y(\rho, P_k)}{\partial \rho^2}\right|_{\rho=\rho_k} = 0, \text{ if } \mathcal{S}(P_k) \cap \mathcal{X}_y = \emptyset. \tag{A.25}$$

Consider any subsequence $\{(\rho_{k_n}, P_{k_n})\}_{n\geq 1}$. Now, if all but a finite number of P_{k_n} satisfy $\mathcal{S}(P_{k_n}) \cap \mathcal{X}_y = \emptyset$, then

$$\lim_{n\to\infty} \left.\frac{\partial^2 g_y(\rho, P_{k_n})}{\partial \rho^2}\right|_{\rho=\rho_{k_n}} = 0, \tag{A.26}$$

owing to (A.25). Suppose this is not the case. We also have[2]

$$\lim_{n\to\infty} \left.\frac{\partial^2 g_y(\rho, P_{k_n})}{\partial \rho^2}\right|_{\rho=\rho_{k_n}} = 0, \tag{A.27}$$

by using the continuity of $f_y(\cdot,\cdot)$, $g_y(\cdot,\cdot)$ and $\frac{\partial g_y(\rho,\cdot)}{\partial \rho}$, along with (A.6), (A.8), (A.9), (A.10), (A.16) and (A.24).

Combining (A.26) and (A.27), we conclude that

$$\lim_{k\to\infty} \left.\frac{\partial^2 g_y(\rho, P_k)}{\partial \rho^2}\right|_{\rho=\rho_k} = 0 = \left.\frac{\partial^2 g_y(\rho, P_o)}{\partial \rho^2}\right|_{\rho=\rho_o}, \tag{A.28}$$

which implies the continuity if $\mathcal{S}(P_o) \cap \mathcal{X}_y = \emptyset$. □

[2]Passing to a further subsequence $\{P_{k_{n_m}}\}_{m\geq 1}$ such that $\mathcal{S}(P_{k_{n_m}}) \cap \mathcal{X}_y \neq \emptyset$, for all $m \in \mathbb{Z}^+$, if necessary.

Note that from (A.5), by using (A.12), (A.13) and (A.21), one can show that

$$\frac{\partial^3 f_y(\rho,P)}{\partial\rho^3} \leq \frac{1}{(1+\rho)^4}\sum_{x\in\mathcal{X}_y} P(x)W(y|x)^{\frac{1}{(1+\rho)}}\left[6\ln\frac{1}{\omega_{\min}(y)} - \frac{(\ln\omega_{\min}(y))^3}{(1+\rho)^2}\right], \tag{A.29}$$

$$\frac{\partial^3 f_y(\rho,P)}{\partial\rho^3} \geq \frac{1}{(1+\rho)^4}\sum_{x\in\mathcal{X}_y} P(x)W(y|x)^{\frac{1}{(1+\rho)}}\left[6\ln\frac{1}{\omega_{\max}(y)} - \frac{6\,\overline{\omega}(y)^2}{(1+\rho)} - \frac{(\ln\omega_{\max}(y))^3}{(1+\rho)^2}\right]. \tag{A.30}$$

Consider any sequence $\{(\rho_k,P_k)\}_{k\geq 1}$ in $\mathbb{R}_+\times\mathcal{P}(\mathcal{X})$ with $\mathcal{S}(P_k)\cap\mathcal{X}_y\neq\emptyset$ for all $k\in\mathbb{R}^+$ and $(\rho_k,P_k)\to(\rho_o,P_o)$ for some $(\rho_o,P_o)\in\mathbb{R}_+\times\mathcal{P}(\mathcal{X})$ with $\mathcal{S}(P_o)\cap\mathcal{X}_y=\emptyset$. Using (A.29) and (A.30), we deduce that

$$\begin{aligned}\mathbb{R}\ni\frac{1}{(1+\rho)^4}\left[6\ln\frac{1}{\omega_{\max}(y)} - \frac{6\,\overline{\omega}(y)^2}{(1+\rho)} - \frac{(\ln\omega_{\max(y)})^3}{(1+\rho)^2}\right] &\leq \liminf_{k\to\infty}\frac{\frac{\partial^3 f_y(\rho,P_k)}{\partial\rho^3}\Big|_{\rho=\rho_k}}{f_y(\rho_k,P_k)}\\ \leq \limsup_{k\to\infty}\frac{\frac{\partial^3 f_y(\rho,P_k)}{\partial\rho^3}\Big|_{\rho=\rho_k}}{f_y(\rho_k,P_k)} &\leq \frac{1}{(1+\rho)^4}\left[6\ln\frac{1}{\omega_{\min}(y)} - \frac{(\ln\omega_{\min(y)})^3}{(1+\rho)^2}\right]\in\mathbb{R}^+.\end{aligned} \tag{A.31}$$

Note that (A.24) is evident if $\mathcal{S}(P_o)\cap\mathcal{X}_y\neq\emptyset$.

Claim 5. *Given any $y\in\mathcal{Y}$, $\frac{\partial^3 g_y(\rho,P)}{\partial\rho^3}$ is continuous for all $(\rho,P)\in\mathbb{R}_+\times\mathcal{P}(\mathcal{X})$.* ♦

Proof. Fix any $y\in\mathcal{Y}$. Consider any $(\rho_o,P_o)\in\mathbb{R}_+\times\mathcal{P}(\mathcal{X})$.

We observe that if $\mathcal{S}(P_o)\cap\mathcal{X}_y\neq\emptyset$, then, by employing the continuity of $f_y(\cdot,\cdot)$, $\frac{\partial f_y(\rho,\cdot)}{\partial\rho}$, $\frac{\partial^2 f_y(\rho,\cdot)}{\partial\rho^2}$, $\frac{\partial^3 f_y(\rho,\cdot)}{\partial\rho^3}$, $g_y(\cdot,\cdot)$, $\frac{\partial g_y(\rho,\cdot)}{\partial\rho}$ and $\frac{\partial^2 g_y(\rho,\cdot)}{\partial\rho^2}$, (A.11) implies the continuity of $\frac{\partial^3 g_y(\rho,\cdot)}{\partial\rho^3}$ at the point (ρ_o,P_o). Hence, suppose $\mathcal{S}(P_o)\cap\mathcal{X}_y=\emptyset$.

Let $\{(\rho_k,P_k)\}_{k\geq 1}$ be arbitrary with $\lim_{k\to\infty}(\rho_k,P_k)=(\rho_o,P_o)$. Observe that (A.8), along with (A.2) and (A.7), ensures that

$$\frac{\partial^3 g_y(\rho,P_k)}{\partial\rho^3}\bigg|_{\rho=\rho_k} = 0, \text{ if } \mathcal{S}(P_k)\cap\mathcal{X}_y=\emptyset. \tag{A.32}$$

Consider any subsequence $\{(\rho_{k_n}, P_{k_n})\}_{n\geq 1}$. Now, if all but a finite number of P_{k_n} satisfy $\mathcal{S}(P_{k_n}) \cap \mathcal{X}_y = \emptyset$, then

$$\lim_{n\to\infty} \frac{\partial^3 g_y(\rho, P_{k_n})}{\partial \rho^3}\bigg|_{\rho=\rho_{k_n}} = 0, \tag{A.33}$$

owing to (A.32). Suppose this is not the case. Further, we have (passing to a further subsequence $\{P_{k_{n_m}}\}_{m\geq 1}$ such that $\mathcal{S}(P_{k_{n_m}}) \cap \mathcal{X}_y \neq \emptyset$, for all $m \in \mathbb{Z}^+$, if necessary)

$$\lim_{n\to\infty} \frac{\partial^3 g_y(\rho, P_{k_n})}{\partial \rho^3}\bigg|_{\rho=\rho_{k_n}} = 0, \tag{A.34}$$

by using the continuity of $f_y(\cdot,\cdot)$, $g_y(\cdot,\cdot)$, $\frac{\partial g_y(\rho,\cdot)}{\partial \rho}$ and $\frac{\partial^2 g_y(\rho,\cdot)}{\partial \rho^2}$, along with (A.6), (A.8), (A.9), (A.10), (A.11), (A.16), (A.24) and (A.31).

Combining (A.32) and (A.33), we conclude that

$$\lim_{k\to\infty} \frac{\partial^3 g_y(\rho, P_k)}{\partial \rho^3}\bigg|_{\rho=\rho_k} = 0 = \frac{\partial^3 g_y(\rho, P_o)}{\partial \rho^3}\bigg|_{\rho=\rho_o}, \tag{A.35}$$

that implies the continuity if $\mathcal{S}(P_o) \cap \mathcal{X}_y = \emptyset$. □

Lastly, recalling the definition of $\mathrm{E_o}(\rho, P)$ and (A.7), it is easy to see that

$$\mathrm{E}_o(\rho, P) = -\ln \sum_{y\in\mathcal{Y}} g_y(\rho, P). \tag{A.36}$$

Using (A.36), one can check that

$$\frac{\partial \mathrm{E_o}(\rho, P)}{\partial \rho} = -\frac{\sum_{y\in\mathcal{Y}} \frac{\partial g_y(\rho,P)}{\partial \rho}}{\sum_{\tilde{y}\in\mathcal{Y}} g_{\tilde{y}}(\rho, P)}, \tag{A.37}$$

$$\frac{\partial^2 \mathrm{E_o}(\rho, P)}{\partial \rho^2} = -\frac{\sum_{y\in\mathcal{Y}} \frac{\partial^2 g_y(\rho,P)}{\partial \rho^2}}{\sum_{\tilde{y}\in\mathcal{Y}} g_{\tilde{y}}(\rho, P)} + \left(\frac{\partial \mathrm{E_o}(\rho, P)}{\partial \rho}\right)^2, \tag{A.38}$$

$$\frac{\partial^3 \mathrm{E_o}(\rho, P)}{\partial \rho^3} = -\frac{\sum_{y\in\mathcal{Y}} \frac{\partial^3 g_y(\rho,P)}{\partial \rho^3}}{\sum_{\tilde{y}\in\mathcal{Y}} g_{\tilde{y}}(\rho, P)} + 3\frac{\partial \mathrm{E_o}(\rho, P)}{\partial \rho}\frac{\partial^2 \mathrm{E_o}(\rho, P)}{\partial \rho^2} - \left(\frac{\partial \mathrm{E_o}(\rho, P)}{\partial \rho}\right)^3. \tag{A.39}$$

The assertions of the lemma now follow:

1) For any given $P \in \mathcal{P}(\mathcal{X})$, the concavity of $\mathrm{E_o}(\cdot, P)$ on $\mathbb{R}_+$ can either be proven by checking the non-positivity of $\frac{\partial^2 E_o(\rho,P)}{\partial \rho^2}$, given in (A.38), or directly applying Hölder's inequality (e.g., [35, Appendix 5B]).

2) By evaluating (A.2), (A.3), (A.7) and (A.9) at $\rho = 0$ and then plugging the result into (A.37), one can easily check the validity of the claim.

3) By evaluating (A.2), (A.3), (A.4), (A.7), (A.9) and (A.10) at $\rho = 0$ and plugging the result into (A.38), one can check the validity of the claim after some algebra.

4) Fix any $P \in \mathcal{P}(\mathcal{X})$. The concavity of $\mathrm{E_o}(\cdot, P)$ on $\mathbb{R}_+$ (recall item 1) above) ensures that $\frac{\partial^2 \mathrm{E_o}(\rho,P)}{\partial \rho^2} \leq 0$, for all $\rho \in \mathbb{R}_+$. This, coupled with item 2) above, implies the claim.

5) The continuity of $g_y(\cdot, \cdot)$ on $P \in \mathcal{P}(\mathcal{X}) \times \mathbb{R}_+$ and Claim 3, along with (A.37), imply the claim.

6) The continuity of $g_y(\cdot, \cdot)$ on $P \in \mathcal{P}(\mathcal{X}) \times \mathbb{R}_+$, Claim 4 and item 5) above, along with (A.38), imply the claim.

7) The continuity of $g_y(\cdot, \cdot)$ on $P \in \mathcal{P}(\mathcal{X}) \times \mathbb{R}_+$, Claim 5 and items 5) and 6) above, along with (A.39), imply the claim. □

APPENDIX B

APPENDICES OF CHAPTER 3

B.1 Proof of Lemma 5

The content of this section resembles Dembo-Zeitouni's proof of Bahadur-Rao theorem (cf., [21, Theorem 3.7.4]). The main difference is the usage of the Berry-Esseen theorem, instead of the asymptotic expansions related to the central limit theorem. The usage of the latter results in the dependence of the lattice nature of the random variable and we choose to use the former in order to avert this technicalities.

First of all, note that since $\Lambda_i(\cdot)$ is finite in a neighborhood of η, $\Lambda_i(\cdot)$ is smooth at η. Moreover, the defining assumption of η (i.e., property (ii) above) implies that

$$\Lambda_n^*(q) = q\eta - \frac{1}{n}\sum_{i=1}^{n}\Lambda_i(\eta), \tag{B.1}$$

since $\frac{1}{n}\sum_{i=1}^{n}\Lambda_i(\delta)$ is convex.

Next, as an immediate consequence of the definition of $\tilde{\lambda}_i$,

$$\mathrm{E}_{\tilde{\lambda}_i}[Z_i] = \frac{1}{M_i(\eta)}\int z e^{\eta z} d\lambda_i(z). \tag{B.2}$$

Moreover, since Λ_i is smooth at η, we also have

$$\Lambda_i'(\eta) = \frac{M_i'(\eta)}{M_i(\eta)} = \frac{1}{M_i(\eta)}\int z e^{\eta z} d\lambda_i(z). \tag{B.3}$$

And hence, we conclude that

$$\mathrm{E}_{\tilde{\lambda}_i}[Z_i] = \Lambda_i'(\eta). \tag{B.4}$$

Also, straightforward algebra reveals that

$$\Lambda_i''(\eta) = \frac{M_i''(\eta)}{M_i(\eta)} - \left[\Lambda_i'(\eta)\right]^2. \tag{B.5}$$

Moreover, since Λ_i is smooth at η, we also have

$$M_i''(\eta) = \int z^2 e^{\eta z} d\lambda_i(z), \tag{B.6}$$

which, in turn, implies that

$$\mathrm{E}_{\tilde{\lambda}_i}[Z_i^2] = \frac{M_i''(\eta)}{M_i(\eta)}. \tag{B.7}$$

Plugging (B.4) and (B.7) into (B.5) yields

$$\mathrm{Var}_{\tilde{\lambda}_i}[Z_i] = \Lambda_i''(\eta). \tag{B.8}$$

Furthermore, recalling the definition of $\tilde{\lambda}_i$, it is obvious that $\tilde{\lambda}_i \ll \lambda_i$, i.e., λ_i dominates $\tilde{\lambda}_i$. Moreover, since Z_i are real-valued and $e^{\eta z - \Lambda_i(\eta)} > 0$, for all $z \in \mathbb{R}$, we have

$$\frac{d\lambda_i}{d\tilde{\lambda}_i}(z) = e^{-\eta z + \Lambda_i(\eta)}, \tag{B.9}$$

which, in turn, implies that $\lambda_i \ll \tilde{\lambda}_i$. Hence, we conclude that $\tilde{\lambda}_i$ and λ_i are equivalent probability measures, i.e., $\lambda_i \equiv \tilde{\lambda}_i$.

Next, we claim that

$$m_{2,n} > 0. \tag{B.10}$$

To see this, note that for any $i \in \{1, \ldots, n\}$,

$$[\Lambda_i''(\eta) = 0] \iff \left[Z_i = \Lambda_i'(\eta) \quad \tilde{\lambda}_i - (\text{a.s.})\right] \tag{B.11}$$

$$\iff [Z_i = \Lambda_i'(\eta) \quad \lambda_i - (\text{a.s.})] \tag{B.12}$$

$$\implies [\mathrm{Var}[Z_i] = 0], \tag{B.13}$$

where (B.11) follows from (B.4) and (B.8), (B.12) follows since $\lambda_i \equiv \tilde{\lambda}_i$. From the assumption that $\sum_{i=1}^n \mathrm{Var}[Z_i] > 0$ and (B.13), we conclude that $\sum_{i=1}^n \Lambda_i''(\eta) > 0$, which implies (B.10).

We continue as follows:

$$\mu_n([q,\infty)) = \int_{\{\hat{S}_n \geq q\}} \lambda_1(dz_1)\dots\lambda_n(dz_n) \tag{B.14}$$

$$= \int_{\{\hat{S}_n \geq q\}} e^{\sum_{i=1}^n [\Lambda_i(\eta)-\eta z_i]} \tilde{\lambda}_1(dz_1)\dots\tilde{\lambda}_n(dz_n) \tag{B.15}$$

$$= e^{\sum_{i=1}^n \Lambda_i(\eta)} \mathrm{E}_{\tilde{\mu}_n}\left[\mathbb{1}_{\{\hat{S}_n \geq q\}} e^{-n\eta\hat{S}_n}\right] \tag{B.16}$$

$$= e^{-n\Lambda_n^*(q)} \mathrm{E}_{\tilde{\mu}_n}\left[\mathbb{1}_{\{\hat{S}_n \geq q\}} e^{-n[\eta\hat{S}_n - \eta q]}\right], \tag{B.17}$$

where (B.16) follows by recalling the definition of $\tilde{\mu}_n$ and (B.17) follows from (B.1).

Note that (B.4) and (B.8) imply that

$$\mathrm{E}_{\tilde{\lambda}_i}[T_i] = 0, \quad \mathrm{Var}_{\tilde{\lambda}_i}[T_i] = \Lambda_i''(\eta). \tag{B.18}$$

Define

$$W_n := \frac{1}{\sqrt{m_{2,n}}} \sum_{i=1}^n T_i. \tag{B.19}$$

Further, observe that

$$\hat{S}_n = \sqrt{m_{2,n}}\frac{W_n}{n} + q, \tag{B.20}$$

which, in turn, implies that

$$\{\hat{S}_n \geq q\} = \left\{\sqrt{m_{2,n}}\frac{W_n}{n} \geq 0\right\}. \tag{B.21}$$

Plugging (B.20) and (B.21) into (B.17) yields

$$\mu_n([q,\infty)) = e^{-n\Lambda_n^*(q)} \mathrm{E}_{\tilde{\mu}_n}\left[\mathbb{1}_{\{W_n \geq 0\}} e^{-\eta\sqrt{m_{2,n}}W_n}\right] \tag{B.22}$$

$$= e^{-n\Lambda_n^*(q)} \int_0^\infty e^{-x\eta\sqrt{m_{2,n}}} dF_n(x) \tag{B.23}$$

$$= e^{-n\Lambda_n^*(q)} \int_0^\infty e^{-t}\left[F_n\left(\frac{t}{\psi_n}\right) - F_n(0)\right] dt, \tag{B.24}$$

where F_n is the distribution of W_n when Z_i are independent with laws $\tilde{\lambda}_i$, $\psi_n := \eta\sqrt{m_{2,n}}$ and (B.24) follows from integration by parts.

Fix some $a > 1$ and note that since Λ_i is smooth at η, $m_{3,n} < \infty$ and hence (recall (B.10)), $t_n(a, q) \in \mathbb{R}^+$.

Next, Berry-Esseen theorem (cf., [9], [25, Theorem III.1]) implies that

$$|F_n(x) - \Phi(x)| \leq c\frac{m_{3,n}}{m_{2,n}^{3/2}}, \ \forall x \in \mathbb{R}, \tag{B.25}$$

where $\Phi(\cdot)$ is the distribution of the standard Gaussian random variable and c is an absolute constant. If the random variables are independent but not identically distributed, then we can take $c = 1$, whereas if they are also identically distributed, then we can take $c = 1/2$, by recalling the fact that the best known constants for each case is smaller than 1 and $1/2$, respectively (cf., [46] for a recent survey of the best known constants in Berry-Esseen theorem).

To deduce (3.1), we approximate $\int_0^\infty e^{-t}\left[F_n\left(\frac{t}{\psi_n}\right) - F_n(0)\right]dt$ as follows:

$$F_n\left(\frac{t}{\psi_n}\right) - F_n(0) \leq \Phi\left(\frac{t}{\psi_n}\right) - \Phi(0) + 2\frac{m_{3,n}}{m_{2,n}^{3/2}} \tag{B.26}$$

$$\leq \frac{t}{\psi_n}\phi(0) + 2\frac{m_{3,n}}{m_{2,n}^{3/2}}, \tag{B.27}$$

where resp. $\phi(\cdot)$ denotes the density of the standard Gaussian random variable, (B.26) follows from (B.25) and (B.27) follows via a Taylor series approximation coupled with the observation that $\phi'(x) = -\frac{x}{\sqrt{2\pi}}e^{-x^2/2} \leq 0$ for all $x \in \mathbb{R}_+$. Plugging (B.27) into (B.24) and carrying out the straightforward algebra gives (3.1). Evidently, if the random variables are i.i.d. then (B.26) holds with $\frac{2m_{3,n}}{m_{2,n}^{3/2}}$ replaced with $\frac{m_{3,n}}{m_{2,n}^{3/2}}$ and hence the claimed upper bound for this case follows.

To prove (3.2), first note that for any $b > 0$

$$\int_b^\infty te^{-t}dt = e^{-b}(1 + b), \tag{B.28}$$

$$\int_b^\infty t^2e^{-t}dt = e^{-b}[1 + (1 + b)^2], \tag{B.29}$$

that can be verified by straightforward algebra.

Further,

$$F_n\left(\frac{t}{\psi_n}\right) - F_n(0) \geq \Phi\left(\frac{t}{\psi_n}\right) - \Phi(0) - 2\frac{m_{3,n}}{m_{2,n}^{3/2}} \tag{B.30}$$

$$\geq \frac{t}{\psi_n}\phi(0) - \frac{t^2}{\psi_n^2}\frac{1}{2\sqrt{2\pi e}} - 2\frac{m_{3,n}}{m_{2,n}^{3/2}}, \tag{B.31}$$

where (B.30) follows from (B.25) and (B.31) follows by a Taylor series approximation, along with the observation that $\mathbb{R}_+ \ni x \mapsto xe^{-x^2/2} \leq e^{-1/2}$. By plugging (B.31) into (B.24), we deduce that

$$\int_0^\infty e^{-t}\left[F_n\left(\frac{t}{\psi_n}\right) - F_n(0)\right]dt \geq \int_{t_n(a,q)}^\infty e^{-t}\left[F_n\left(\frac{t}{\psi_n}\right) - F_n(0)\right]dt \tag{B.32}$$

$$\geq \int_{t_n(a,q)}^\infty e^{-t}\left[\frac{t}{\eta\sqrt{2\pi m_{2,n}}}\left(1 - \frac{1}{a}\right) - \frac{t^2}{\psi_n^2 2\sqrt{2\pi e}}\right]dt. \tag{B.33}$$

Equations (B.28), (B.29) and (B.33), along with elementary algebra, imply that (3.2) holds.

To prove (3.3), we lower bound the right side of (B.22) by using the fact that $\eta \leq 1$ to have

$$\mu_n([q,\infty)) \geq e^{-n\Lambda_n^*(q)}\mathrm{E}_{\tilde{\mu}_n}\left[\mathbb{1}_{\{W_n \geq 0\}}e^{-\sqrt{m_{2,n}}W_n}\right] \tag{B.34}$$

$$= e^{-n\Lambda_n^*(q)}\int_0^\infty e^{-x\sqrt{m_{2,n}}}dF_n(x) \tag{B.35}$$

$$= e^{-n\Lambda_n^*(q)}\int_0^\infty e^{-t}[F_n(t/\sqrt{m_{2,n}}) - F_n(0)]dt, \tag{B.36}$$

where (B.36) follows by letting $t := x\sqrt{m_{2,n}}$ and integration by parts.

By using similar arguments to approximate the integrand on the right side of (B.36), one can verify that

$$\int_0^\infty e^{-t}\left[F_n\left(\frac{t}{\sqrt{m_{2,n}}}\right) - F_n(0)\right]dt \geq \int_{K_n(q)}^\infty e^{-t}\left[F_n\left(\frac{t}{\sqrt{m_{2,n}}}\right) - F_n(0)\right]dt \tag{B.37}$$

$$\geq \frac{e^{-K_n(q)}}{\sqrt{2\pi m_{2,n}}}\left(1 - \frac{1 + (1 + K_n(q))^2}{2\sqrt{m_{2,n}}}\right). \tag{B.38}$$

Plugging (B.38) into (B.24) yields

$$\mu_n([q,\infty)) \geq \frac{e^{-n\Lambda_n^*(q)}e^{-K_n(q)}}{\sqrt{2\pi m_{2,n}}}\left(1-\frac{1+(1+K_n(q))^2}{2\sqrt{m_{2,n}}}\right). \tag{B.39}$$

□

B.2 Proof of Proposition 2

Claim 6. *For any $R > R_\infty$*

$$E_{SP}(R,P) = \max_{\rho\in\mathbb{R}_+}\min_{q\in\mathcal{P}(\mathcal{Y})}\left\{-\rho R-(1+\rho)\Lambda_{Q,P}\left(\frac{\rho}{1+\rho}\right)\right\}, \tag{B.40}$$

for all $P \in \mathcal{P}(\mathcal{X})$. ♦

Proof. The proof is clear from basic optimization theoretic arguments, (e.g., [20, Exercise 2.5.23]), we just reproduce the steps for the sake of completeness.

$$\begin{aligned}
\mathrm{E_{SP}}(R,P) &= \max_{\rho\in\mathbb{R}_+}\min_{V\in\mathcal{P}(\mathcal{Y}|\mathcal{X})}\{\mathrm{D}(V\|W|P)+\rho[\mathrm{I}(P;V)-R]\} && \text{(B.41)}\\
&= \max_{\rho\in\mathbb{R}_+}\min_{V\in\mathcal{P}(\mathcal{Y}|\mathcal{X})}\left\{\mathrm{D}(V\|W|P)+\rho\left[\min_{Q\in\mathcal{P}(\mathcal{Y})}\mathrm{D}(V\|Q|P)-R\right]\right\} && \text{(B.42)}\\
&= \max_{\rho\in\mathbb{R}_+}\left\{-\rho R+\min_{Q\in\mathcal{P}(\mathcal{Y})}\min_{V\in\mathcal{P}(\mathcal{Y}|\mathcal{X})}\left[\mathrm{D}(V\|W|P)+\rho\mathrm{D}(V\|Q|P)\right]\right\} && \text{(B.43)}\\
&= \max_{\rho\in\mathbb{R}_+}\min_{Q\in\mathcal{P}(\mathcal{Y})}\left\{-\rho R-(1+\rho)\Lambda_{Q,P}\left(\frac{\rho}{1+\rho}\right)\right\}. && \text{(B.44)}
\end{aligned}$$

□

Remark 20. *Recalling the definitions of $\mathcal{P}_{P,W}(\mathcal{Y})$ and $\tilde{\mathcal{P}}_{P,W}(\mathcal{Y})$ (cf.,* (3.18) *and* (3.19)*), we note the following facts:*

(i) $\mathcal{P}_{P,W}(\mathcal{Y})$ and $\tilde{\mathcal{P}}_{P,W}(\mathcal{Y})$ are convex sets and $\tilde{\mathcal{P}}_{P,W}(\mathcal{Y}) \subset \mathcal{P}_{P,W}(\mathcal{Y})$.

(ii) From the basic facts about convex sets (e.g., [10, Proposition 1.4.1 (c), Proposition 1.4.3 (b)]), $ri(\mathbb{R}_+) = \mathbb{R}^+$ and $ri(\mathcal{P}_{P,W}(\mathcal{Y})) = ri(\mathcal{P}(\mathcal{Y})) = \{Q \in \mathcal{P}(\mathcal{Y}) : Q(y) > 0, \forall y \in \mathcal{Y}\}$.

(iii) For any $Q \in \mathcal{P}_{P,W}(\mathcal{Y})$, $\Lambda_{Q,P}(\lambda) \in \mathbb{R}$, for all $\lambda \in [0, 1)$.

(iv) For any $Q \in \mathcal{P}(\mathcal{Y})\backslash\mathcal{P}_{P,W}(\mathcal{Y})$, $\Lambda_{Q,P}(\lambda) = -\infty$, for all $\lambda \in (0, 1)$ and hence given any $R > R_\infty$, $P \in \mathcal{P}(\mathcal{X})$ and $Q \in \mathcal{P}(\mathcal{Y})\backslash\mathcal{P}_{P,W}(\mathcal{Y})$, $K_{R,P}(\rho, Q) = \infty$ for all $\rho \in \mathbb{R}^+$. $\diamond$

Claim 7. *Consider any $R > R_\infty$ and $P \in \mathcal{P}(\mathcal{X})$.*

(i) Given any $\rho \in \mathbb{R}_+$ (resp. $\rho \in \mathbb{R}^+$), $K_{R,P}(\rho, \cdot)$ is (resp. strictly) convex on $\mathcal{P}_{P,W}(\mathcal{Y})$ (resp. $\tilde{\mathcal{P}}_{P,W}(\mathcal{Y})$).

(ii) Given any $Q \in \mathcal{P}_{P,W}(\mathcal{Y})$, $K_{R,P}(\cdot, Q)$ is concave on $\mathbb{R}_+$. $\blacklozenge$

Proof. Let $R > R_\infty$ and $P \in \mathcal{P}(\mathcal{X})$ be arbitrary.

(i) Given any $x \in \mathcal{S}(P)$ and $\lambda \in [0, 1)$ define $f_{x,\lambda} : \mathcal{P}_{P,W}(\mathcal{Y}) \to \mathbb{R}^+$ such that

$$f_{x,\lambda}(Q) := \begin{cases} \sum_{y\in\mathcal{Y}} W(y|x)^{1-\lambda} Q(y)^\lambda, & \text{if } \lambda \in (0, 1), \\ 1, & \text{if } \lambda = 0, \end{cases} \tag{B.45}$$

for any $Q \in \mathcal{P}_{P,W}(\mathcal{Y})$. Let $Q_1, Q_2 \in \mathcal{P}_{P,W}(\mathcal{Y})$ and $\theta \in (0, 1)$ be arbitrary. For any $\lambda \in (0, 1)$, we have

$$f_{x,\lambda}(\theta Q_1 + (1-\theta)Q_2) = \sum_{y\in\mathcal{Y}} W(y|x)^{1-\lambda}[\theta Q_1(y) + (1-\theta)Q_2(y)]^\lambda \tag{B.46}$$

$$\geq \sum_{y\in\mathcal{Y}} W(y|x)^{1-\lambda}[\theta Q_1(y)^\lambda + (1-\theta)Q_2(y)^\lambda] \tag{B.47}$$

$$= \theta f_{x,\lambda}(Q_1) + (1-\theta) f_{x,\lambda}(Q_2), \tag{B.48}$$

where (B.47) follows from the concavity of $(\cdot)^\lambda$ on $\mathbb{R}_+$ for any $\lambda \in (0,1)$. Clearly, (B.48) is true for $\lambda = 0$.

Since $\ln(\cdot)$ is strictly increasing and strictly concave on $\mathbb{R}^+$, (B.48) implies that

$$\ln(f_{x,\lambda}(\theta Q_1 + (1-\theta)Q_2)) \geq \ln(\theta f_{x,\lambda}(Q_1) + (1-\theta) f_{x,\lambda}(Q_2)) \tag{B.49}$$

$$\geq \theta \ln(f_{x,\lambda}(Q_1)) + (1-\theta)\ln(f_{x,\lambda}(Q_2)). \tag{B.50}$$

(B.50) implies that given any $\rho \in \mathbb{R}_+$, $\Lambda_{\cdot,P}\left(\frac{\rho}{1+\rho}\right)$ is concave on $\mathcal{P}_{P,W}(\mathcal{Y})$. By recalling the definition of $K_{R,P}$ (cf., (3.20)), this implies that $K_{R,P}(\rho,\cdot)$ is convex on $\mathcal{P}_{P,W}(\mathcal{Y})$.

Strict concavity follows by noting that for any $Q_1, Q_2 \in \tilde{\mathcal{P}}_{P,W}(\mathcal{Y})$ such that $Q_1 \neq Q_2$ and $\lambda \in (0,1)$, the inequality in (B.47) is strict owing to the strict concavity of $(\cdot)^\lambda$ on $\mathbb{R}^+$ for any $\lambda \in (0,1)$.

(ii) For any $\lambda \in (0,1)$, $Q \in \mathcal{P}_{P,W}(\mathcal{Y})$ and $x \in \mathcal{S}(P)$ define

$$\forall y \in \mathcal{Y},\ \tilde{W}_{\lambda,Q}(y|x) := \frac{W(y|x)^{1-\lambda}Q(y)^\lambda}{\sum_{\tilde{y}\in\mathcal{Y}} W(\tilde{y}|x)^{1-\lambda}Q(\tilde{y})^\lambda}. \tag{B.51}$$

Recalling the definition of $\mathcal{P}_{P,W}(\mathcal{Y})$, $\tilde{W}_{\lambda,Q}(\cdot|x)$ is a well-defined probability measure on $\mathcal{Y}$. It is easy to check that[1]

$$\Lambda'_{Q,P}(\lambda) = \sum_{x\in\mathcal{S}(P)} P(x)\mathrm{E}_{\tilde{W}_{\lambda,Q}(\cdot|x)}\left[\ln\frac{Q(Y)}{W(Y|x)}\right], \tag{B.52}$$

$$\Lambda''_{Q,P}(\lambda) = \sum_{x\in\mathcal{S}(P)} P(x)\mathrm{Var}_{\tilde{W}_{\lambda,Q}(\cdot|x)}\left[\ln\frac{Q(Y)}{W(Y|x)}\right], \tag{B.53}$$

for any $Q \in \mathcal{P}_{P,W}(\mathcal{Y})$ and $\lambda \in (0,1)$. Recalling the definition of $K_{R,P}$ (cf., (3.20)), (B.53) implies that

$$\frac{\partial^2 K_{R,P}(\rho,q)}{\partial\rho^2} = -\frac{1}{(1+\rho)^3}\Lambda''_{Q,P}\left(\frac{\rho}{1+\rho}\right) \leq 0, \tag{B.54}$$

[1]For the sake of notational convenience $\Lambda'_{Q,P}(\lambda)$ (resp. $\Lambda''_{Q,P}(\lambda)$) denotes $\frac{\partial\Lambda_{Q,P}(\lambda)}{\partial\lambda}$ (resp. $\frac{\partial^2\Lambda_{Q,P}(\lambda)}{\partial\lambda^2}$) in the sequel.

for any $Q \in \mathcal{P}_{P,W}(\mathcal{Y})$ and $\rho \in \mathbb{R}^+$.

Now, fix any $Q \in \mathcal{P}_{P,W}(\mathcal{Y})$. (B.54) implies that $-K_{R,P}(\cdot, Q)$ is convex on $\mathbb{R}^+$, equivalently, the epigraph of $-K_{R,P}(\cdot, Q)$ with its domain restricted to $\mathbb{R}^+$ is a convex set. Furthermore,

$$\lim_{\rho \downarrow 0} -K_{R,P}(\rho, Q) \leq 0 = -K_{R,P}(0, Q).$$

Hence, after adding 0 into the domain of $K_{R,P}(\cdot, Q)$, its epigraph remains to be convex.

□

Definition 11. *Let $G \subset \mathbb{R}^n$ and $f : G \to \mathbb{R}$. (G, f) is "convex and closed in Fenchel's sense" (cf., [54, pg. 151], [32, end of Section 2]) (resp. "concave and closed in Fenchel's sense") provided that:*

(i) G is convex.

(ii) f is convex (resp. concave) and lower (resp. upper) semi-continuous.

(iii) Any accumulation point of G that does not belong to G satisfies $\lim f(\cdot) = \infty$ (resp. $\lim f(\cdot) = -\infty$). ◊

Claim 8. *Let $R > R_\infty$ and $P \in \mathcal{P}(\mathcal{X})$ be arbitrary. For any $Q \in ri(\mathcal{P}_{P,W}(\mathcal{Y}))$ (resp. $\rho \in ri(\mathbb{R}_+)$), $(\mathbb{R}_+, K_{P,R}(\cdot, Q))$ (resp. $(\mathcal{P}_{P,W}(\mathcal{Y}), K_{P,R}(\rho, \cdot))$) is concave (resp. convex) and closed in Fenchel's sense.* ♦

Proof. Fix any $R > R_\infty$ and $P \in \mathcal{P}(\mathcal{X})$.

First, fix an arbitrary $Q \in \tilde{P}_{P,W}(\mathcal{Y})$. Observe that $\Lambda_{Q,P}(\lambda) \in \mathbb{R}$ for all $\lambda \in (0, 1)$, which in turn implies that $\Lambda_{q,P}(\lambda)$ is infinitely differentiable with respect to λ for all $\lambda \in (0, 1)$. Moreover, recalling the definition of $\tilde{P}_{P,W}(\mathcal{Y})$, it is easy to check that for

any $Q \in \tilde{P}_{P,W}(\mathcal{Y})$, $\lim_{\lambda \downarrow 0} \Lambda_{Q,P}(\lambda) = 0 = \Lambda_{Q,P}(0)$. These two observations ensure the continuity (and *a fortiori* upper semi-continuity) of $K_{R,P}(\cdot, Q)$ on $\mathbb{R}_+$. By noting (recall item (ii) of Remark 20) $\mathrm{ri}(\mathcal{P}_{P,W}(\mathcal{Y})) \subset \tilde{P}_{P,W}(\mathcal{Y})$, the fact that $\mathbb{R}_+$ is closed and convex and the concavity of $K_{R,P}(\cdot, Q)$ (cf., item (ii) of Claim 7) this suffices to conclude that $(\mathbb{R}_+, K_{R,P}(\cdot, Q))$ is concave and closed in Fenchel's sense.

Next, fix an arbitrary $\rho \in \mathrm{ri}(\mathbb{R}_+) = \mathbb{R}^+$ (cf., item (ii) of Remark 20). Observe that any accumulation point of $\mathcal{P}_{P,W}(\mathcal{Y})$ which does not belong to $\mathcal{P}_{P,W}(\mathcal{Y})$, say Q_0, satisfies $Q_0 \in \mathcal{P}(\mathcal{Y}) \backslash \mathcal{P}_{P,W}(\mathcal{Y})$, owing to the compactness of $\mathcal{P}(\mathcal{Y})$, and hence $K_{R,P}(\rho, Q_0) = \infty$. Further, item (i) of Remark 20 and item (i) of Claim 7 ensures that in order to conclude that $K_{R,P}(\rho, \cdot)$ is convex and closed in Fenchel's sense, we only need to verify the lower semi-continuity. Implied by its convexity, $K_{R,P}(\rho, \cdot)$ is continuous on $\mathrm{ri}(\mathcal{P}(\mathcal{Y}))$. Let $Q_0 \in \mathcal{P}_{P,W}(\mathcal{Y}) \backslash \mathrm{ri}(\mathcal{P}(\mathcal{Y}))$ be arbitrary. Consider an arbitrary sequence $\{Q_k\}_{k \geq 1}$ such that $Q_k \in \mathcal{P}_{P,W}(\mathcal{Y})$ and $\lim_{k \to \infty} Q_k = Q_0$. Lastly, define $\lambda := \frac{\rho}{1+\rho} \in (0, 1)$. We have

$$\lim_{k \to \infty} \Lambda_{Q_k,P}(\lambda) = \lim_{k \to \infty} \sum_{x \in \mathcal{S}(P)} P(x) \ln \sum_{y \in \mathcal{Y}} W(y|x)^{1-\lambda} Q_k(y)^{\lambda} \tag{B.55}$$

$$= \sum_{x \in \mathcal{S}(P)} P(x) \ln \sum_{y \in \mathcal{Y}} W(y|x)^{1-\lambda} Q_0(y)^{\lambda} \tag{B.56}$$

$$= \Lambda_{Q_0,P}(\lambda), \tag{B.57}$$

where (B.56) follows from the continuity of $\ln(\cdot)$ and $(\cdot)^{\lambda}$. □

Now, we are ready to prove the existence of a saddle-point. To this end, fix arbitrary $R > R_\infty$ and $P \in \mathcal{P}(\mathcal{X})$ from now on.

We first establish

$$-\infty < \max_{\rho \in \mathbb{R}_+} \inf_{Q \in \mathcal{P}_{P,W}(\mathcal{Y})} K_{R,P}(\rho, Q) = \min_{Q \in \mathcal{P}_{P,W}(\mathcal{Y})} \sup_{\rho \in \mathbb{R}_+} K_{R,P}(\rho, Q) < \infty. \tag{B.58}$$

In order to prove (B.58), we use a minimax theorem of Rockafellar, [54, Theorem 8]. Claim 8 ensures that $(\mathbb{R}_+, \mathcal{P}_{P,W}(\mathcal{Y}), K_{R,P})$ is a "closed saddle-element" (cf., [54, pg. 151])

and the boundedness of $\mathcal{P}_{P,W}(\mathcal{Y})$ guarantees the fulfillment of condition (II) for the validity of the aforementioned theorem (cf., [54, pg. 172]). Therefore [54, eq. (7.2)] implies that

$$-\infty < \sup_{\rho \in \mathbb{R}_+} \inf_{Q \in \mathcal{P}_{P,W}(\mathcal{Y})} K_{R,P}(\rho, Q) = \min_{Q \in \mathcal{P}_{P,W}(\mathcal{Y})} \sup_{\rho \in \mathbb{R}_+} K_{R,P}(\rho, Q). \tag{B.59}$$

Next, we claim that

$$\forall\, \rho \in \mathbb{R}_+, \ \inf_{Q \in \mathcal{P}_{P,W}(\mathcal{Y})} K_{R,P}(\rho, Q) = \inf_{Q \in \mathcal{P}(\mathcal{Y})} K_{R,P}(\rho, Q). \tag{B.60}$$

Since $\Lambda_{Q,P}(0) = 0$, for all $q \in \mathcal{P}(\mathcal{Y})$, (B.60) is trivially true for $\rho = 0$. On the other hand, for any $\rho \in \mathbb{R}^+$, item (iv) of Remark 20 implies that

$$\forall\, Q \in \mathcal{P}(\mathcal{Y}) \backslash \mathcal{P}_{P,W}(\mathcal{Y}), \ K_{R,P}(\rho, Q) = \infty, \tag{B.61}$$

which, in turn, implies (B.60). Equation (B.40) and (B.60) imply that

$$\mathrm{E_{SP}}(R, P) = \max_{\rho \in \mathbb{R}_+} \min_{Q \in \mathcal{P}(\mathcal{Y})} K_{R,P}(\rho, Q) = \max_{\rho \in \mathbb{R}_+} \inf_{Q \in \mathcal{P}_{P,W}(\mathcal{Y})} K_{R,P}(\rho, Q) < \infty. \tag{B.62}$$

Equation (B.59) and (B.62) imply that

$$-\infty < \max_{\rho \in \mathbb{R}_+} \inf_{Q \in \mathcal{P}_{P,W}(\mathcal{Y})} K_{R,P}(\rho, Q) = \min_{Q \in \mathcal{P}_{P,W}(\mathcal{Y})} \sup_{\rho \in \mathbb{R}_+} K_{R,P}(\rho, Q) < \infty, \tag{B.63}$$

which is (B.58).

From [55, Lemma 36.2], (B.58) ensures the existence of a saddle-point on $\mathbb{R}_+ \times \mathcal{P}_{P,W}(\mathcal{Y})$ and (B.62) implies the saddle-value is $\mathrm{E_{SP}}(R, P)$. Hence we conclude the proof of the first assertion of the proposition.

Next, we prove the second assertion.

Claim 9. *Consider any $R > R_\infty$ and $P \in \mathcal{P}(\mathcal{X})$. If $0 \in S(R, P)|_{\mathbb{R}_+}$, then $E_{SP}(R, P) = 0$, equivalently, if $E_{SP}(R, P) > 0$, then $0 \notin S(R, P)|_{\mathbb{R}_+}$.* ♦

Proof. Consider any $R > R_\infty$ and $P \in \mathcal{P}(\mathcal{X})$. Assume $0 \in S(R,P)|_{\mathbb{R}_+}$. We clearly have $K_{R,P}(0,Q) = 0$, for all $Q \in \mathcal{P}_{P,W}(\mathcal{Y})$, which in turn implies that (recall the definition of the saddle-point) $K_{R,P}(0,\hat{Q}) = 0$ for any $\hat{Q} \in \mathcal{P}_{P,W}(\mathcal{Y})$ satisfying $(0,\hat{Q}) \in S(R,P)$. From the first assertion of Proposition 2, this implies the claim. □

Recalling the definition of $\mathcal{P}_R(\mathcal{X})$ (cf., (3.17)), Claim 9 immediately implies the following result.

Corollary 4. *For any $C > R > R_\infty$ and $P \in \mathcal{P}_R(\mathcal{X})$, $S(R,P)|_{\mathbb{R}_+} \subset \mathbb{R}^+$.* ♦

Claim 10. *For any $C > R > R_\infty$ and $P \in \mathcal{P}_R(\mathcal{X})$, $S(R,P)|_{\mathcal{P}_{P,W}(\mathcal{Y})} \subset \tilde{\mathcal{P}}_{P,W}(\mathcal{Y})$.* ♦

Proof. Fix any $C > R > R_\infty$ and $P \in \mathcal{P}_R(\mathcal{X})$. Let $\hat{\rho} \in S(R,P)|_{\mathbb{R}_+}$ be arbitrary. Note that owing to Corollary 4, $\hat{\rho} \in \mathbb{R}^+$. Define $\lambda := \frac{\hat{\rho}}{1+\hat{\rho}} \in (0,1)$ and recall that (cf., proof of Claim 7) $\Lambda_{\cdot,P}(\lambda)$ is concave on $\mathcal{P}_{P,W}(\mathcal{Y})$.

For any $\hat{Q} \in \mathcal{P}_{P,W}(\mathcal{Y})$ such that $(\hat{\rho},\hat{Q}) \in S(R,P)$ we have

$$K_{R,P}(\hat{\rho},\hat{Q}) = \min_{Q \in \mathcal{P}_{P,W}(\mathcal{Y})} K_{R,P}(\hat{\rho},Q) = -\hat{\rho}R - (1+\hat{\rho}) \max_{Q \in \mathcal{P}_{P,W}(\mathcal{Y})} \Lambda_{Q,P}\left(\frac{\hat{\rho}}{1+\hat{\rho}}\right), \tag{B.64}$$

from the definition of the saddle-point.

Now, consider any $Q \in \mathcal{P}_{P,W}(\mathcal{Y})$ and for any $x \in \mathcal{S}(P)$, define $\Lambda_{Q,x}(\lambda) := \ln \sum_{y \in \mathcal{Y}} W(y|x)^{1-\lambda} Q(y)^\lambda$. Note that we have 3 possibilities for the partial derivatives of $\Lambda_{Q,x}(\lambda)$ with respect to $Q(y)$:

1. If $y \in \mathcal{S}(W(\cdot|x)) \cap \mathcal{S}(Q)$, then

$$\frac{\partial \Lambda_{Q,x}(\lambda)}{\partial Q(y)} = \frac{\lambda W(y|x)^{1-\lambda} Q(y)^{\lambda-1}}{\sum_{\tilde{y} \in \mathcal{Y}} W(\tilde{y}|x)^{1-\lambda} Q(\tilde{y})^\lambda}, \tag{B.65}$$

which is continuous in $Q(y)$.

2. If $y \notin \mathcal{S}(W(\cdot|x))$, then (since any variation along this direction does not change the value of the function)

$$\frac{\partial \Lambda_{Q,x}(\lambda)}{\partial Q(y)} = 0, \tag{B.66}$$

which is continuous in $Q(y)$.

3. If $y \notin \mathcal{S}(Q)$ and $y \in \mathcal{S}(W(\cdot|x))$, then

$$\frac{\partial \Lambda_{Q,x}(\lambda)}{\partial Q(y)} = \infty. \tag{B.67}$$

Then, [35, Theorem 4.4.1] implies that[2] a necessary and sufficient condition for any $Q \in \mathcal{P}_{P,W}(\mathcal{Y})$ to achieve the maximum in (B.64) is:

$$\frac{\partial \Lambda_{Q,P}(\lambda)}{\partial Q(y)} = \delta, \ \forall\, y \in \mathcal{S}(Q), \tag{B.68}$$

$$\frac{\partial \Lambda_{Q,P}(\lambda)}{\partial Q(y)} \leq \delta, \forall\, y \notin \mathcal{S}(Q), \tag{B.69}$$

for some $\delta \in \mathbb{R}$. Clearly, if $Q \notin \tilde{\mathcal{P}}_{P,W}(\mathcal{Y})$ then it cannot satisfy (B.68) and (B.69) (cf., (B.67)). Hence, any minimizer of (B.64) belongs to $\tilde{\mathcal{P}}_{P,W}(\mathcal{Y})$. □

Corollary 4 and Claim 10 imply the second assertion of the proposition. □

B.3 Proof of Proposition 3

Claim 11. *Consider any $C > R > R_\infty$ and $P \in \mathcal{P}_R(\mathcal{X})$. For any $\hat{\rho} \in S(R,P)|_{\mathbb{R}_+}$, there exists a unique $\hat{Q} \in \mathcal{P}_{P,W}(\mathcal{Y})$, such that $(\hat{\rho}, \hat{Q}) \in S(R,P)$.* ♦

[2] Strictly speaking the statement of the aforementioned theorem requires the cost function of the maximization problem to be continuously differentiable (with possible infinite value on the boundary) on the whole probability simplex. However, it is easy to verify that the proof given by Gallager is also applicable to our case. Indeed, for sufficiency, item (iv) of Remark 20 ensures that the value of the cost function evaluated at any Q satisfying (B.68) and (B.69) is not smaller than its counterpart for any $Q \in \mathcal{P}(\mathcal{Y}) \backslash \mathcal{P}_{P,W}(\mathcal{Y})$. For necessity, again item (iv) of Remark 20 ensures that any optimizer cannot be in $\mathcal{P}(\mathcal{Y}) \backslash \mathcal{P}_{P,W}(\mathcal{Y})$.

Proof. Consider any $C > R > R_\infty$ and $P \in \mathcal{P}_R(\mathcal{X})$. Let $\hat{\rho} \in S(R,P)|_{\mathbb{R}_+}$ be arbitrary. Existence of a $\hat{Q} \in \mathcal{P}_{P,W}(\mathcal{Y})$, such that $(\hat{\rho}, \hat{Q}) \in S(R,P)$ is guaranteed by item (i) of saddle-point proposition, i.e., Proposition 2, hence we prove the uniqueness.

To this end, note that owing to item (ii) of saddle-point proposition, (Corollary 4 to be precise), $\hat{\rho} \in \mathbb{R}^+$. Moreover, the same result (Claim 10 to be precise) also implies that any $\hat{Q} \in \mathcal{P}_{P,W}(\mathcal{Y})$, such that $(\hat{\rho}, \hat{Q}) \in S(R,P)$ satisfies $Q \in \tilde{\mathcal{P}}_{P,W}(\mathcal{Y})$ and attains the minimum in the following expression

$$\min_{Q \in \tilde{\mathcal{P}}_{P,W}(\mathcal{Y})} K_{R,P}(\hat{\rho}, Q), \tag{B.70}$$

as a direct consequence of the definition of the saddle-point. However, item (i) of Claim 7 implies that $K_{R,P}(\hat{\rho}, \cdot)$ is strictly convex on $\tilde{\mathcal{P}}_{P,W}(\mathcal{Y})$ and hence the minimizer of (B.70) is unique. □

Claim 12. *Consider any $C > R > R_\infty$ and $P \in \mathcal{P}_R(\mathcal{X})$. For any $\hat{Q} \in S(R,P)|_{\mathcal{P}_{P,W}(\mathcal{Y})}$,*

$$\forall\, \rho \in \mathbb{R}^+,\ \frac{\partial^2 K_{R,P}(\rho, \hat{Q})}{\partial \rho^2} = -\frac{1}{(1+\rho)^3} \Lambda''_{\hat{Q},P}\left(\frac{\rho}{1+\rho}\right) < 0, \tag{B.71}$$

and there exists a unique $\hat{\rho} \in \mathbb{R}_+$, such that $(\hat{\rho}, \hat{Q}) \in S(R,P)$. ♦

Proof. Consider any $C > R > R_\infty$ and $P \in \mathcal{P}_R(\mathcal{X})$. Let $\hat{Q} \in S(R,P)|_{\mathcal{P}_{P,W}(\mathcal{Y})}$ be arbitrary. The existence of a $\hat{\rho} \in \mathbb{R}_+$, such that $(\hat{\rho}, \hat{Q}) \in S(R,P)$ is guaranteed by item (i) of saddle-point proposition, i.e., Proposition 2, hence we prove the uniqueness.

To this end, note that on account of item (ii) of saddle-point proposition, (Claim 10, in particular), $\hat{Q} \in \tilde{\mathcal{P}}_{P,W}(\mathcal{Y})$, and hence $\Lambda_{\hat{Q},P}(\lambda)$ is infinitely differentiable with respect to λ on $(0,1)$.

We first claim that

$$\Lambda''_{\hat{Q},P}(\lambda) > 0,\ \forall \lambda \in (0,1). \tag{B.72}$$

For contradiction, suppose there exists a $\lambda \in (0,1)$ such that $\Lambda''_{\hat{Q},P}(\lambda) = 0$. Note that

$$\Big[\exists\, \lambda \in (0,1),\ \text{s.t. } \Lambda''_{\hat{Q},P}(\lambda) = 0\Big] \iff [\exists\, \lambda \in (0,1),\ \text{s.t.} \sum_{x\in\mathcal{S}(P)} P(x)\mathrm{Var}_{\tilde{W}_{\lambda,\hat{Q}}(\cdot|x)}\left[\ln\frac{\hat{Q}(Y)}{W(Y|x)}\right] = 0\Big] \tag{B.73}$$

$$\iff [\exists\, \lambda \in (0,1),\ \text{s.t. } \forall\, x \in \mathcal{S}(P), \mathrm{Var}_{\tilde{W}_{\lambda,\hat{Q}}(\cdot|x)}\left[\ln\frac{\hat{Q}(Y)}{W(Y|x)}\right] = 0\Big], \tag{B.74}$$

where $\Lambda'_{\hat{Q},x}(\lambda) := \mathrm{E}_{\tilde{W}_{\lambda,\hat{Q}}(\cdot|x)}\left[\ln\frac{\hat{Q}(Y)}{W(Y|x)}\right]$ (cf., (B.52)) and (B.73) follows from (B.53). From (B.74), we infer that

$$\Big[\exists\, \lambda \in (0,1),\ \text{s.t. } \Lambda''_{\hat{Q},P}(\lambda) = 0\Big] \iff [\exists\, \lambda \in (0,1),\ \text{s.t. } \forall\, x \in \mathcal{S}(P), \hat{Q}(y) = W(y|x)e^{\Lambda'_{\hat{Q},x}(\lambda)},\ \forall\, y \in \mathcal{S}(W(\cdot|x))\Big], \tag{B.75}$$

By the contradiction assumption, the left side of (B.75) is true. Fix any such $\lambda \in (0,1)$. Then, for any $\rho \in \mathbb{R}^+$, we have

$$\Lambda_{\hat{Q},P}\left(\frac{\rho}{1+\rho}\right) = \sum_{x\in\mathcal{S}(P)} P(x)\ln \sum_{y\in\mathcal{S}(W(\cdot|x))} W(y|x)^{1/(1+\rho)}\hat{Q}(y)^{\rho/(1+\rho)} \tag{B.76}$$

$$= \frac{\rho}{1+\rho}\sum_{x\in\mathcal{S}(P)} P(x)\Lambda'_{\hat{Q},x}(\lambda), \tag{B.77}$$

where (B.77) follows from (B.75). We further have,

$$\mathrm{E_{SP}}(R,P) = \max_{\rho\in\mathbb{R}_+} K_{R,P}(\rho,\hat{Q}) \tag{B.78}$$

$$= \max\left\{0, \sup_{\rho\in\mathbb{R}^+} K_{R,P}(\rho,\hat{Q})\right\}, \tag{B.79}$$

where (B.78) follows by recalling the definition of the saddle-point and item (i) of saddle-point proposition, i.e., Proposition 2, and (B.79) follows by noting the fact that $K_{R,P}(0,Q) = 0$ for all $Q \in \mathcal{P}_{P,W}(\mathcal{Y})$.

Also, (B.77) implies that

$$\sup_{\rho\in\mathbb{R}^+} K_{R,P}(\rho,\hat{Q}) = \sup_{\rho\in\mathbb{R}^+}\left\{-\rho R-\rho\sum_{x\in\mathcal{S}(P)}P(x)\Lambda'_{\hat{Q},x}(\lambda)\right\} \tag{B.80}$$

$$= \sup_{\rho\in\mathbb{R}^+} -\rho\left\{R+\Lambda'_{\hat{Q},P}(\lambda)\right\}, \tag{B.81}$$

where (B.81) follows by recalling (B.52). Equations (B.79) and (B.81) clearly imply that either $\mathrm{E_{SP}}(R,P)=\infty$, which is impossible since $R>R_\infty$, or $\mathrm{E_{SP}}(R,P)=0$, which is impossible since $P\in\mathcal{P}_R(\mathcal{X})$. Hence, (B.72) follows. A direct calculation reveals that (B.72) implies (B.71).

Next, recalling the definition of the saddle-point, we note that any $\hat{\rho}\in\mathbb{R}_+$ such that $(\hat{\rho},\hat{Q})\in S(R,P)$ satisfies

$$K_{R,P}(\hat{\rho},\hat{Q}) = \max_{\rho\in\mathbb{R}_+} K_{R,P}(\rho,\hat{Q}) \tag{B.82}$$

$$= \max_{\rho\in\mathbb{R}^+} K_{R,P}(\rho,\hat{Q}), \tag{B.83}$$

where (B.83) follows by recalling the assumption that $P\in\mathcal{P}_R(\mathcal{X})$. Equation (B.71) ensures that $K_{R,P}(\cdot,\hat{Q})$ is strictly concave on $\mathbb{R}^+$ and hence the maximizer of the right side of (B.83) is unique. □

In order to conclude the proof, fix any $C>R>R_\infty$ and $P\in\mathcal{P}_R(\mathcal{X})$ and observe that (e.g., [42, Proposition VII.4.1.3]) $S(R,P)=S(R,P)|_{\mathbb{R}_+}\times S(R,P)|_{\mathcal{P}_{P,W}(\mathcal{Y})}$. Combining this fact with Claims 11 and 12 implies that $S(R,P)$ is a singleton. □

B.4 Proof of Proposition 4

First, we define the set of Lagrange multipliers of $\mathrm{E_{SP}}(R,P)$ as follows: For any $R > R_\infty$ and $P \in \mathcal{P}(\mathcal{X})$,

$$\mathcal{L}(R,P) := \left\{ \hat{\rho} \in \mathbb{R}_+ \,:\, \hat{\rho} \text{ attains } \max_{\rho \in \mathbb{R}_+} \min_{V \in \mathcal{P}(\mathcal{Y}|\mathcal{X})} [\mathrm{D}(V\|W|P) + \rho(\mathrm{I}(P;V) - R)] \right\}. \tag{B.84}$$

Claim 13. *For any $R > R_\infty$ and $P \in \mathcal{P}(\mathcal{X})$, we have $\mathcal{L}(R,P) = S(R,P)|_{\mathbb{R}_+}$.* ♦

Proof. First of all, owing to the positivity of the relative entropy, it is easy to verify that

$$\mathrm{I}(P;V) = \min_{Q \in \mathcal{P}(\mathcal{Y})} \mathrm{D}(V\|Q|P), \tag{B.85}$$

which, in turn, implies that (by solving the convex optimization problem)

$$\forall\, \rho \in \mathbb{R}_+,\ \min_{V \in \mathcal{P}(\mathcal{Y}|\mathcal{X})} \{\mathrm{D}(V\|W|P) + \rho(\mathrm{I}(P;V) - R)\} = \min_{Q \in \mathcal{P}(\mathcal{Y})} \left\{ -\rho R - (1+\rho)\Lambda_{Q,P}\left(\frac{\rho}{1+\rho}\right) \right\}. \tag{B.86}$$

Further, since for any $Q \in \mathcal{P}(\mathcal{Y})$, $\Lambda_{Q,P}(0) = 0$ and for any $\rho \in \mathbb{R}^+$, $\Lambda_{Q,P}\left(\frac{\rho}{1+\rho}\right) = -\infty$, if $Q \notin \mathcal{P}_{P,W}(\mathcal{Y})$ (cf., item (iv) of Remark 20), we have

$$\min_{Q \in \mathcal{P}(\mathcal{Y})} \left\{ -\rho R - (1+\rho)\Lambda_{Q,P}\left(\frac{\rho}{1+\rho}\right) \right\} = \inf_{Q \in \mathcal{P}_{P,W}(\mathcal{Y})} \left\{ -\rho R - (1+\rho)\Lambda_{Q,P}\left(\frac{\rho}{1+\rho}\right) \right\}. \tag{B.87}$$

Lastly, [55, Lemma 36.2] ensures that $\hat{\rho} \in S(R,P)|_{\mathbb{R}_+}$ if and only if $\hat{\rho}$ attains $\max_{\rho \in \mathbb{R}_+} \left\{ \inf_{Q \in \mathcal{P}_{P,W}(\mathcal{Y})} K_{R,P}(\rho, Q) \right\}$, which (owing to (B.86) and (B.87)) implies that $\mathcal{L}(R,P) = S(R,P)|_{\mathbb{R}_+}$. □

Claim 14. *For any $R > R_\infty$ and $P \in \mathcal{P}(\mathcal{X})$, we have $S(R,P)|_{\mathbb{R}_+} = -\partial E_{SP}(\cdot,P)(R)$, where $\partial E_{SP}(\cdot,P)(R)$ is the* subdifferential of $\mathrm{E_{SP}}(\cdot,P)$ at R *(cf., [55, pg. 215]).* ♦

Proof. We note that (cf., [55, Theorem 29.1][3]) $\mathcal{L}(R,P) = -\partial \mathrm{E_{SP}}(\cdot,P)(R)$. The claim follows by recalling Claim 13. □

[3] Strictly speaking, this result is stated for a finite dimensional Euclidean space. However, one can represent the stochastic matrices in $\mathbb{R}^{|\mathcal{X}||\mathcal{Y}|}$ and update each function accordingly and easily check this representation obeys the conditions of the aforementioned theorem. This reasoning applies to the similar situations in the sequel.

Uniqueness of the saddle-point proposition, i.e., Proposition 3, and Claim 14 immediately imply that for any $C > R > R_\infty$ and $P \in \mathcal{P}_R(\mathcal{X})$,

$$S(R,P)|_{\mathbb{R}_+} = -\left.\frac{\partial \mathrm{E_{SP}}(r,P)}{\partial r}\right|_{r=R}. \tag{B.88}$$

By recalling the definition of $\rho^*_{R,P}$ (e.g., (3.23)), (B.88) implies that

$$\rho^*_{R,P} = -\left.\frac{\partial \mathrm{E_{SP}}(r,P)}{\partial r}\right|_{r=R}. \tag{B.89}$$

□

B.5 Proof of Proposition 5

Let $C > R > R_\infty$ be arbitrary. Fix any $P_0 \in \mathcal{P}_R(\mathcal{X})$ and consider any $\{P_k\}_{k\geq 1}$ such that $P_k \in \mathcal{P}_R(\mathcal{X})$, $\forall\, k \in \mathbb{Z}^+$ and $\lim_{n\to\infty} P_k = P_0$.

We begin with showing the continuity of $\rho^*_{R,\cdot}$. Recalling (3.23) and the differentiability of $\mathrm{E_{SP}}(\cdot, P)$ proposition, i.e., Proposition 4, we have

$$\forall k \in \mathbb{Z}_+,\ \rho^*_{R,P_k} = -\left.\frac{\partial \mathrm{E_{SP}}(r,P_k)}{\partial r}\right|_{r=R}. \tag{B.90}$$

Further, continuity of $\mathrm{E_{SP}}(\cdot,\cdot)$ on $(R_\infty,\infty)\times\mathcal{P}(\mathcal{X})$ (e.g., Claim 30) implies that

$$\lim_{k\to\infty} \mathrm{E_{SP}}(R,P_k) = \mathrm{E_{SP}}(R,P_0). \tag{B.91}$$

On account of (B.90), (B.91) and a continuity result of Hiriart-Urruty and Lemaréchal ([42, Corollary VI.6.2.8]) we conclude that

$$\lim_{k\to\infty} \rho^*_{R,P_k} = \rho^*_{R,P_0}, \tag{B.92}$$

which implies that $\rho^*_{R,\cdot}$ is continuous on $\mathcal{P}_R(\mathcal{X})$.

Next, we claim the continuity of $Q^*_{R,\cdot}$. Owing to the compactness of $\mathcal{P}(\mathcal{Y})$, there exists a subsequence $\{k_n\}_{n\geq 1}$ such that $\lim_{n\to\infty} Q^*_{R,P_{k_n}} = Q_0$ for some $Q_0 \in \mathcal{P}(\mathcal{Y})$. Consider such a subsequence.

Recalling the saddle-point proposition, i.e., Proposition 2, and the definitions of $\rho^*_{R,\cdot}$ and $Q^*_{R,\cdot}$ (e.g., (3.23) and (3.24)), we have

$$\forall\, n \in \mathbb{Z}^+,\, \mathrm{E_{SP}}(R, P_{k_n}) = -R\rho^*_{R,P_{k_n}} - (1+\rho^*_{R,P_{k_n}})\Lambda_{Q^*_{R,P_{k_n}},P_{k_n}}\left(\frac{\rho^*_{R,P_{k_n}}}{1+\rho^*_{R,P_{k_n}}}\right). \tag{B.93}$$

Next, we define $f : \mathbb{R}_+ \times \mathbb{R}^+ \to \mathbb{R}$, such that $f(a,b) := a^b$ for any $(a,b) \in \mathbb{R}_+ \times \mathbb{R}^+$ and note that f is continuous on $\mathbb{R}_+ \times \mathbb{R}^+$. Using this, the continuity of $\rho^*_{R,\cdot}$ and $\ln(\cdot)$, we deduce that

$$\lim_{n\to\infty} \Lambda_{Q^*_{R,P_{k_n}},P_{k_n}}\left(\frac{\rho^*_{R,P_{k_n}}}{1+\rho^*_{R,P_{k_n}}}\right) = \Lambda_{Q_0,P_0}\left(\frac{\rho^*_{R,P_{k_0}}}{1+\rho^*_{R,P_{k_0}}}\right). \tag{B.94}$$

Equations (B.93), (B.94) and the continuity of $\rho^*_{R,\cdot}$ imply that

$$\mathrm{E_{SP}}(R, P_0) = -R\rho^*_{R,P_0} - (1+\rho^*_{R,P_0})\Lambda_{Q_0,P_0}\left(\frac{\rho^*_{R,P_0}}{1+\rho^*_{R,P_0}}\right) \tag{B.95}$$

$$= \min_{Q\in\mathcal{P}_{P,W}(\mathcal{Y})}\left\{-R\rho^*_{R,P_0} - (1+\rho^*_{R,P_0})\Lambda_{Q,P_0}\left(\frac{\rho^*_{R,P_0}}{1+\rho^*_{R,P_0}}\right)\right\} \tag{B.96}$$

$$= \min_{Q\in\mathcal{P}(\mathcal{Y})}\left\{-R\rho^*_{R,P_0} - (1+\rho^*_{R,P_0})\Lambda_{Q,P_0}\left(\frac{\rho^*_{R,P_0}}{1+\rho^*_{R,P_0}}\right)\right\}, \tag{B.97}$$

where (B.96) follows from recalling the definition of the saddle-point and (B.97) follows from item (iv) of Remark 20. The uniqueness of the saddle-point proposition, i.e., Proposition 3, the definition of $Q^*_{R,P}$ (e.g., (3.24)) and (B.97) imply that $Q_0 = Q^*_{R,P_0}$. Since $\{k_n\}_{n\geq 1}$ is arbitrary, we conclude that

$$\lim_{k\to\infty} Q^*_{R,P_k} = Q^*_{R,P_0}, \tag{B.98}$$

which implies that $Q^*_{R,\cdot}$ is continuous on $\mathcal{P}_R(\mathcal{X})$. □

B.6 Proof of Proposition 6

Fix an arbitrary $C(W) > R > R_\infty$ and $P \in \mathcal{P}_R(\mathcal{X})$. Define $L(V,\rho) := \mathrm{D}(V\|W|P) + \rho(\mathrm{I}(P;V) - R)$, for any $V \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ and $\rho \in \mathbb{R}_+$. We have

$$\mathrm{E_{SP}}(R,P) = \min_{V\in\mathcal{P}(\mathcal{Y}|\mathcal{X})} \sup_{\rho\in\mathbb{R}_+} L(V,\rho) = \max_{\rho\in\mathbb{R}_+} \min_{V\in\mathcal{P}(\mathcal{Y}|\mathcal{X})} L(V,\rho), \tag{B.99}$$

where the second equality follows from (B.41). (B.99) ensures that $L(\cdot,\cdot)$ has a saddle-point on $\mathcal{P}(\mathcal{Y}|\mathcal{X}) \times \mathbb{R}_+$. It is well-known that (e.g., [55, Corollary 28.3.1]) $\hat{V} \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ is a minimizer of $\mathrm{E_{SP}}(R,P)$ if and only if there exists some $\hat{\rho} \in \mathbb{R}_+$, such that $(\hat{V},\hat{\rho})$ is a saddle-point of $L(\cdot,\cdot)$.

Recalling the definition of the saddle-point, the definition of $\rho^*_{R,P}$ (e.g., (3.23)), (B.84) and Claim 13, we conclude that an equivalent condition for $V^*_{R,P}$ to be an optimizer of $\mathrm{E_{SP}}(R,P)$ is

$$V^*_{R,P} \in \arg\min_{V\in\mathcal{P}(\mathcal{Y}|\mathcal{X})} L(V,\rho^*_{R,P}). \tag{B.100}$$

Further,

$$\begin{aligned}
\mathrm{E_{SP}}(R,P) &= \min_{V\in\mathcal{P}(\mathcal{Y}|\mathcal{X})} L(V,\rho^*_{R,P}) && \text{(B.101)}\\
&= \min_{Q\in\mathcal{P}(\mathcal{Y})} \min_{V\in\mathcal{P}(\mathcal{Y}|\mathcal{X})} \Big\{\mathrm{D}(V\|W|P) + \rho^*_{R,P}[\mathrm{D}(V\|Q|P) - R]\Big\} && \text{(B.102)}\\
&\le \min_{V\in\mathcal{P}(\mathcal{Y}|\mathcal{X})} \Big\{\mathrm{D}(V\|W|P) + \rho^*_{R,P}[\mathrm{D}(V\|Q^*_{R,P}|P) - R]\Big\} && \text{(B.103)}\\
&\le K_{R,P}(\rho^*_{R,P}, Q^*_{R,P}) && \text{(B.104)}\\
&= \mathrm{E_{SP}}(R,P), && \text{(B.105)}
\end{aligned}$$

where (B.101) follows from (B.100), (B.102) follows from (B.85), (B.104) follows by plugging in $\tilde{W}_{\frac{\rho^*_{R,P}}{1+\rho^*_{R,P}},Q^*_{R,P}}$ (cf., (B.51)) and (B.105) follows from the saddle-point proposition, i.e., Proposition 2 and the uniqueness of the saddle-point proposition, i.e., Propo-

sition 3. Hence, we deduce that

$$\min_{V\in\mathcal{P}(\mathcal{Y}|\mathcal{X})} L(V,\rho^*_{R,P}) = \min_{V\in\mathcal{P}(\mathcal{Y}|\mathcal{X})} \Big\{\mathrm{D}(V\|W|P) + \rho^*_{R,P}[\mathrm{D}(V\|Q^*_{R,P}|P) - R]\Big\} = \mathrm{E_{SP}}(R,P), \tag{B.106}$$

and $\tilde{W}_{\frac{\rho^*_{R,P}}{1+\rho^*_{R,P}},Q^*_{R,P}}$ is an optimizer of $\min_{V\in\mathcal{P}(\mathcal{Y}|\mathcal{X})}\Big\{\mathrm{D}(V\|W|P) + \rho^*_{R,P}[\mathrm{D}(V\|Q^*_{R,P}|P) - R]\Big\}$. Moreover, since

$$L(V,\rho^*_{R,P}) \leq \mathrm{D}(V\|W|P) + \rho^*_{R,P}[\mathrm{D}(V\|Q^*_{R,P}|P) - R], \forall\, V \in \mathcal{P}(\mathcal{Y}|\mathcal{X}), \tag{B.107}$$

we notice that (B.106) further implies that $\tilde{W}_{\frac{\rho^*_{R,P}}{1+\rho^*_{R,P}},Q^*_{R,P}} \in \arg\min_{V\in\mathcal{P}(\mathcal{Y}|\mathcal{X})} L(V,\rho^*_{R,P})$, and hence $\tilde{W}_{\frac{\rho^*_{R,P}}{1+\rho^*_{R,P}},Q^*_{R,P}}$ is a minimizer of $\mathrm{E_{SP}}(R,P)$, owing to (B.100).

Next, we note that on account of (B.65), for any $Q \in \tilde{\mathcal{P}}_{P,W}(\mathcal{Y})$, we have

$$\frac{\partial\Lambda_{Q,P}\left(\frac{\rho^*_{R,P}}{1+\rho^*_{R,P}}\right)}{\partial Q(y)} = \frac{\rho^*_{R,P}}{1+\rho^*_{R,P}} \sum_{x\in\mathcal{S}(P)} P(x)\frac{W(y|x)^{1/(1+\rho^*_{R,P})}Q(y)^{-1/(1+\rho^*_{R,P})}}{\sum_{\tilde{y}\in\mathcal{Y}} W(\tilde{y}|x)^{1/(1+\rho^*_{R,P})}Q(\tilde{y})^{\rho^*_{R,P}/(1+\rho^*_{R,P})}}, \tag{B.108}$$

for all $y \in \mathcal{S}(Q)$. Moreover, (B.66) implies that for any $Q \in \tilde{\mathcal{P}}_{P,W}(\mathcal{Y})$,

$$\frac{\partial\Lambda_{Q,P}\left(\frac{\rho^*_{R,P}}{1+\rho^*_{R,P}}\right)}{\partial Q(y)} = 0,\ \forall\, y \notin \mathcal{S}(Q). \tag{B.109}$$

KKT conditions that $Q^*_{R,P}$ satisfies, i.e., (B.68) and (B.69), coupled with (B.108) and (B.109) (by choosing $\delta = \frac{\rho^*_{R,P}}{1+\rho^*_{R,P}}$ to ensure that $Q^*_{R,P}$ sums to 1) imply that

$$Q^*_{R,P}(y) = \sum_{x\in\mathcal{S}(P)} P(x)\frac{W(y|x)^{1/(1+\rho^*_{R,P})}Q^*_{R,P}(y)^{\rho^*_{R,P}/(1+\rho^*_{R,P})}}{\sum_{\tilde{y}\in\mathcal{Y}} W(\tilde{y}|x)^{1/(1+\rho^*_{R,P})}Q^*_{R,P}(\tilde{y})^{\rho^*_{R,P}/(1+\rho^*_{R,P})}},\ \forall\, y \in \mathcal{Y}. \tag{B.110}$$

Clearly, (B.110) implies that

$$\sum_{x\in\mathcal{S}(P)} P(x)\tilde{W}_{\frac{\rho^*_{R,P}}{1+\rho^*_{R,P}},Q^*_{R,P}}(y|x) = Q^*_{R,P}(y),\ \forall\, y \in \mathcal{Y}, \tag{B.111}$$

which, in turn, implies that (since $\tilde{W}_{\frac{\rho^*_{R,P}}{1+\rho^*_{R,P}},Q^*_{R,P}}$ is an optimizer of $\mathrm{E_{SP}}(R,P)$)

$$\mathrm{I}\left(P;\tilde{W}_{\frac{\rho^*_{R,P}}{1+\rho^*_{R,P}},Q^*_{R,P}}\right) = \mathrm{D}\left(\tilde{W}_{\frac{\rho^*_{R,P}}{1+\rho^*_{R,P}},Q^*_{R,P}}\|Q^*_{R,P}|P\right) \leq R. \tag{B.112}$$

Next, we conclude the proof as follows. First,

$$\mathrm{e}_{\mathrm{SP}}(R,P) = \inf_{V\in\mathcal{P}(\mathcal{Y}|\mathcal{X})} \sup_{\rho\in\mathbb{R}_+} \left\{\mathrm{D}(V\|W|P) + \rho[\mathrm{D}(V\|Q^*_{R,P}|P) - R]\right\} \tag{B.113}$$

$$\geq \inf_{V\in\mathcal{P}(\mathcal{Y}|\mathcal{X})} \left\{\mathrm{D}(V\|W|P) + \rho^*_{R,P}[\mathrm{D}(V\|Q^*_{R,P}|P) - R]\right\} \tag{B.114}$$

$$= \mathrm{E}_{\mathrm{SP}}(R,P), \tag{B.115}$$

where (B.115) follows from (B.106).

On the other hand, (B.112) and the fact that $\tilde{W}_{\frac{\rho^*_{R,P}}{1+\rho^*_{R,P}},Q^*_{R,P}}$ is a minimizer of $\mathrm{E}_{\mathrm{SP}}(R,P)$ ensure that

$$\mathrm{e}_{\mathrm{SP}}(R,P) \leq \mathrm{D}\left(\tilde{W}_{\frac{\rho^*_{R,P}}{1+\rho^*_{R,P}},Q^*_{R,P}}\|W|P\right) = \mathrm{E}_{\mathrm{SP}}(R,P). \tag{B.116}$$

Combining (B.115) and (B.116), we infer that

$$\mathrm{e}_{\mathrm{SP}}(R,P) = \min_{V\in\mathcal{P}(\mathcal{Y}|\mathcal{X})\,:\,\mathrm{D}(V\|Q^*_{R,P}|P)\leq R} \mathrm{D}(V\|W|P) = \mathrm{E}_{\mathrm{SP}}(R,P). \tag{B.117}$$

□

B.7 Analysis of the case $P \in \mathcal{P}^c_{R,\nu}$

First, we define the following set: $\mathcal{P}_W(\mathcal{Y}|\mathcal{X}) := \{V \in \mathcal{P}(\mathcal{Y}|\mathcal{X}) : \forall\, x \in \mathcal{X},\, V(\cdot|x) \ll W(\cdot|x)\}$. One can check the following by elementary calculation.

Claim 15. *$\mathcal{P}_W(\mathcal{Y}|\mathcal{X})$ is convex and compact.* ♦

Next result will also be used in different parts of the chapter.

Lemma 30. *$E_{SP}(\cdot,\cdot)$ is continuous on $(R_\infty,\infty)\times\mathcal{P}(\mathcal{X})$.* ♦

Proof. The proof follows similar lines to those of [20, Lemma 2.2.2], which proves continuity of the rate-distortion function.

First, note that given any $P \in \mathcal{P}(\mathcal{X})$, $\mathrm{E_{SP}}(\cdot, P)$ is convex on (R_∞, ∞). Fix an arbitrary $(R_0, P_0) \in (R_\infty, \infty) \times \mathcal{P}(\mathcal{X})$ and a sequence $\{(R_n, P_n)\}_{n\geq 1}$ such that $(R_n, P_n) \in (R_\infty, \infty) \times \mathcal{P}(\mathcal{X})$ and $\lim_{n\to\infty}(R_n, P_n) = (R_0, P_0)$.

Because of the convexity, $\mathrm{E_{SP}}(\cdot, P_0)$ is continuous on (R_∞, ∞). Hence, for any $\epsilon \in \mathbb{R}^+$ one can choose $V \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ such that $\mathrm{I}(P_0; V) < R_0$ and $\mathrm{D}(V\|W|P_0) < \mathrm{E_{SP}}(R_0, P_0) + \epsilon$. Moreover, on account of continuity of $\mathrm{D}(V\|W|\cdot)$ and $\mathrm{I}(\cdot; V)$, we have

$$\mathrm{D}(V\|W|P_n) < \mathrm{E_{SP}}(R_0, P_0) + 2\epsilon, \quad \mathrm{I}(P_n; V) \leq R_n, \tag{B.118}$$

for sufficiently large n, which, in turn, implies that

$$\limsup_{n\to\infty} \mathrm{E_{SP}}(R_n, P_n) \leq \mathrm{E_{SP}}(R_0, P_0). \tag{B.119}$$

Conversely, let $V_n \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ be a minimizer of $\mathrm{E_{SP}}(R_n, P_n)$ and without loss of generality suppose[4] $V_n \in \mathcal{P}_W(\mathcal{Y}|\mathcal{X})$. Let $\{n_k\}_{k\geq 1}$ be a subsequence such that

$$\lim_{k\to\infty} \mathrm{E_{SP}}(R_{n_k}, P_{n_k}) = \liminf_{n\to\infty} \mathrm{E_{SP}}(R_n, P_n), \tag{B.120}$$

and

$$\lim_{k\to\infty} V_{n_k} = V, \tag{B.121}$$

for some $V \in \mathcal{P}_W(\mathcal{Y}|\mathcal{X})$. Note that existence of such a subsequence is ensured by the compactness of $\mathcal{P}_W(\mathcal{Y}|\mathcal{X})$ (cf., Claim 15). Equation (B.121) further implies that

$$\lim_{k\to\infty} \mathrm{I}(P_{n_k}; V_{n_k}) = \mathrm{I}(P_0; V) \leq R_0, \tag{B.122}$$

$$\lim_{k\to\infty} \mathrm{D}(V_{n_k}\|W|P_{n_k}) = \mathrm{D}(V\|W|P_0), \tag{B.123}$$

where (B.122) follows from the continuity of $\mathrm{I}(\cdot;\cdot)$ and (B.123) follows from the continuity of $\mathrm{D}(\cdot\|W|\cdot)$ on $\mathcal{P}_W(\mathcal{Y}|\mathcal{X}) \times \mathcal{P}(\mathcal{X})$. Equations (B.120), (B.122) and (B.123) imply

[4]To see why this does not yield a loss of generality, first note that since $\mathrm{E_{SP}}(R_n, P_n) < \infty$, we necessarily have $V_n(\cdot|x) \ll W(\cdot|x)$, for all $x \in \mathcal{S}(P_n)$. On the other hand, $x \notin \mathcal{S}(P_n)$ does not affect neither the cost nor the constraint and hence the corresponding rows of the alternate channel, i.e., optimization variable of $\mathrm{E_{SP}}(R_n, P_n)$, can be chosen arbitrarily without affecting optimality.

that

$$\mathrm{E_{SP}}(R_0, P_0) \leq \liminf_{n\to\infty} \mathrm{E_{SP}}(R_n, P_n). \tag{B.124}$$

Equations (B.119) and (B.124) imply that

$$\lim_{n\to\infty} \mathrm{E_{SP}}(R_n, P_n) = \mathrm{E_{SP}}(R_0, P_0). \tag{B.125}$$

□

Consider any $R_\infty < R < C$. For any $\nu \in \mathbb{R}^+$,

$$\mathcal{P}_{R,\nu}(\mathcal{X}) := \{P \in \mathcal{P}(\mathcal{X}) \,:\, \mathrm{E_{SP}}(R, P) \geq \nu\}. \tag{B.126}$$

Let

$$\epsilon := (R - R_\infty)/2, \tag{B.127}$$

and fix an arbitrary $a \in (1, 2)$. Note that since $\mathrm{E_{SP}}(\cdot)$ is convex, it is easy to see that it is Lipschitz continuous on $[R - \epsilon, R]$ (e.g., [55, Theorem 10.4]), i.e., there exists $L \in \mathbb{R}^+$, such that

$$\forall\, r_1, r_2 \in [R - \epsilon, R], \quad |\mathrm{E_{SP}}(r_1) - \mathrm{E_{SP}}(r_2)| \leq L|r_1 - r_2|. \tag{B.128}$$

Next, we consider an arbitrary $\nu \in \mathbb{R}^+$ satisfying:

$$\nu \leq \min\left\{(a-1),\ \frac{\epsilon}{2},\ \frac{\mathrm{E_{SP}}(R)(2-a)}{a(2L+1)}\right\}. \tag{B.129}$$

We claim that[5]

$$\max_{P \in \mathrm{cl}(\mathcal{P}_{R,\nu}(\mathcal{X})^c)} \mathrm{E_{SP}}(R - \nu, P) \leq \frac{\mathrm{E_{SP}}(R)}{a}. \tag{B.130}$$

For contradiction, suppose

$$\max_{P \in \mathrm{cl}(\mathcal{P}_{R,\nu}(\mathcal{X})^c)} \mathrm{E_{SP}}(R - \nu, P) > \frac{\mathrm{E_{SP}}(R)}{a}, \tag{B.131}$$

[5]Owing to Lemma 30, the maximum is well-defined.

with a maximizer $\tilde{P}$. Since $\mathrm{E_{SP}}(\cdot, \tilde{P})$ is convex and non-decreasing, (B.131) implies that

$$\mathrm{E_{SP}}(R - 2\nu, \tilde{P}) > \frac{\mathrm{E_{SP}}(R)}{a} + \nu\left(\frac{\mathrm{E_{SP}}(R)}{a\nu} - 1\right) = \frac{2\mathrm{E_{SP}}(R)}{a} - \nu. \tag{B.132}$$

Further, owing to (B.129), we have

$$\frac{2\mathrm{E_{SP}}(R)}{a} - \nu \geq \mathrm{E_{SP}}(R) + 2L\nu. \tag{B.133}$$

Also, (B.128) and (B.129) imply that

$$\mathrm{E_{SP}}(R - 2\nu) \leq \mathrm{E_{SP}}(R) + 2L\nu. \tag{B.134}$$

Plugging (B.133) and (B.134) into (B.132) yields

$$\mathrm{E_{SP}}(R - 2\nu, \tilde{P}) > \mathrm{E_{SP}}(R - 2\nu), \tag{B.135}$$

which is a contradiction, by recalling the definition of $\mathrm{E_{SP}}(\cdot)$, and hence (B.130) follows.

Let $P \in \mathrm{cl}(\mathcal{P}_{R,\nu}(\mathcal{X})^c)$ be arbitrary. We have

$$(1 + \nu)\mathrm{E_{SP}}(R - \nu, P) \leq \frac{(1 + \nu)\mathrm{E_{SP}}(R)}{a} \tag{B.136}$$

$$\leq \mathrm{E_{SP}}(R), \tag{B.137}$$

where (B.136) follows from (B.130) and (B.137) follows from (B.129).

Let (f, φ) be an (N, R) constant composition code with common composition $P \in \mathrm{cl}(\mathcal{P}_{R,\nu}(\mathcal{X})^c)$. For all sufficiently large N, which only depends on $\nu, |\mathcal{X}|, |\mathcal{Y}|$, we have

$$e(f, \varphi) \geq \frac{1}{2}\exp(-N(1 + \nu)\mathrm{E_{SP}}(R - \nu, P)) \tag{B.138}$$

$$\geq \frac{1}{2}\exp(-N\mathrm{E_{SP}}(R)), \tag{B.139}$$

where (B.138) follows from the sphere packing lower bound for constant composition codes (cf., [20, Theorem 2.5.3]) and (B.139) follows from (B.137). Hence, we have the following lemma.

Lemma 31. *Fix $R_\infty < R < C$ and $\nu > 0$ satisfying* (B.129)*. Then, for all sufficiently large N, which only depends on $\nu, |\mathcal{X}|$, and $|\mathcal{Y}|$, any (N, R) constant composition code with common composition $P \in cl(\mathcal{P}_{R,\nu}(\mathcal{X})^c)$ satisfies*

$$e(f, \varphi) \geq \frac{1}{2} \exp(-NE_{SP}(R)). \tag{B.140}$$

♦

B.8 Proof of Lemma 6

We begin with the proof of item (i). First, note that

$$\begin{aligned} \mathrm{D}(V||W^-_{R,P}|P) &= \sum_{x\in\mathcal{S}(P)} P(x) \sum_{y\in\mathcal{S}(V(\cdot|x))} V(y|x) \ln \frac{V(y|x)}{W^-_{R,P}(y|x)} && \text{(B.141)} \\ &= \sum_{x\in\mathcal{S}(P)} P(x) \left\{ \ln Q^*_{R,P}\{\mathcal{S}(W(\cdot|x))\} + \mathrm{D}(V(\cdot|x)||Q^*_{R,P}) \right\} && \text{(B.142)} \\ &= \mathrm{D}(V||Q^*_{R,P}|P) + \sum_{x\in\mathcal{S}(P)} P(x) \ln Q^*_{R,P}\{\mathcal{S}(W(\cdot|x))\}, && \text{(B.143)} \end{aligned}$$

where (B.142) follows from (3.41).

Similarly,

$$\begin{aligned} \mathrm{D}(W^-_{R,P}||Q^*_{R,P}|P) &= \sum_{x\in\mathcal{S}(P)} P(x) \sum_{y\in\mathcal{S}(W(\cdot|x))} W^-_{R,P}(y|x) \ln \frac{W^-_{R,P}(y|x)}{Q^*_{R,P}(y)} && \text{(B.144)} \\ &= -\sum_{x\in\mathcal{S}(P)} P(x) \ln Q^*_{R,P}\{\mathcal{S}(W(\cdot|x))\} \sum_{y\in\mathcal{S}(W(\cdot|x))} W^-_{R,P}(y|x) && \text{(B.145)} \\ &= -\sum_{x\in\mathcal{S}(P)} P(x) \ln Q^*_{R,P}\{\mathcal{S}(W(\cdot|x))\}, && \text{(B.146)} \end{aligned}$$

where (B.145) follows from the fact that $Q^*_{R,P} \in \tilde{\mathcal{P}}_{P,W}(\mathcal{Y})$ (cf., item (ii) of Proposition 2) and noting $W^-_{R,P}(\cdot|x) \equiv W(\cdot|x)$, for all $x \in \mathcal{X}$. Plugging (B.146) into (B.143) gives item (i) of the lemma.

In order to prove item (ii), observe that $(\rho^*_{R,P}, Q^*_{R,P})$ is the unique saddle-point of $K_{R,P}(\cdot,\cdot)$. We have

$$K_{R,P}(\rho^*_{R,P}, Q^*_{R,P}) = \max_{\rho\in\mathbb{R}_+} K_{R,P}(\rho, Q^*_{R,P}) \tag{B.147}$$

$$= \max_{\rho\in\mathbb{R}^+} K_{R,P}(\rho, Q^*_{R,P}), \tag{B.148}$$

where (B.148) follows by noting that $\mathrm{E_{SP}}(R,P) = K_{R,P}(\rho^*_{R,P}, Q^*_{R,P}) > 0$ (cf., (B.105)) and $K_{R,P}(0, Q^*_{R,P}) = 0$. Observe that $\rho^*_{R,P} \in \mathbb{R}^+$ is the unique maximizer of the right side of (B.148) and hence

$$\left.\frac{\partial K_{R,P}(\rho, Q^*_{R,P})}{\partial\rho}\right|_{\rho=\rho^*_{R,P}} = -R - \Lambda_{Q^*_{R,P},P}\left(\frac{\rho^*_{R,P}}{1+\rho^*_{R,P}}\right) - \frac{1}{(1+\rho^*_{R,P})}\Lambda'_{Q^*_{R,P},P}\left(\frac{\rho^*_{R,P}}{1+\rho^*_{R,P}}\right) = 0. \tag{B.149}$$

Further,

$$\lim_{\lambda\uparrow 1}\Lambda_{Q^*_{R,P},P}(\lambda) = \lim_{\lambda\uparrow 1}\sum_{x\in\mathcal{S}(P)} P(x)\ln\sum_{y\in\mathcal{S}(W(\cdot|x))} W(y|x)^{1-\lambda}Q^*_{R,P}(y)^{\lambda} \tag{B.150}$$

$$= \sum_{x\in\mathcal{S}(P)} P(x)\ln\lim_{\lambda\uparrow 1}\sum_{y\in\mathcal{S}(W(\cdot|x))} W(y|x)^{1-\lambda}Q^*_{R,P}(y)^{\lambda} \tag{B.151}$$

$$= \sum_{x\in\mathcal{S}(P)} P(x)\ln\sum_{y\in\mathcal{S}(W(\cdot|x))} Q^*_{R,P}(y) \tag{B.152}$$

$$= -\mathrm{D}(W^-_{R,P}\|Q^*_{R,P}|P), \tag{B.153}$$

where (B.153) follows from (B.146).

Moreover, recalling (3.31) and (3.32), for any $x \in \mathcal{S}(P)$

$$\lim_{\lambda\uparrow 1}\tilde{W}_{\lambda,Q^*_{R,P}}(y|x) = W^-_{R,P}(y|x), \tag{B.154}$$

for all $y \in \mathcal{Y}$. One can check that (e.g., (B.52))

$$\Lambda'_{Q^*_{R,P},P}(\lambda) = \sum_{x\in\mathcal{S}(P)} P(x)\mathrm{E}_{\tilde{W}_{\lambda,Q^*_{R,P}}(\cdot|x)}\left[\ln\frac{Q^*_{R,P}(Y)}{W(Y|x)}\right], \tag{B.155}$$

which, coupled with (B.154), implies that

$$\lim_{\lambda\uparrow 1}\Lambda'_{Q^*_{R,P},P}(\lambda)=\sum_{x\in\mathcal{S}(P)}P(x)\sum_{y\in\mathcal{S}(W(\cdot|x))}W^-_{R,P}(y|x)\ln\frac{Q^*_{R,P}(y)}{W(y|x)}\in\mathbb{R}, \tag{B.156}$$

which, in turn, implies that

$$\lim_{\rho\to\infty}\frac{1}{(1+\rho)}\Lambda'_{Q^*_{R,P},P}\left(\frac{\rho}{1+\rho}\right)=0. \tag{B.157}$$

We have

$$\begin{aligned}0&>\lim_{\rho\to\infty}\frac{\partial K_{R,P}(\rho,Q^*_{R,P})}{\partial\rho} &\text{(B.158)}\\ &=\lim_{\rho\to\infty}-R-\Lambda_{Q^*_{R,P},P}\left(\frac{\rho}{1+\rho}\right)-\frac{1}{(1+\rho)}\Lambda'_{Q^*_{R,P},P}\left(\frac{\rho}{1+\rho}\right)\\ &=\mathrm{D}(W^-_{R,P}\|Q^*_{R,P}|P)-R, &\text{(B.159)}\end{aligned}$$

where (B.158) follows from (B.149) and (B.71) and (B.159) follows from (B.153) and (B.157). Hence, we conclude that $R>\mathrm{D}(W^-_{R,P}\|Q^*_{R,P}|P)$. □

B.9 Proof of Lemma 9

Let $(\lambda_0,P_0)\in(0,1]\times\mathcal{P}_R(\mathcal{X})$ be arbitrary. Further, consider any $\{(\lambda_k,P_k)\}_{k\geq 1}$ such that $(\lambda_k,P_k)\in(0,1]\times\mathcal{P}_R(\mathcal{X})$, for all $k\in\mathbb{Z}^+$ and $\lim_{k\to\infty}(\lambda_k,P_k)=(\lambda_0,P_0)$.

Note that for all sufficiently large $k\in\mathbb{Z}^+$, $\mathcal{S}(P_0)\subset\mathcal{S}(P_k)$. Consider such a $k\in\mathbb{Z}^+$. Recalling (3.54) and (3.55), we have

$$\Lambda'_{0,P_k}(\lambda_k)=\sum_{x\in\mathcal{S}(P_0)}P_k(x)\mathrm{E}_{\tilde{W}_{\lambda_k,P_k}(\cdot|x)}\left[\ln\frac{W^-_{R,P_k}(Y|x)}{W(Y|x)}\right]+\sum_{x\in\mathcal{S}(P_0)^c}P_k(x)\mathrm{E}_{\tilde{W}_{\lambda_k,P_k}(\cdot|x)}\left[\ln\frac{W^-_{R,P_k}(Y|x)}{W(Y|x)}\right]. \tag{B.160}$$

Using the continuity of the saddle-point proposition, i.e., Proposition 5, (3.31),

(3.33) and the continuity of $\ln(\cdot)$, it is easy to see that

$$\lim_{k\to\infty} P_k(x)\mathrm{E}_{\tilde{W}_{\lambda_k,P_k}(\cdot|x)}\left[\ln\frac{W^-_{R,P_k}(Y|x)}{W(Y|x)}\right] = P_0(x)\mathrm{E}_{\tilde{W}_{\lambda_0,P_0}(\cdot|x)}\left[\ln\frac{W^-_{R,P_0}(Y|x)}{W(Y|x)}\right],\ \forall\, x\in\mathcal{S}(P_0), \tag{B.161}$$

which, in turn, implies that

$$\lim_{k\to\infty}\sum_{x\in\mathcal{S}(P_0)} P_k(x)\mathrm{E}_{\tilde{W}_{\lambda_k,P_k}(\cdot|x)}\left[\ln\frac{W^-_{R,P_k}(Y|x)}{W(Y|x)}\right] = \sum_{x\in\mathcal{S}(P_0)} P_0(x)\mathrm{E}_{\tilde{W}_{\lambda_0,P_0}(\cdot|x)}\left[\ln\frac{W^-_{R,P_0}(Y|x)}{W(Y|x)}\right]. \tag{B.162}$$

Next, we claim that

$$\lim_{k\to\infty} P_k(x)\mathrm{E}_{\tilde{W}_{\lambda_k,P_k}(\cdot|x)}\left[\ln\frac{W^-_{R,P_k}(Y|x)}{W(Y|x)}\right] = 0, \tag{B.163}$$

for any $x\in\mathcal{S}(P_0)^c$. To see this, fix an arbitrary $x\in\mathcal{S}(P_0)^c$. If $x\in\mathcal{S}(P_k)$ for only finite number of k, then owing to (3.31), (B.163) is trivially true; hence suppose this is not the case. Let $\{k_n\}_{n\geq 1}$ be an arbitrary subsequence such that $x\in\mathcal{S}(P_{k_n})$, for all $n\in\mathbb{Z}^+$. Owing to the compactness of $\mathcal{P}(\mathcal{Y}|\mathcal{X})$ (swtiching to a subsubsequence if necessary) there exists $W_0(\cdot|x)\in\mathcal{P}(\mathcal{Y}|\mathcal{X})$, such that

$$\lim_{n\to\infty} W^-_{R,P_{k_n}}(\cdot|x) = W_0(\cdot|x). \tag{B.164}$$

Since $W^-_{R,P_{k_n}}(\cdot|x)\ll W(\cdot|x)$ for all $n\in\mathbb{Z}^+$, it is easy to see that (cf., proof of Claim 15) $W_0(\cdot|x)\ll W(\cdot|x)$. This fact, along with the continuity of $\ln(\cdot)$ and (B.164), implies that

$$\lim_{m\to\infty}\mathrm{E}_{\tilde{W}_{\lambda_{k_n},P_{k_n}}(\cdot|x)}\left[\ln\frac{W^-_{R,P_{k_n}}(Y|x)}{W(Y|x)}\right] = \mathrm{E}_{\tilde{W}_{\lambda_0,W_0(\cdot|x)}}\left[\ln\frac{W_0(Y|x)}{W(Y|x)}\right] < \infty. \tag{B.165}$$

Noting $\lim_{m\to\infty} P_{k_{n_m}}(x) = P_0(x) = 0$ and the arbitrariness of the subsequence, (B.165) implies (B.163). Plugging (B.162) and (B.163) into (B.160) implies that

$$\lim_{k\to\infty}\Lambda'_{0,P_k}(\lambda_k) = \Lambda'_{0,P_0}(\lambda_0), \tag{B.166}$$

and hence we conclude $\Lambda'_{0,\cdot}(\cdot)$ is continuous on $(0,1]\times\mathcal{P}_R(\mathcal{X})$.

By following exactly the same steps given above and noting the continuity of $(\cdot)^2$ (resp. $|\cdot|^3$), one can conclude the continuity of $\Lambda''_{0,\cdot}(\cdot)$ (resp. $m_{0,3}(\cdot,\cdot)$) on $(0,1]\times\mathcal{P}_R(\mathcal{X})$.

Finally, the proof of item (iv) follows from the similar arguments given in the proof of item (i). □

B.10 Proof of Lemma 12

Let $s^*(R,P,r) \in \mathbb{R}_+$ be as defined in (3.76). Since it is the unique maximizer of $\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r)$, it should satisfy

$$r = \left.\frac{\partial e_o(s,P)}{\partial s}\right|_{s^*_{R,P,r}}. \tag{B.167}$$

It is easy to verify that

$$\frac{\partial e_o(s,P)}{\partial s} = -\Lambda_{0,P}\left(\frac{s}{1+s}\right) - \frac{1}{1+s}\Lambda'_{0,P}\left(\frac{s}{1+s}\right), \tag{B.168}$$

Owing to (B.167) and (B.168), we have

$$r = -\Lambda_{0,P}\left(\frac{s^*(R,P,r)}{1+s^*(R,P,r)}\right) - \frac{1}{(1+s^*(R,P,r))}\Lambda'_{0,P}\left(\frac{s^*(R,P,r)}{1+s^*(R,P,r)}\right). \tag{B.169}$$

By noting (recall (3.70))

$$e_o(s^*(R,P,r),P) = -(1+s^*(R,P,r))\Lambda_{0,P}\left(\frac{s^*(R,P,r)}{1+s^*(R,P,r)}\right), \tag{B.170}$$

Lemma 10, Corollary 1, (3.76) and (B.169) imply that

$$\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r) = \frac{s^*(R,P,r)}{1+s^*(R,P,r)}\Lambda'_{0,P}\left(\frac{s^*(R,P,r)}{1+s^*(R,P,r)}\right) - \Lambda_{0,P}\left(\frac{s^*(R,P,r)}{1+s^*(R,P,r)}\right). \tag{B.171}$$

Due to (B.169) and (B.171), we deduce that

$$\Lambda'_{0,P}\left(\frac{s^*(R,P,r)}{1+s^*(R,P,r)}\right) = \tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r) - r. \tag{B.172}$$

Using (3.79), (B.171) and (B.172), it is easy to see that (recall (B.1))

$$\Lambda^*_{0,P}(\tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r) - r) = \tilde{\mathrm{e}}_{\mathrm{SP}}(R,P,r), \tag{B.173}$$

which proves item (i).

Item (ii) immediately follows from (3.58), (3.59), (3.79), (3.80) and the item (i).

In order to see item (iii), first note that $\tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, \cdot)$ is a non-increasing function. Further, it is clear that $\tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, 0) = \mathrm{D}(W^{-}_{R,P} \| W|P)$ and $\tilde{\mathrm{e}}_{\mathrm{SP}}(R, P, \mathrm{D}(W\|W^{-}_{R,P}|P)) = 0$. These observations, along with (3.60), (3.61) and the positive variance lemma, i.e., Lemma 8, suffice to conclude the existence and uniqueness of $\eta(R, P, r) \in (0, 1)$ with the stated property. Finally, recalling (B.172), one can see that $\eta(R, P, r) = \frac{s^*(R,P,r)}{1+s^*(R,P,r)}$. □

APPENDIX C

APPENDICES OF CHAPTER 4

C.1 On ensemble average error probability of BEC below the critical rate

This section points out a small oversight in [36]. In particular, the subexponential prefactor that is given in [36, eq. (18)] is too optimistic for certain channels, including BEC, as we now demonstrate.

Recall that P_1, as given by [36, eq. (16)], can be expressed as

$$P_1 = (M-1)\Pr\left[\sum_{n=1}^{N} \ln \frac{W(Y_n|X_n(m'))}{W(Y_n|X_n(m))} \geq 0\right], \tag{C.1}$$

where the probability measure is

$$Q(\mathbf{x}^N(m))W(\mathbf{y}^N|\mathbf{x}^N(m))Q(\mathbf{x}^N(m')) = \prod_{n=1}^{N} Q(x_n(m))W(y_n|x_n(m))Q(x_n(m')). \tag{C.2}$$

Here Q is an arbitrary probability distribution on the channel input alphabet.

In [36, eq. (18)], it is claimed that[1]

$$P_1 = (M-1)\left\{\sum_y \left[\sum_x Q(x)\sqrt{W(y|x)}\right]^2\right\}^N \left[\frac{g}{\sqrt{N}} + o\left(\frac{1}{\sqrt{N}}\right)\right], \tag{C.3}$$

where g is a constant that is explicitly characterized.

Note that the standard moment-generating function techniques cited in [36] to prove this formula require some regularity conditions on $\ln \frac{W(Y_n|X_n(m'))}{W(Y_n|X_n(m)}$. In particular, the log moment-generating function (also known as semi-invariant moment-generating function) of the random variable $\ln \frac{W(Y_n|X_n(m'))}{W(Y_n|X_n(m)}$ should be finite around a neighborhood of the

[1] By correcting the obvious typo.

origin, as pointed out in [35, Appendix 5A]. This condition will not hold in general if the channel transition matrix has 0 entries.

As a counterexample, consider the BEC with parameter $\epsilon \in (0,1)$, i.e., let the channel input (resp. output) alphabet defined as $\mathcal{X} := \{0,1\}$ (resp. $\mathcal{Y} := \{0,1,E\}$) and

$$W(y|x) := \begin{cases} 1-\epsilon & \text{if } (x,y) \in \{(0,0),(1,1)\}, \\ \epsilon & \text{if } (x,y) \in \{(0,E),(1,E)\}, \\ 0 & \text{else.} \end{cases} \tag{C.4}$$

Let Q be the uniform distribution on $\mathcal{X}$, i.e., $Q(0) = Q(1) = 1/2$. One can check (by using the KKT conditions given by [35, Theorem 5.6.5]) that this choice uniquely attains $\max_Q \mathrm{E}_0(\rho, Q)$ for all $\rho \in \mathbb{R}^+$. Define

$$\mathcal{S} := \{(x,y,x') \in \mathcal{X} \times \mathcal{Y} \times \mathcal{X} : Q(x), Q(x') > 0,\ W(y|x), W(y|x') > 0\}. \tag{C.5}$$

Also, let $\mathcal{S}^N$ denote the N-fold cartesian product of $\mathcal{S}$. One can verify that (C.5) implies

$$\Pr(\mathcal{S}) = \frac{1+\epsilon}{2}, \tag{C.6}$$

where the probability measure is $Q(x)W(y|x)Q(x')$. Under this distribution, $\ln \frac{W(y|x')}{W(y|x)}$ is a binary-valued random variable taking values in $\{-\infty, 0\}$. In particular, we have

$$\Pr\left[\ln \frac{W(Y|X')}{W(Y|X)} = 0\right] = \frac{1+\epsilon}{2}, \quad \Pr\left[\ln \frac{W(Y|X')}{W(Y|X)} = -\infty\right] = \frac{1-\epsilon}{2}. \tag{C.7}$$

This implies that

$$P_1 = (M-1)\Pr\left[\sum_{n=1}^{N} \ln \frac{W(Y_n|X_n(m'))}{W(Y_n|X_n(m))} \geq 0, (\mathbf{X}^N(m), \mathbf{Y}^N, \mathbf{x}^N(m')) \in \mathcal{S}^N\right] \tag{C.8}$$

$$= (M-1)\Pr\left\{\mathcal{S}^N\right\} \tag{C.9}$$

$$= (M-1)\left(\frac{1+\epsilon}{2}\right)^N, \tag{C.10}$$

where (C.9) follows from (C.7) and (C.10) follows from (C.6) because the probability measure under which (C.9) is evaluated is i.i.d.

However, one can directly verify that

$$\sum_{y}\left[\sum_{x} Q(x)\sqrt{W(y|x)}\right]^{2} = \frac{1+\epsilon}{2}, \tag{C.11}$$

which means that (C.10) can be written as

$$P_1 = (M-1)\left\{\sum_{y}\left[\sum_{x} Q(x)\sqrt{W(y|x)}\right]^{2}\right\}^{N}. \tag{C.12}$$

Note that the right side of (C.12) is greater than the right side of (C.3) for sufficiently large N. Since the arguments leading to [36, eq. (25)] are still valid, one can check that (recall that our choice of Q maximizes $\mathrm{E_o}(1, Q)$) (C.12) implies

$$(1 - O(e^{-N}))e^{-N\mathrm{E_r}(R)} \leq \bar{P}_{e,m} \leq e^{-N\mathrm{E_r}(R)}, \quad R < R_{\mathrm{cr}}. \tag{C.13}$$

This shows that the $O\left(1/\sqrt{N}\right)$ pre-factor in [36, eq. (18)], which is claimed to hold for all channels ([36, eq. (28)]), does not hold for BEC.

C.2 Proof of Lemma 14

Throughout this section, fix an arbitrary $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ such that $\mathrm{V} > 0$ and $Q \in \mathcal{P}(\mathcal{X})$ such that $\mathrm{E_r}(R, Q) > 0$ for some $R > R_\infty$.

(i) Since $\mathrm{E_r}(R, Q) \in \mathbb{R}^+$, one can see that $R \in (0, \mathrm{I}(Q; W))$. This observation enables us to invoke [35, Theorem 5.6.3], which, in turn, ensures that

$$\frac{\partial^2 \mathrm{E_o}(\rho, Q)}{\partial \rho^2} \leq 0, \tag{C.14}$$

for all $\rho \in \mathbb{R}_+$. Moreover, [35, Theorem 5.6.3] also guarantees that if (C.14) holds with equality for some $\rho \in \mathbb{R}_+$, then the same should be true for all $\rho \in \mathbb{R}_+$. For contradiction, assume (C.14) holds with equality for some $\rho \in \mathbb{R}_+$, which, in turn, implies that $\frac{\partial \mathrm{E_o}(\rho,Q)}{\partial \rho} = \mathrm{I}(Q;W)$. Since $\mathrm{E_o}(0,Q) = 0$, we have

$$\mathrm{E_o}(\rho, Q) = \rho \mathrm{I}(Q;W). \tag{C.15}$$

To conclude the proof, consider

$$\mathrm{E_{SP}}(R, Q) := \sup_{\rho \geq 0} \{-\rho R + \mathrm{E_o}(\rho, Q)\}, \tag{C.16}$$

and notice that plugging (C.15) into (C.16) yields $\mathrm{E_{SP}}(R,Q) = \infty$, which contradicts $R > R_\infty$.

(ii) We only need to prove (4.28), since the rest directly follows from item (i). To this end, fix some $r \in \left(\frac{\partial \mathrm{E_o}(\rho,Q)}{\partial \rho}\Big|_{\rho=1}, \mathrm{I}(Q;W) \right)$ and consider

$$\mathrm{E_r}(r, Q) = \max_{\rho \in [0,1]} \{-\rho r + \mathrm{E_o}(\rho, Q)\}. \tag{C.17}$$

Using the the characterization of the subdifferential of the maximum function (e.g., [56, Theorem 2.87]), we have

$$\partial \mathrm{E_r}(\cdot, Q)(r) = \mathrm{conv}\left(\{-\rho : \mathrm{E_r}(r,Q) = -\rho r + \mathrm{E_o}(\rho, Q)\}\right). \tag{C.18}$$

Thanks to item (i) of this lemma and the fact that $r \in \left(\frac{\partial \mathrm{E_o}(\rho,Q)}{\partial \rho}\Big|_{\rho=1}, \mathrm{I}(Q;W) \right)$, (C.17) has a unique maximizer, which is $\rho_R^*(Q)$, because of (4.27). Therefore, (C.18) reduces to

$$\partial \mathrm{E_r}(\cdot, Q)(r) = \{-\rho_R^*(Q)\}, \tag{C.19}$$

which, in turn, implies (4.28). □

C.3 Auxiliary results

This section contains some auxiliary results that will be used in the proof Theorem 4. Throughout the section, fix an arbitrary $W \in \mathcal{P}(\mathcal{Y}|\mathcal{X})$ such that $\mathrm{V} > 0$ and $Q \in \mathcal{P}(\mathcal{X})$ such that $\mathrm{E_r}(R, Q) > 0$ for some $R > R_\infty$. Fix some[2] $r \in \left(-\left.\frac{\partial \mathrm{E_o}(\rho,Q)}{\partial \rho}\right|_{\rho=1}, \mathrm{I}(Q;W)\right)$. Let $\rho_r^*(Q) := -\left.\frac{\partial \mathrm{E_r}(a,Q)}{\partial a}\right|_{a=r}$, which is well-defined due to (4.28), and note that $\rho_r^*(Q) \in (0,1)$, because of item (ii) of Lemma 14.

Definition 12. *(i) For any $y \in \mathcal{Y}$ and $\rho \in \mathbb{R}_+$,*

$$P_Y^\rho(y) := \frac{\left[\sum_{x\in\mathcal{X}} Q(x)W(y|x)^{1/(1+\rho)}\right]^{1+\rho}}{\sum_{b\in\mathcal{Y}}\left[\sum_{a\in\mathcal{X}} Q(a)W(b|a)^{1/(1+\rho)}\right]^{1+\rho}}. \tag{C.20}$$

Observe that P_Y^ρ is a well-defined probability measure on $\mathcal{Y}$, for any $\rho \in \mathbb{R}_+$. For the sake of notational convenience, we define $f_r^* := P_Y^{\rho_r^*(Q)}$.

(ii) For any $\rho \in \mathbb{R}_+$,

$$P_{X|Y}^\rho(x|y) := \begin{cases} \frac{Q(x)W(y|x)^{1/(1+\rho)}}{\sum_{a\in\mathcal{X}} Q(a)W(y|a)^{1/(1+\rho)}} & \text{if } y \in \mathcal{S}(P_Y^\rho), \\ 0 & \text{else.} \end{cases} \tag{C.21}$$

Note that $P_{X|Y}^\rho$ is a well-defined conditional probability measure for all $\rho \in \mathbb{R}_+$.

(iii) For any $(x,y) \in \mathcal{X}\times\mathcal{Y}$ and $\rho \in \mathbb{R}_+$

$$P_{X,Y}^\rho(x,y) := P_{X|Y}^\rho(x|y)P_Y^\rho(y). \tag{C.22}$$

For the sake of notational convenience, we let $P_{X,Y}^0(x,y) =: P_{X,Y}(x,y) = Q(x)W(y|x)$, for any $(x,y) \in \mathcal{X}\times\mathcal{Y}$.

(iv)

$$E_F(r,Q) := D\left(P_{X,Y}^{\rho_r^*(Q)} \| Q\times W\right) = \sum_{x,y} P_{X,Y}^{\rho_r^*(Q)}(x,y) \ln \frac{P_{X,Y}^{\rho_r^*(Q)}(x,y)}{Q(x)W(y|x)}. \tag{C.23}$$

[2]The non-emptiness of the following interval is ensured by item (i) of Lemma 14.

(v) For any $\lambda \in \mathbb{R}$,

$$\Lambda_r(\lambda) := \ln E_{P_{X,Y}}\left[e^{\lambda \ln \frac{f_r^*(Y)}{W(Y|X)}}\right]. \tag{C.24}$$

◊

Lemma 32.

$$\frac{\partial E_o(\rho, Q)}{\partial \rho} = \sum_{x,y} P^{\rho}_{X,Y}(x,y) \ln \frac{P^{\rho}_{X|Y}(x|y)}{Q(x)}, \tag{C.25}$$

for all $\rho \in \mathbb{R}_+$. ♦

Proof. Define $h_y(\rho, Q) := \sum_x Q(x)W(y|x)^{1/(1+\rho)}$ and $g_y(\rho, Q) := h_y(\rho, Q)^{1+\rho}$. From the definition of $\mathrm{E_o}(\cdot,\cdot)$

$$\frac{\partial \mathrm{E_o}(\rho, Q,)}{\partial \rho} = -\frac{\sum_y \frac{\partial g_y(\rho,Q)}{\partial \rho}}{\sum_b g_b(\rho, Q)}. \tag{C.26}$$

Note that if $\mathcal{S}(Q) \cap \mathcal{X}_y = \emptyset$, then $h_y(\rho, Q) = g_y(\rho, Q) = 0$, for all $\rho \in \mathbb{R}_+$. Also, observe that there exists $y \in \mathcal{Y}$, such that $\mathcal{S}(Q) \cap \mathcal{X}_y \neq \emptyset$. Further, one can check that provided that $\mathcal{S}(Q) \cap \mathcal{X}_y \neq \emptyset$,

$$\frac{\partial h_y(\rho, Q)}{\partial \rho} = -\frac{1}{(1+\rho)^2} \sum_x Q(x)W(y|x)^{1/(1+\rho)} \ln W(y|x), \tag{C.27}$$

$$\frac{\partial g_y(\rho, Q)}{\partial \rho} = g_y(\rho, Q)\left[(1+\rho)\frac{\frac{\partial h_y(\rho,Q)}{\partial \rho}}{h_y(\rho, Q)} + \ln h_y(\rho, Q)\right]. \tag{C.28}$$

Equations (C.26) and (C.28) imply that

$$\frac{\partial \mathrm{E_o}(\rho, Q)}{\partial \rho} = -\sum_{y:\mathcal{X}_y \cap \mathcal{S}(Q) \neq \emptyset} \frac{g_y(\rho, Q)}{\sum_a g_a(\rho, Q)}\left[(1+\rho)\frac{\frac{\partial h_y(\rho,Q)}{\partial \rho}}{h_y(\rho, Q)} + \ln h_y(\rho, Q)\right] \tag{C.29}$$

$$= -\sum_{y:\mathcal{X}_y \cap \mathcal{S}(Q) \neq \emptyset} P^{\rho}_Y(y)\left[(1+\rho)\frac{\frac{\partial h_y(\rho,Q)}{\partial \rho}}{h_y(\rho, Q)} + \ln h_y(\rho, Q)\right], \tag{C.30}$$

where (C.30) follows from the definition of P^{ρ}_Y, i.e., (C.20). Consider any y with $\mathcal{X}_y \cap$

$\mathcal{S}(Q) \neq \emptyset$. We have

$$(1+\rho)\frac{\frac{\partial h_y(\rho,Q)}{\partial \rho}}{h_y(\rho,Q)} + \ln h_y(\rho,Q) = \sum_x \frac{Q(x)W(y|x)^{1/(1+\rho)}}{\sum_a Q(a)W(y|a)^{1/(1+\rho)}} \ln \frac{1}{W(y|x)^{\frac{1}{1+\rho}}} + \ln \sum_z Q(z)W(y|z)^{1/(1+\rho)} \tag{C.31}$$

$$= \sum_x P^{\rho}_{X|Y}(x|y) \ln \sum_z Q(z)W(y|z)^{\frac{1}{1+\rho}} + \sum_x P^{\rho}_{X|Y}(x|y) \ln \frac{1}{W(y|x)^{\frac{1}{1+\rho}}} \tag{C.32}$$

$$= \sum_x P^{\rho}_{X|Y}(x|y) \ln \frac{Q(x)}{P^{\rho}_{X|Y}(x|y)}, \tag{C.33}$$

where (C.31) follows from (C.27), (C.32) and (C.33) follow from the definition of $P^{\rho}_{X|Y}$, i.e., (C.21). Plugging (C.33) into (C.30) and and remembering the definition of $P^{\rho}_{X,Y}$, i.e., (C.22), we conclude that (C.25) holds. □

Lemma 33.

$$E_F(r,Q) = E_r(r,Q). \tag{C.34}$$

♦

Proof. Observe that owing to the definitions of $P^{\rho}_{X|Y}$ and $P^{\rho}_{X,Y}$, i.e., (C.21) and (C.22), along with the definition of $\mathrm{E}_F(r,Q)$, i.e., (C.23), we have

$$\mathrm{E_F}(r,Q) = \sum_{(x,y)\in\mathcal{S}_{Q,W}} P^{\rho^*_r(Q)}_{X,Y}(x,y) \ln \frac{P^{\rho^*_r(Q)}_{Y}(y)}{W(y|x)^{\frac{\rho^*_r(Q)}{1+\rho^*_r(Q)}} \left[\sum_a Q(a)W(y|a)^{\frac{1}{1+\rho^*_r(Q)}}\right]}. \tag{C.35}$$

Moreover,

$$\mathrm{E_r}(r, Q) = -r\rho_r^*(Q) + \mathrm{E_o}(\rho_r^*(Q), Q) \tag{C.36}$$

$$= -\rho_r^*(Q) \sum_{(x,y)\in\mathcal{S}_{Q,W}} P_{X,Y}^{\rho_r^*(Q)}(x,y) \ln \frac{P_{X|Y}^{\rho_r^*(Q)}(x|y)}{Q(x)} + \mathrm{E_o}(\rho_r^*(Q), Q) \tag{C.37}$$

$$= \sum_{(x,y)\in\mathcal{S}_{Q,W}} P_{X,Y}^{\rho_r^*(Q)}(x,y) \ln \frac{\left(\sum_{z\in\mathcal{X}} Q(z)W(y|z)^{\frac{1}{1+\rho_r^*(Q)}}\right)^{\rho_r^*(Q)}}{W(y|x)^{\frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}}\left[\sum_{b\in\mathcal{Y}}\left(\sum_{a\in\mathcal{X}} Q(a)W(b|a)^{\frac{1}{1+\rho_r^*(Q)}}\right)^{1+\rho_r^*(Q)}\right]} \tag{C.38}$$

$$= \sum_{(x,y)\in\mathcal{S}_{Q,W}} P_{X,Y}^{\rho_r^*(Q)}(x,y) \ln \frac{P_Y^{\rho_r^*(Q)}(y)}{W(y|x)^{\frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}}\left[\sum_{a\in\mathcal{X}} Q(a)W(y|a)^{\frac{1}{1+\rho_r^*(Q)}}\right]}, \tag{C.39}$$

where (C.36) follows from item (i) of Lemma 14 and (4.27), (C.37) follows from (C.25), (C.38) follows from the definition of $\mathrm{E_o}(\rho, Q)$, i.e., (1.11), and the definition of $P_{X|Y}^{\rho}$, i.e., (C.21), and (C.39) follows from the definition of P_Y^{ρ}, i.e., (C.20). Equations (C.35) and (C.39) together imply (C.34). □

Lemma 34.

$$\Lambda_r\left(\frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}\right) = \frac{1}{1+\rho_r^*(Q)} \ln \sum_y \left[\sum_x Q(x)W(y|x)^{\frac{1}{1+\rho_r^*(Q)}}\right]^{1+\rho_r^*(Q)}. \tag{C.40}$$

$$\Lambda_r'\left(\frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}\right) = \sum_{(x,y)\in\mathcal{S}_{Q,W}} P_{X,Y}^{\rho_r^*(Q)}(x,y) \ln \frac{f_r^*(y)}{W(y|x)}. \tag{C.41}$$

$$E_F(r, Q) = \frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}\Lambda_r'\left(\frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}\right) - \Lambda_r\left(\frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}\right). \tag{C.42}$$

$$r = -\frac{1}{1+\rho_r^*(Q)}\Lambda_r'\left(\frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}\right) - \Lambda_r\left(\frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}\right). \tag{C.43}$$

♦

Proof.

$$\Lambda_r\left(\frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}\right) = \ln \sum_{(x,y)\in\mathcal{S}_{Q,W}} Q(x)W(y|x)^{\frac{1}{1+\rho_r^*(Q)}} \left[\frac{\left(\sum_z Q(z)W(y|z)^{\frac{1}{1+\rho_r^*(Q)}}\right)^{1+\rho_r^*(Q)}}{\sum_b \left(\sum_a Q(a)W(b|a)^{\frac{1}{1+\rho_r^*(Q)}}\right)^{1+\rho_r^*(Q)}}\right]^{\frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}} \tag{C.44}$$

$$= \frac{1}{1+\rho_r^*(Q)} \ln \sum_y \left(\sum_x Q(x)W(y|x)^{\frac{1}{1+\rho_r^*(Q)}}\right)^{1+\rho_r^*(Q)}, \tag{C.45}$$

where (C.44) follows from the definition of P_Y^ρ, i.e., (C.20).

Next, one can check that

$$\Lambda_r'\left(\frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}\right) = \sum_{(x,y)\in\mathcal{S}_{Q,W}} \frac{Q(x)W(y|x)^{\frac{1}{1+\rho_r^*(Q)}} f_r^*(y)^{\frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}}}{\sum_{(a,b)\in\mathcal{S}_{Q,W}} Q(a)W(b|a)^{\frac{1}{1+\rho_r^*(Q)}} f_r^*(b)^{\frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}}} \ln \frac{f_r^*(y)}{W(y|x)}. \tag{C.46}$$

By recalling the definition of P_Y^ρ, i.e., (C.20), for any $(x,y) \in \mathcal{S}_{Q,W}$, we have

$$\frac{Q(x)W(y|x)^{\frac{1}{1+\rho_r^*(Q)}} f_r^*(y)^{\frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}}}{\sum_{(a,b)\in\mathcal{S}_{Q,W}} Q(a)W(b|a)^{\frac{1}{1+\rho_r^*(Q)}} f_r^*(b)^{\frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}}} = \frac{Q(x)W(y|x)^{\frac{1}{1+\rho_r^*(Q)}} \left[\sum_z Q(z)W(y|z)^{\frac{1}{1+\rho_r^*(Q)}}\right]^{\rho_r^*(Q)}}{\sum_b \left[\sum_a Q(a)W(b|a)^{\frac{1}{1+\rho_r^*(Q)}}\right]^{1+\rho_r^*(Q)}} \tag{C.47}$$

$$= P_{X|Y}^{\rho_r^*(Q)}(x|y) P_Y^{\rho_r^*(Q)}(y) \tag{C.48}$$

$$= P_{X,Y}^{\rho_r^*(Q,W)}(x,y), \tag{C.49}$$

where (C.48) follows from the definitions of P_Y^ρ and $P_{X|Y}^\rho$, i.e., (C.20) and (C.21), (C.49) follows from the definition of $P_{X,Y}^\rho$, i.e., (C.22). Plugging (C.49) into (C.46) implies (C.41).

From the definition of $\mathrm{E_F}(r,Q)$, i.e., (C.23), and the definition of P_Y^ρ, i.e., (C.20), we have

$$\mathrm{E_F}(r,Q) = \sum_{(x,y)\in\mathcal{S}_{Q,W}} P_{X,Y}^{\rho_r^*(Q)}(x,y)\ln\frac{P_Y^{\rho_r^*(Q)}(y)}{W(y|x)} + \sum_{(x,y)\in\mathcal{S}_{Q,W}} P_{X,Y}^{\rho_r^*(Q)}(x,y)\ln\frac{P_{X|Y}^{\rho_r^*(Q)}(x|y)}{Q(x)} \tag{C.50}$$

$$= \Lambda'\left(\frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}\right) + \sum_{(x,y)\in\mathcal{S}_{Q,W}} P_{X,Y}^{\rho_r^*(Q)}\ln\frac{W(y|x)^{\frac{1}{1+\rho_r^*(Q)}}}{\sum_z Q(z)W(y|z)^{\frac{1}{1+\rho_r^*(Q)}}} \tag{C.51}$$

$$= \frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}\Lambda_r'\left(\frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}\right) + \sum_{(x,y)\in\mathcal{S}_{Q,W}} P_{X,Y}^{\rho_r^*(Q)}\ln\frac{f_r^*(y)^{1/(1+\rho_r^*(Q))}}{\sum_z Q(z)W(y|z)^{\frac{1}{1+\rho_r^*(Q)}}} \tag{C.52}$$

$$= \frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}\Lambda_r'\left(\frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}\right) + \sum_{(x,y)\in\mathcal{S}_{Q,W}} P_{X,Y}^{\rho_r^*(Q)}\ln\frac{1}{\left[\sum_b\left(\sum_a Q(a)W(b|a)^{\frac{1}{1+\rho_r^*(Q)}}\right)^{(1+\rho_r^*(Q))}\right]^{\frac{1}{1+\rho_r^*(Q)}}} \tag{C.53}$$

$$= \frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}\Lambda_r'\left(\frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}\right) - \Lambda_r\left(\frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}\right), \tag{C.54}$$

where (C.51) and (C.52) follow from (C.41), (C.53) follows from the definition of P_Y^{ρ}, i.e., (C.20), and (C.54) follows from (C.40).

Lastly, the fact that $\left.\frac{\partial \mathrm{E_o}(\rho,Q)}{\partial\rho}\right|_{\rho=\rho_r^*(Q)} = r$, which is established in (4.27), along with Lemma 32, implies that

$$r = \sum_{(x,y)\in\mathcal{S}_{Q,W}} P_{X,Y}^{\rho_r^*(Q)}(x,y)\ln\frac{P_{X|Y}^{\rho_r^*(Q)}(x|y)}{Q(x)} \tag{C.55}$$

$$= \sum_{(x,y)\in\mathcal{S}_{Q,W}} P_{X,Y}^{\rho_r^*(Q)}(x,y)\ln\frac{P_{X,Y}^{\rho_r^*(Q)}(x,y)}{Q(x)W(y|x)} + \sum_{(x,y)\in\mathcal{S}_{Q,W}} P_{X,Y}^{\rho_r^*(Q)}(x,y)\ln\frac{W(y|x)}{P_Y^{\rho_r^*(Q)}(y)} \tag{C.56}$$

$$= \mathrm{E_F}(r,Q) - \Lambda_r'\left(\frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}\right) \tag{C.57}$$

$$= -\frac{1}{1+\rho_r^*(Q)}\Lambda_r'\left(\frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}\right) - \Lambda_r\left(\frac{\rho_r^*(Q)}{1+\rho_r^*(Q)}\right), \tag{C.58}$$

where (C.57) follows from the definition of $\mathrm{E_F}(r,Q)$, i.e., (C.23), (C.25) and (C.41), and (C.58) follows from (C.42). □

C.4 Proof of Lemma 15

(i) By elementary calculation,

$$\frac{\partial \Lambda_{1,\rho}(\mathbf{v}_1, \mathbf{v}_2)}{\partial \mathbf{v}_2} = \sum_{(x,y,z)\in\tilde{\mathcal{S}}_Q} \frac{Q(x)W(y|x)^{1+\mathbf{v}_1-\mathbf{v}_2} f_\rho(y)^{-\mathbf{v}_1} Q(z)W(y|z)^{\mathbf{v}_2}}{\sum_{(a,b,c)\in\tilde{\mathcal{S}}_Q} Q(a)W(b|a)^{1+\mathbf{v}_1-\mathbf{v}_2} f_\rho(b)^{-\mathbf{v}_1} Q(c)W(b|c)^{\mathbf{v}_2}} \ln \frac{W(y|z)}{W(y|x)}, \tag{C.59}$$

and

$$\frac{\partial \Lambda_{1,\rho}(\mathbf{v}_1, \mathbf{v}_2)}{\partial \mathbf{v}_1} = \sum_{(x,y,z)\in\tilde{\mathcal{S}}_Q} \frac{Q(x)W(y|x)^{1+\mathbf{v}_1-\mathbf{v}_2} f_\rho(y)^{-\mathbf{v}_1} Q(z)W(y|z)^{\mathbf{v}_2}}{\sum_{(a,b,c)\in\tilde{\mathcal{S}}_Q} Q(a)W(b|a)^{1+\mathbf{v}_1-\mathbf{v}_2} f_\rho(b)^{-\mathbf{v}_1} Q(c)W(b|c)^{\mathbf{v}_2}} \ln \frac{W(y|x)}{f_\rho(y)}. \tag{C.60}$$

Evaluating the right side of (C.59) at $\tilde{\mathbf{v}}$ yields[3]

$$\left.\frac{\partial \Lambda_{1,\rho}(\tilde{\mathbf{v}}_1, \mathbf{v}_2)}{\partial \mathbf{v}_2}\right|_{\mathbf{v}_2=\tilde{\mathbf{v}}_2} = 0, \tag{C.61}$$

owing to the symmetry of the resulting expression.

Equation (C.60) further implies that

$$\frac{\partial \Lambda_{1,\rho}(\mathbf{v}_1, \mathbf{v}_2)}{\partial \mathbf{v}_1} = \sum_{(x,y)\in\mathcal{S}_Q} \frac{Q(x)W(y|x)^{1+\mathbf{v}_1-\mathbf{v}_2} f_\rho(y)^{-\mathbf{v}_1} \left[\sum_{z\in\mathcal{S}(Q)\cap\mathcal{X}_y} Q(z)W(y|z)^{\mathbf{v}_2}\right]}{\sum_{(a,b)\in\mathcal{S}_Q} Q(a)W(b|a)^{1+\mathbf{v}_1-\mathbf{v}_2} f_\rho(b)^{-\mathbf{v}_1} \left[\sum_{c\in\mathcal{S}(Q)\cap\mathcal{X}_b} Q(c)W(b|c)^{\mathbf{v}_2}\right]} \ln \frac{W(y|x)}{f_\rho(y)}. \tag{C.62}$$

Evaluating the right side of (C.62) at $\tilde{\mathbf{v}}$ yields

$$\left.\frac{\partial \Lambda_{1,\rho}(\mathbf{v}_1, \tilde{\mathbf{v}}_2)}{\partial \mathbf{v}_1}\right|_{\mathbf{v}_1=\tilde{\mathbf{v}}_1} = \sum_{(x,y)\in\mathcal{S}_Q} \frac{Q(x)W(y|x)^{\tilde{\mathbf{v}}_2} f_\rho(y)^{1-2\tilde{\mathbf{v}}_2} \left[\sum_{z\in\mathcal{S}(Q)\cap\mathcal{X}_y} Q(z)W(y|z)^{\tilde{\mathbf{v}}_2}\right]}{\sum_{(a,b)\in\mathcal{S}_Q} Q(a)W(b|a)^{\tilde{\mathbf{v}}_2} f_\rho(b)^{1-2\tilde{\mathbf{v}}_2} \left[\sum_{c\in\mathcal{S}(Q)\cap\mathcal{X}_b} Q(c)W(b|c)^{\tilde{\mathbf{v}}_2}\right]} \ln \frac{W(y|x)}{f_\rho(y)}. \tag{C.63}$$

[3]Note that the particular value of $\tilde{\mathbf{v}}_2$ does not matter as long as one has $\tilde{\mathbf{v}}_1 = -1 + 2\tilde{\mathbf{v}}_2$.

Note that for any $y \in \mathcal{Y}$, such that $\mathcal{X}_y \cap \mathcal{S}(Q) \neq \emptyset$, we have

$$\left[\left(\sum_x Q(x)W(y|x)^{1/(1+\rho)}\right)^{1+\rho}\right]^{-\tilde{\mathbf{v}}_2} = \frac{1}{\sum_x Q(x)W(y|x)^{1/(1+\rho)}}. \tag{C.64}$$

By plugging (C.64) into (C.63), along with the definition of f_ρ and (C.41) in Appendix C.3, we conclude that

$$\left.\frac{\partial \Lambda_{1,\rho}(\mathbf{v}_1, \tilde{\mathbf{v}}_2)}{\partial \mathbf{v}_1}\right|_{\mathbf{v}_1 = \tilde{\mathbf{v}}_1} = -\Lambda_\rho'\left(\frac{\rho}{1+\rho}\right). \tag{C.65}$$

Equations (C.61) and (C.65) together imply (4.41).

(ii) Note that

$$\Lambda_{1,\rho}(\tilde{\mathbf{v}}) = \ln \sum_{(x,y,z)\in\tilde{\mathcal{S}}_Q} \tilde{P}_{X,Y,Z}(x,y,z)\left(\frac{W(y|x)}{f_\rho(y)}\right)^{\tilde{\mathbf{v}}_1}\left(\frac{W(y|z)}{W(y|x)}\right)^{\tilde{\mathbf{v}}_2} \tag{C.66}$$

$$= -\ln P_{X,Y,Z}\left\{\tilde{\mathcal{S}}_Q\right\} + \nu_{\tilde{\mathbf{v}}}, \tag{C.67}$$

where we define

$$\nu_{\tilde{\mathbf{v}}} := \ln \sum_{(x,y,z)\in\tilde{\mathcal{S}}_Q} Q(x)W(y|x)^{\tilde{\mathbf{v}}_2} Q(z)W(y|z)^{\tilde{\mathbf{v}}_2} f_\rho(y)^{-\tilde{\mathbf{v}}_1}. \tag{C.68}$$

Observe that for any $y \in \mathcal{Y}$ such that $\mathcal{X}_y \cap \mathcal{S}(Q) \neq \emptyset$, we have

$$f_\rho(y)^{-\tilde{\mathbf{v}}_1} = \frac{f_\rho(y)^{\rho/(1+\rho)}}{\sum_x Q(x)W(y|x)^{1/(1+\rho)}}\left[\sum_b\left(\sum_a Q(a)W(b|a)^{1/(1+\rho)}\right)^{1+\rho}\right]^{1/(1+\rho)}, \tag{C.69}$$

owing to the definitions of f_ρ and $\tilde{\mathbf{v}}$. Rearranging (C.69) gives

$$\sum_z Q(z)W(y|z)^{1/(1+\rho)} f_\rho(y)^{-\tilde{\mathbf{v}}_1} = f_\rho(y)^{\rho/(1+\rho)}\left[\sum_b\left(\sum_a Q(a)W(b|a)^{1/(1+\rho)}\right)^{1+\rho}\right]^{1/(1+\rho)}, \tag{C.70}$$

provided that $y \in \mathcal{Y}$ satisfies $\mathcal{X}_y \cap \mathcal{S}(Q) \neq \emptyset$. By plugging (C.70) into (C.68) and

noting the definition of $\tilde{\mathbf{v}}$, we deduce that

$$\nu_{\tilde{\mathbf{v}}} = \ln \sum_{(x,y)\in\mathcal{S}_Q} Q(x)W(y|x)^{1/(1+\rho)} f_\rho(y)^{\rho/(1+\rho)} \left[\sum_b \left(\sum_a Q(a)W(b|a)^{1/(1+\rho)}\right)^{1+\rho}\right]^{1/(1+\rho)} \tag{C.71}$$

$$= \Lambda_\rho\left(\frac{\rho}{1+\rho}\right) + \frac{\ln \sum_y \left[\sum_x Q(x)W(y|x)^{1/(1+\rho)}\right]^{1+\rho}}{(1+\rho)} \tag{C.72}$$

$$= 2\Lambda_\rho\left(\frac{\rho}{1+\rho}\right), \tag{C.73}$$

where (C.72) follows from the definition of $\Lambda_\rho(\cdot)$ and (C.73) follows from (C.40). Plugging (C.73) into (C.67) yields (4.42). □

C.5 Proof of Lemma 19

We first claim that

$$\mathrm{Var}_{\tilde{Q}^{\tilde{\mathbf{v}},\rho}_{X,Y,Z}}\left[\ln \frac{W(Y|X)}{f_\rho}\right], \mathrm{Var}_{\tilde{Q}^{\tilde{\mathbf{v}},\rho}_{X,Y,Z}}\left[\ln \frac{W(Y|Z)}{W(Y|X)}\right] \in \mathbb{R}^+. \tag{C.74}$$

To see (C.74), note that

$$\left[\mathrm{Var}_{\tilde{Q}^{\tilde{\mathbf{v}},\rho}_{X,Y,Z}}\left[\ln \frac{W(Y|X)}{f_\rho(Y)}\right] = 0\right] \iff \left[\ln \frac{W(y|x)}{f_\rho(y)} = -\Lambda'_\rho\left(\frac{\rho}{1+\rho}\right),\ \forall (x,y)\in\mathcal{S}_Q\right] \tag{C.75}$$

$$\implies [(Q,W) \text{ pair is singular}]. \tag{C.76}$$

Evidently, the right side of (C.76) yields a contradiction, and hence we conclude that $\mathrm{Var}_{\tilde{Q}^{\tilde{\mathbf{v}},\rho}_{X,Y,Z}}\left[\ln \frac{W(Y|X)}{f_\rho(Y)}\right] \in \mathbb{R}^+$.

Similarly,

$$\left[\mathrm{Var}_{\tilde{Q}^{\tilde{\mathbf{v}},\rho}_{X,Y,Z}}\left[\ln \frac{W(Y|Z)}{W(Y|X)}\right] = 0\right] \iff \left[\ln \frac{W(y|z)}{W(y|x)} = 0,\ \forall (x,y,z)\in\tilde{\mathcal{S}}_Q\right] \tag{C.77}$$

$$\implies [(Q,W) \text{ pair is singular}]. \tag{C.78}$$

Evidently, the right side of (C.78) yields a contradiction, and hence we conclude that $\mathrm{Var}_{\tilde{Q}^{\tilde{\mathbf{v}},\rho}_{X,Y,Z}}\left[\ln \frac{W(Y|Z)}{W(Y|X)}\right] > 0$.

Further, as an immediate consequence of the nonsingularity of the pair (Q, W), there is no $\alpha \in \mathbb{R}$ satisfying

$$\ln \frac{W(y|z)}{W(y|x)} = \alpha\left(\ln \frac{W(y|x)}{f_\rho(y)} + \Lambda'_\rho\left(\frac{\rho}{1+\rho}\right)\right),\ \forall (x,y,z) \in \tilde{\mathcal{S}}_Q. \tag{C.79}$$

This last observation, coupled with (C.74) and the Cauchy-Schwarz inequality, implies (4.104). □

C.6 Proof of Lemma 20

The proof follows from essentially the same arguments as in one dimensional case given in Appendix B.1. The only significant difference is the usage of a "concentration function" theorem for sums of independent random vectors by Esseen [26, Theorem 6.2], instead of the Berry-Esseen theorem.

For notational convenience, we define

$$\mathbf{A}_n(N) := \left[\ln \frac{W(Y_n|X_n)}{f^*_N(Y_n)},\ \ln \frac{W(Y_n|Z_n)}{W(Y_n|X_n)}\right]^T, \quad \mathbf{S}_N := \frac{1}{N}\sum_{n=1}^{N} \mathbf{A}_n(N), \tag{C.80}$$

and let μ_N denote the law of $\mathbf{S}_N$ when $\mathbf{A}_n(N)$ is distributed according to $\tilde{P}_{X,Y,Z}$. Clearly, $\tilde{\alpha}_N = \mu_N(\mathcal{B}(N))$.

Define $\mathbf{T}_n(N) := \mathbf{A}_n(N) - \mathbf{b}(N)$ and $\mathbf{W}_N := \frac{1}{\sqrt{N}}\sum_{n=1}^{N} \mathbf{T}_n(N)$. Note that

$$\begin{aligned}
&\mathrm{E}_{\tilde{Q}^{\mathbf{v}^*(N)}_{X,Y,Z}}\left[\left[\ln \frac{W(Y|X)}{f^*_N(Y)}, \ln \frac{W(Y|Z)}{W(Y|X)}\right]^T\right] \\
&= \left[\left.\frac{\partial \Lambda_{1,N}(\mathbf{v}_1, \mathbf{v}^*_2(N))}{\partial \mathbf{v}_1}\right|_{\mathbf{v}_1=\mathbf{v}^*_1(N)}, \left.\frac{\partial \Lambda_{1,N}(\mathbf{v}^*_1(N), \mathbf{v}_2)}{\partial \mathbf{v}_2}\right|_{\mathbf{v}_2=\mathbf{v}^*_2(N)}\right]^T \qquad \text{(C.81)} \\
&= [-\Lambda'_N(\rho^*_N/(1+\rho^*_N)), 0]^T, \qquad \text{(C.82)}
\end{aligned}$$

where (C.81) follows by evaluating the right sides of (C.59) and (C.60) in Appendix C.4 at $\mathbf{v}^*(N)$ and (C.82) follows from item (i) of Lemma 15. Equation (C.82) ensures that $\mathrm{E}_{\tilde{Q}^{\mathbf{v}^*(N)}_{X,Y,Z}}[\mathbf{T}_n(N)] = \mathbf{0}$.

By elementary calculation, one can check that

$$\mu_N(\mathcal{B}(N)) = e^{-N\Lambda^*_{1,N}(\mathbf{b}(N))} \int_0^\infty \int_0^\infty e^{-\sqrt{N}\langle \mathbf{v}^*(N),\mathbf{x}\rangle} dF_N(\mathbf{x}), \tag{C.83}$$

where F_N is the distribution of $\mathbf{W}_N$ when $\mathbf{A}_n(N)$ are i.i.d. with $\tilde{Q}^{\mathbf{v}^*(N)}_{X,Y,Z}$.

Since $e^{-\sqrt{N}\langle \mathbf{v},\mathbf{x}\rangle}$ is a continuous function of bounded variation and $F_N(\mathbf{x})$ is a function of bounded variation, we apply the integration by parts formula of Young [73, Eq. 4] to deduce that

$$\begin{aligned}\int_0^\infty \int_0^\infty e^{-\sqrt{N}\langle \mathbf{v}^*(N),\mathbf{x}\rangle} dF_N(\mathbf{x}) = \int_0^\infty \int_0^\infty e^{-\langle \mathbf{1},\mathbf{t}\rangle} \Bigg[& F_N\left(\frac{t_1}{\mathbf{v}^*_1(N)\sqrt{N}}, \frac{t_2}{\mathbf{v}^*_2(N)\sqrt{N}}\right) + F_n(0,0) \\ & - F_N\left(0, \frac{t_2}{\mathbf{v}^*_2(N)\sqrt{N}}\right) - F_N\left(\frac{t_1}{\mathbf{v}^*_1(N)\sqrt{N}}, 0\right)\Bigg] dt_1 dt_2 \end{aligned} \tag{C.84}$$

$$\begin{aligned} = \int_0^\infty \int_0^\infty & e^{-\langle \mathbf{1},\mathbf{t}\rangle} \\ & \Pr\left\{\mathbf{W}_N \in \left(0, \frac{t_1}{\mathbf{v}^*_1(N)\sqrt{N}}\right] \times \left(0, \frac{t_2}{\mathbf{v}^*_2(N)\sqrt{N}}\right]\right\} dt_1 dt_2, \end{aligned} \tag{C.85}$$

where the probability is computed when $A_n(N)$ are i.i.d. with $\tilde{Q}^{\mathbf{v}^*(N)}_{X,Y,Z}$.

In order to conclude the proof, we upper bound the right side of (C.85) by using a concentration inequality of Esseen [26, Corollary to Theorem 6.2]. To state his result, we need the following definitions.

Let $\mathbf{T}^s_n(N) := \mathbf{T}_n(N) - \mathbf{T}'_n(N)$, where $\mathbf{T}'_n(N)$ and $\mathbf{T}_n(N)$ are i.i.d. Let $\tilde{\nu}^s_N$ denote the law of $\mathbf{T}^s_n(N)$. Following [26, eq. (6.4)], define

$$\kappa_N(u) := \inf_{|\mathbf{t}|=1} \int_{|\mathbf{x}|<u} (\langle \mathbf{t},\mathbf{x}\rangle)^2 d\tilde{\nu}^s_N(\mathbf{x}). \tag{C.86}$$

Finally, let $\mathcal{S}_\rho(\mathbf{c}_\mathrm{o})$ denote the sphere in $\mathbb{R}^2$ with radius ρ and center $\mathbf{c}_\mathrm{o}$.

In our case, [26, Corollary to Theorem 6.2] reads as follows: for any $\rho \in \mathbb{R}^+$,

$$\sup_{\mathbf{c}_\mathrm{o}\in\mathbb{R}^2} \Pr\left\{\sum_{n=1}^{N} \mathbf{A}_n(N) \in \mathcal{S}_\rho(\mathbf{c}_\mathrm{o})\right\} \leq c\left(\frac{\rho}{\tau}\right)^2 \left(\frac{1}{N \sup_{u\geq\tau} u^{-2}\kappa_N(u)}\right),\ \forall\, \tau \in (0,\rho], \tag{C.87}$$

where c is a universal constant that only depends on the dimension of the random vector, which is 2 in our case.

Next, we explain how to use (C.87) to conclude the proof. Since

$$\lim_{N\to\infty} \mathbf{A}_n(N) = \mathbf{A}_n := \left[\ln \frac{W(Y_n|X_n)}{f^*(Y_n)},\ \ln \frac{W(Y_n|Z_n)}{W(Y_n|X_n)}\right]^T,\ \tilde{P}_{X,Y,Z} - \text{(a.s.)}, \tag{C.88}$$

$\mathbf{A}_n$ is bounded almost surely under $\tilde{P}_{X,Y,Z}$. Further, $\tilde{Q}_{X,Y,Z}^{\mathbf{v}^*(N)}$ is equivalent to $\tilde{P}_{X,Y,Z}$ for all N. These two observations imply that there exists $k(R,W,Q) \in \mathbb{R}^+$ and a sufficiently large N_1 that only depends on R, W and Q such that $\max\{\mathbf{T}_{1,n}(N)^s, \mathbf{T}_{2,n}(N)^s\} \leq k(R,W,Q)$, almost surely under $\tilde{\nu}_N^s$ for all $N \geq N_1$.

Consider any $N \geq N_1$ from now on. One can also check that

$$\mathbf{S}_N^s := \mathrm{E}_{\tilde{\nu}^s}\left[\mathbf{T}_n^s(N)\mathbf{T}_n^s(N)^T\right] = 2\mathbf{S}_N, \tag{C.89}$$

which, in turn, implies that for any $u \geq k(R,W,Q)$,

$$\kappa_N(u) = \inf_{|\mathbf{t}|=1} \int (\langle \mathbf{t}, \mathbf{x}\rangle)^2 d\tilde{\nu}_N^s(\mathbf{x}) = \inf_{|\mathbf{t}|=1} \mathbf{t}^T\mathbf{S}_N^s\mathbf{t} = 2\inf_{|\mathbf{t}|=1} \mathbf{t}^T\mathbf{S}_N\mathbf{t} = 2\lambda_{\min}(\mathbf{S}_N). \tag{C.90}$$

Since $\det(\mathbf{S}_N) > 0$, which follows from Lemma 19, we also have $\lambda_{\min}(\mathbf{S}_N) > 0$.

By letting $\rho := \sqrt{\frac{t_1^2}{(\mathbf{v}_1^*(N))^2} + \frac{t_2^2}{(\mathbf{v}_2^*(N))^2}}$, $\mathbf{c}_\mathrm{o} = \mathbf{0}$ and $\tau = \rho$, (C.87) implies that

$$\Pr\left\{\mathbf{W}_N \in \left(0, \frac{t_1}{\mathbf{v}_1^*(N)\sqrt{N}}\right] \times \left(0, \frac{t_2}{\mathbf{v}_2^*(N)\sqrt{N}}\right]\right\} \leq \Pr\left\{\sum_{n=1}^{N} \mathbf{A}_n(N) \in \mathcal{S}_\rho(\mathbf{c}_\mathrm{o})\right\} \tag{C.91}$$

$$\leq \frac{c}{N} \inf_{u \geq \rho} \frac{u^2}{\kappa_N(u)} \tag{C.92}$$

$$\leq \frac{c}{2\lambda_{\min}(\mathbf{\Sigma}_N)N} \times \left(k(R, W, Q)^2 + \frac{t_1^2}{(\mathbf{v}_1^*(N))^2} + \frac{t_2^2}{(\mathbf{v}_2^*(N))^2}\right), \tag{C.93}$$

where (C.93) follows from (C.90). By plugging (C.93) into (C.85) and carrying out the calculation, we deduce that

$$\int_0^\infty \int_0^\infty e^{-\sqrt{N}\langle \mathbf{v}^*(N), \mathbf{x}\rangle} dF_N(\mathbf{x}) \leq \frac{c}{2\lambda_{\min}(\mathbf{\Sigma}_N)N}\left(k(R, W, Q)^2 + \frac{2}{(\mathbf{v}_1^*(N))^2} + \frac{2}{(\mathbf{v}_2^*(N))^2}\right), \tag{C.94}$$

which, in light of (C.83), suffices to conclude the proof. □

C.7 Proof of Lemma 21

First, we note that

$$\forall\, (i, j) \in \{1, 2\}^2,\ \lim_{N\to\infty} \mathbf{S}_N(i, j) = \mathbf{S}(i, j), \tag{C.95}$$

which, in turn, implies that

$$\forall\, (i, j) \in \{1, 2\}^2,\ \lim_{N\to\infty} \mathbf{S}_N^{-1}(i, j) = \mathbf{S}^{-1}(i, j), \tag{C.96}$$

where $\mathbf{S}(i, j)$ denotes the (i, j)-th entry of the matrix $\mathbf{S}$. From (C.96), one can deduce that

$$\lim_{N\to\infty} \|\mathbf{S}_N^{-1}\|_2 = \|\mathbf{S}^{-1}\|_2, \tag{C.97}$$

where $\|\cdot\|_2$ denotes the *Frobenius norm* (e.g., [44, pg. 291]). Also, because of the fact that $\mathbf{S}_N$ and $\mathbf{S}$ are symmetric matrices, we have

$$\lambda_{\min}(\mathbf{S}_N) = |||\mathbf{S}_N^{-1}|||_2, \quad \lambda_{\min}(\mathbf{S}) = |||\mathbf{S}^{-1}|||_2, \tag{C.98}$$

where $|||\cdot|||_2$ denotes the *spectral norm* (e.g., [44, pg. 295]). Using [44, Ex. 5.6.23], we deduce that

$$\|\mathbf{S}^{-1}\|_2 \leq \sqrt{2}|||\mathbf{S}^{-1}|||_2, \quad \|\mathbf{S}_N^{-1}\|_2 \geq |||\mathbf{S}_N^{-1}|||_2. \tag{C.99}$$

Equations (C.97), (C.98) and (C.99) imply (4.109). □

APPENDIX D

APPENDICES OF CHAPTER 5

D.1 Proof of Lemma 22

Thanks to the symmetry of the channel, $\tilde{\mathrm{E}}_{\mathrm{SP}}(R) = \tilde{\mathrm{E}}_{\mathrm{SP}}(R, U_{\mathcal{X}})$ (e.g., [35, pg. 145]). Moreover, by recalling the fact that $\mathrm{E}_{\mathrm{SP}}(R) = \tilde{\mathrm{E}}_{\mathrm{SP}}(R)$ and $\mathrm{E}_{\mathrm{SP}}(R, P) \geq \tilde{\mathrm{E}}_{\mathrm{SP}}(R, P)$ for all $P \in \mathcal{P}(\mathcal{X})$, which have been noted before, we conclude that $\mathrm{E}_{\mathrm{SP}}(R) = \mathrm{E}_{\mathrm{SP}}(R, U_{\mathcal{X}})$. Hence, item (i) follows.

To prove item (ii), fix any $\rho \in \mathbb{R}_+$ and consider the following convex optimization problem[1]

$$\min_{Q \in \mathcal{P}(\mathcal{X})} \sum_{y \in \mathcal{Y}} \left(\sum_{x \in \mathcal{X}} Q(x) W(y|x)^{\frac{1}{1+\rho}} \right)^{1+\rho}. \tag{D.1}$$

Next, we state the necessary and sufficient conditions for $Q \in \mathcal{P}(\mathcal{X})$ to attain the minimum in (D.1), derived by Gallager (e.g., [35, Theorem 5.6.5])

$$\forall x \in \mathcal{X}, \sum_{y \in \mathcal{Y}} W(y|x)^{\frac{1}{1+\rho}} \left(\sum_{z \in \mathcal{X}} Q(z) W(y|z)^{\frac{1}{1+\rho}} \right)^{\rho} \geq \sum_{y \in \mathcal{Y}} \left(\sum_{z \in \mathcal{X}} Q(z) W(y|z)^{\frac{1}{1+\rho}} \right)^{1+\rho}, \tag{D.2}$$

with equality if $Q(x) > 0$. Thanks to the symmetry of the channel, $U_{\mathcal{X}}$ is an optimizer of (D.1) (e.g., [35, pg. 145]) and hence (D.2) implies (5.11).

To prove the rest, we first note the following, which is an easy consequence of basic convex optimization arguments (e.g., [20, Ex. 2.5.23])

$$\mathrm{E}_{\mathrm{SP}}(R, U_{\mathcal{X}}) = \max_{\rho \geq 0} \min_{q \in \mathcal{P}(\mathcal{Y})} \left\{ -\rho R - (1+\rho) \sum_{x \in \mathcal{X}} U_{\mathcal{X}}(x) \ln \sum_{y \in \mathcal{Y}} W(y|x)^{\frac{1}{1+\rho}} q(y)^{\frac{\rho}{1+\rho}} \right\}. \tag{D.3}$$

Due to Propositions 2 and 3 in Chapter 3, (D.3) has a unique saddle-point. Further, Proposition 4 in Chapter 3 ensures that $\rho_R(U_{\mathcal{X}})$ is the $\mathbb{R}_+$ component of this saddle-point. Owing to the properties of the saddle-points (e.g., [55, Lemma 36.2]) $\rho_R(U_{\mathcal{X}})$

[1] Convexity has been verified by Gallager in [35, Theorem 5.6.5].

attains the maximum in (D.3) and the fact that $\mathrm{E_{SP}}(R) = \mathrm{E_{SP}}(R, U_{\mathcal{X}}) > 0$ ensures its positivity. Hence,

$$\mathrm{E_{SP}}(R, U_{\mathcal{X}}) = \min_{q} \left\{ -\rho_R(U_{\mathcal{X}})R - (1+\rho_R(U_{\mathcal{X}})) \sum_{x\in\mathcal{X}} U_{\mathcal{X}}(x) \ln \sum_{y\in\mathcal{Y}} W(y|x)^{\frac{1}{1+\rho_R(U_{\mathcal{X}})}} q(y)^{\frac{\rho_R(U_{\mathcal{X}})}{1+\rho_R(U_{\mathcal{X}})}} \right\} \tag{D.4}$$

$$\leq -\rho_R(U_{\mathcal{X}})R - (1+\rho_R(U_{\mathcal{X}})) \sum_{x\in\mathcal{X}} U_{\mathcal{X}}(x) \ln \sum_{y\in\mathcal{Y}} W(y|x)^{\frac{1}{1+\rho_R(U_{\mathcal{X}})}} q_R(y)^{\frac{\rho_R(U_{\mathcal{X}})}{1+\rho_R(U_{\mathcal{X}})}} \tag{D.5}$$

$$= -\rho_R(U_{\mathcal{X}})R + \mathrm{E_o}(\rho_R(U_{\mathcal{X}}), U_{\mathcal{X}}) \tag{D.6}$$

$$\leq \tilde{\mathrm{E}}_{\mathrm{SP}}(R, U_{\mathcal{X}}), \tag{D.7}$$

where (D.6) follows from item (ii) of this lemma by recalling the definitions of q_R and $\mathrm{E_o}(\cdot,\cdot)$.

In light of item (i) of this lemma, (D.7) implies that $\rho_R(U_{\mathcal{X}})$ attains the maximum in the definition of $\tilde{\mathrm{E}}_{\mathrm{SP}}(R, U_{\mathcal{X}})$ and hence item (iii) follows.

Item (iv) is evident in light of (D.7) and item (i) of this lemma. □

D.2 Proof of Lemma 24

We begin with the following optimization problem (e.g., (D.3))

$$\mathrm{E_{SP}}(R, U_{\mathcal{X}}) = \max_{\rho\in\mathbb{R}_+} \min_{q\in\mathcal{P}(\mathcal{Y})} \left\{ -\rho R - (1+\rho) \sum_{x\in\mathcal{X}} U_{\mathcal{X}}(x) \ln \sum_{y:W(y|x)>0} W(y|x)^{1/(1+\rho)} q(y)^{\rho/(1+\rho)} \right\}. \tag{D.8}$$

As noted in Appendix D.1, the right-side of (D.8) has a unique saddle-point and ρ_R is the $\mathbb{R}_+$ component of this saddle-point. Further, due to the definition of a saddle-point (e.g., [55, pg. 380]), item (iv) of Lemma 22 ensures that q_R is the $\mathcal{P}(\mathcal{Y})$ component of

the saddle-point. Hence, we conclude that (ρ_R, q_R) pair is the unique saddle-point of the right side of (D.8).

By establishing this, we are in a position to invoke the results proved in Chapter 3 to deduce the claim. In particular, item (i) is a direct consequence of item (ii) of Lemma 6 in Chapter 3.

Moreover, given any $\mathrm{D}(W_R\|q_R|U_{\mathcal{X}}) < r \leq R$, we have

$$\mathrm{e}_{\mathrm{SP}}(r,R) = \max_{\rho\in\mathbb{R}_+} \min_{V\in\mathcal{P}(\mathcal{Y}|\mathcal{X})} \{\mathrm{D}(V\|W|U_{\mathcal{X}}) + \rho\,(\mathrm{D}(V\|q_R|U_{\mathcal{X}}) - r)\} \tag{D.9}$$

$$= \max_{\rho\in\mathbb{R}_+} \left\{-\rho r + (1+\rho)\Lambda\left(\frac{\rho}{1+\rho}\right)\right\}, \tag{D.10}$$

where (D.9) follows since the convex program $\mathrm{e}_{\mathrm{SP}}(r,R)$ has zero duality gap, thanks to the fact that Slater's condition (e.g., [55, Corollary 28.2.1]) holds, which is a direct consequence of item (i) of this lemma, and (D.10) follows by solving the convex minimization problem on the right side of (D.9). Equation (D.10) establishes item (ii).

Item (iii) directly follows from Proposition 6 in Chapter 3 that can be invoked thanks to the observation that (ρ_R, q_R) pair is the unique saddle-point of $\mathrm{E}_{\mathrm{SP}}(R, U_{\mathcal{X}})$, i.e., the right side of (D.8). □

D.3 Proof of Lemma 25

(i) The proof goes by contradiction. Assume that there exists $\lambda_{\mathrm{o}} \in [0,1)$ with $\Lambda''(\lambda_{\mathrm{o}}) = 0$. From (5.19), this is equivalent to

$$W(Y|x_{\mathrm{o}}) = q_R(Y)e^{-\Lambda'(\lambda_{\mathrm{o}})},\ \forall\, y \in \mathcal{S}(W(\cdot|x_{\mathrm{o}})). \tag{D.11}$$

Further, item (ii) of Lemma 24 and (D.11), along with the definition of $\Lambda(\cdot)$, imply that

$$\mathrm{e}_{\mathrm{SP}}(R,R) = \max_{\rho\in\mathbb{R}_+} -\rho(R+\Lambda'(\lambda_{\mathrm{o}})). \tag{D.12}$$

Since $\mathrm{e}_{\mathrm{SP}}(R,R) = \mathrm{E}_{\mathrm{SP}}(R)$, which is established in item (iii) of Lemma 24, (D.12) implies that either $\mathrm{E}_{\mathrm{SP}}(R,R) = 0$, which contradicts the fact that $\mathrm{E}_{\mathrm{SP}}(R) > 0$ (e.g., [35, pg. 158]), or $\mathrm{E}_{\mathrm{SP}}(R) = \infty$, which contradicts the fact that $R > R_\infty$. Hence, we conclude that for all $\lambda \in [0,1)$, $\Lambda''(\lambda) > 0$.

(ii) For notational convenience, let $\mathrm{e}_{\mathrm{o}}(\rho,R) := -(1+\rho)\Lambda\left(\frac{\rho}{1+\rho}\right)$. From item (ii) of Lemma 24, we have

$$\mathrm{e}_{\mathrm{SP}}(r,R) = \max_{\rho\in\mathbb{R}_+} \left\{-\rho r + \mathrm{e}_{\mathrm{o}}(\rho,R)\right\}. \tag{D.13}$$

$\mathrm{e}_{\mathrm{SP}}(\cdot,R)$ is differentiable owing to Corollary 2 in Chapter 3, which can be invoked thanks to the fact that (ρ_R, q_R) pair is the unique saddle-point of $\mathrm{E}_{\mathrm{SP}}(R, U_X)$ that has been shown in Appendix D.2, and hence we conclude that s_r is well-defined. Since differentiable convex functions of one variable are continuously differentiable, the second assertion follows.

To verify the last two assertions, observe that (D.13) is the Lagrangian dual of the convex program $\mathrm{e}_{\mathrm{SP}}(r,R)$, which is established in (D.9) and (D.10). Hence, we can use the subdifferential characterization of the Lagrange multipliers (e.g., [55, Theorem 29.1]) to deduce that the set of optimizers in (D.13) coincides with the negative of the subdifferential of $\mathrm{e}_{\mathrm{SP}}(\cdot,R)$ at r, i.e., $\rho \in \mathbb{R}_+$ maximizes (D.13) if and only if $\rho \in -\partial\mathrm{e}_{\mathrm{SP}}(\cdot,R)(r)$. Since $\mathrm{e}_{\mathrm{SP}}(\cdot,R)$ is differentiable at r, $-\partial\mathrm{e}_{\mathrm{SP}}(\cdot,R)(r) = \{s_r\}$ and hence s_r uniquely attains the maximum in (D.13). Further, since $\mathrm{e}_{\mathrm{SP}}(r,R) \geq \mathrm{e}_{\mathrm{SP}}(R,R) = \mathrm{E}_{\mathrm{SP}}(R) > 0$, we have $s_r \in \mathbb{R}^+$.

Moreover, via elementary calculation, one can verify that

$$\frac{\partial^2}{\partial\rho^2}\left[-\rho r + \mathrm{e}_{\mathrm{o}}(\rho,R)\right] = \frac{\partial^2 \mathrm{e}_{\mathrm{o}}(\rho,R)}{\partial\rho^2} = -\frac{1}{(1+\rho)^3}\Lambda''\left(\frac{\rho}{1+\rho}\right) < 0, \tag{D.14}$$

where the inequality follows from item (i) of this lemma. As a direct consequence of (D.14), we conclude that s_r is the unique positive real number satisfying $r = \frac{\partial \mathrm{e_o}(\rho,R)}{\partial \rho}\Big|_{\rho=s_r}$. This observation, coupled with (D.14) and the inverse function theorem, further implies that s_r is strictly decreasing in r.

(iii) Since $\Lambda(\cdot)$ is a convex function (e.g., [21, Lemma 2.2.5, item (a)]), $\lambda[\mathrm{e_{SP}}(r,R)-r]-\Lambda(\lambda)$ is a concave function of λ and hence the following is a sufficient condition for $\lambda_\mathrm{o} \in \mathbb{R}$ to attain $\Lambda^*(\mathrm{e_{SP}}(r,R)-r)$

$$\Lambda'(\lambda_\mathrm{o}) = \mathrm{e_{SP}}(r,R) - r. \tag{D.15}$$

As noted above, s_r is the unique positive real number satisfying $r = \frac{\partial \mathrm{e_o}(\rho,R)}{\rho}\Big|_{\rho=s_r}$, hence, an elementary calculation implies that

$$r = -\Lambda\left(\frac{s_r}{1+s_r}\right) - \frac{1}{(1+s_r)}\Lambda'\left(\frac{s_r}{1+s_r}\right), \tag{D.16}$$

and hence

$$\mathrm{e_{SP}}(r,R) = \frac{s_r}{(1+s_r)}\Lambda'\left(\frac{s_r}{1+s_r}\right) - \Lambda\left(\frac{s_r}{1+s_r}\right). \tag{D.17}$$

Equations (D.16) and (D.17) imply that

$$\Lambda'\left(\frac{s_r}{1+s_r}\right) = \mathrm{e_{SP}}(r,R) - r. \tag{D.18}$$

Equations (D.16) and (D.18) ensure that $s_r/(1+s_r)$ attains $\Lambda^*(\mathrm{e_{SP}}(r,R)-r)$ and hence

$$\Lambda^*(\mathrm{e_{SP}}(r,R)-r) = \left(\frac{s_r}{1+s_r}\right)(\mathrm{e_{SP}}(r,R)-r) - \Lambda\left(\frac{s_r}{1+s_r}\right) = \mathrm{e_{SP}}(r,R),$$

where the second equality follows by plugging (D.18) into (D.17).

Finally, let $\eta_r := s_r/(1+s_r) \in \mathbb{R}^+$, since $s_r \in \mathbb{R}^+$. Hence, (D.18) implies the existence of $\eta_r \in (0,1)$ with $\Lambda'(\eta_r) = \mathrm{e_{SP}}(r,R) - r$. To verify the uniqueness, it suffices to note that $\mathrm{e_{SP}}(\cdot,R) - (\cdot)$ is strictly decreasing, along with item (i) of this lemma and the inverse function theorem. □

D.4 Proof of Lemma 27

The proof follows from essentially the same arguments given in Section 3.2.5. We provide an outline for completeness.

First of all, we notice that (e.g., [21, Ex. 2.2.24]) $\Lambda^*(\cdot)$ is a smooth function over $(-\mathrm{D}(W\|q_R|U_X), \mathrm{D}(W_R\|W|U_X))$, which, along with the inverse function theorem and items (i) and (iii) of Lemma 25, implies that

$$\Lambda^{*\prime}(\mathrm{e}_{\mathrm{SP}}(r,R)-r)=\eta_r, \quad \Lambda^{*\prime\prime}(\mathrm{e}_{\mathrm{SP}}(r,R)-r)=\frac{1}{\Lambda''(\eta_r)}, \tag{D.19}$$

for any $r \in [\bar{R}, R]$. Via calculations similar to the ones leading to (3.105), one can verify that

$$\begin{aligned}\Lambda^*(\mathrm{e}_{\mathrm{SP}}(R_N,R)-R_N) = \Lambda^*(\mathrm{e}_{\mathrm{SP}}(R,R)-R)+\epsilon_N\eta_R+(\mathrm{e}_{\mathrm{SP}}(R_N,R)-\mathrm{e}_{\mathrm{SP}}(R,R))\eta_R \\ +\frac{\Lambda^{*\prime\prime}(\bar{x})\left[\mathrm{e}_{\mathrm{SP}}(R_N,R)-R_N-\mathrm{e}_{\mathrm{SP}}(R,R)+R\right]^2}{2},\end{aligned} \tag{D.20}$$

for some $\bar{x} \in (\mathrm{e}_{\mathrm{SP}}(R,R)-R, \mathrm{e}_{\mathrm{SP}}(R_N,R)-R_N)$. Using items (ii) and (iii) of Lemma 25 and recalling the definition of ϵ_N, (D.20) further implies that

$$\mathrm{e}_{\mathrm{SP}}(R_N,R)=\mathrm{e}_{\mathrm{SP}}(R,R)+\epsilon_N s_R+\epsilon_N^2\frac{(1+s_R)\Lambda^{*\prime\prime}(\bar{x})}{2}\left(1+\frac{\mathrm{e}_{\mathrm{SP}}(R_N,R)-\mathrm{e}_{\mathrm{SP}}(R,R)}{\epsilon_N}\right)^2. \tag{D.21}$$

By using (D.19), along with the fact that $\mathrm{e}_{\mathrm{SP}}(\cdot,R)-(\cdot)$ is a strictly decreasing and continuous function over $[\bar{R}, R]$, one can see that

$$\Lambda^{*\prime\prime}(\bar{x}) \leq \frac{1}{m_{2,\min}} \in \mathbb{R}^+. \tag{D.22}$$

Moreover, (3.121), which can be invoked thanks to the fact that (ρ_R, q_R) pair is the unique saddle-point of $\mathrm{E}_{\mathrm{SP}}(R, U_X)$ that has been shown in Appendix D.2, implies that

$$s_R = \left|\mathrm{E}'_{\mathrm{SP}}(R)\right|. \tag{D.23}$$

Finally, via a first-order power series approximation, along with items (ii) and (iii) of Lemma 25, one can verify that

$$\left(1 + \frac{\mathrm{e}_{\mathrm{SP}}(R_N, R) - \mathrm{e}_{\mathrm{SP}}(R, R)}{\epsilon_N}\right)^2 \leq (1 + s_{\bar{R}})^2. \tag{D.24}$$

By plugging (D.22), (D.23) and (D.24) into (D.21), along with the fact that $\mathrm{E}_{\mathrm{SP}}(R) = \mathrm{e}_{\mathrm{SP}}(R, R)$, which is shown in item (iii) of Lemma 24, one can check that (5.45) holds. □

D.5 Proof of Lemma 28

Consider any $\mathbf{x}^N \in \mathcal{X}^N$. We have

$$W\left\{\mathcal{S}(R_N)|\mathbf{x}^N\right\} = \sum_{\mathbf{y}^N} W(\mathbf{y}^N|\mathbf{x}^N)\mathbb{1}\left\{\frac{1}{N}\sum_{n=1}^{N} \ln\frac{1}{\alpha_{y_n}} \leq R_N\right\} \tag{D.25}$$

$$= \sum_{\mathbf{y}^N} W(\mathbf{y}^N|\mathbf{x}^N)\mathbb{1}\left\{\frac{1}{N}\sum_{n=1}^{N} \ln\frac{W(y_n|x_n)}{q(y_n)} \leq R_N\right\} \tag{D.26}$$

$$= W\left\{\frac{1}{N}\sum_{n=1}^{N} \ln\frac{W(Y_n|x_n)}{q(Y_n)} \leq R_N \mid \mathbf{x}^N\right\}, \tag{D.27}$$

where (D.26) follows by noting whenever $W(y|x) > 0$, $\frac{W(y|x)}{q(y)} = \frac{1}{\alpha_y}$, which is a direct consequence of the fact that W is singular.

Next, for any $x \in \mathcal{X}$ and $\lambda \in \mathbb{R}$, we define $M_x(\lambda) := \sum_{y:W(y|x)>0} W(y|x)^{1-\lambda} q(y)^{\lambda}$. Evidently, $M_x(\cdot) \in \mathbb{R}$ for any $x \in \mathcal{X}$.

We claim that given any $\lambda \in \mathbb{R}$, $M_x(\lambda)$ is constant in x, whose proof is similar to Lemma 23. Specifically, let $\{\mathcal{Y}_l\}_{l=1}^{L}$ be a partition[2] of the columns of W mentioned in Definition 9. Since each column is a permutation of every other column within the partition, $q(y)$ is the same for any $y \in \mathcal{Y}_l$. This observation, along with the fact that all rows are permutations of every other row, implies that $M_x(\cdot)$ is the same for all $x \in \mathcal{X}$.

[2]The choice of the partition is immaterial in what follows.

Using the fact that $M_x(\lambda)$ is constant in x and the uniqueness theorem for the moment generating function (e.g., [11, Ex. 26.7]), we deduce that

$$W\left\{\frac{1}{N}\sum_{n=1}^{N}\ln\frac{q(Y_n)}{W(Y_n|x_n)} \geq -R_N \mid \mathbf{x}^N\right\} = W\left\{\frac{1}{N}\sum_{n=1}^{N}\ln\frac{q(Y_n)}{W(Y_n|x_{\mathrm{o}})} \geq -R_N \mid \mathbf{x}_{\mathrm{o}}^N\right\}, \quad \text{(D.28)}$$

which, in light of (D.27), implies item (i) of the lemma.

To prove item (ii), we define

$$\Lambda(\lambda) := \ln \mathrm{E}_{W(\cdot|x_{\mathrm{o}})}\left[e^{\lambda \ln \frac{q(Y)}{W(Y|x_{\mathrm{o}})}}\right] = \ln \sum_{y:W(y|x_{\mathrm{o}})>0} W(y|x_{\mathrm{o}})^{1-\lambda} q(y)^{\lambda}. \quad \text{(D.29)}$$

Evidently,

$$\Lambda(\lambda) = \ln \sum_{y:W(y|x_{\mathrm{o}})>0} \delta_y \alpha_y^{\lambda}. \quad \text{(D.30)}$$

We observe that for any $\lambda \in \mathbb{R}_+$,

$$\Lambda(\lambda) = \ln \sum_{y\in\mathcal{Y}} \delta_y \alpha_y^{1+\lambda} = -\mathrm{E}_{\mathrm{o}}(\lambda, U_X), \quad \text{(D.31)}$$

where $\mathrm{E}_{\mathrm{o}}(\cdot,\cdot)$ is as defined in (5.4), the first equality follows from item (ii) of Lemma 22 and the second equality follows from elementary calculation by noticing the singularity of the channel.

Via straightforward calculation, one can check that

$$\Lambda'(\lambda) = \sum_{y\in\mathcal{Y}} \frac{\delta_y \alpha_y^{1+\lambda}}{\sum_{b\in\mathcal{Y}} \delta_b \alpha_b^{1+\lambda}} \ln \alpha_y \quad \text{and} \quad \Lambda''(\lambda) = \sum_{y\in\mathcal{Y}} \frac{\delta_y \alpha_y^{1+\lambda}}{\sum_{b\in\mathcal{Y}} \delta_b \alpha_b^{1+\lambda}} \left(\ln \alpha_y - \Lambda'(\lambda)\right)^2 \geq 0, \quad \text{(D.32)}$$

for any $\lambda \in \mathbb{R}_+$. Further, define

$$m_3(\lambda) := \sum_{y\in\mathcal{Y}} \frac{\delta_y \alpha_y^{1+\lambda}}{\sum_{b\in\mathcal{Y}} \delta_b \alpha_b^{1+\lambda}} \left|\ln \alpha_y - \Lambda'(\lambda)\right|^3. \quad \text{(D.33)}$$

Evidently, $\Lambda'(\cdot)$, $\Lambda''(\cdot)$ and $m_3(\cdot)$ are continuous over $\mathbb{R}_+$.

Next, we prove that

$$\forall\, \lambda \in \mathbb{R}_+,\ \Lambda''(\lambda) > 0. \quad \text{(D.34)}$$

To see (D.34), first note that for all $\lambda \in \mathbb{R}_+$, $\Lambda''(\lambda) \geq 0$, due to (D.32). For contradiction, assume there exists $\lambda_{\mathrm{o}} \in \mathbb{R}_+$ with $\Lambda''(\lambda_{\mathrm{o}}) = 0$. This, however, implies that the dispersion of the channel is 0, owing to (D.31), [35, Theorem 5.6.3] and the fact that $U_{\mathcal{X}}$ is a capacity achieving input distribution for W (e.g., [35, Theorem 4.5.2]). Since the channel has positive dispersion, this yields a contradiction.

For any $r \in [\bar{R}, R]$, let $\eta_r := -\left.\frac{\partial \mathrm{E}_{\mathrm{SP}}(a, U_{\mathcal{X}})}{\partial a}\right|_{a=r}$, which is well-defined owing to item (iii) of Lemma 22. Further, observe that for any $r \in [\bar{R}, R]$,

$$-r = \Lambda'(\eta_r), \tag{D.35}$$

which is evident in light of

$$r = \left.\frac{\partial \mathrm{E}_{\mathrm{o}}(\rho, U_{\mathcal{X}})}{\partial \rho}\right|_{\rho=\eta_r} = -\Lambda'(\eta_r), \tag{D.36}$$

where the first equality follows by recalling the fact that η_r attains $\tilde{\mathrm{E}}_{\mathrm{SP}}(r, U_{\mathcal{X}})$, which is shown in Lemma 22, and the second equality follows from (D.31). Moreover, since η_r attains $\tilde{\mathrm{E}}_{\mathrm{SP}}(r, U_{\mathcal{X}})$ and $\tilde{\mathrm{E}}_{\mathrm{SP}}(r, U_{\mathcal{X}}) \geq \tilde{\mathrm{E}}_{\mathrm{SP}}(R, U_{\mathcal{X}}) = \tilde{\mathrm{E}}_{\mathrm{SP}}(R) > 0$, for any $r \in [\bar{R}, R]$, we deduce that $\eta_r \in \mathbb{R}^+$. Further, (D.34), (D.35) and the inverse function theorem ensures that $\eta_{(\cdot)}$ is strictly non-increasing over $[\bar{R}, R]$.

Fix some $a > 1$ and define

$$t_{\max} := a2\sqrt{2\pi}\eta_{\bar{R}} \max_{\lambda \in [0, \eta_{\bar{R}}]} \frac{m_3(\lambda)}{\Lambda''(\lambda)}, \tag{D.37}$$

$$m_{2,\min} := \min_{\lambda \in [0, \eta_{\bar{R}}]} \Lambda''(\lambda), \tag{D.38}$$

$$m_{2,\max} := \max_{\lambda \in [0, \eta_{\bar{R}}]} \Lambda''(\lambda). \tag{D.39}$$

Clearly, all of the above quantities are well-defined and positive. For convenience, let

$$k_{\mathrm{o}} := \frac{e^{-t_{\max}}\left(1 - \frac{1}{a}\right)}{\eta_{\bar{R}} 2\sqrt{2\pi m_{2,\max}}} \in \mathbb{R}^+. \tag{D.40}$$

Let $N \in \mathbb{Z}^+$ be sufficienttly large such that

$$R_N \geq \bar{R} \quad \text{and} \quad \frac{[1 + (1 + t_{\max})^2]}{\eta_R \left(1 - \frac{1}{a}\right) 2\sqrt{eNm_{2,\min}}} \leq \frac{1}{2}. \tag{D.41}$$

We have

$$W\left\{\mathcal{S}(R_N)|\mathbf{x}_{\mathrm{o}}^N\right\} \geq \frac{k_{\mathrm{o}}\left(1 + a2\sqrt{2\pi}\eta_{R_N}\frac{m_3(\eta_{R_N})}{\Lambda''(\eta_{R_N})}\right)}{\sqrt{N}} e^{-N\Lambda^*(-R_N)} \tag{D.42}$$

$$\geq \frac{k_{\mathrm{o}}}{\sqrt{N}} e^{-N\Lambda^*(-R_N)}, \tag{D.43}$$

where $\Lambda^*(-R_N) := \sup_{\lambda\in\mathbb{R}}\{-\lambda R_N - \Lambda(\lambda)\}$ and (D.42) follows from Lemma 5, in particular (3.2), which is applicable thanks to (D.34) and (D.35), along with (D.41). Since $\eta_{(\cdot)} \in \mathbb{R}^+$ is non-increasing and $\Lambda(\cdot)$ is convex, (D.35) implies that

$$\Lambda^*(-R_N) = \max_{0\leq\lambda\leq\eta_{\bar{R}}}\left\{-\lambda\left(R - \frac{k}{N}\right) - \Lambda(\lambda)\right\} \leq \frac{k\eta_{\bar{R}}}{N} + \max_{0\leq\lambda\leq\eta_{\bar{R}}}\{-\lambda R - \Lambda(\lambda)\} = \frac{k\eta_{\bar{R}}}{N} + \Lambda^*(-R). \tag{D.44}$$

By plugging (D.44) into (D.43), we deduce that (5.50) holds. □

BIBLIOGRAPHY

[1] Y. Altuğ and A. B. Wagner. Moderate deviation analysis of channel coding: Discrete memoryless case. In *Information Theory Proceedings (ISIT), 2010 IEEE International Symposium on*, pages 265–269. IEEE, 2010.

[2] Y. Altuğ and A. B. Wagner. Refinement of the sphere packing bound for symmetric channels. In *Communication, Control, and Computing (Allerton), 2011 49th Annual Allerton Conference on*, pages 30–37. IEEE, 2011.

[3] Y. Altuğ and A. B. Wagner. A refinement of the random coding bound. In *Communication, Control, and Computing (Allerton), 2012 50th Annual Allerton Conference on*, pages 663–670. IEEE, 2012.

[4] Y. Altuğ and A. B. Wagner. Refinement of the random coding bound. In *International Zurich Seminar on Communications, 2012. IZS'12 Zurich. IEEE*. IEEE, 2012.

[5] Y. Altuğ and A. B. Wagner. Refinement of the sphere–packing bound. In *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, pages 2949–2953. IEEE, 2012.

[6] Y. Altuğ and A. B. Wagner. Refinement of the sphere–packing bound: Asymmetric channels. *arXiv preprint arXiv:1211.6697*, 2012.

[7] R. R. Bahadur and R. R. Rao. On deviations of the sample mean. *The Annals of Mathematical Statistics*, 31(4):1015–1027, 1960.

[8] C. Berrou, A. Glavieux, and P. Thitimajshima. Near shannon limit error-correcting coding and decoding: Turbo-codes. 1. In *Communications, 1993. ICC 93. Geneva. Technical Program, Conference Record, IEEE International Conference on*, volume 2, pages 1064–1070. IEEE, 1993.

[9] A. C. Berry. The accuracy of the gaussian approximation to the sum of independent variates. *Transactions of the American Mathematical Society*, 49(1):122–136, 1941.

[10] D. P. Bertsekas, A. Nedić, and A. E. Ozdaglar. *Convex analysis and optimization*. Athena Scientific Belmont, 2003.

[11] P. Billingsley. *Probability and measure. 3rd ed.* John Wiley & Sons, 1995.

[12] R. E. Blahut. Hypothesis testing and information theory. *Information Theory, IEEE Transactions on*, 20(4):405–417, 1974.

[13] R. E. Blahut. *Principles and practice of information theory*. Addison-Wesley Longman Publishing Co., Inc., 1987.

[14] S. Boyd and L. Vandenberghe. *Convex optimization*. Cambridge university press, 2004.

[15] N. R. Chaganty and J. Sethuraman. Strong large deviation and local limit theorems. *The Annals of Probability*, pages 1671–1690, 1993.

[16] N. R. Chaganty and J. Sethuraman. Multidimensional strong large deviation theorems. *Journal of statistical planning and inference*, 55(3):265–280, 1996.

[17] J. Chen, D.-k. He, A. Jagmohan, and L. A. Lastras-Montaño. On the redundancy-error tradeoff in slepian–wolf coding and channel coding. In *Information Theory, 2007. ISIT 2007. IEEE International Symposium on*, pages 1326–1330. IEEE, 2007.

[18] T. M. Cover and J. A. Thomas. *Elements of information theory. 2nd ed.* Wiley-interscience, 2006.

[19] H. Cramér. Sur un nouveau théorème-limite de la théorie des probabilités. *Actualités scientifiques et industrielles*, 736(5-23):115, 1938.

[20] I. Csiszár and J. Körner. *Information theory: Coding theorems for discrete memoryless systems*. Academic Press (New York and Budapest), 1981.

[21] A. Dembo and O. Zeitouni. *Large deviations techniques and applications*. Springer, 1998.

[22] R. L. Dobrushin. Asymptotic estimates of the probability of error for transmission of messages over a discrete memoryless communication channel with a symmetric transition probability matrix. *Theory of Probability & Its Applications*, 7(3):270–300, 1962.

[23] R. Durrett. *Probability: Theory and Examples*. Thomson Brooks/Cole, 2005.

[24] P. Elias. Coding for two noisy channels. In *Information Theory, Third London Symposium*, pages 61–76. London, England, 1955.

[25] C.-G. Esseen. Fourier analysis of distribution functions. a mathematical study of the laplace–gaussian law. *Acta Mathematica*, 77(1):1–125, 1945.

[26] C.-G. Esseen. On the concentration function of a sum of independent random variables. *Probability Theory and Related Fields*, 9(4):290–308, 1968.

[27] R. M. Fano. *Transmission of information: a statistical theory of communication*. Mit Press, 1961.

[28] A. Feinstein. A new basic theorem of information theory. *Information Theory, IRE Transactions on*, 4(4):2–22, 1954.

[29] W. Feller. Generalization of a probability limit theorem of cramér. *Transactions of the American Mathematical Society*, 54(3):361–372, 1943.

[30] W. Feller. Limit theorems for probabilities of large deviations. *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete*, 14(1):1–20, 1969.

[31] W. Feller. *An Introduction to Probability Theory, vol. II, 2nd ed.* Wiley, 1971.

[32] W. Fenchel. On conjugate convex functions. *Canad. J. Math*, 1:73–77, 1949.

[33] R. G. Gallager. *Low-density parity-check codes*. Mit Press, 1963.

[34] R. G. Gallager. A simple derivation of the coding theorem and some applications. *Information Theory, IEEE Transactions on*, 11(1):3–18, 1965.

[35] R. G. Gallager. *Information theory and reliable communication*. Wiley, 1968.

[36] R. G. Gallager. The random coding bound is tight for the average code (corresp.). *Information Theory, IEEE Transactions on*, 19(2):244–246, 1973.

[37] R. G. Gallager. *Personal communication*. 2011.

[38] E. A. Haroutunian. Estimates of the error exponents for the semi-continuous memoryless channel. *Probl. Per. Inf.*, 4:37–48, 1968.

[39] D.-k. He, L. A. Lastras-Montaño, and E.-h. Yang. A lower bound for variable rate slepian–wolf coding. In *Information Theory, 2006 IEEE International Symposium on*, pages 341–345. IEEE, 2006.

[40] D.-k. He, L. A. Lastras-Montaño, and E.-h. Yang. On the relationship between redundancy and decoding error in slepian–wolf coding. In *Information Theory Workshop, 2006. ITW'06 Chengdu. IEEE*, pages 332–336. IEEE, 2006.

[41] D.-k. He, L. A. Lastras-Montaño, E.-h. Yang, A. Jagmohan, and J. Chen. On the redundancy of slepian–wolf coding. *Information Theory, IEEE Transactions on*, 55(12):5607–5627, 2009.

[42] J.-B. Hiriart-Urruty and C. Lemaréchal. *Convex Analysis and Minimization Algorithms I: Fundamentals (Grundlehren Der Mathematischen Wissenschaften)*. Springer, 1993.

[43] E. Hof, I. Sason, and S. Shamai (Shitz). Performance bounds for nonbinary linear block codes over memoryless symmetric channels. *Information Theory, IEEE Transactions on*, 55(3):977–996, 2009.

[44] R. A. Horn and C. R. Johnson. *Matrix analysis*. Cambridge university press, 1985.

[45] I. A. Ibragimov and Yu. V. Linnik. *Independent and stationary sequences of random variables*. Wolters-Noordhoff, 1971.

[46] V. Yu. Korolev and I. G. Shevtsova. A new moment-type estimate of convergence rate in the lyapunov theorem. *Theory of Probability & Its Applications*, 55(3):505–509, 2011.

[47] D. J. C. MacKay and R. M. Neal. Near shannon limit performance of low density parity check codes. *Electronics letters*, 33(6):457–458, 1997.

[48] K. Marton. Error exponent for source coding with a fidelity criterion. *Information Theory, IEEE Transactions on*, 20(2):197–199, 1974.

[49] V. V. Petrov. Generalization of cramér's limit theorem. *Uspekhi Matematicheskikh Nauk*, 9(4):195–202, 1954.

[50] K.V. Petrovskii. Limit theorems for large deviations of sums of independent lattice random vectors. *Discrete Mathematics and Applications*, 6(4):361–378, 1996.

[51] Y. Polyanskiy. *Channel coding: non-asymptotic fundamental limits*. PhD thesis, Princeton University, 2010.

[52] Y. Polyanskiy, H. V. Poor, and S. Verdú. Channel coding rate in the finite block-

length regime. *Information Theory, IEEE Transactions on*, 56(5):2307–2359, 2010.

[53] Y. Polyanskiy and S. Verdú. Channel dispersion and moderate deviations limits for memoryless channels. In *Communication, Control, and Computing (Allerton), 2010 48th Annual Allerton Conference on*, pages 1334–1339. IEEE, 2010.

[54] R. T. Rockafellar. Minimax theorems and conjugate saddle-functions. *Math. Scand*, 14:151–173, 1964.

[55] R. T. Rockafellar. *Convex analysis*. Princeton university press, 1970.

[56] A. Ruszczyński. *Nonlinear optimization*. Princeton university press, 2006.

[57] I. Sason. Moderate deviations analysis of binary hypothesis testing. In *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, pages 821–825. IEEE, 2012.

[58] I. Sason and S. Shamai (Shitz). *Performance analysis of linear codes under maximum-likelihood decoding: a tutorial*. Now Pub, 2006.

[59] J. Scarlett, A. Martinez, and A. Guillén i Fàbregas. A derivation of the asymptotic random-coding prefactor. *arXiv preprint arXiv:1306.6203*, 2013.

[60] S. Shamai (Shitz) and I. Sason. Variations on the gallager bounds, connections, and applications. *Information Theory, IEEE Transactions on*, 48(12):3029–3051, 2002.

[61] C. E. Shannon. A mathematical theory of communication. *Bell Syst. Tech. J.*, 27:379–423, 623–656, 1948.

[62] C. E. Shannon. Certain results in coding theory for noisy channels. *Information and control*, 1(1):6–25, 1957.

[63] C. E. Shannon, R. G. Gallager, and E. R. Berlekamp. Lower bounds to error probability for coding on discrete memoryless channels. i. *Information and Control*, 10(1):65–103, 1967.

[64] N. Shulman and M. Feder. Random coding techniques for nonrandom codes. *Information Theory, IEEE Transactions on*, 45(6):2101–2104, 1999.

[65] D. Slepian and J. Wolf. Noiseless coding of correlated information sources. *Information Theory, IEEE Transactions on*, 19(4):471–480, 1973.

[66] V. Strassen. Asymptotische abschätzungen in shannon's informationstheorie. In *Trans. Third Prague Conf. Information Theory*, pages 689–723, 1962.

[67] V. Y. F. Tan. Moderate-deviations of lossy source coding for discrete and gaussian sources. In *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, pages 920–924. IEEE, 2012.

[68] İ. E. Telatar. *Multi-access communications with decision feedback decoding*. PhD thesis, Massachusetts Institute of Technology, 1992.

[69] M. Twitto, I. Sason, and S. Shamai (Shitz). Tightened upper bounds on the ml decoding error probability of binary linear block codes. *Information Theory, IEEE Transactions on*, 53(4):1495–1510, 2007.

[70] A. Valembois and M. Fossorier. Sphere-packing bounds revisited for moderate block lengths. *Information Theory, IEEE Transactions on*, 50(12):2998–3014, 2004.

[71] G. Wiechman and I. Sason. An improved sphere-packing bound for finite-length codes over symmetric memoryless channels. *Information Theory, IEEE Transactions on*, 54(5):1962–1990, 2008.

[72] J. Wolfowitz. The coding of messages subject to chance errors. *Illinois Journal of Mathematics*, 1(4):591–606, 1957.

[73] W. H. Young. On multiple integration by parts and the second theorem of the mean. *Proceedings of the London Mathematical Society*, 2(1):273–293, 1917.