

University of Technology Sydney  
Faculty of Engineering and Information Technology

## Error Exponent Analysis in Quantum Information Theory



**Hao-Chung Cheng**

Supervisor: Min-Hsiu Hsieh

Co-supervisor: Marco Tomamichel

This dissertation is submitted for the degree of

*Doctor of Philosophy*

October 2018

## Certification of Original Authorship

I certify that this thesis “Error Exponent Analysis in Quantum Information Theory” has been written by me. This thesis is the result of a research candidature conducted with another University as part of a collaborative Doctoral degree. Any help that I have received in my research and in the preparation of the thesis itself has been fully acknowledged. In addition, I certify that all information sources and literature used are quoted in the thesis

Production Note:

Signature: Signature removed prior to publication.

Date: 28 November 2018

## Abstract

Error exponent analysis aims at evaluating the exponential behaviour of the performance of the underlying system given a certain fixed coding rate. It is arguably a significant research topic in information theory because the analysis characterizes the trade-offs between the error probability of an information task, the size of the coding scheme, and the coding rate that determines the efficiency of the task. In this thesis, we give an exposition of error exponent analysis to two important quantum information processing protocols—classical data compression with quantum side information, and classical communications over quantum channels.

We first prove substantial properties of various exponent functions, which allow us to better characterize the error behaviours of the tasks. Second, we establish accurate achievability and optimality finite blocklength bounds for the optimal error probability, providing useful and measurable benchmarks for future quantum information technology design. Finally, we extend the error exponent analysis to a more general setting where the coding rate is not fixed anymore, a research topic known as moderate deviation analysis. In other words, we show that the data recovery can be reliable when the compression rate approaches the conditional entropy slowly, and the reliable communication over a classical-quantum channel is possible as the transmission rate approaches channel capacity slowly.

This line of research lies in the intersection of statistical analysis, matrix analysis, and information theory. Thus, the techniques employed in this studies could potentially be applicable to various areas such as classical and quantum information community, detection and estimation theory, statistics, and secrecy.

*Keywords:* error exponent analysis, moderate deviation analysis, quantum information theory, classical-quantum channel, Slepian-Wolf coding, quantum side information, reliability function, large deviation theory, matrix analysis.

## Acknowledgements

I sincerely thank my supervisor Min-Hsiu Hsieh and co-supervisor Marco Tomamichel for guiding me into the research field of quantum information theory. Under their supervision, I learn the knowledge and techniques of quantum information, quantum machine learning, quantum Markovian process, entropies, and matrix analysis. I cannot finish this thesis without their help.

I want to thank University of Technology Sydney and Centre for Quantum Software and Information (UTS:Q|SI) for generously providing me the financial support not only for my living in Sydney, Australia, but also for the travel funding to many academic conferences. I'm eternally grateful.

I would like to thank all the members, staff, and students in UTS:Q|SI for all your support of my study in Sydney. All of you teach me a lot. I also want to thank my dear friends: Deborah, Summer, James, Ellen, Ching-Yi, Xin, Yinan, Kun, Anny, and Rachel. You make my life in Sydney fruitful.

I want to thank my collaborators Prof. Nilanjana Datta, Eric P. Hanson, Li Gao, Barış Nakiboğlu, and Jon Tyson. I'm so happy and grateful when working with you.

Last but not least, I want to thank my dear family. Thank you for supporting me doing what I like as always. This thesis is dedicated to you all.

# Contents

<b>List of Figures</b>	<b>iv</b>
<b>List of Tables</b>	<b>v</b>
<b>1 Introduction</b>	<b>1</b>
1.1 Backgrounds . . . . .	1
1.2 Quantum Information Processing Protocols . . . . .	4
1.2.1 Information Storage with a Quantum Helper (Source Coding) . . . . .	5
1.2.2 Information Transmission over a Quantum Channel (Channel Coding) . . . . .	7
1.3 Main Contributions . . . . .	9
1.4 Structure of the Thesis . . . . .	11
<b>I Fundamentals</b>	<b>13</b>
<b>2 Mathematical Tools</b>	<b>14</b>
2.1 Matrix Analysis . . . . .	14
2.2 Large Deviation Theory . . . . .	19
<b>3 Quantum Entropic Quantities and Notation</b>	<b>26</b>
3.1 Quantum Rényi divergence . . . . .	27
3.2 Conditional Rényi Entropy . . . . .	29
3.3 Rényi and Augustin Information . . . . .	30
<b>4 Quantum Hypothesis Testing</b>	<b>39</b>
4.1 Achievability . . . . .	40
4.2 Optimality . . . . .	41
4.2.1 Nussbaum-Szkoła Distributions . . . . .	44
4.2.2 Proofs of Theorem 4.4 and Corollary 4.1 . . . . .	44
4.3 Moderate Deviation Analysis . . . . .	47
4.3.1 Proof of Theorem 4.5 . . . . .	48
4.3.2 Proof of Theorem 4.6 . . . . .	52
<b>II Classical Information Storage with a Quantum Helper</b>	<b>54</b>
<b>5 Error Exponent Functions (Source Coding)</b>	<b>55</b>
5.1 Variational Representations . . . . .	56
5.2 Properties of Auxiliary Functions . . . . .	57
5.2.1 Proof of Proposition 5.1 . . . . .	58
5.2.2 Proof of Proposition 5.2 . . . . .	61
5.3 Properties of Error Exponent Functions and Saddle-Point . . . . .	62

<b>6 Achievability (Source Coding)</b>	<b>66</b>
6.1 I.I.D. Sources . . . . .	67
6.2 Type-Dependent Sources . . . . .	69
<b>7 Optimality (Source Coding)</b>	<b>73</b>
7.1 One-Shot Converse Bound (Hypothesis Testing Reduction) . . . . .	73
7.2 Proof of Main Result, Theorem 7.1 . . . . .	76
<b>8 Moderate Deviation Analysis (Source Coding)</b>	<b>78</b>
8.1 Asymptotic Expansion of Error Exponent around Slepian-Wolf Limit . . . . .	81
<b>III Classical Information Transmission over a Quantum Channel</b>	<b>84</b>
<b>9 Error Exponent Functions (Channel Coding)</b>	<b>85</b>
9.1 Variational Representations . . . . .	87
9.2 Properties of Auxiliary Functions . . . . .	90
9.2.1 Proof of Proposition 9.1 . . . . .	93
9.2.2 Proof of Proposition 9.2 . . . . .	98
9.2.3 Proof of Proposition 9.3 . . . . .	100
9.2.4 Proof of Proposition 9.4 . . . . .	100
9.3 Properties of Error Exponent Functions and Saddle-Point . . . . .	102
9.3.1 Proof of Proposition 9.5 . . . . .	104
9.3.2 Proof of Proposition 9.6 . . . . .	110
<b>10 Achievability (Channel Coding)</b>	<b>112</b>
10.1 Random Codes with I.I.D. Ensemble . . . . .	113
10.2 Random Codes with Constant Composition Ensemble . . . . .	116
<b>11 Optimality (Channel Coding)</b>	<b>120</b>
11.1 Literature Review of Classical Sphere-Packing Bound . . . . .	121
11.2 A Weak Sphere-Packing Bound via Wolfowitz Strong Converse . . . . .	123
11.2.1 Proof of Wolfowitz's Strong Converse, Proposition 11.1 . . . . .	125
11.3 A Strong Sphere-Packing Bound . . . . .	126
11.3.1 One-Shot Converse Bound (Hypothesis Testing Reduction) . . . . .	127
11.3.2 Chebyshev's Type Converse Bound . . . . .	127
11.3.3 A Sharp Converse Bound . . . . .	130
11.3.4 Uniform Continuity . . . . .	133
11.3.5 Proofs of Main Result, Theorem 11.1 and Corollary 11.1 . . . . .	137
11.4 Symmetric Classical-Quantum Channels . . . . .	139
<b>12 Moderate Deviation Analysis (Channel Coding)</b>	<b>142</b>
12.1 Proof of Achievability, Theorem 12.1 . . . . .	143
12.2 Proof of Optimality, Theorem 12.2 . . . . .	144
12.3 Asymptotic Expansions of Error-Exponent around Capacity . . . . .	148
<b>13 Conclusions and Open problems</b>	<b>152</b>
13.1 Open Problems . . . . .	153
13.1.1 Properties of Error Exponent Functions and Auxiliary Functions . . . . .	153
13.1.2 Achievability: Random Coding Bound . . . . .	154
13.1.3 Optimality: Sphere-Packing Bound . . . . .	155
13.1.4 Moderate Deviation Analysis . . . . .	156



# List of Figures

1.1	We are given $n$ copies of a classical source $X$ which is correlated with a quantum system $B$ . We compress the source into an index set $\mathcal{I}_n$ via the encoder $\mathcal{E}_n$ , and then perform a decoding via $\mathcal{D}_n$ which has access to the side information $\rho_{B^n}$ . This yields the output $\hat{X}_n$ with associated alphabets $\mathcal{X}^n$ . The decoder $\mathcal{D}_n$ here is a family of positive operator-valued measurement (POVM) $\{\Pi_{X^n}^{(w^n)}\}_{w^n \in \mathcal{I}^n}$ . The red-dotted lines indicate classical information, while the blue-solid lines stand for quantum information. . . . .	7
1.2	We encode the (classical) message $m$ to an $n$ -blocklength sequence $x^n$ . Then, input sequence will be mapped to an $n$ -product channel output state $W_{\mathbf{x}^n}^{\otimes n}$ . Lastly, the decoder, a positive operator-valued measurement (POVM), measures the channel output state to obtain the estimated message $\hat{m}$ . The red-dotted lines indicate classical information, while the blue-solid lines stand for quantum information. . . . .	8
1.3	Structure of the thesis. . . . .	12
9.1	This figure illustrates three cases of the strong sphere-packing exponent $E_{\text{sp}}(R)$ over $R \geq 0$ . In the first case $0 = R_\infty < C_W$ (the left figure), $E_{\text{sp}}(R)$ is only infinite at $R = 0$ and finite otherwise. In the second case $0 < R_\infty < C_W$ (the central figure), $E_{\text{sp}}(R) = +\infty$ for $R < R_\infty$ , and $E_{\text{sp}}(R) < +\infty$ for $R \geq R_\infty$ . In the third case $0 < R_\infty = C_W$ (the right figure), $E_{\text{sp}}(R) = +\infty$ for $R < C_W$ , and $E_{\text{sp}}(R) = 0$ for $R \geq C_W$ . Without loss of generality, we assume $R_\infty < C_W$ to exclude the last case throughout this paper. . . . .	105
13.1	Sphere-packing exponents in two quantum information processing protocols. . . . .	153

# List of Tables

1.1 This table compares the asymptotic error behaviors of quantum hypothesis testing and classical-quantum channel coding in three error probability regimes: (i) large error (central limit theorem), (ii) medium error (moderate deviation principle), and (iii) small error (large deviation principle). The quantity $S_n$ denotes the sum of $n$ independent and identically distributed random variables with zero mean and variance $v$ . The exponent $\Lambda^*$ is the Legendre-Fenchel transform of the normalized cumulant generating function of $S_n$ [1]. The error $\widehat{\alpha}_{\exp\{-nr\}}$ is defined as the minimum type-I error with the type-II error smaller than $\exp\{-nr\}$ . The quantities $D$ and $V$ in the hypothesis testing column denote the quantum relative entropy and the relative entropy variance, respectively. The optimal error probability with blocklength $n$ and rate $R$ is denoted by $\epsilon^*(n, R)$ . The quantities $C$ and $V$ in the channel coding column indicate the channel capacity and the channel dispersion, respectively. The sequence $(a_n)_{n \in \mathbb{N}}$ satisfies Eq. (1.7). The quantity $E(R)$ is the reliability function of the classical-quantum channel [2], and has not been fully characterized yet. . . . .	5
11.1 Different sphere-packing bounds are compared by (i) the bound is finite blocklength or asymptotical; (ii) whether or not they are dependent on the constant composition codes; (iii) & (iv) the asymptotics of $f(n)$ and $g(n)$ ; (v) the corresponding c-q generalizations. The parameter $t$ in rows (e) and (f) is some value in the range $t > 1/2$ ; and (vi) whether their error exponent expressions for c-q channels are in the strong form (Eq. (1.4)) or weak form (Eq. (12.51)). . . . .	121
13.1 The comparison of the error exponent analysis for Slepian-Wolf coding with quantum side information and classical-quantum channel coding. We note that we only obtained suboptimal achievability results (i.e. with the exponent $E_r^\downarrow(R)$ instead of $E_r(R)$ ). . . . .	152

# Chapter 1

## Introduction

Information processing and transmission under the framework of quantum mechanics has emerged as a promising technology in the forthcoming future. For example, Bennett and Brassard [3, 4] proposed a quantum key distribution protocol, which provides us a secure way for sharing secret keys between two parties. The task of quantum teleportation is to noiselessly transfer a quantum state to a remote user [5] and it has become a key ingredient of quantum computation [6, 7]. In view of the latest and most significant achievements of communicating quantumly from a launched satellite with base stations [8], it is generally believed that the laboratory testing of novel quantum communication experiments will soon be complete.

To practically implement such quantum information processing (QIP) technologies, it would require universal quantum computation as the principle component (e.g. to perform the decoding strategies). Nevertheless, the state-of-the-art quantum computers, at least for the near future, is limited to around 50 qubits. Thus, evaluating how well a QIP system behaves in practical domains only with finite resources becomes a pressing matter [9, 10]. The goal of this thesis is to investigate two fundamental QIP tasks and characterize their performance benchmarks, providing invaluable guidance to the design of the next-generation quantum technology.

In this thesis, we are interested in the QIP protocols that benefits and advances current information processing systems. Namely, we study the problems of (1) *information storage with a quantum helper*, and (2) *information transmission over a quantum channel*. Due to the probabilistic nature of quantum mechanics, the processing errors are inevitable. Therefore, our ultimate goal is to provide an accurate error analysis for these QIP protocols. In Section 1.1, we give the backgrounds and literature review of this research topic. In Section 1.2, we introduce the mathematical formalisms of the studied QIP protocols. Our contributions are listed in Section 1.3. Lastly, we illustrate the structure of the thesis in Section 1.4.

### 1.1 Backgrounds

One of the core purposes in information theory is to protect the information when compressing and transmitting. In Shannon's seminal work [11], it was shown that the reliable<sup>1</sup> communication over a channel is possible, provided that the transmission rate is below the *channel capacity*  $C$ , and an

---

<sup>1</sup>Here, by *reliable*, we mean that the error probability of recovering information approaches zero when more powerful coding strategy is employed, e.g. the size or the blocklength of the codes tends to infinity.

arbitrary large coding scheme is given. On the other hand, Slepian and Wolf [12] studied a source compression scenario with an assistance of the side information. Let  $X$  denote the random variable of the source and  $Y$  be that of the side information. They showed that the reliable source recovery is feasible as long as the compression rate is above the *conditional entropy*  $H(X|Y)$  and an arbitrary large block code is provided.

Therefore, investigating the interplay between the compression/transmission rate, coding blocklength and the probability of error is one of the fundamental problems in information theory. Based on different ranges of the error probability, analysis of the information processing performance roughly falls into the following three categories: (i) *large error probability* or *non-vanishing error probability* regime; (ii) *medium error probability* regime; and (iii) *small error probability* regime.

In the non-vanishing error probability regime, the largest code rate, given a coding length  $n$  and an error probability no more than  $\epsilon$ , is one of the main research focuses. Strassen [13] first demonstrated that the maximum size of an  $n$ -blocklength code through a discrete memoryless channel (DMC)  $\mathcal{W}$ , denoted by  $M^*(\mathcal{W}^n, \epsilon)$ , yields an asymptotic expansion to the order  $\sqrt{n}$ , and hence this is called *second-order analysis*:

$$\log M^*(\mathcal{W}^n, \epsilon) = nC + \sqrt{nV} \Phi^{-1}(\epsilon) + O(\log n), \quad (1.1)$$

where the quantities  $C$  and  $V$  denote the capacity [11] and the dispersion [14] of the channel, and  $\Phi$  is the cumulative distribution function of a standard normal random variable. Equivalently, Eq. (1.1) yields the following relationship between the optimal decoding error with blocklength  $n$  and rate  $C - A/\sqrt{n}$  for any constant  $A$ :

$$\lim_{n \rightarrow +\infty} \epsilon^*(n, C - A/\sqrt{n}) = \Phi\left(\frac{A}{\sqrt{V}}\right). \quad (1.2)$$

Strassen's result relied on the *Gaussian approximation* or the *central limit theorem (CLT)*, and is also called the *small deviation regime*. His work was latter refined by Hayashi [15], Polyanskiy *et al.* [14], and extended to quantum channels [16, 17, 18, 9]. The results for higher-order asymptotics are referred to Refs. [19, 20, 21].

In the *small error probability* regime, Shannon [22] introduced the *reliability function*  $E(R)$  as the optimal error exponent:

$$\lim_{n \rightarrow +\infty} -\frac{1}{n} \log \epsilon^*(n, R) = E(R), \quad (1.3)$$

for rate  $R$  below the channel capacity<sup>2</sup>  $C$ . The quantity  $E(R)$  then provides a measure of how rapidly the error probability approaches zero with an increase in blocklength. This characterization of the reliability function is hence called the *reliability function analysis* or the *error exponent analysis*. This seminal work entails the analysis of a broad class of channels [24, 23, 25, 26, 27, 28]. The exponential decay of the error probability in Eq. (1.3) is a consequence of the *large deviation principle (LDP)* [1]. In summary, the errors in Eqs. (1.2) and (1.3), respectively, fall into the CLT regime and large-deviation regime.

---

<sup>2</sup>To the best of our knowledge, the reliability function  $E(R)$  is only known in the high rate regime, i.e. at rates above a *critical rate* (see e.g. [23, p. 160]).

Given a classical channel, lower bounds for the reliability function (termed *achievability*), can be established by random coding arguments [29, 24, 30, 23]. However, upper bounds (also called *optimality*) require different techniques since the code-dependent bounds on the error probability need to be optimized over all codebooks. The first result—the *sphere-packing bound*  $E(R) \leq E_{\text{sp}}(R)$ —was developed by Shannon, Gallager, and Berlekamp [31]. The *sphere-packing exponent*  $E_{\text{sp}}(R)$  is defined as

$$E_{\text{sp}}(R) := \sup_{s \geq 0} \left\{ \max_P E_0(s, P) - sR \right\}, \quad (1.4)$$

where  $P$  is maximized over all probability distributions on the input alphabet, and  $E_0(s, P)$  is the *auxiliary function* or *Gallager's function* [30]. Unlike Shannon-Gallager-Berlekamp's technique which relates channel coding to binary hypothesis testing, Haroutunian [32, 26] employed a combinatorial method and obtained an upper bound for the reliability function in terms of the following expression

$$\tilde{E}_{\text{sp}}(R) := \max_P \min_{\bar{\mathcal{W}}} \{ D(\bar{\mathcal{W}} \parallel \mathcal{W}|P) : I(P, \bar{\mathcal{W}}) \leq R \}, \quad (1.5)$$

where  $\bar{\mathcal{W}}$  is minimized over all dummy channels with the same output alphabet as  $\mathcal{W}$ ,  $D(\bar{\mathcal{W}} \parallel \mathcal{W}|P)$  is the conditional relative entropy between the dummy channel  $\bar{\mathcal{W}}$  and the true channel  $\mathcal{W}$ , and  $I(P, \bar{\mathcal{W}})$  is the mutual information of the channel  $\bar{\mathcal{W}}$  (the detailed definitions are given in Chapter 3). It was later realized that the two quantities in Eqs. (1.4) and (1.5) are equivalent: they are related by convex program duality [33, 34, 27]. Therefore, these two expressions, Eqs. (1.4) or (1.5), are both called sphere-packing exponents.

Error exponent analysis in classical-quantum (c-q) channels is more challenging because of the noncommutative nature of quantum mechanics. Burnashev and Holevo [35] introduced a quantum version of the auxiliary function [2, 36] and initialized the study of reliability functions in c-q channels. However, the random coding bound (i.e. achievability) for c-q channels is still unsolved. Winter [37] derived a sphere-packing bound (i.e. optimality) for c-q channels in the form of  $\tilde{E}_{\text{sp}}(R)$  in Eq. (1.5), generalizing Haroutunian's idea [32]. Dalai [38] employed Shannon-Gallager-Berlekamp's approach [31] to establish a sphere-packing bound with Gallager's exponent in Eq. (1.4). In the follow-up work [39], Dalai and Winter pointed out that these two exponents are not equal in c-q channels. We remark that both Dalai and Winter's results are asymptotic and not finite blocklength.

The Slepian-Wolf coding with quantum side information (QSI) was studied by Devetak and Winter [40]. They generalized Slepian and Wolf's result [12] to the quantum case: the optimal probability of error asymptotically vanishes as the compression rate is above the *quantum conditional entropy*  $H(X|B)_\rho$ , where  $B$  denotes the quantum system. Similar to the role of channel capacity in channel coding, we term  $H(X|B)_\rho$  the *Slepian-Wolf limit*. The non-vanishing error probability regime was later studied by Renes and Renner [41], and Tomamichel and Hayashi [16]. A second-order asymptotics similar Eq. (1.1) was established.

The most paragraph of this thesis will focus on the error exponent analysis for both Slepian-Wolf coding with QSI and classical-quantum channel coding. We especially focus on the finite blocklength characterizations of the optimal error probability. In Chapters 6 and 7, we establish finite blocklength bounds for Slepian-Wolf coding with QSI. In Chapters 10 and 11, we review the best-to-date achievability bound for c-q channel coding, and prove a tight sphere-packing bound in finite blocklengths.

The study of the medium error probability regime was pioneered by Altuğ and Wagner [42, 43]. They investigated the asymptotic behavior of the optimal decoding error when the coding rate converges to capacity sufficiently slowly. Specifically, they studied under which conditions the error is asymptotically equal to<sup>3</sup>

$$\epsilon^*(n, C - a_n) \sim \Phi\left(\frac{\sqrt{n}a_n}{\sqrt{v}}\right) \sim e^{-\frac{na_n^2}{2v}}, \quad (1.6)$$

where the sequence of positive numbers  $(a_n)_{n \in \mathbb{N}}$  satisfies

$$\begin{aligned} \text{(i)} \quad & \lim_{n \rightarrow +\infty} a_n = 0; \\ \text{(ii)} \quad & \lim_{n \rightarrow +\infty} a_n \sqrt{n} = +\infty. \end{aligned} \quad (1.7)$$

Evidently, the transmission rate in Eq. (1.6) approaches capacity slower than  $1/\sqrt{n}$ . A DMC with errors satisfying Eq. (1.6) possesses a *moderate deviation property (MDP)* [1, Section 3.7], and hence it is also called the *moderate deviation* regime. The constant  $v$  in Eq. (1.6) equals the channel dispersion  $V$  when both the limit in Eq. (1.2) and MDP hold [44, Theorem 1]. We refer the interested readers to Refs. [44, 45, 46, 47, 43] for further results in classical channel coding.

As an application of our established error exponent bounds, we extend our techniques to the moderate deviation regime. In Chapters 8 and 12, we demonstrate that the optimal error probability of the both two QIP tasks vanishes when the compression rate approaches the Slepian-Wolf limit and the transmission rate approaches the channel capacity, respectively. Specifically, we show that

$$\lim_{n \rightarrow +\infty} \frac{\log \epsilon^*(n, H(X|B)_\rho + a_n)}{na_n^2} = -\frac{1}{2V}; \quad (1.8)$$

$$\lim_{n \rightarrow +\infty} \frac{\log \epsilon^*(n, C - a_n)}{na_n^2} = -\frac{1}{2V}, \quad (1.9)$$

where  $(a_n)_{n \in \mathbb{N}}$  is any sequence satisfying Eq. (1.7).

We remark that these error probability regime described above—(i), (ii), and (iii)—all have theoretical significance and practical value. The non-vanishing error probability regime, (i), has been relatively well studied in the quantum scenario, while the small and medium error probability, (ii) and (iii), are rarely explored, which is the ultimate goal and purpose of this thesis. We summarize the error behaviors in these three regimes in Table 1.1.

Our methodology contains a varieties of matrix inequalities and matrix calculus. Moreover, we employ the sharp concentration inequalities—Bahadur-Ranga Rao’s concentration inequality [48] and Chaganty-Sethuraman’s concentration inequality [49]—in strong large deviation theory to establish our finite blocklength bounds. We collect the mathematical tools of matrix analysis and large deviation theory in Chapter 2.

## 1.2 Quantum Information Processing Protocols

In the following, we introduce two quantum information processing protocols studied in this thesis—(1) information storage with a quantum helper, and (2) information transmission over a quantum channel.

---

<sup>3</sup>We denote  $f_n \sim g_n$  if and only if  $\lim_{n \rightarrow +\infty} \frac{f_n}{g_n} = 1$ .

Error Regimes	Concentration Phenomena	Hypothesis Testing	Source \ Channel Coding
Large Error	CLT: $\Pr(S_n \geq \sqrt{n}x) \rightarrow 1 - \Phi\left(\frac{x}{\sqrt{v}}\right)$	$\widehat{\alpha}_{\exp\{-n[D - \frac{A}{\sqrt{n}}]\}} \rightarrow \Phi\left(\frac{A}{\sqrt{V}}\right)$	$\varepsilon^*\left(n, H + \frac{A}{\sqrt{n}}\right) \rightarrow \Phi\left(\frac{A}{\sqrt{V}}\right)$
			$\varepsilon^*\left(n, C - \frac{A}{\sqrt{n}}\right) \rightarrow \Phi\left(\frac{A}{\sqrt{V}}\right)$
Medium Error	MDP: $\Pr(S_n \geq na_n x) = e^{-\frac{na_n^2}{2v}x + o(na_n^2)}$	$\widehat{\alpha}_{\exp\{-n[D - a_n]\}} = e^{-\frac{na_n^2}{2V} + o(na_n^2)}$	$\varepsilon^*(n, H + a_n) = e^{-\frac{na_n^2}{2V} + o(na_n^2)}$
			$\varepsilon^*(n, C - a_n) = e^{-\frac{na_n^2}{2V} + o(na_n^2)}$
Small Error	LDP: $\Pr(S_n \geq nx) = e^{-n\Lambda^*(x) + o(n)}$	$\widehat{\alpha}_{\exp\{-nr\}} = e^{-n\phi(r) + o(n)}$	$\varepsilon^*(n, R) = e^{-nE(R) + o(n)}$

Table 1.1: This table compares the asymptotic error behaviors of quantum hypothesis testing and classical-quantum channel coding in three error probability regimes: (i) large error (central limit theorem), (ii) medium error (moderate deviation principle), and (iii) small error (large deviation principle). The quantity  $S_n$  denotes the sum of  $n$  independent and identically distributed random variables with zero mean and variance  $v$ . The exponent  $\Lambda^*$  is the Legendre-Fenchel transform of the normalized cumulant generating function of  $S_n$  [1]. The error  $\widehat{\alpha}_{\exp\{-nr\}}$  is defined as the minimum type-I error with the type-II error smaller than  $\exp\{-nr\}$ . The quantities  $D$  and  $V$  in the hypothesis testing column denote the quantum relative entropy and the relative entropy variance, respectively. The optimal error probability with blocklength  $n$  and rate  $R$  is denoted by  $\varepsilon^*(n, R)$ . The quantities  $C$  and  $V$  in the channel coding column indicate the channel capacity and the channel dispersion, respectively. The sequence  $(a_n)_{n \in \mathbb{N}}$  satisfies Eq. (1.7). The quantity  $E(R)$  is the reliability function of the classical-quantum channel [2], and has not been fully characterized yet.

The interested readers can refer to the books [7, 50] for more detailed and various quantum information processing protocols.

### 1.2.1 Information Storage with a Quantum Helper (Source Coding)

We consider a source of classical information which is produced with some quantum side information. That is, for some finite alphabet  $\mathcal{X}$ , with some probability  $p(x)$ , the source produces the classical information  $x \in \mathcal{X}$ , along with a quantum state  $\rho_B^x$  on a finite-dimensional Hilbert space  $\mathcal{H}_B$ . Such a source is characterized by a classical-quantum (c-q) state

$$\rho_{XB} := \sum_{x \in \mathcal{X}} p(x) |x\rangle\langle x| \otimes \rho_B^x. \quad (1.10)$$

where  $\{|x\rangle\}_{x \in \mathcal{X}}$  is an orthonormal basis of a Hilbert space  $\mathcal{H}_X$  of dimension  $|\mathcal{X}|$ . We note that the quantum state  $\rho_B$  on a finite Hilbert space  $\mathcal{H}_B$  can be characterized by a *density operator* (or *density matrix*) such that  $\rho_B$  is positive semidefinite  $\rho_B \geq 0$  and has unit trace  $\text{Tr}[\rho_B]$  [7, 51, 50].

The task is to compress the classical information produced by the source to a smaller index set  $\mathcal{I}$  and to later decompress the information with the assistance of the quantum side information as a helper. For convenience, we also term this task *Slepian-Wolf coding with quantum side information* or shorthand *CQSW*.

A deterministic encoder is map  $\mathcal{E} : \mathcal{X} \rightarrow \mathcal{I}$  where the alphabet  $\mathcal{I}$  has size  $|\mathcal{I}|$ . A decoder, denoted by  $\mathcal{D}$ , receives the compressed symbol  $\mathcal{E}(x)$  along with the quantum state  $\rho_B^x$ , and produces  $\hat{x} \in \mathcal{X}$ , aiming to achieve  $\hat{x} = x$ .

Thus, the decoding is a map

$$\mathcal{I} \times \mathcal{S}(B) \ni (w, \rho_B) \rightarrow \mathcal{D}(w, \rho_B) \in \mathcal{X}. \quad (1.11)$$

If we fix the first argument as  $w \in \mathcal{W}$ , we have that the decoder  $\mathcal{D}(w, \cdot)$  is a map from  $\mathcal{S}(B) \rightarrow \mathcal{X}$ , i.e. is a positive operator-valued measurement (POVM), and we denote by  $\mathcal{S}(B)$  the set of quantum states on Hilbert space  $\mathcal{H}_B$ . Thus, we can represent the decoding by a collection of POVMs  $\{\mathcal{P}_w\}_{w \in \mathcal{W}}$ , where  $\mathcal{P}_w = \{\Pi_{\hat{x}}^{(w)}\}_{\hat{x} \in \mathcal{X}}$  with  $\Pi_{\hat{x}}^{(w)} \geq 0$  and  $\sum_{\hat{x} \in \mathcal{X}} \Pi_{\hat{x}}^{(w)} = \mathbf{1}$ , for each  $w \in \mathcal{I}$ . That is, if the message  $x$  is sent, the decoder receives  $\mathcal{E}(x)$ , and measures the state  $\rho_B^x$  with the POVM  $\{\Pi_{\hat{x}}^{(\mathcal{E}(x))}\}_{\hat{x} \in \mathcal{X}}$ .

A random encoding  $F$  from  $\mathcal{X}$  to  $\mathcal{W}$  is one which maps  $x$  to  $w$  with some probability  $p(w|x)$ . We can see the random encoding therefore as applying the deterministic encoding

$$(x_1, \dots, x_{|\mathcal{X}|}) \mapsto (i_1, \dots, i_{|\mathcal{X}|}) \quad (1.12)$$

with probability  $p(i_1|x_1)p(i_2|x_2)\cdots p(i_{|\mathcal{X}|}|x_{|\mathcal{X}|})$ . Let us write  $\mathcal{F} =: \{\mathcal{E}_j : j = 1, \dots, |\mathcal{F}|\}$  for the collection of deterministic encoders. Then a random encoding  $\mathcal{F}$  applies  $\mathcal{E}_j$  with some probability  $P_j$ .

An  $(1, R)$ -Slepian-Wolf code for the c-q state  $\rho_{XB}$  is an ordered pair  $\mathcal{C} = (\mathcal{F}, \mathcal{D})$  consisting of a (possibly random) encoder  $\mathcal{F}$  and decoder  $\mathcal{D}$ , such that the alphabet  $\mathcal{I}$  has size  $R = \log |\mathcal{W}|$ .  $R$  is called the *compression rate* of the code  $\mathcal{C}$ . Using the above notation, the *probability of success* of  $\mathcal{C}$  is given by

$$P_s(\mathcal{C}) = \sum_{x \in \mathcal{X}} p(x) \sum_{j=1}^{|\mathcal{F}|} P_j \text{Tr}[\rho_B^x \Pi_x^{(\mathcal{E}_j(x))}] \quad (1.13)$$

where  $\mathcal{C} := (\mathcal{F}, \mathcal{D})$  for the possibly random encoding  $\mathcal{F}$  which gives the deterministic encoding  $\mathcal{E}_j$  with probability  $P_j$ , and decoding  $\mathcal{D}$  which is defined via the collection of POVMs  $\{\mathcal{P}_w\}_{w \in \mathcal{W}}$ , and  $\mathcal{P}_w = \{\Pi_x^{(w)}\}_{x \in \mathcal{X}}$ . We may likewise define the probability of error of the code  $\mathcal{C}$  by

$$P_e(\mathcal{C}) := 1 - P_s(\mathcal{C}) \quad (1.14)$$

In the following, we define the *optimal one-shot compression rate*:

$$R^*(1, \varepsilon) = \inf \{R : \text{for some } R' \leq R, \exists (1, R')\text{-Slepian Wolf code } \mathcal{C} \text{ for } \rho_{XB} \text{ s.t. } P_e(\mathcal{C}) \leq \varepsilon\}, \quad (1.15)$$

Here, ‘1’ means that the code is used only one time, and thus we called “one-shot”. Similarly, the *optimal one-shot probability of error* for  $\rho_{XB}$  is defined as:

$$\varepsilon^*(1, R) := \inf \{P_e(\mathcal{C}) : \mathcal{C} \text{ is an } (1, R')\text{-Slepian Wolf code for } \rho_{XB} \text{ for some } R' \leq R\}. \quad (1.16)$$

The Slepian-Wolf coding can be easily applied to the  $n$ -shot case when the underlying c-q state  $\rho_{XB} \in \mathcal{S}(XB)$  has an independent and identically distributed extension  $\rho_{X^n B^n} = \rho_{XB}^{\otimes n}$ . In this case, an  $(n, R)$ -Slepian Wolf code for the state  $\rho_{XB}$  is defined as a  $(1, nR)$ -Slepian Wolf code for the state  $\rho_{XB}^{\otimes n}$ . We define the *optimal  $n$ -shot probability of error* for  $\rho_{XB}$  as

$$\varepsilon^*(n, R) := \inf \{P_e(\mathcal{C}) : \mathcal{C} \text{ is an } (n, R')\text{-Slepian Wolf code for } \rho_{XB} \text{ for some } R' \leq R\}, \quad (1.17)$$

and likewise the *optimal n-shot compression rate* for  $\rho_{XB}$  as

$$R^*(n, \varepsilon) = \inf \{R : \text{for some } R' \leq R, \exists (n, R')\text{-Slepian Wolf code } \mathcal{C} \text{ for } \rho_{XB} \text{ s.t. } P_e(\mathcal{C}) \leq \varepsilon\}. \quad (1.18)$$

We illustrate the protocol of Slepian-Wolf coding with QSI Figure 1.1 below.

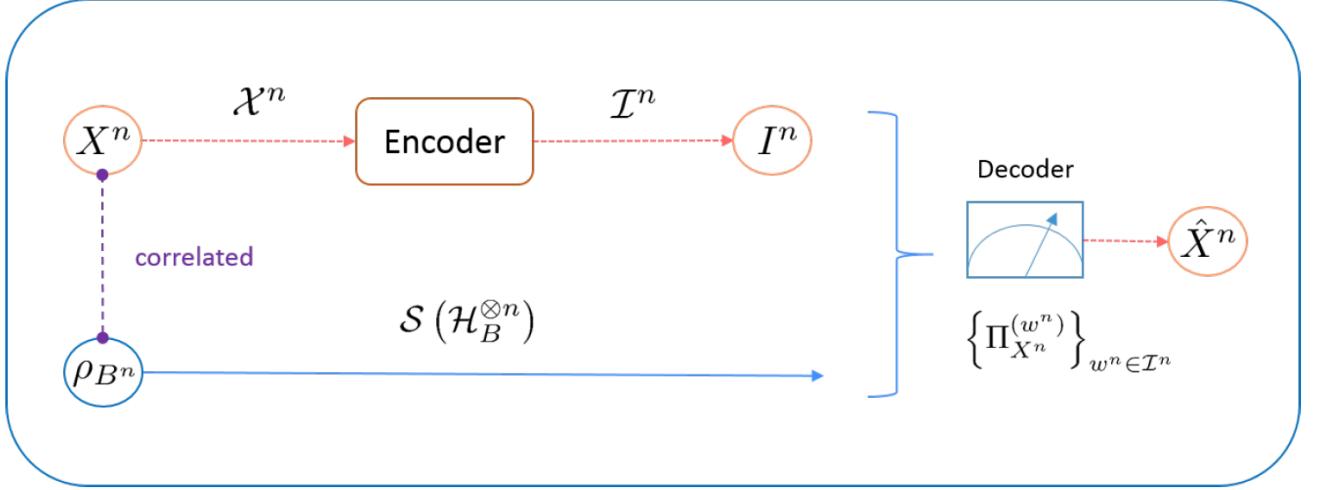


Figure 1.1: We are given  $n$  copies of a classical source  $X$  which is correlated with a quantum system  $B$ . We compress the source into an index set  $\mathcal{I}_n$  via the encoder  $\mathcal{E}_n$ , and then perform a decoding via  $\mathcal{D}_n$  which has access to the side information  $\rho_{B^n}$ . This yields the output  $\hat{X}_n$  with associated alphabets  $\mathcal{X}^n$ . The decoder  $\mathcal{D}_n$  here is a family of positive operator-valued measurement (POVM)  $\{\Pi_{X^n}^{(w^n)}\}_{w^n \in \mathcal{I}^n}$ . The red-dotted lines indicate classical information, while the blue-solid lines stand for quantum information.

### 1.2.2 Information Transmission over a Quantum Channel (Channel Coding)

Let  $\mathcal{M}$  be a finite alphabetical set with size  $M = |\mathcal{M}|$ . An ( $n$ -blocklength) *encoder* is a map  $\mathcal{F}_n : \mathcal{M} \rightarrow \mathcal{X}^n$  that encodes each message  $m \in \mathcal{M}$  to a codeword  $\mathbf{x}^n(m) := x_1(m)x_2(m)\dots x_n(m) \in \mathcal{X}^n$ . Here, we assume that the input alphabet  $\mathcal{X}$  is finite. The codeword  $\mathbf{x}^n(m)$  is then mapped to a state  $\rho_{\mathbf{x}^n(m)}^n$  in the  $n$ -fold of Hilbert space  $\mathcal{H}$ . The *decoder* is described by a POVM  $\Pi_n = \{\Pi_{n,1}, \dots, \Pi_{n,M}\}$  on  $\mathcal{H}^{\otimes n}$ , where  $\Pi_{n,i} \geq 0$  and  $\sum_{i=1}^M \Pi_{n,i} = \mathbb{1}$ . Throughout this thesis, we assume that the channel output state  $\rho_{\mathbf{x}^n(m)}^n$  has a tensor product structure. That is,  $\rho_{\mathbf{x}^n(m)}^n$  can be presented as

$$W_{\mathbf{x}^n(m)}^{\otimes n} = W_{x_1(m)} \otimes W_{x_2(m)} \otimes \dots \otimes W_{x_n(m)} \in \mathcal{S}(\mathcal{H}^{\otimes n}). \quad (1.19)$$

Then, this protocol is equivalent to a c-q channel coding with a c-q channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$ . We leave the scenarios of classical message communications over general quantum channels as future work; see also the open problems in Chapter 13.

The pair  $(\mathcal{F}_n, \Pi_n) =: \mathcal{C}_n$  is called a *code* with *coding rate* (or called *transmission rate*)  $R = \frac{1}{n} \log |\mathcal{C}_n| = \frac{1}{n} \log M$ . The error probability of sending a message  $m$  with the code  $\mathcal{C}_n$  is given by the Born rule  $\varepsilon_m(\mathcal{C}_n) := 1 - \text{Tr}(\Pi_{n,m} W_{\mathbf{x}^n(m)}^{\otimes n})$ . We use  $\varepsilon_{\max}(\mathcal{C}_n) = \max_{m \in \mathcal{M}} \varepsilon_m(\mathcal{C}_n)$  and  $\bar{\varepsilon}(\mathcal{C}_n) = \frac{1}{M} \sum_{m \in \mathcal{M}} \varepsilon_m(\mathcal{C}_n)$  to denote the *maximal* error probability and the *average* error probability, respec-

tively. Given a sequence  $\mathbf{x}^n \in \mathcal{X}^n$ , we denote by

$$P_{\mathbf{x}^n}(x) := \frac{1}{n} \sum_{i=1}^n \mathbf{1}\{x = x_i\} \quad (1.20)$$

the empirical distribution of  $\mathbf{x}^n$ , where  $x_i$  is the  $i$ -th position of  $\mathbf{x}^n$ . A constant composition code with a composition  $P_{\mathbf{x}^n}$  refers to a codebook whose codewords all have the same distribution  $P_{\mathbf{x}^n}$ .

Denote by  $\varepsilon^*(n, R)$  the smallest average probability of error among all the coding strategies with a blocklength  $n$  and coding rate  $R$ . Our goal in this thesis is then to characterize  $\varepsilon^*(n, R)$  as a function of  $(n, R)$ ; see Part II. Figure 1.2 below depicts the protocol of c-q channel coding.

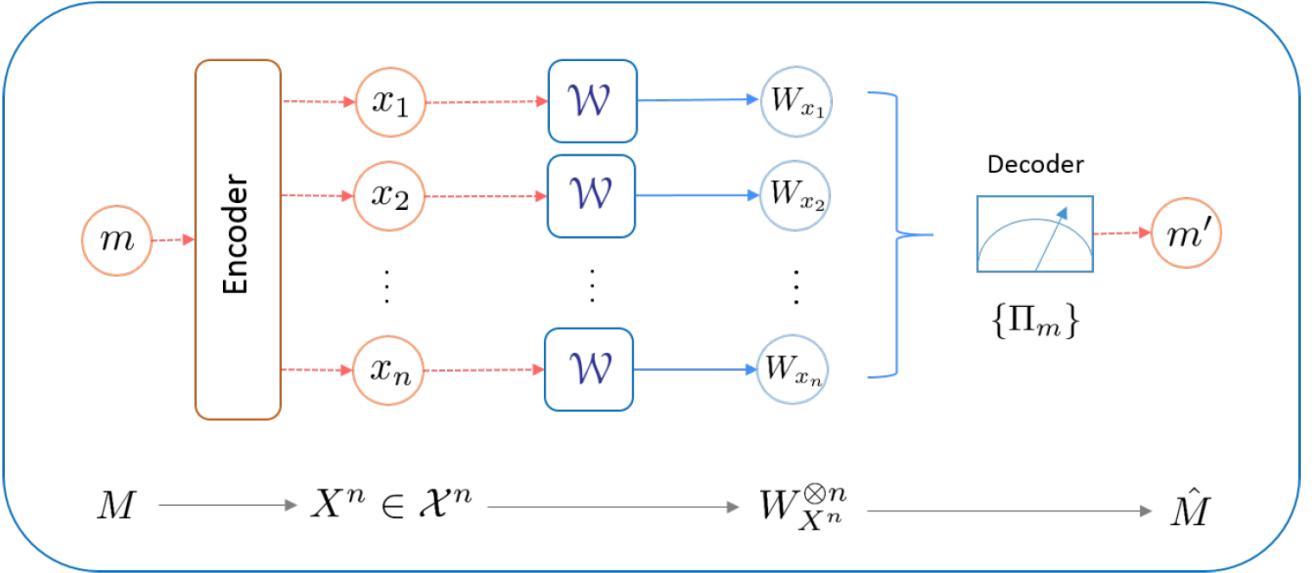


Figure 1.2: We encode the (classical) message  $m$  to an  $n$ -blocklength sequence  $x^n$ . Then, input sequence will be mapped to an  $n$ -product channel output state  $W_{\mathbf{x}^n}^{\otimes n}$ . Lastly, the decoder, a positive operator-valued measurement (POVM), measures the channel output state to obtain the estimated message  $\hat{m}$ . The red-dotted lines indicate classical information, while the blue-solid lines stand for quantum information.

### 1.3 Main Contributions

Although the aim of this thesis is to give an exposition to the current development of the error exponent analysis in quantum information theory, we list our contributions in the following. The results can also be found in the papers [36, 28, 52, 53, 54].

- (I) We prove major properties of error exponent functions and auxiliary functions for both Slepian-Wolf coding with QSI (Chapter 5) and classical-quantum (c-q) channel coding (Chapter 9). More specifically,
  - (a) We show that the error exponent functions introduced by Blahut [33, 25], Haroutunian [32, 26], and Csiszár-Körner [55, 56, 27] have variational representations (Theorems 5.1 and 9.1). These representations are equivalent to the Gallager's expressions [30, 23, 57] in the classical case. However, in the quantum case, they are expressed by the log-Euclidean Rényi divergence [58, 59], while Gallager's expressions correspond to Petz's Rényi divergence [60]. As a consequence of the Golden-Thompson inequality [61, 62], the variational representations are weaker than Gallager's expressions in the optimality part, i.e. the converse (see Theorem 9.1). Nevertheless, they have applications in the strong converse domain<sup>4</sup> [59, 53] and the moderate deviation analysis (see Section 12.2).
  - (b) Since the error exponent functions are the *Lengendre-Fenchel transform* of the auxiliary functions, the properties of the auxiliary functions immediately characterize that of the error exponent functions. We prove the concavity properties, which solves an open problem addressed by Holevo [2], and the first-order/second-order derivatives (Propositions 5.1, 5.2, 9.1, 9.2, and 9.3).
  - (c) We prove the continuity and the saddle-point property of the error exponent functions, which is one of the crucial steps of establishing finite blocklength results (Propositions 5.3 and 9.5).
  - (d) An asymptotic expansion of error exponent functions when the compression rate (resp. transmission rate) approaches the Slepian-Wolf limit (resp. channel capacity) is shown in Propositions 8.1 and 12.2. This property results in the moderate deviation analysis (see Chapters 8 and 12).
- (II) We establish a finite blocklength achievability bound of the Slepian-Wolf coding with QSI for both i.i.d. sources and type-dependent sources (Theorems 6.1 and 6.2), which has the following applications.
  - (a) We recover Devetak and Winter's asymptotic achievability result, i.e. the source compression is reliable for any compression rate larger than the Slepian-Wolf limit.
  - (b) The established result shows how fast the error probability exponentially decays for both i.i.d. sources and type-dependent sources.
  - (c) Our result implies achievability of the moderate deviation analysis (Theorem 8.1).

---

<sup>4</sup>The strong converse domain means that the compression rate (resp. transmission rate) is smaller (resp. larger) than the Slepian-Wolf limit (resp. channel capacity). In this case, the optimal probability of success exponentially decays [37, 63, 64, 58, 59, 65, 53]. This thesis does not include contents of the strong converse part.

- (d) The employed techniques provide proof ingredients in the achievability of strong converse domain and the joint source-channel coding with QSI [53, 54, 66].
- (III) We establish a finite blocklength achievability bound of c-q channel coding with constant composition codes (Theorem 10.2), which has the following features.
- (a) The established result is the strongest achievability bound to the best of our knowledge.
  - (b) Via an operational duality proved in [54], the result for channel coding (Theorem 10.2) yields the achievability bound for source coding (Theorem 6.2).
  - (c) Our method might have future applications of determining the optimal error exponent of constant composition codes in c-q channel coding and joint source-channel coding with QSI.
- (IV) For the optimality part in both tasks, we establish a series of following results.
- (a) We give a sharp converse Hoeffding bound (see Theorem 4.4 and Corollary 4.1) for binary quantum hypothesis testing, which is the main ingredient for the finite blocklength error exponent analysis and moderate deviation analysis in quantum information theory;
  - (b) By proving an one-shot converse bound to relate the source coding problem to hypothesis testing (Proposition 7.1), we employ the above sharp converse Hoeffding bound to show the finite blocklength sphere-packing bound of Slepian-Wolf coding with QSI (Theorem 7.1).
  - (c) With an one-shot converse bound reducing the channel coding problem to hypothesis testing (Proposition 11.3), we prove the finite blocklength sphere-packing bound of c-q channel coding. Under the assumption of using constant composition codes, i.e. the composition for each codeword in the codebook is the same, we derive the exact prefactor (see Theorem 11.1). For general codes, the obtained prefactor is significantly improved from the previous result of subexponential [38] to polynomial (see Corollary 11.1). We remark that the exact prefactor for general codes remains open even in the classical case.
- (V) For the moderate deviation regime, we discuss the trade-offs between the rate, optimal probability of error, and the blocklength for both the Slepian-Wolf coding with QSI and c-q channel coding.
- (a) When the exponential decaying rate of the type-II error in quantum hypothesis testing approaches the relative entropy from below with the speed not faster than  $O(1/\sqrt{n})$ , we show that the optimal type-I error vanishes asymptotically (Theorems 4.5 and 4.6):

$$\lim_{n \rightarrow +\infty} \frac{1}{na_n^2} \log \widehat{\alpha}_{\exp\{-n[D(\rho\|\sigma)-a_n]\}} (\rho^{\otimes n}\|\sigma^{\otimes n}) = -\frac{1}{2V(\rho\|\sigma)}, \quad (1.21)$$

where  $\widehat{\alpha}_\mu$  denotes the smallest type-I error when the type-II error does not exceed  $\mu$ ;  $D(\rho\|\sigma)$  and  $V(\rho\|\sigma)$  denote the relative entropy and relative variance of  $\rho$  and  $\sigma$ , respectively.

- (b) When the compression rate approaches the Slepian-Wolf limit from above with the speed not faster than  $O(1/\sqrt{n})$ , we show that the optimal probability vanishes asymptotically (Theorem 8.1):

$$\lim_{n \rightarrow +\infty} \frac{\log \epsilon^*(n, H(X|B)_\rho + a_n)}{na_n^2} = -\frac{1}{2V}. \quad (1.22)$$

- (c) When the transmission rate approaches the channel capacity from below with the speed not faster than  $O(1/\sqrt{n})$ , we show that the optimal probability vanishes asymptotically (Theorems 12.1 and 12.2):

$$\lim_{n \rightarrow +\infty} \frac{\log \epsilon^*(n, C - a_n)}{na_n^2} = -\frac{1}{2V}. \quad (1.23)$$

## 1.4 Structure of the Thesis

### *Organization.*

The thesis is divided into three parts. *Part I: Fundamentals* collects the necessary mathematical tools—matrix analysis and large deviation theory (Chapter 2), the notation of all quantum entropic quantities and their properties (Chapter 3), and the error exponent analysis for quantum hypothesis testing (Chapter 4). The two quantum information tasks investigated in this thesis are presented in Parts II and III, respectively.

*Part II: Information Storage with a Quantum Helper* discusses the source coding scenario—the error exponent analysis for Slepian-Wolf coding with QSI. We introduce the error exponent functions in Chapter 5 and prove their properties. The achievability and optimality are studied in Chapters 6 and 7. Next, we move on to the moderate deviation regime in Chapter 8, which heavily relies on the established results in achievability and optimality.

*Part III: Information Transmission over a Quantum Channel* investigates the channel coding scheme—the error exponent analysis for communications over classical-quantum channels. The organization is similar to Part II: the error exponent function, achievability, optimality, and the moderate deviation analysis are presented in Chapters 9, 10, 11, and 12, respectively. Lastly, we conclude this thesis in Chapter 13 and provide open problems for future study.

### *Structure.*

The structure of the thesis is depicted in Figure 1.3. The matrix mathematics provided in Chapter 2.1 will be useful in proving properties of the quantum entropic quantities in Chapter 3, properties of error exponent functions in Chapters 5 and 9, and the achievability in Chapters 4, 6 and 10. The techniques of large deviation theory in chapter 2.2 will be applied in the optimality part in Chapters 4, 7, and 11. The optimality in Chapters 7 and 11 requires the sharp converse bound of quantum hypothesis testing in Chapter 4. In either Part II or Part III, the moderate deviation analysis (Chapters 8 and 12) relies on the properties of error exponent functions (Chapters 5 and 9), achievability (Chapters 6 and 10), and optimality (Chapters 7 and 11).

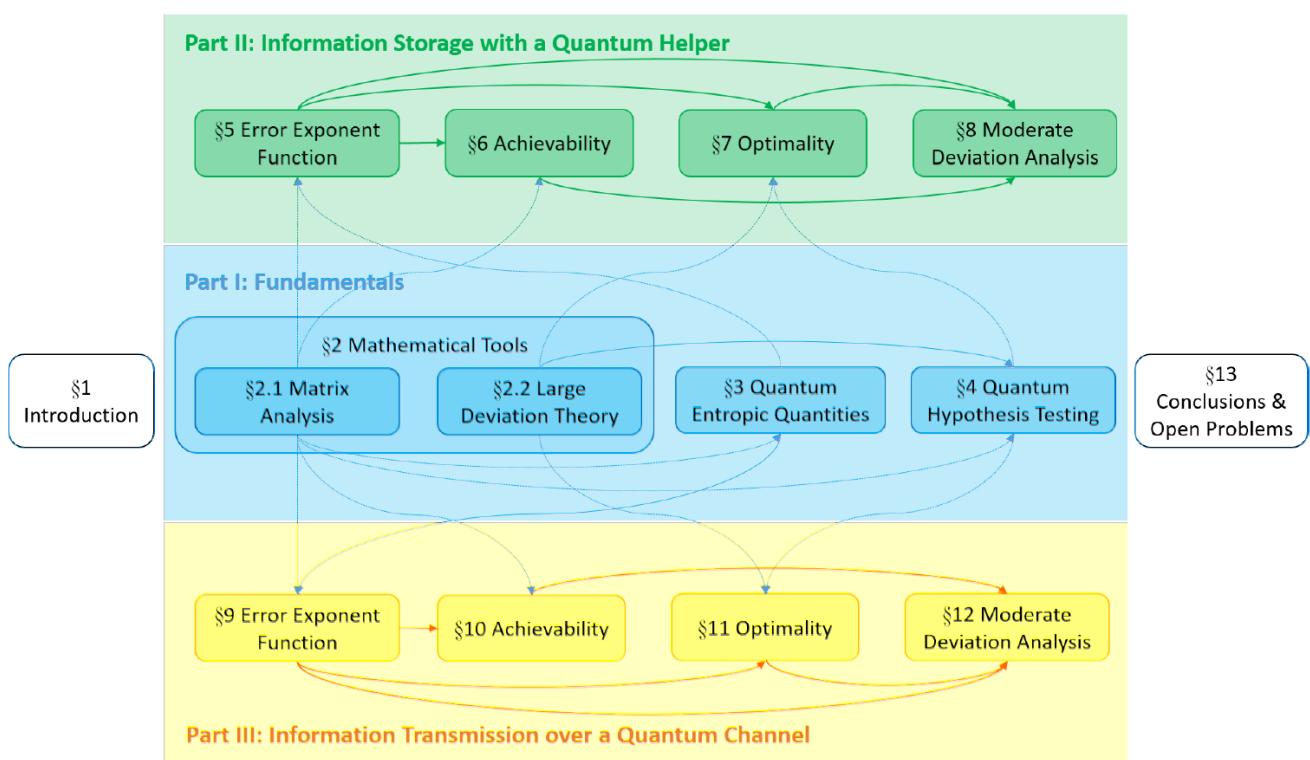


Figure 1.3: Structure of the thesis.

# Part I

## Fundamentals

## Chapter 2

# Mathematical Tools

We provide preliminaries mathematical tools in this Chapter. The introductory matrix analysis is given in Section 2.1. In Section 2.2, we present the backgrounds of large deviation theory.

### 2.1 Matrix Analysis

In this section, we provide backgrounds of matrix analysis. For a general treatment of this topic, interested readers can refer to [67, Section 2.1], [68, Chapter 17], [69, Section X.4], [70, Section 5.3], and [71, Chapter 3].

We denote by  $\mathbb{M}^{\text{sa}}$  the set of self-adjoint operators, and by  $\mathbb{M}_d^{\text{sa}}$  the set of Hermitian  $d \times d$  matrices. Similarly, let  $\mathbb{M}_d^+$  and  $\mathbb{M}_d^{++}$  be the set of  $d \times d$  positive semi-definite matrices and positive definite matrices, respectively. For  $A, B \in \mathbb{M}_d^{\text{sa}}$ , we denote by  $A \geq B$  to indicate that  $A - B \in \mathbb{M}_d^+$ . The notation of " $\leq$ " follows similarly.

Let  $\mathcal{U}, \mathcal{W}$  be real Banach spaces. The *Fréchet derivative* of a function  $\mathbf{f} : \mathcal{U} \rightarrow \mathcal{W}$  at a point  $\mathbf{X} \in \mathcal{U}$ , if it exists<sup>1</sup>, is a unique linear mapping  $D\mathbf{f}[\mathbf{X}] : \mathcal{U} \rightarrow \mathcal{W}$  such that

$$\frac{\|\mathbf{f}(\mathbf{X} + \mathbf{E}) - \mathbf{f}(\mathbf{X}) - D\mathbf{f}[\mathbf{X}](\mathbf{E})\|_{\mathcal{W}}}{\|\mathbf{E}\|_{\mathcal{U}}} \rightarrow 0 \quad \text{as } \mathbf{E} \in \mathcal{U} \text{ and } \|\mathbf{E}\|_{\mathcal{U}} \rightarrow 0,$$

or, equivalently,

$$\|\mathbf{f}(\mathbf{X} + \mathbf{E}) - \mathbf{f}(\mathbf{X}) - D\mathbf{f}[\mathbf{X}](\mathbf{E})\|_{\mathcal{W}} = o(\|\mathbf{E}\|_{\mathcal{U}}),$$

where  $\|\cdot\|_{\mathcal{U}(\mathcal{W})}$  is a norm in  $\mathcal{U}$  (resp.  $\mathcal{W}$ ). The notation  $D\mathbf{f}[\mathbf{X}](\mathbf{E})$  then is interpreted as "the Fréchet derivative of  $\mathbf{f}$  at  $\mathbf{X}$  in the direction  $\mathbf{E}$ ". Furthermore, the Fréchet derivative implies the Gâteaux derivative such that the differentiation of  $\mathbf{f}(\mathbf{X} + t\mathbf{E})$  with respect to the real variable  $t$  is

$$\frac{\mathbf{f}(\mathbf{X} + t\mathbf{E}) - \mathbf{f}(\mathbf{X})}{t} \rightarrow D\mathbf{f}[\mathbf{X}](\mathbf{E}) \quad \text{as } t \rightarrow 0.$$

For example, if the operator-valued function is the inversion  $\mathbf{f}(\mathbf{X}) = \mathbf{X}^{-1}$  for each invertible matrix  $\mathbf{X}$ , then (see e.g. [69, Example X.4.2])

$$D\mathbf{f}[\mathbf{X}](\mathbf{Y}) = -\mathbf{X}^{-1}\mathbf{Y}\mathbf{X}^{-1}. \tag{2.1}$$

---

<sup>1</sup>We assume the functions considered in the paper are Fréchet differentiable. The readers can refer to, e.g. [72, 73], for conditions for when a function is Fréchet differentiable.

The Fréchet derivative also satisfies several properties similar to conventional derivatives of real-valued functions (see e.g. [71, Theorem 3.4]):

**Proposition 2.1** (Properties of Fréchet Derivatives). *Let  $\mathcal{U}, \mathcal{V}$  and  $\mathcal{W}$  be real Banach spaces.*

1. (*Sum Rule*) If  $f_1 : \mathcal{U} \rightarrow \mathcal{W}$  and  $f_2 : \mathcal{U} \rightarrow \mathcal{W}$  are Fréchet differentiable at  $\mathbf{A} \in \mathcal{U}$ , then so is  $\mathbf{f} = \alpha f_1 + \beta f_2$  and  $D\mathbf{f}[\mathbf{A}](\mathbf{E}) = \alpha \cdot Df_1[\mathbf{A}](\mathbf{E}) + \beta \cdot Df_2[\mathbf{A}](\mathbf{E})$ .
2. (*Product Rule*) If  $f_1 : \mathcal{U} \rightarrow \mathcal{W}$  and  $f_2 : \mathcal{U} \rightarrow \mathcal{W}$  are Fréchet differentiable at  $\mathbf{A} \in \mathcal{U}$  and assume the multiplication is well-defined in  $\mathcal{W}$ , then so is  $\mathbf{f} = f_1 \cdot f_2$  and  $D\mathbf{f}[\mathbf{A}](\mathbf{E}) = Df_1[\mathbf{A}](\mathbf{E}) \cdot f_2(\mathbf{A}) + f_1(\mathbf{A}) \cdot Df_2[\mathbf{A}](\mathbf{E})$ .
3. (*Chain Rule*) Let  $f_1 : \mathcal{U} \rightarrow \mathcal{V}$  and  $f_2 : \mathcal{V} \rightarrow \mathcal{W}$  be Fréchet differentiable at  $\mathbf{A} \in \mathcal{U}$  and  $f_1(\mathbf{A})$  respectively, and let  $\mathbf{f} = f_2 \circ f_1$  (i.e.  $\mathbf{f}(\mathbf{A}) = f_2(f_1(\mathbf{A}))$ ). Then  $\mathbf{f}$  is Fréchet differentiable at  $\mathbf{A}$  and  $D\mathbf{f}[\mathbf{A}](\mathbf{E}) = Df_2[f_1(\mathbf{A})](Df_1[\mathbf{A}](\mathbf{E}))$ .

Similarly, the  $m$ -th Fréchet derivative  $D^m \mathbf{f}[\mathbf{X}]$  is a unique multi-linear map from  $\mathcal{U}^m \triangleq \mathcal{U} \times \cdots \times \mathcal{U}$  ( $m$  times) to  $\mathcal{W}$  that satisfies

$$\begin{aligned} & \|D^{m-1} \mathbf{f}[\mathbf{X} + \mathbf{E}_m](\mathbf{E}_1, \dots, \mathbf{E}_{m-1}) - D^{m-1} \mathbf{f}[\mathbf{X}](\mathbf{E}_1, \dots, \mathbf{E}_{m-1}) \\ & \quad - D^m \mathbf{f}[\mathbf{X}](\mathbf{E}_1, \dots, \mathbf{E}_m)\|_{\mathcal{W}} = o(\|\mathbf{E}_m\|_{\mathcal{U}}) \end{aligned}$$

for each  $\mathbf{E}_i \in \mathcal{U}, i = 1, \dots, m$ . If  $D^m \mathbf{f}[\mathbf{X}]$  is continuous at  $\mathbf{X}$ , then the  $m$ -th Fréchet derivative can be expressed as a mixed partial derivative [74, Section 9] (see also [75, Theorem 2.3.1]).

$$D^m \mathbf{f}[\mathbf{X}](\mathbf{E}_1, \dots, \mathbf{E}_m) = \frac{\partial}{\partial s_1} \cdots \frac{\partial}{\partial s_m} \Big|_{s_1=\dots=s_m=0} \mathbf{f}(\mathbf{X} + s_1 \mathbf{E}_1 + \cdots + s_m \mathbf{E}_m).$$

We can observe, from the above equation, that the  $m$ -th Fréchet derivative is symmetric about all  $\mathbf{E}_i$ ; see [76, Theorem 8], [69, p. 313], and [77, Theorem 4.3.4]. We refer to Refs. [78, Section 8.12], [68, Chapter 17], [77, Section 4.3], and [79] for further information about higher order Fréchet derivatives.

The following proposition relates the second order Fréchet derivative with the convexity of a matrix-valued function, i.e.  $\mathbf{f}(t\mathbf{A}) + \mathbf{f}((1-t)\mathbf{B}) \preceq \mathbf{f}(t\mathbf{A} + (1-t)\mathbf{B})$  for all  $0 \leq t \leq 1$ .

**Proposition 2.2** (Convexity of twice Fréchet differentiable matrix functions [80, Proposition 2.2]). *Let  $U$  be an open convex subset of a real Banach space  $\mathcal{U}$ , and  $\mathcal{W}$  is also a real Banach space. Then a twice Fréchet differentiable function  $\mathbf{f} : U \rightarrow \mathcal{W}$  is convex if and only if  $D^2 \mathbf{f}(\mathbf{X})(\mathbf{h}, \mathbf{h}) \succeq \mathbf{0}$  for each  $\mathbf{X} \in U$  and  $\mathbf{h} \in \mathcal{U}$ .*

The *partial Fréchet derivative* of multivariate functions can be defined as follows [70, Section 5.3]. Let  $\mathcal{U}, \mathcal{V}$  and  $\mathcal{W}$  be real Banach spaces,  $\mathbf{f} : \mathcal{U} \times \mathcal{V} \rightarrow \mathcal{W}$ . For a fixed  $\mathbf{v}_0 \in \mathcal{V}$ ,  $\mathbf{f}(\mathbf{u}, \mathbf{v}_0)$  is a function of  $\mathbf{u}$  whose derivative at  $\mathbf{u}_0$ , if it exists, is called the partial Fréchet derivative of  $\mathbf{f}$  with respect to  $\mathbf{u}$ , and is denoted by  $D_{\mathbf{u}} \mathbf{f}[\mathbf{u}_0, \mathbf{v}_0]$ . The partial Fréchet derivative  $D_{\mathbf{v}} \mathbf{f}[\mathbf{u}_0, \mathbf{v}_0]$  is defined similarly.

The Fréchet derivative and the partial Fréchet derivative can be related as follows.

**Proposition 2.3** (Partial Fréchet derivative [70, Proposition 5.3.15]). *If  $\mathbf{f} : \mathcal{U} \times \mathcal{V} \rightarrow \mathcal{W}$  is Fréchet differentiable at  $(\mathbf{X}, \mathbf{Y}) \in \mathcal{U} \times \mathcal{V}$ , then the partial Fréchet derivatives  $D_{\mathbf{X}} \mathbf{f}[\mathbf{X}, \mathbf{Y}]$  and  $D_{\mathbf{Y}} \mathbf{f}[\mathbf{X}, \mathbf{Y}]$  exist, and*

$$D\mathbf{f}[\mathbf{X}, \mathbf{Y}](\mathbf{h}, \mathbf{k}) = D_{\mathbf{X}} \mathbf{f}[\mathbf{X}, \mathbf{Y}](\mathbf{h}) + D_{\mathbf{Y}} \mathbf{f}[\mathbf{X}, \mathbf{Y}](\mathbf{k}).$$

Now let  $\mathbf{f} : \mathcal{U}^n \rightarrow \mathcal{W}$  and assume it is a holomorphic function (i.e. Fréchet differential in a neighborhood of every point in its domain), then the *Taylor expansion*  $\mathbf{f}(\underline{\mathbf{X}} + \underline{\mathbf{E}})$  at  $\underline{\mathbf{X}} \triangleq (\mathbf{X}_1, \dots, \mathbf{X}_n)$ ,  $\underline{\mathbf{E}} \triangleq (\mathbf{E}_1, \dots, \mathbf{E}_n) \in \mathcal{U}^n$  can be expressed as

$$\begin{aligned}\mathbf{f}(\underline{\mathbf{X}} + \underline{\mathbf{E}}) &= \mathbf{f}(\underline{\mathbf{X}}) + \sum_{k=1}^{\infty} \frac{1}{k!} \mathsf{D}^k \mathbf{f}[\underline{\mathbf{X}}] (\underbrace{\mathbf{E}, \dots, \mathbf{E}}_k) \\ &= \mathbf{f}(\underline{\mathbf{X}}) + \sum_{j=1}^n \mathsf{D}_{\mathbf{X}_j} \mathbf{f}[\underline{\mathbf{X}}](\mathbf{E}_j) + \frac{1}{2!} \sum_{j=1}^n \sum_{k=1}^n \mathsf{D}_{\mathbf{X}_j \mathbf{X}_k}^2(\mathbf{E}_j, \mathbf{E}_k) + \text{Remaining terms.}\end{aligned}\quad (2.2)$$

For any map  $\mathbf{f} : \mathcal{U} \rightarrow \mathcal{W}$  and an operator  $\mathbf{X} \in \mathcal{U}$ , we define the induced norm of the Fréchet derivative  $\mathsf{D}\mathbf{f}[\mathbf{X}]$  as

$$\|\mathsf{D}\mathbf{f}[\mathbf{X}]\| \triangleq \sup_{\mathbf{E} \neq \mathbf{0}} \frac{\|\mathsf{D}\mathbf{f}[\mathbf{X}](\mathbf{E})\|}{\|\mathbf{E}\|}, \quad (2.3)$$

where the norm can be any consistent norm (e.g.  $\|\mathsf{D}\mathbf{f}[\mathbf{X}]\|_2 = \sup_{\mathbf{E} \neq \mathbf{0}} \|\mathsf{D}\mathbf{f}[\mathbf{X}](\mathbf{E})\|_2 / \|\mathbf{E}\|_2$ ).

The norm of the Fréchet derivative is closely related to the condition numbers, which measure the sensitivity of an operator-valued function to perturbations in the variables. Hence, the *absolute condition number* is defined by

$$\text{cond}_{\text{abs}}(\mathbf{f}, \mathbf{X}) \triangleq \lim_{\varepsilon \rightarrow 0} \sup_{\|\mathbf{E}\| \leq \varepsilon} \frac{\|\mathbf{f}(\mathbf{X} + \mathbf{E}) - \mathbf{X}\|}{\varepsilon}. \quad (2.4)$$

Then the norm of the Fréchet derivative can be expressed by the absolute condition number [81]

$$\text{cond}_{\text{abs}}(\mathbf{f}, \mathbf{X}) = \|\mathsf{D}\mathbf{f}[\mathbf{X}]\|.$$

We note that there are several algorithms and software packages that can compute the absolute condition number; see [71, Section 3], [82] and references therein.

Next, we introduce the *standard matrix functions*. For each self-adjoint and bounded operator  $\mathbf{A} \in \mathbb{M}^{\text{sa}}$  with the spectrum  $\sigma(\mathbf{A})$  and the spectral measure  $\mathbf{E}$ , the *spectral decomposition* is given as

$$\mathbf{A} = \int_{\lambda \in \sigma(\mathbf{A})} \lambda d\mathbf{E}(\lambda). \quad (2.5)$$

Hence, each scalar function can be extended to a standard matrix function as follows.

**Definition 2.1** (Standard Matrix Function). Let  $f : I \rightarrow \mathbb{R}$  be a real-valued function on an interval  $I$  of the real line. Suppose that  $\mathbf{A} \in \mathbb{M}^{\text{sa}}(I)$  has the spectral decomposition (2.5). Then

$$f(\mathbf{A}) \triangleq \int_{\lambda \in \sigma(\mathbf{A})} f(\lambda) d\mathbf{E}(\lambda).$$

From this equation, it is clear that  $\sigma(f(\mathbf{A})) = f(\sigma(\mathbf{A}))$ , which is called the *spectral mapping theorem*.

A function  $f : I \rightarrow \mathbb{R}$  is called *operator convex* if for each  $\mathbf{A}, \mathbf{B} \in \mathbb{M}^{\text{sa}}(I)$  and  $0 \leq t \leq 1$ ,

$$f(t\mathbf{A}) + f((1-t)\mathbf{B}) \leq f(t\mathbf{A} + (1-t)\mathbf{B}).$$

Similarly, a function  $f : I \rightarrow \mathbb{R}$  is called *operator monotone* if for each  $\mathbf{A}, \mathbf{B} \in \mathbb{M}^{\text{sa}}(I)$ ,

$$\mathbf{A} \leq \mathbf{B} \Rightarrow f(\mathbf{A}) \leq f(\mathbf{B}).$$

It is remarkable that not all convex (resp. monotone) functions are operator convex (resp. monotone). For example, the exponential function is not operator convex nor operator monotone on  $[0, \infty)$ ; the power functions that are operator convex are  $f(x) = x^p$  for  $p \in [-1, 0] \cup [1, 2]$  and  $f(x) = -x^p$  for  $p \in [0, 1]$ . However, the trace function on  $\mathbb{M}^{\text{sa}}$  given by  $\mathbf{A} \rightarrow \text{Tr}[f(\mathbf{A})]$  preserves the convexity or monotonicity.

**Proposition 2.4** (Convexity and Monotonicity for Trace Functions [83, Section 2.2]). *Consider a real-valued function  $f : I \rightarrow \mathbb{R}$ . If  $f$  is convex (resp. monotone) on  $U \subseteq I$ , then the function  $\mathbf{A} \rightarrow \text{Tr}[f(\mathbf{A})]$  is convex (resp. monotone) on  $\mathbb{M}^{\text{sa}}(U)$ .*

We refer the readers to Refs. [75] and [84] for general expositions to operator convex and monotone functions.

If the scalar function is continuously differentiable, then it is convenient to introduce the following two properties for the trace function of Fréchet derivatives.

**Proposition 2.5** ([84, Theorem 3.23]). *Let  $\mathbf{A}, \mathbf{X} \in \mathbb{M}^{\text{sa}}$  and  $t \in \mathbb{R}$ . Assume  $f : I \rightarrow \mathbb{R}$  is a continuously differentiable function defined on interval  $I$  and assume that the eigenvalues of  $\mathbf{A} + t\mathbf{X} \subset I$ . Then*

$$\frac{d}{dt} \text{Tr } f(\mathbf{A} + t\mathbf{X}) \Big|_{t=t_0} = \text{Tr}[\mathbf{X} f'(\mathbf{A} + t_0\mathbf{X})].$$

In the following, we collect necessary matrix inequalities that will be employed later in this thesis. Let  $x := (x_1, \dots, x_d) \in \mathbb{R}^d$  be a  $d$ -dimensional vector with positive elements. Denote by  $x^\downarrow := (x_1^\downarrow, \dots, x_d^\downarrow)$  the *decreasing arrangement* of  $x$ , i.e.  $x_1^\downarrow \geq \dots \geq x_d^\downarrow$ . We say that  $x$  is *weak majorized* by  $y$ , denoted by  $x \prec_w y$ , if

$$\sum_{j=1}^k x_j^\downarrow \leq \sum_{j=1}^k y_j^\downarrow, \quad 1 \leq k \leq d. \quad (2.6)$$

The *weak log-majorization*  $x \prec_{w\log} y$  is defined when  $\log x \prec_w \log y$ , where we denote by  $\log x$  the vector whose components equal to the logarithm of the components of  $x$ . It is well-known that  $x \prec_{w\log} y$  implies  $x \prec_w y$  [69, Example II.3.5]. Let  $\lambda(X)$  denote the vector of eigenvalues of the matrix  $X$ . For two positive semi-definite matrices  $A$  and  $B$ , the weak majorization  $\lambda(A) \prec_w \lambda(B)$  is equivalent to  $\|\|A\|\| \leq \|\|B\|\|$  for all unitarily-invariant norm  $\|\cdot\|$  [84, Theorem 6.23].

For  $A, B \in \mathbb{M}_d^{++}$ , we definite the *matrix geometric mean* with parameter  $s \in \mathbb{R}$  [85, 86, 69, 87] by

$$A \#_s B := A^{\frac{1}{2}} \left( A^{-\frac{1}{2}} B A^{-\frac{1}{2}} \right)^s A^{\frac{1}{2}}. \quad (2.7)$$

The definition can be naturally extended to the positive semi-definite operators on infinite dimensional Hilbert space, i.e.

$$A \#_s B := \lim_{\gamma \downarrow 0} A_\gamma^{\frac{1}{2}} \left( A_\gamma^{-\frac{1}{2}} B_\gamma A_\gamma^{-\frac{1}{2}} \right)^s A_\gamma^{\frac{1}{2}} \quad (2.8)$$

for  $A_\gamma = A + \gamma \mathbb{1}$  and  $B_\gamma = B + \gamma$ .

In the following, we collect useful facts regarding matrix geometric means.

**Lemma 2.1** ([88, Theorem 2.10]). *For any  $A, B \in \mathbb{M}_d^{++}$ , and  $0 \leq s \leq 1$ . Then*

$$\lambda(A \#_s B) \prec_{\text{wlog}} \lambda(A^{1-s} B^s). \quad (2.9)$$

**Lemma 2.2** (Araki-Lieb-Thirring Inequality [89]; see also [69, Theorem IX.2.10]). *Let  $A, B \in \mathbb{M}_d^+$ . Then, we have*

$$\lambda(B^t A^t B^t) \prec_w \lambda((BAB)^t), \text{ for } t \in [0, 1], \quad (2.10)$$

$$\lambda(B^t A^t B^t) \succ_w \lambda((BAB)^t), \text{ for } t \geq 1. \quad (2.11)$$

**Lemma 2.3** ([69, Example II.3.5]). *Let  $x, y \in \mathbb{R}_{\geq 0}^d$  (the set of  $d$ -dimensional vectors of non-negative real numbers). Then*

$$x \prec_w y \quad \text{implies} \quad x^t \prec_w y^t \quad (2.12)$$

for all  $t \geq 1$ .

**Lemma 2.4** (See, e.g. [83, Section 2.2]). *Let  $f$  be a monotonically increasing function on the real line. Then  $A \preceq B$  implies*

$$\text{Tr}[f(A)] \leq \text{Tr}[f(B)]. \quad (2.13)$$

**Lemma 2.5** (Matrix Hölder's Inequality [69, Corollary IV.2.6]). *Let  $A, B \in \mathbb{M}_d^+$ . Then*

$$\text{Tr}[AB] \leq \left(\text{Tr}\left[A^{\frac{1}{\theta}}\right]\right)^\theta \left(\text{Tr}\left[B^{\frac{1}{1-\theta}}\right]\right)^{1-\theta} \quad (2.14)$$

for all  $0 \leq \theta \leq 1$ .

**Lemma 2.6.** *Let  $A, B \in \mathbb{M}_d^{++}$ . Then, for every  $t \geq 1$  and  $0 \leq \tau \leq 1$ , we have*

$$\text{Tr}[(A \#_\tau B)^t] \leq \text{Tr}\left[A^{t(1-\tau)} B^{t\tau}\right]. \quad (2.15)$$

*Proof of Lemma 2.6.* From Lemma 2.1, we have

$$\lambda(A \#_\tau B) \prec_w \lambda(A^{1-\tau} B^\tau) \quad (2.16)$$

$$= \lambda\left(A^{\frac{1-\tau}{2}} B^\tau A^{\frac{1-\tau}{2}}\right) \quad (2.17)$$

$$\prec_w \lambda\left(\left(A^{\frac{t(1-\tau)}{2}} B^{t\tau} A^{\frac{t(1-\tau)}{2}}\right)^{\frac{1}{t}}\right), \quad (2.18)$$

where we employ the fact that  $\lambda(XY) = \lambda(YX)$  for any two square matrices  $X, Y$  in Eq. (2.17) (see e.g. [84, Example 1.19]). The last inequality (2.18) follows from Eq. (2.10) in Lemma 2.2. Next, applying Lemma 2.3 on the above inequality yields

$$\lambda((A \#_\tau B)^t) \prec_w \lambda\left(A^{\frac{t(1-\tau)}{2}} B^{t\tau} A^{\frac{t(1-\tau)}{2}}\right). \quad (2.19)$$

Finally, since the trace function is the summation of eigenvalues, the weak majorization in Eq. (2.19) implies the trace norm inequality in Eq. (2.15).  $\square$

**Lemma 2.7** (Golden-Thompson Inequality [61, 90, 62]). *For any two operators  $A, B \geq 0$ , it follows that*

$$\mathrm{Tr} [\mathrm{e}^{A+B}] \leq \mathrm{Tr} [\mathrm{e}^A \mathrm{e}^B]. \quad (2.20)$$

**Lemma 2.8** ([91, Theorem 1], [92, Theorem 2] ). *For any two operators  $A, B \geq 0$ , and  $t \in [0, 1]$ , we have*

$$\mathrm{Tr} [A^t B^{1-t}] \geq \mathrm{Tr} [\{A - B > 0\} B] + \mathrm{Tr} [\{A - B \leq 0\} A] \quad (2.21)$$

$$= \mathrm{Tr} [A + B - |A - B|] / 2. \quad (2.22)$$

**Lemma 2.9** (Hayashi-Nagaoka Inequality [93, Lemma 2] ). *For operators  $0 \leq S \leq \mathbb{1}$ , and  $T \geq 0$ , we have*

$$I - (S + T)^{-\frac{1}{2}} S (S + T)^{-\frac{1}{2}} \leq 2(\mathbb{1} - S) + 4T. \quad (2.23)$$

**Lemma 2.10** ([94, Lemma 1]). *For any two operators  $A, B \geq 0$ , and  $t \in [0, 1/2]$ , we have*

$$\mathrm{Tr} [A^t B^{1-t}] \geq \mathrm{Tr} [\{A^{1-t} - B^{1-t} > 0\} B] + \mathrm{Tr} [\{A^{1-t} - B^{1-t} \leq 0\} A]. \quad (2.24)$$

**Lemma 2.11** ([84, Theorem 3.23]). *Let  $\mathbf{A}, \mathbf{X}$  be  $d \times d$  Hermitian matrices, and  $t \in \mathbb{R}$ . Assume  $f : I \rightarrow \mathbb{R}$  is a continuously differentiable function. Then*

$$\left. \frac{d}{dt} \mathrm{Tr} f(\mathbf{A} + t\mathbf{X}) \right|_{t=t_0} = \mathrm{Tr}[\mathbf{X} f'(\mathbf{A} + t_0\mathbf{X})].$$

**Lemma 2.12.** [95, Corollary 3.6] *Let  $A_i$  be  $m \times m$  positive semi-definite matrix and  $Z_i$  be  $n \times m$  matrix for  $i = 1, \dots, k$ . Then, for all unitarily invariant norms  $\|\cdot\|$  and  $\gamma > 0$ , the map*

$$(p, t) \mapsto \left\| \left( \sum_{i=1}^k Z_i^* A_i^{t/p} Z_i \right)^{\gamma p} \right\| \quad (2.25)$$

*is jointly log-convex on  $(0, +\infty) \times (-\infty, +\infty)$ . Here, we use  $Z^*$  to denote the complex conjugate of  $Z$ .*

## 2.2 Large Deviation Theory

In this section, we will see that the Legendre-Fenchel transform is closely related to the error-exponent function of hypothesis testing and channel coding. Consider the following binary classical hypotheses:

$$\begin{aligned} \mathsf{H}_0 : p^n &:= p_{x_1} \otimes p_{x_2} \otimes \cdots \otimes p_{x_n}, \\ \mathsf{H}_1 : q^n &:= q_{x_1} \otimes q_{x_2} \otimes \cdots \otimes q_{x_n}, \end{aligned} \quad (2.26)$$

where  $p_{x_i}, q_{x_i}$  are probability mass functions; and  $x_i$  belongs to some finite alphabet  $\mathcal{X}$  and  $n \in \mathbb{N}$  be fixed. Given any  $r \geq 0$ , recall the definition of the error-exponent function in Eq. (4.7):

$$\phi_n(r) = \phi_n(r|p^n\|q^n) = \sup_{\alpha \in (0,1]} \left\{ \frac{1-\alpha}{\alpha} \left( \frac{1}{n} D_\alpha(p^n\|q^n) - r \right) \right\}, \quad (2.27)$$

where

$$D_\alpha(p\|q) := \frac{1}{\alpha-1} \log \int \left( \frac{dp}{d\nu} \right)^\alpha \left( \frac{dq}{d\nu} \right)^{1-\alpha} d\nu \quad (2.28)$$

is the *classical order  $\alpha$  Rényi divergence* [96, 97], and  $\nu$  is any reference measure such that  $p$  and  $q$  are absolutely continuous with respect to  $\nu$ , i.e. we denote by  $p \ll \nu$  and  $q \ll \nu$ . Without loss of generality, we assume that  $p^n \ll q^n$  have the same support since elements of  $q_{x_i}$ , that do not lie in the support of  $p_{x_i}$ , do not contribute to  $\phi_n(r)$ .

Let  $Z$  be a random variable with probability measure  $\mu$ . Further, we assume  $Z$  is finite on  $\text{supp}(\mu)$ . The cumulant generating function (c.g.f.) of  $Z$  is defined as

$$\Lambda(t) := \log \mathbb{E}_\mu [e^{tZ}], \quad t \in \mathbb{R}. \quad (2.29)$$

The *Lengendre-Fenchel transform* of  $\Lambda(t)$  is

$$\Lambda^*(z) := \sup_{t \in \mathbb{R}} \{zt - \Lambda(t)\}. \quad (2.30)$$

Such a transform plays a significant role in concentration inequalities, convex analysis, and large deviation theory [1].

Let  $P_{\mathbf{x}^n}$  be the empirical distribution of the sequence  $\mathbf{x}^n = x_1 x_2 \dots x_n$ . Let  $Z_0 = \log \frac{q^n}{p^n}$  with probability measure  $p^n$ ,  $Z_1 = \log \frac{p^n}{q^n}$  with probability measure  $q^n$ , and denote

$$\begin{aligned} \Lambda_{0,P_{\mathbf{x}^n}}(t) &:= \frac{1}{n} \log \mathbb{E}_{p^n} [e^{tZ_0}] = \sum_{x \in \mathcal{X}} P_{\mathbf{x}^n}(x) \Lambda_{0,x_i}(t), \\ \Lambda_{1,P_{\mathbf{x}^n}}(t) &:= \frac{1}{n} \log \mathbb{E}_{q^n} [e^{tZ_1}] = \sum_{x \in \mathcal{X}} P_{\mathbf{x}^n}(x) \Lambda_{1,x_i}(t); \end{aligned} \quad (2.31)$$

where

$$\Lambda_{0,x_i}(t) := \log \mathbb{E}_{p_{x_i}} \left[ e^{t \log \frac{q_{x_i}}{p_{x_i}}} \right], \quad \Lambda_{1,x_i}(t) := \log \mathbb{E}_{q_{x_i}} \left[ e^{t \log \frac{p_{x_i}}{q_{x_i}}} \right]. \quad (2.32)$$

Rewrite the right-hand side of Eq. (2.27) with  $\alpha = \frac{1}{1+s}$ , and observe that

$$\sum_{x \in \mathcal{X}} P_{\mathbf{x}^n}(x) s D_{\frac{1}{1+s}}(p_x\|q_x) = -(1+s) \Lambda_{0,P_{\mathbf{x}^n}} \left( \frac{s}{1+s} \right) \quad (2.33)$$

$$=: E_0^{(2)}(s, P_{\mathbf{x}^n}). \quad (2.34)$$

Then the error-exponent function in Eq. (2.27) can also be viewed as a Lengendre-Fenchel transform

of  $E_0^{(2)}(s, P_{\mathbf{x}^n})$ :

$$\phi_n(r) = \sup_{s \geq 0} \left\{ E_0^{(2)}(s, P_{\mathbf{x}^n}) - sr \right\}. \quad (2.35)$$

The following lemma relates  $\phi_n(r)$  to  $\Lambda_{j,P_{\mathbf{x}^n}}^*(z)$ , the Legendre-Fenchel transform of Eq. (2.31):

$$\Lambda_{j,P_{\mathbf{x}^n}}^*(z) := \sup_{t \in \mathbb{R}} \{tz - \Lambda_{j,P_{\mathbf{x}^n}}(t)\}, \quad j \in \{0, 1\}. \quad (2.36)$$

**Lemma 2.13** (Regularity). *Let  $p^n$  and  $q^n$ ,  $n \in \mathbb{N}$ , be described as above. Assume  $r > \frac{1}{n}D_0(p^n \| q^n)$  and  $\phi_n(r) > 0$ . The following hold:*

$$(a) \quad \Lambda_{0,P_{\mathbf{x}^n}}''(t) > 0 \text{ for all } t \in [0, 1].$$

$$(b) \quad \Lambda_{0,P_{\mathbf{x}^n}}^*(\phi_n(r) - r) = \phi_n(r).$$

$$(c) \quad \Lambda_{1,P_{\mathbf{x}^n}}^*(r - \phi_n(r)) = r.$$

$$(d) \quad \text{Let } t^* := t_{r,P_{\mathbf{x}^n}}^* \text{ be the optimizer of } \Lambda_{0,P_{\mathbf{x}^n}}^*(z) \text{ in Eq. (2.36), and } s^* := s_{r,P_{\mathbf{x}^n}}^* \text{ be the optimizer of } \phi_n(r) \text{ in Eq. (2.35). The optimizer } t^* \in (0, 1) \text{ is unique, and satisfies } \Lambda_{0,P_{\mathbf{x}^n}}'(t^*) = \phi_n(r) - r. \\ \text{In particular, one has } t^* = \frac{s^*}{1+s^*}; \quad s^* = -\frac{\partial \phi_n(r)}{\partial r}; \quad \text{and } \frac{\partial^2 \phi_n(r)}{\partial r^2} = -\left(\frac{\partial^2 E_0^{(2)}(s, P_{\mathbf{x}^n})}{\partial s^2}\Big|_{s=s^*}\right)^{-1} = \\ \frac{(1+s_{r,P_{\mathbf{x}^n}}^*)^3}{\Lambda_{0,P_{\mathbf{x}^n}}''(t^*)} > 0.$$

Before proving Lemma 2.13, we will need the following partial derivatives with respect to  $t$ :

$$\Lambda'_{0,x_i}(t) = \mathbb{E}_{\hat{q}_{x_i,t}} \left[ \log \frac{q_{x_i}}{p_{x_i}} \right], \quad \Lambda'_{1,x_i}(t) = \mathbb{E}_{\hat{q}_{x_i,1-t}} \left[ \log \frac{p_{x_i}}{q_{x_i}} \right]; \quad (2.37)$$

$$\Lambda''_{0,x_i}(t) = \text{Var}_{\hat{q}_{x_i,t}} \left[ \log \frac{q_{x_i}}{p_{x_i}} \right], \quad \Lambda''_{1,x_i}(t) = \text{Var}_{\hat{q}_{x_i,1-t}} \left[ \log \frac{p_{x_i}}{q_{x_i}} \right], \quad (2.38)$$

where we denote the *tilted distributions* for every  $i \in [n]$  and  $t \in [0, 1]$  by

$$\hat{q}_{x_i,t}(\omega) := \frac{p_{x_i}(\omega)^{1-t} q_{x_i}(\omega)^t}{\sum_{\omega \in \text{supp}(p_{x_i})} p_{x_i}(\omega)^{1-t} q_{x_i}(\omega)^t}, \quad \omega \in \text{supp}(p_{x_i}). \quad (2.39)$$

It is also easy to verify that

$$\Lambda_{0,x_i}(t) = \Lambda_{1,x_i}(1-t), \quad \Lambda'_{0,x_i}(t) = -\Lambda'_{1,x_i}(1-t), \quad \Lambda''_{0,x_i}(t) = \Lambda''_{1,x_i}(1-t). \quad (2.40)$$

This lemma closely follows Ref. [98, Lemma 9]; however, the major difference is that we prove the claim using  $\phi_n(r|\rho^n \| \sigma^n)$  in Eq. (4.7) instead of the discrimination function:  $\min \{D(\tau\|\rho) : D(\tau\|\sigma) \leq r\}$  in Eq. (9.21). This expression is crucial to obtaining the sphere-packing bound in Theorem 11.1 in the strong form, cf. Eq. (1.4), instead of the weak form, cf. Eq. (1.5).

*Proof of Lemma 2.13.*

(2.13-(a)) We will prove this statement by contradiction. Let  $t \in [0, 1]$ , Assuming that  $\Lambda''_{0,P_{\mathbf{x}^n}}(t) = 0$ ,

implies  $\Lambda''_{0,x}(t) = 0, \forall x \in \text{supp}(P_{\mathbf{x}^n})$ . Recall from Eq. (2.38)

$$0 = \Lambda''_{0,x}(t) = \text{Var}_{\hat{q}_{x,t}} \left[ \log \frac{q_x}{p_x} \right], \quad (2.41)$$

which is equivalent to

$$p_x(\omega) = q_x(\omega) \cdot e^{-\Lambda'_{0,x}(t)}, \quad \forall \omega \in \text{supp}(p_x). \quad (2.42)$$

Summing both sides of Eq. (2.42) over  $\omega \in \text{supp}(p_x)$  gives

$$1 = \text{Tr} [p_x^0 q_x] e^{-\Lambda'_{0,x}(t)}. \quad (2.43)$$

Then, Eqs. (2.42) and (2.43) imply that

$$\phi_n(r) = \sup_{0 < \alpha \leq 1} \frac{\alpha - 1}{\alpha} \left( r - \sum_{x \in \mathcal{X}} P_{\mathbf{x}^n}(x) D_\alpha(p_x \| q_x) \right) \quad (2.44)$$

$$= \sup_{0 < \alpha \leq 1} \frac{\alpha - 1}{\alpha} \left( r + \sum_{x \in \mathcal{X}} P_{\mathbf{x}^n}(x) \log \text{Tr} [p_x^0 q_x] \right) \quad (2.45)$$

$$= 0, \quad (2.46)$$

where Eq. (2.46) follows since  $r > \frac{1}{n} D_0(p^n \| q^n) = -\frac{1}{n} \sum_{x \in \mathcal{X}} P_{\mathbf{x}^n}(x) \log \text{Tr} [p_x^0 q_x]$  by assumption. However, this contradicts with the assumption  $\phi_n(r) > 0$ . Hence, we conclude item (a).

(2.13-(b)) Observe that  $E_0^{(2)}(s, P_{\mathbf{x}^n}) - sr$  in Eq. (2.35) is strictly concave in  $s \in \mathbb{R}_{\geq 0}$  since

$$\frac{\partial^2 E_0^{(2)}(s, P_{\mathbf{x}^n})}{\partial s^2} = -\frac{1}{(1+s)^3} \Lambda''_{0,P_{\mathbf{x}^n}} \left( \frac{s}{1+s} \right) < 0, \quad (2.47)$$

owing to Eqs. (2.34), (2.38), and Lemma (a). Moreover,  $s = 0$  cannot be an optimum in Eq. (2.35); otherwise, it will violate the assumption  $\phi_n(r) \geq 0$ . Thus a unique maximizer  $s^* \in \mathbb{R}_{>0}$  exists such that

$$\phi_n(r) = -s^*r + E_0^{(2)}(s^*, P_{\mathbf{x}^n}) \quad (2.48)$$

$$= \frac{s^*}{1+s^*} \Lambda'_{0,P_{\mathbf{x}^n}} \left( \frac{s^*}{1+s^*} \right) - \Lambda_{0,P_{\mathbf{x}^n}} \left( \frac{s^*}{1+s^*} \right). \quad (2.49)$$

where in the second equality we use Eq. (2.34) and

$$r = \left. \frac{\partial E_0^{(2)}(s, P_{\mathbf{x}^n})}{\partial s} \right|_{s=s^*} \quad (2.50)$$

$$= -\frac{1}{1+s^*} \Lambda'_{0,P_{\mathbf{x}^n}} \left( \frac{s^*}{1+s^*} \right) - \Lambda_{0,P_{\mathbf{x}^n}} \left( \frac{s^*}{1+s^*} \right). \quad (2.51)$$

Comparing Eq. (2.49) with (2.51) gives

$$\Lambda'_{0,P_{\mathbf{x}^n}} \left( \frac{s^*}{1+s^*} \right) = \phi_n(r) - r, \quad (2.52)$$

which is exactly the optimum solution to  $\Lambda_{0,P_{\mathbf{x}^n}}^*(z)$  in Eq. (2.36) with

$$t^* = \frac{s^*}{1+s^*} \in (0, 1), \quad (2.53)$$

$$z = \phi_n(r) - r. \quad (2.54)$$

Hence, we obtain

$$\Lambda_{0,P_{\mathbf{x}^n}}^*(\phi_n(r) - r) = t^*z - \Lambda_{0,P_{\mathbf{x}^n}}(t^*) \quad (2.55)$$

$$= \frac{s^*}{1+s^*} (\phi_n(r) - r) - \Lambda_{0,P_{\mathbf{x}^n}} \left( \frac{s^*}{1+s^*} \right) \quad (2.56)$$

$$= \frac{s^*}{1+s^*} \Lambda'_{0,P_{\mathbf{x}^n}} \left( \frac{s^*}{1+s^*} \right) - \Lambda_{0,P_{\mathbf{x}^n}} \left( \frac{s^*}{1+s^*} \right) \quad (2.57)$$

$$= \phi_n(r), \quad (2.58)$$

where Eqs. (2.52) and (2.49) are used in the third and last equalities.

(2.13-(c)) This proof follows from similar arguments in item (b) and Eq. (2.40). Eqs. (2.52) and (2.40) lead to

$$\Lambda'_{1,P_{\mathbf{x}^n}} \left( \frac{1}{1+s^*} \right) = r - \phi_n(r), \quad (2.59)$$

which satisfies the optimum solution to  $\Lambda_{1,P_{\mathbf{x}^n}}(z)$  in Eq. (2.36) with  $t^* = \frac{1}{1+s^*} \in (0, 1)$  and  $z = r - \phi_n(r)$ . Then,

$$\Lambda_{1,P_{\mathbf{x}^n}}^*(r - \phi_n(r)) = t^*z - \Lambda_{1,P_{\mathbf{x}^n}}(t^*) \quad (2.60)$$

$$= \frac{1}{1+s^*} (r - \phi_n(r)) - \Lambda_{1,P_{\mathbf{x}^n}} \left( \frac{s^*}{1+s^*} \right) \quad (2.61)$$

$$= \frac{1}{1+s^*} \Lambda'_{1,P_{\mathbf{x}^n}} \left( \frac{1}{1+s^*} \right) - \Lambda_{1,P_{\mathbf{x}^n}} \left( \frac{1}{1+s^*} \right) \quad (2.62)$$

$$= r, \quad (2.63)$$

where the third equality is due to Eq. (2.59), and the last equality follows from Eqs. (2.40) and (2.51).

(2.13-(d)) The fact that a unique optimizer  $t^* \in (0, 1)$  exists such that  $\Lambda'_{0,P_{\mathbf{x}^n}}(t^*) = \phi_n(r) - r$  follows directly from Eqs. (2.52), (2.53) and  $\Lambda''_{0,P_{\mathbf{x}^n}}(t) > 0$ , for  $t \in [0, 1]$ .

Moreover, Eqs. (2.48), (2.50), and (2.47) yield

$$-\frac{\partial \phi_n(r)}{\partial r} = s^*, \quad (2.64)$$

$$\left. \frac{\partial^2 \phi_n(r)}{\partial r^2} = -\frac{\partial s^*}{\partial r} = -\left( \frac{\partial^2 E_0^{(2)}(s, P_{\mathbf{x}^n})}{\partial s^2} \right)^{-1} \right|_{s=s^*} = \frac{(1+s^*)^3}{\Lambda_{0,P_{\mathbf{x}^n}}\left(\frac{s^*}{1+s^*}\right)}, \quad (2.65)$$

which completes the claim in item (d).  $\square$

Let  $(Z_i)_{i=1}^n$  be a sequence of independent, real-valued random variables with probability measures  $(\mu_i)_{i=1}^n$ . Let  $\Lambda_i(t) := \log \mathbb{E}[e^{tZ_i}]$  and define the Legendre-Fenchel transform of  $\frac{1}{n} \sum_{i=1}^n \Lambda_i(\cdot)$  to be:

$$\Lambda_n^*(z) := \sup_{t \in \mathbb{R}} \left\{ zt - \frac{1}{n} \sum_{i=1}^n \Lambda_i(t) \right\}, \quad \forall z \in \mathbb{R}. \quad (2.66)$$

Then there exists a real number  $t^* \in (0, 1]$  for every  $z \in \mathbb{R}$  such that

$$z = \frac{1}{n} \sum_{i=1}^n \Lambda'_i(t^*); \quad (2.67)$$

$$\Lambda_n^*(z) = zt^* - \frac{1}{n} \sum_{i=1}^n \Lambda_i(t^*). \quad (2.68)$$

Define the probability measure  $\tilde{\mu}_i$  via

$$\frac{d\tilde{\mu}_i}{d\mu_i}(z_i) := e^{t^* z_i - \Lambda_i(t^*)}, \quad (2.69)$$

and let  $\bar{Z}_i := Z_i - \mathbb{E}_{\tilde{\mu}_i}[Z_i]$ . Furthermore, define  $m_{2,n} := \sum_{i=1}^n \text{Var}_{\tilde{\mu}_i}[\bar{Z}_i]$ ,  $m_{3,n} := \sum_{i=1}^n \mathbb{E}_{\tilde{\mu}_i}[|\bar{Z}_i|^3]$ , and  $K_n(t^*) := \frac{15\sqrt{2\pi}m_{3,n}}{m_{2,n}}$ . With these definitions, we can now state the following sharp concentration inequality for  $\frac{1}{n} \sum_{i=1}^n Z_i$ :

**Theorem 2.1** (Bahadur-Ranga Rao's Concentration Inequality [98, Proposition 5], [48]). *Provided that  $\sqrt{m_{2,n}} \geq 1 + (1 + K_n(t^*))^2$ , then*

$$\Pr \left\{ \frac{1}{n} \sum_{i=1}^n Z_i \geq z \right\} \geq e^{-n\Lambda_n^*(z)} \frac{e^{-K_n(t^*)}}{2\sqrt{2\pi m_{2,n}}}. \quad (2.70)$$

Chaganty and Sethuraman in Ref. [49, Theorem 3.3] considered a more general sequence of random variables  $\{Z_n\}_{n \in \mathbb{N}}$ , which are not necessarily the sum of random variables.

Let  $(X_i)_{i \in \mathbb{N}}$  be a sequence of independent, real-valued random variables with probability measures  $(\mu_i)_{i=1}^n$ . Let  $Z_n := \sum_{i=1}^n X_i$  and let  $\Lambda_n(t) := \log \mathbb{E}[e^{tZ_n}]$ . Define the Legendre-Fenchel transform of  $\frac{1}{n} \Lambda_n(\cdot)$  by:

$$\Lambda_n^*(z) := \sup_{t \in \mathbb{R}} \left\{ zt - \frac{1}{n} \Lambda_n(t) \right\}, \quad \forall z \in \mathbb{R}. \quad (2.71)$$

Let  $(T_n)_{n \in \mathbb{N}}$  be a bounded sequence of real numbers and  $(t_n^*)_{n \in \mathbb{N}}$  be a sequence satisfying for all  $n \in \mathbb{N}$

$$t_n^* \in (0, 1); \quad T_n = \frac{1}{n} \Lambda'_n(t_n^*); \quad \Lambda_n^*(T_n) = T_n t_n^* - \frac{1}{n} \Lambda_n(t_n^*). \quad (2.72)$$

With these definitions, we can now state the following sharp concentration inequality for  $\frac{1}{n} Z_n$ :

**Theorem 2.2** (Chaganty-Sethuraman's Concentration Inequality [49, Theorem 3.3] ). *For any  $\eta \in (0, 1)$ , there exists an  $N_0 \in \mathbb{N}$  such that, for all  $n \geq N_0$ ,*

$$\Pr \left\{ \frac{1}{n} Z_n \geq T_n, \right\} \geq \frac{1 - \eta}{t_n^* \sqrt{2\pi n m_{2,n}}} \exp\{-n\Lambda_n^*(T_n)\}, \quad (2.73)$$

where  $m_{2,n} := \frac{1}{n} \sum_{i=1}^n \text{Var}_{\tilde{\mu}_{n,i}}[X_i]$ , and the measure  $\tilde{\mu}_{n,i}$  is defined via

$$\frac{d\tilde{\mu}_{n,i}}{d\mu_i}(y) := \frac{e^{yt_n^*}}{\mathbb{E}[e^{t_n^* X_i}]} \quad (2.74)$$

*Remark 2.1.* Chaganty and Sethuraman proved Theorem 2.2 provided that the following condition is satisfied: there exists  $\delta_0 > 0$  such that for any  $\delta$  and  $\lambda$  with  $0 < \delta < \delta_0 < \lambda$ ,

$\sup_{\delta < |t| \leq \lambda t_n^*} \left| \frac{\exp\{\Lambda_n(t_n^* + it)\}}{\exp\{\Lambda_n(t_n^*)\}} \right| = o(1/\sqrt{n})$ , where the supremum is defined to be 0 if  $\{t : \delta < |t| \leq \lambda t_n^*\}$  is empty. In the case of  $Z_n$  being a sum of random variables,  $\exp\{\Lambda_n(t_n^* + it)\}/\exp\{\Lambda_n(t_n^*)\}$  is the product of the characteristic functions of  $\{X_i\}_{i=1}^n$ . Since the supremum of a characteristic function on a compact interval not containing 0 is less than 1, this condition is thus satisfied.

We note that the lower bound in Theorem 2.2 for the general sequence of random variables  $(X_i)_{i \in \mathbb{N}}$  suffices to establish the converse bound in moderate deviation analysis for c-q channel coding, Theorem 12.2 in Chapter 12 later. We do not particularly consider the case of lattice valued random variables (see e.g. [49, Theorem 3.5]).  $\diamond$

## Chapter 3

# Quantum Entropic Quantities and Notation

In this chapter, we introduce necessary notation in quantum information theory. In Section 3.1, we present various quantum generalizations of the classical Rényi divergence [96], and their mathematical properties. As we will see in quantum hypothesis testing discussed in Chapter 4, some specific definitions of the quantum Rényi divergence naturally arise in the exponent function. In Sections 3.2 and 3.3, we define the conditional Rényi entropies and Rényi mutual information, which play significant roles in th Parts II and III, respectively. We refer the interested readers to books [99, 50, 10] for more comprehensive discussions.

*Notation.* Throughout this thesis, we consider a finite-dimensional Hilbert space  $\mathcal{H}$ . The set of density operators (i.e. positive semi-definite operators with unit trace) and the set of full-rank density operators on  $\mathcal{H}$  are defined as  $\mathcal{S}(\mathcal{H})$  and  $\mathcal{S}(\mathcal{H})_{>0}$ . For  $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ , we write  $\rho \ll \sigma$  if the support of  $\rho$  is contained in the support of  $\sigma$ . The identity operator on  $\mathcal{H}$  is denoted by  $\mathbb{1}_{\mathcal{H}}$ . If there is no possibility of confusion, we will skip the subscript  $\mathcal{H}$ . We use  $\text{Tr}[\cdot]$  as the standard trace function. Let  $\mathbb{N}$ ,  $\mathbb{R}$ ,  $\mathbb{R}_{\geq 0}$ , and  $\mathbb{R}_{>0}$  denote the set of integers, real numbers, non-negative real numbers, and positive real numbers, respectively. Define  $[n] := \{1, 2, \dots, n\}$  for  $n \in \mathbb{N}$ .

F For a positive semi-definite operator  $A$  whose spectral decomposition is  $A = \sum_i a_i P_i$ , where  $(a_i)_i$  and  $(P_i)_i$  are the eigenvalues and eigenprojections of  $A$ , its power is defined as:  $A^p := \sum_{i:a_i \neq 0} a_i^p P_i$ . In particular,  $A^0$  denotes the projection onto  $\text{supp}(A)$ , where we use  $\text{supp}(A)$  to denote the support of the operator  $A$ . Further,  $A \perp B$  means  $\text{supp}(A) \cap \text{supp}(B) = \emptyset$ , and  $A \ll B$  indicates  $\text{supp}(A) \subseteq \text{supp}(B)$ . We denote by  $\log$  the natural logarithm. We use  $f \vee g$  (resp.  $a \wedge b$ ) to denote the pointwise maximum (resp. minimum) between two functions  $f$  and  $g$ .

Given a pair of positive semi-definite operators  $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ , we define *quantum relative entropy* [100, 101] as

$$D(\rho\|\sigma) := \text{Tr} [\rho (\log\rho - \log\sigma)]. \quad (3.1)$$

We define two types of the *quantum relative entropy variances* [16, 17, 18] by

$$V(\rho\|\sigma) := \text{Tr} [\rho (\log \rho - \log \sigma)^2] - D(\rho\|\sigma)^2 \quad (3.2)$$

$$\tilde{V}(\rho\|\sigma) := \int_0^1 dt \text{Tr} [\rho^{1-t} (\log \rho - \log \sigma) \rho^t (\log \rho - \log \sigma)] - D(\rho\|\sigma)^2. \quad (3.3)$$

They are defined to be  $+\infty$  when  $\rho \not\ll \sigma$ . We note that when  $\rho$  and  $\sigma$  commute,  $D(\rho\|\sigma)$  reduces to the classical Kullback-Leibler divergence [102]. It is well-known that both the quantities are non-negative, and  $D(\rho\|\sigma) = 0$  if and only if  $\rho = \sigma$ , which in turn shows that

$$V(\rho\|\sigma) > 0 \quad \text{implies} \quad D(\rho\|\sigma) > 0. \quad (3.4)$$

### 3.1 Quantum Rényi divergence

For density operators  $\rho, \sigma \in \mathcal{S}(\mathcal{H})_{>0}$ , and every  $\alpha \in [0, \infty)$ , we define the following two families of quantum Rényi divergences [60, 58, 59]:

$$D_\alpha(\rho\|\sigma) := \frac{1}{\alpha-1} \log Q_\alpha(\rho\|\sigma), \quad Q_\alpha(\rho\|\sigma) := \text{Tr} [\rho^\alpha \sigma^{1-\alpha}]; \quad (3.5)$$

$$D_\alpha^\flat(\rho\|\sigma) := \frac{1}{\alpha-1} \log Q_\alpha^\flat(\rho\|\sigma), \quad Q_\alpha^\flat(\rho\|\sigma) := \text{Tr} [e^{\alpha \log \rho + (1-\alpha) \log \sigma}]. \quad (3.6)$$

We term the above quantities as the (*Petz*)  $\alpha$ -Rényi divergence, and the log-Euclidean  $\alpha$ -Rényi divergence, respectively. The log-Euclidean Rényi divergence arises from the *log-Euclidean operator mean* (also called the *chaotic mean*):  $A \diamond_\alpha B := \exp((1-\alpha) \log A + \alpha \log B)$  for  $0 \leq \alpha \leq 1$ . For general density operators  $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ , the above definitions can be extended as

$$Q_\alpha(\rho\|\sigma) := \lim_{\delta \searrow 0} Q_\alpha(\rho + \delta \mathbb{1} \| \sigma + \delta \mathbb{1}) \quad \text{and} \quad Q_\alpha^\flat(\rho\|\sigma) := \lim_{\delta \searrow 0} Q_\alpha^\flat(\rho + \delta \mathbb{1} \| \sigma + \delta \mathbb{1}). \quad (3.7)$$

For  $\alpha = 1$ , we define (see e.g. [59, Lemma 3.5]):

$$Q_1(\rho\|\sigma) := \text{Tr} [\rho \sigma^0] \quad \text{and} \quad Q_1^\flat(\rho\|\sigma) := \text{Tr} [\rho \sigma^0]; \quad (3.8)$$

$$D_1(\rho\|\sigma) := \lim_{\alpha \rightarrow 1} D_\alpha(\rho\|\sigma) = \mathbb{D}(\rho\|\sigma) \quad \text{and} \quad D_1^\flat(\rho\|\sigma) := \lim_{\alpha \rightarrow 1} D_\alpha^\flat(\rho\|\sigma) = \mathbb{D}(\rho\|\sigma). \quad (3.9)$$

In addition, these two quantities are related by the Golden-Thompson inequality given in Lemma 2.7:

$$Q_\alpha^\flat(\rho\|\sigma) \leq Q_\alpha(\rho\|\sigma), \quad \forall \alpha \in [0, 1]. \quad (3.10)$$

The log-Euclidean Rényi divergence is closely related to the quantum version of the *Hellinger arc* in statistics [103, 104], [59, Section 3]. Lemma 3.1 will be useful to prove the variational representations in Sections 5.1 and 9.1 later.

**Lemma 3.1** ([59, Theorem 3.6]). *Let  $\rho, \tau \in \mathcal{S}(\mathcal{H})$  with  $\rho \ll \tau$ . For all  $s > -1$ , it follows that*

$$\min_{\sigma \in \mathcal{S}(\mathcal{H})} D(\sigma\|\rho) + sD(\sigma\|\tau) = sD_{\frac{1}{1+s}}^\flat(\rho\|\tau). \quad (3.11)$$

In the following, we provide useful mathematical properties. Most of them can be found in

Refs. [105, 59, 106].

**Lemma 3.2.** *The following hold:*

- (a) *For every  $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ , the map  $\alpha \mapsto D_\alpha(\rho\|\sigma)$  is continuous and monotone increasing on  $[0, 1]$ .*
- (b) *Let  $\rho \in \mathcal{S}(\mathcal{H})$ , positive semi-definite operators  $\sigma_1$  and  $\sigma_2$  on  $\mathcal{H}$ , and  $\alpha \in [0, 1]$ . If  $\sigma_1 \leq \sigma_2$ , then  $D_\alpha(\rho\|\sigma_1) \geq D_\alpha(\rho\|\sigma_2)$ . Moreover, if  $\sigma_1 = \gamma\sigma_2$  for some  $\gamma > 0$ , then  $D_\alpha(\rho\|\sigma_1) = D_\alpha(\rho\|\sigma_2) - \log \gamma$ .*
- (c) *For every  $\rho \in \mathcal{S}(\mathcal{H})$  and  $\alpha \in [0, 1]$ , the map  $\sigma \mapsto D_\alpha(\rho\|\sigma)$  is convex and lower semi-continuous on  $\mathcal{S}(\mathcal{H})$ .*
- (d) *For every  $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ , the map  $\alpha \mapsto (\alpha - 1)D_\alpha(\rho\|\sigma)$  is convex on  $(0, 1)$ .*
- (e) *For any positive semi-definite operators  $\rho, \sigma$  on  $\mathcal{H}$ , we have*

$$D_\alpha(\rho\|\sigma) \leq D_\alpha^b(\rho\|\sigma), \quad \alpha \in [0, 1]. \quad (3.12)$$

We note that item (a) was proved in [59, Lemma 3.12, Corollary 3.15]; item (b) was proved in [59, Lemma 3.24]; item (c) was shown in [107, 105, 60] [59, Theorem 3.16]<sup>1</sup>; item (d) was proved in [59, Lemma 3.12] item (e) is due to Golden-Thompson inequality [61, 90, 62] (see also Lemma 2.7, [59, Proposition 3.20]).

Let  $\mathcal{X} = \{1, 2, \dots, |\mathcal{X}|\}$  be a finite alphabet, and let  $\mathcal{P}(\mathcal{X})$  be the set of probability distributions on  $\mathcal{X}$ . Let  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  be a c-q channel. We denote a c-q state by:

$$P \circ \mathcal{W} := \sum_{x \in \mathcal{X}} P(x) |x\rangle\langle x| \otimes W_x. \quad (3.13)$$

We also express the input distribution  $P \in \mathcal{P}(\mathcal{X})$  as a diagonalized matrix with respect to the computational basis  $(|x\rangle)_{x \in \mathcal{X}}$ , i.e.  $P = \sum_{x \in \mathcal{X}} P(x) |x\rangle\langle x|$ .

We define the *conditional quantum relative entropy* of two sets of density operators  $\bar{\mathcal{W}}, \mathcal{W}$  and  $P \in \mathcal{P}(\mathcal{X})$  as

$$D(\bar{\mathcal{W}}\|\mathcal{W}|P) := \sum_{x \in \mathcal{X}} P(x) D(\bar{W}_x\|W_x). \quad (3.14)$$

Similarly, we define the following conditional entropic quantities for  $\sigma \in \mathcal{S}(\mathcal{H})$  and  $P \in \mathcal{P}(\mathcal{X})$ :

$$D(\mathcal{W}\|\sigma|P) := \sum_{x \in \mathcal{X}} P(x) D(W_x\|\sigma), \quad (3.15)$$

$$D_\alpha(\mathcal{W}\|\sigma|P) := \sum_{x \in \mathcal{X}} P(x) D_\alpha(W_x\|\sigma), \quad (3.16)$$

$$V(\mathcal{W}\|\sigma|P) := \sum_{x \in \mathcal{X}} P(x) V(W_x\|\sigma), \quad (3.17)$$

$$\tilde{V}(\mathcal{W}\|\sigma|P) := \sum_{x \in \mathcal{X}} P(x) \tilde{V}(W_x\|\sigma). \quad (3.18)$$

---

<sup>1</sup>It was shown in [59, Corollary 3.27] that the map  $\sigma \mapsto D_\alpha(\rho\|\sigma)$  is lower semi-continuous on  $\mathcal{S}(\mathcal{H})$  for all  $\alpha \in (0, 1)$ . The argument can be extended to the range  $\alpha \in [0, 1]$  by the same method in [59, Lemma 3.26, Corollary 3.27].

### 3.2 Conditional Rényi Entropy

For  $\rho_{AB} \in \mathcal{S}(AB)$ ,  $\alpha \geq 0$  and  $t = \{\}$ , or  $\{\flat\}$ , the *quantum conditional Rényi entropies* are given by

$$\begin{aligned} H_\alpha^{t,\uparrow}(A|B)_\rho &:= \sup_{\sigma_B \in \mathcal{S}(B)} -D_\alpha^t(\rho_{AB}\|\mathbb{1}_A \otimes \sigma_B), \\ H_\alpha^{t,\downarrow}(A|B)_\rho &:= -D_\alpha^t(\rho_{AB}\|\mathbb{1}_A \otimes \rho_B). \end{aligned} \quad (3.19)$$

In (3.19) When  $\alpha = 1$  and  $t = \{\}$ , or  $\{\flat\}$ , both quantities coincide with the usual *quantum conditional entropy*:

$$H_1^{t,\uparrow}(A|B)_\rho = H_1^{t,\downarrow}(A|B)_\rho = H(A|B)_\rho := H(AB)_\rho - H(B)_\rho, \quad (3.20)$$

where  $H(A)_\rho := -\text{Tr}[\rho_A \log \rho_A]$  denotes the *von Neumann entropy* [7].

We also define the *conditional information variance* [16] as:

$$V(A|B)_\rho := V(\rho_{AB}\|\mathbb{1}_A \otimes \rho_B). \quad (3.21)$$

**Proposition 3.1** (Properties of  $\alpha$ -Rényi Conditional Entropy). *Given any classical-quantum state  $\rho_{XB} \in \mathcal{S}(XB)$ , the following holds:*

- (a) *The map  $\alpha \mapsto H_\alpha^\uparrow(X|B)_\rho$  is continuous and monotonically decreasing on  $[0, 1]$ .*
- (b) *The map  $\alpha \mapsto \frac{1-\alpha}{\alpha} H_\alpha^\uparrow(X|B)_\rho$  is concave on  $(0, 1)$ .*

*Proof of Proposition 3.1.*

(3.1)-(a) Fix an arbitrary sequence  $(\alpha_k)_{k \in \mathbb{N}}$  such that  $\alpha_k \in [0, 1]$  and  $\lim_{k \rightarrow +\infty} \alpha_k = \alpha_\infty \in [0, 1]$ . Let

$$\sigma_k^* \in \arg \min_{\sigma \in \mathcal{S}(\mathcal{H})} D_{\alpha_k}(\rho_{XB}\|\mathbb{1}_X \otimes \sigma), \quad \forall k \in \mathbb{N} \cup \{+\infty\}. \quad (3.22)$$

The definition in Eq. (3.19) implies that

$$\limsup_{k \rightarrow +\infty} H_{\alpha_k}^\uparrow(X|B)_\rho = -\liminf_{k \rightarrow +\infty} D_{\alpha_k}(\rho_{XB}\|\mathbb{1}_X \otimes \sigma_k^*) \quad (3.23)$$

$$\leq -D_{\alpha_\infty} \left( \rho_{XB} \left\| \mathbb{1}_X \otimes \left( \lim_{k \rightarrow +\infty} \sigma_k^* \right) \right\| \right) \quad (3.24)$$

$$\leq -\min_{\sigma \in \mathcal{S}(\mathcal{H})} D_{\alpha_\infty}(\rho_{XB}\|\mathbb{1}_X \otimes \sigma) \quad (3.25)$$

$$= H_{\alpha_\infty}^\uparrow(X|B)_\rho, \quad (3.26)$$

where, in order to establish (3.24), we used the lower semi-continuity of the map  $\sigma \mapsto D_{\alpha_k}(\rho_{XB}\|\mathbb{1}_X \otimes \sigma)$  (Lemma 3.2-(c)) and the continuity of  $\alpha \mapsto D_\alpha(\rho_{XB}\|\mathbb{1}_X \otimes \sigma_k^*)$  (Lemma 3.2-(a)).

Next, we let

$$\sigma_k := (1 - \varepsilon_k) \sigma_\infty^* + \varepsilon_k \frac{\mathbb{1}}{d}, \quad \forall k \in \mathbb{N}, \quad (3.27)$$

where  $(\varepsilon_k)_{k \in \mathbb{N}}$  is an arbitrary positive sequence that converges to zero. Then, it follows that

$$\liminf_{k \rightarrow +\infty} H_{\alpha_k}^{\uparrow}(X|B)_{\rho} \geq -\limsup_{k \rightarrow +\infty} \{D_{\alpha_k}(\rho_{XB} \| \mathbb{1}_X \otimes \sigma_k)\} \quad (3.28)$$

$$= -D_{\alpha_{\infty}}(\rho_{XB} \| \mathbb{1}_X \otimes \sigma_{\infty}^*) \quad (3.29)$$

$$= H_{\alpha_{\infty}}^{\uparrow}(X|B)_{\rho}. \quad (3.30)$$

Here, equality (3.29) holds because  $\mathbb{1}_X \otimes \sigma_k \gg \rho_{XB}$  for all  $k \in \mathbb{N} \cup \{+\infty\}$ . Thus, the map  $(\alpha_k, \sigma_k) \mapsto D_{\alpha_k}(\rho_{XB} \| \mathbb{1}_X \otimes \sigma_k)$  is continuous for  $k \in \mathbb{N} \cup \{+\infty\}$ . Hence, we prove the continuity.

Now, we show the monotonicity. For all  $\sigma_B \in \mathcal{S}(B)$ , Lemma 3.2-(a) implies that  $-D_{\alpha}(\rho_{XB} \| \mathbb{1} \otimes \sigma_B)$  is monotonically decreasing in  $\alpha \geq 0$ . Since  $H_{\alpha}^{\uparrow}(X|B)_{\rho}$  is the pointwise supremum of the above function, we conclude that  $H_{\alpha}^{\uparrow}(X|B)_{\rho}$  is monotonically decreasing in  $\alpha \geq 0$ . Hence, item (a) is proven.

- (3.1)-(b) For convenience, we make a substitution  $\alpha = 1/(1+s)$ . The concavity for  $s \geq 0$  can be proved with the geometric matrix means in [36]. Here, we present another proof by the following matrix inequality. Let  $\rho_{XB} = \sum_{x \in \mathcal{X}} P(x)|x\rangle\langle x| \otimes W_x$ ,  $t = \gamma = 1$ ,  $i = x$ ,  $k = |\mathcal{X}|$ ,  $A_i = P(x)W_x$ , and  $Z_i = I_{n,m}$ . We obtain the log-convexity of the map by applying Lemma 2.12:

$$p \mapsto \text{Tr} \left( \sum_{x \in \mathcal{X}} (P(x)W_x)^{\frac{1}{p}} \right)^p, \quad \forall p > 0, \quad (3.31)$$

which is exactly the concavity of the map  $s \mapsto sH_{1/(1+s)}^{\uparrow}(X|B)_{\rho}$  for all  $s > 0$ .

□

### 3.3 Rényi and Augustin Information

The *mutual information* of a c-q channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  with a prior distribution  $P \in \mathcal{P}(\mathcal{X})$  is defined by

$$I(P, \mathcal{W}) := D(P \circ \mathcal{W} \| P \otimes P\mathcal{W}) = D(\mathcal{W} \| P\mathcal{W}|P), \quad (3.32)$$

where  $P \circ \mathcal{W} := \sum_{x \in \mathcal{X}} P(x)|x\rangle\langle x| \otimes W_x$  and  $P\mathcal{W} := \sum_{x \in \mathcal{X}} P(x)W_x$ . Hence, the *information radius* or *information capacity*<sup>2</sup> of  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  is

$$C_{\mathcal{W}} := \sup_{P \in \mathcal{P}(\mathcal{X})} I(P, \mathcal{W}). \quad (3.33)$$

The *conditional information variance* and the *unconditional information variance* of  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  with a prior distribution  $P \in \mathcal{P}(\mathcal{X})$  are defined, respectively, by

$$\begin{aligned} V(P, \mathcal{W}) &:= V(\mathcal{W} \| P\mathcal{W}|P), \\ U(P, \mathcal{W}) &:= V(P \circ \mathcal{W} \| P \otimes P\mathcal{W}). \end{aligned} \quad (3.34)$$

---

<sup>2</sup>We note that  $C_{\mathcal{W}}$  equals to the capacity of classical communications over quantum channels [108, 109, 110]. It is usually term *classical capacity* [50], though it is a quantity in quantum information processing.

Note that  $V(P^*, \mathcal{W}) = U(P^*, \mathcal{W})$  for every capacity-achieving distribution  $P^* \in \mathcal{P}(\mathcal{X})$ , i.e.  $I(P^*, \mathcal{W}) = C_{\mathcal{W}}$ , can be easily verified from the similar argument in [14, Lemma 62]. We also define the unconditional information variance in terms of  $\tilde{V}(\rho\|\sigma)$ :

$$\tilde{V}(P, \mathcal{W}) := \tilde{V}(\mathcal{W}\|P\mathcal{W}|P). \quad (3.35)$$

The *minimal peripheral information variance* and its variant are defined by

$$V_{\mathcal{W}} := \inf_{P \in \mathcal{P}(\mathcal{X}): I(P, \mathcal{W}) = C_{\mathcal{W}}} V(P, \mathcal{W}), \quad (3.36)$$

$$\tilde{V}_{\mathcal{W}} := \inf_{P \in \mathcal{P}(\mathcal{X}): I(P, \mathcal{W}) = C_{\mathcal{W}}} \tilde{V}(P, \mathcal{W}). \quad (3.37)$$

Furthermore, one can easily verify that

$$V_{\mathcal{W}} > 0 \quad \text{implies} \quad C_{\mathcal{W}} > 0. \quad (3.38)$$

In the following, We define two related information quantities: for every  $\alpha \in [0, 1]$ ,

$$I_{\alpha}^{(1)}(P, \mathcal{W}) := \inf_{\sigma \in \mathcal{S}(\mathcal{H})} D_{\alpha}(P \circ \mathcal{W}\|P \otimes \sigma); \quad (3.39)$$

$$I_{\alpha}^{(2)}(P, \mathcal{W}) := \inf_{\sigma \in \mathcal{S}(\mathcal{H})} D_{\alpha}(\mathcal{W}\|\sigma|P). \quad (3.40)$$

The term  $I_{\alpha}^{(1)}(P, \mathcal{W})$  is called the  $\alpha$ -Rényi mutual information [111, 65, 59, 112] or the *generalized Holevo quantity*. The second term  $I_{\alpha}^{(2)}(P, \mathcal{W})$  can be viewed as a variant of the  $\alpha$ -Rényi mutual information, called  $\alpha$ -Augustin mutual information [113, 114]. It can be verified that these two functions are related by Jensen's inequality:

$$I_{\alpha}^{(1)}(P, \mathcal{W}) \leq I_{\alpha}^{(2)}(P, \mathcal{W}). \quad (3.41)$$

For the case of  $\alpha = 1$ , they both equal conventional mutual information, i.e.  $I_1^{(1)}(P, \mathcal{W}) = I_1^{(2)}(P, \mathcal{W}) = I(P, \mathcal{W})$ . Mosonyi and Ogawa [59, Proposition 4.2] showed that for all  $\alpha \in [0, 1]$ ,

$$C_{\alpha, \mathcal{W}} := \sup_{P \in \mathcal{P}(\mathcal{X})} I_{\alpha}^{(1)}(P, \mathcal{W}) = \sup_{P \in \mathcal{P}(\mathcal{X})} I_{\alpha}^{(2)}(P, \mathcal{W}), \quad (3.42)$$

and it is termed the *Rényi radius* or the *Rényi capacity* of order  $\alpha$ . Moreover, Proposition 3.2 below and the compactness of  $\mathcal{P}(\mathcal{X})$  show that the suprema in Eq. (3.42) can be replaced with maxima.

We note that  $I_{\alpha}^{(1)}$  admits a closed form for  $\alpha \in (0, 1]$  due to the quantum Sibson's identity below. The minimizer in Eq. (3.40) will be studied in Proposition 3.2.

**Lemma 3.3** (Quantum Sibson's Identity [115]). *Fix an  $\alpha \in (0, 1]$ . Let  $\rho_{AB} \in \mathcal{S}(AB)$  and let  $\sigma_B^*$  be the minimizer of  $\min_{\sigma_B \in \mathcal{S}(B)} D_{\alpha}(\rho_{AB}\|\rho_A \otimes \sigma_B)$ . Then, one has*

$$\sigma^* = \frac{(\mathrm{Tr}_A[\rho_{AB}^{\alpha}])^{\frac{1}{\alpha}}}{\mathrm{Tr}\left[(\mathrm{Tr}_A[\rho_{AB}^{\alpha}])^{\frac{1}{\alpha}}\right]}. \quad (3.43)$$

The following proposition presents important properties of  $\alpha$ -Augustin mutual information and

radius.

**Proposition 3.2** (Properties of order  $\alpha$  Augustin Information and Radius). *Given any classical-quantum channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  with  $|\mathcal{X}| < \infty$ , the following hold:*

- (a) *For every  $P \in \mathcal{P}(\mathcal{X})$ ,  $\alpha \mapsto I_\alpha^{(2)}(P, \mathcal{W})$  is monotone increasing on  $[0, 1]$ , and  $I_\alpha^{(2)}(P, \mathcal{W}) \leq \log |\mathcal{X}|$  for all  $\alpha \in [0, 1]$ .*
- (b) *For every  $(\alpha, P) \in (0, 1] \times \mathcal{P}(\mathcal{X})$ , there exists a unique  $\sigma_{\alpha, P} \in \mathcal{S}(\mathcal{H})$ , termed Augustin mean, such that*

$$I_\alpha^{(2)}(P, \mathcal{W}) = D_\alpha(\mathcal{W} \| \sigma_{\alpha, P} | P), \quad (3.44)$$

and

$$\mathsf{T}_{\alpha, P}(\sigma) = \sigma \text{ and } \sigma \gg P\mathcal{W} \text{ if and only if } \sigma = \sigma_{\alpha, P}, \quad (3.45)$$

where the map  $\mathsf{T}_{\alpha, P} : \mathcal{S}_{P, \mathcal{W}}(\mathcal{H}) \rightarrow \mathcal{S}(\mathcal{H})$  is defined as

$$\mathsf{T}_{\alpha, P}(\sigma) = \sum_{x \in \mathcal{X}} P(x) \frac{\sigma^{\frac{1-\alpha}{2}} W_x^\alpha \sigma^{\frac{1-\alpha}{2}}}{\text{Tr}[W_x^\alpha \sigma^{1-\alpha}]} \quad (3.46)$$

- (c) *For every  $\alpha \in [0, 1]$ , the map  $P \mapsto I_\alpha^{(2)}(P, \mathcal{W})$  is concave on  $\mathcal{P}(\mathcal{X})$ .*
- (d) *For every  $P \in \mathcal{P}(\mathcal{X})$ ,  $\alpha \mapsto \frac{1-\alpha}{\alpha} I_\alpha^{(2)}(P, \mathcal{W})$  is concave on  $(0, 1]$ .*
- (e) *For every  $P \in \mathcal{P}(\mathcal{X})$ ,  $\alpha \mapsto I_\alpha^{(2)}(P, \mathcal{W})$  is continuous on  $[0, 1]$ .*
- (f) *The family of functions  $\{I_\alpha^{(2)}(P, \mathcal{W})\}_{\alpha \in [0, 1]}$  is uniformly equicontinuous in  $P \in \mathcal{P}(\mathcal{X})$ . Moreover, The map  $(\alpha, P) \mapsto I_\alpha^{(2)}(P, \mathcal{W})$  is jointly continuous on  $[0, 1] \times \mathcal{P}(\mathcal{X})$ .*
- (g) *The map  $(\alpha, P) \mapsto \sigma_{\alpha, P}$  is jointly continuous on  $(0, 1] \times \mathcal{P}(\mathcal{X})$ .*
- (h) *The map  $\alpha \mapsto C_{\alpha, \mathcal{W}}$  is continuous and monotone increasing on  $[0, 1]$ .*

*Proof of Proposition 3.2.*

- (3.2)-(a) Recalling the definition of  $I_\alpha^{(2)}$  given in Eq. (3.40). The statement immediately follows from Lemma 3.2-(a) (see also [59, Lemma 4.6]) because the minimization over  $\sigma \in \mathcal{S}(\mathcal{H})$  preserves the monotonicity. Hence, we have  $I_\alpha^{(2)}(P, \mathcal{W}) \leq I_1(P, \mathcal{W}) \leq \log |\mathcal{X}|$ , where the last inequality follows from the well-known upper bound for the Holevo quantity (see e.g. [7, Chapter 12]).
- (3.2)-(b) We first note that the infimum in Eq. (3.40) can be attained. This can be verified by the following argument. Lemma 3.2-(c) shows that  $D_\alpha$  is lower semi-continuous in its second argument. Hence, the linear combination, i.e.  $D_\alpha(\mathcal{W} \| \sigma | P)$ , is also lower semi-continuous on  $\mathcal{S}(\mathcal{H})$ . Further,  $\mathcal{S}(\mathcal{H})$  is compact owing to the assumption of the finite-dimensional Hilbert space  $\mathcal{H}$ . Thus, the extreme value theorem [116, Chapter 30§12.2] guarantees that the infimum can be attained

For  $\alpha = 1$ , it is well-known that (see e.g. [108])  $\sigma_{1,P} = P\mathcal{W}$ . Using the fact  $P\mathcal{W} \gg W_x$  for all  $x \in \text{supp}(P)$ , the statements immediately follow.

We fix an arbitrary  $(\alpha, P) \in (0, 1) \times \mathcal{P}(\mathcal{X})$  subsequently. Without loss of generality, we may further assume

$$\bigcup_{x \in \text{supp}(P)} \text{supp}(W_x) = \mathbb{1}_{\mathcal{H}}, \quad (3.47)$$

and hence  $P\mathcal{W}$  has full support. We first show that the minimizer  $\sigma_{\alpha,P}$  has full support too. Second, we prove the fixed-point property Eq. (3.45). Finally, we establish the uniqueness of  $\sigma_{\alpha,P}$ . We remark that the uniqueness has been proven by Dalai and Winter [39, Appendix D]. Here, we provide an alternative proof for the completeness. Our approach follows closely from Hayashi and Tomamichel [111, Appendix C].

Define

$$\mathcal{M}_\alpha(\mathcal{H}) := \arg \min_{\sigma \in \mathcal{S}(\mathcal{H})} D_\alpha(\mathcal{W} \| \sigma | P) = \arg \max_{\sigma \in \mathcal{S}(\mathcal{H})} g_\alpha(\sigma) = \arg \max_{\sigma \in \mathcal{S}_{P,\mathcal{W}}(\mathcal{H})} g_\alpha(\sigma) \quad (3.48)$$

where

$$g_\alpha(\sigma) := \sum_{x \in \mathcal{X}} P(x) \log \text{Tr} [W_x^\alpha \sigma^{1-\alpha}]. \quad (3.49)$$

To show that the optimizer of  $g_\alpha(\cdot)$  has full support, we observe that the directional derivative on the boundary of  $\mathcal{S}(\mathcal{H})$  where at least one eigenvalue is zero in a direction that increases its rank diverges to positive infinite. Namely, it suffices to show

$$\lim_{t \rightarrow 0} \frac{g_\alpha((1-t)\sigma + t\sigma^\perp) - g_\alpha(\sigma)}{t} = +\infty, \quad (3.50)$$

where  $\sigma \in \mathcal{S}_{P,\mathcal{W}}(\mathcal{H})$  is some singular density operator, and  $\sigma^\perp := \frac{(\mathbb{1}_{\mathcal{H}} - \sigma)}{\text{Tr}[\mathbb{1}_{\mathcal{H}} - \sigma]}$ . For  $x \in \text{supp}(P)$  with  $W_x \ll \sigma$ , we have  $W_x \perp \sigma^\perp$ . It is not hard to see that

$$\lim_{t \rightarrow 0} P(x) \frac{\log \text{Tr} [W_x^\alpha ((1-t)\sigma + t\sigma^\perp)^{1-\alpha}] - \log \text{Tr} [W_x^\alpha \sigma^{1-\alpha}]}{t} \quad (3.51)$$

$$= \lim_{t \rightarrow 0} P(x) \frac{\log \text{Tr} [W_x^\alpha ((1-t)^{1-\alpha} \sigma^{1-\alpha} + t^{1-\alpha} (\sigma^\perp)^{1-\alpha})] - \log \text{Tr} [W_x^\alpha \sigma^{1-\alpha}]}{t} \quad (3.52)$$

$$= \lim_{t \rightarrow 0} P(x) \frac{(1-\alpha) \log(1-t)}{t} \quad (3.53)$$

$$= \lim_{t \rightarrow 0} P(x) \frac{-(1-\alpha)}{1-t} \quad (3.54)$$

$$= -P(x)(1-\alpha) \quad (3.55)$$

$$> -\infty \quad (3.56)$$

where Eq. (3.52) holds because  $\sigma \perp \sigma^\perp$ ; Eq. (3.53) is due to  $W_x \perp \sigma^\perp$ ; and Eq. (3.54) is owing to L'Hôpital's rule.

On the other hand, since  $\sigma$  is singular, there must be some  $x \in \text{supp}(P)$  such that  $W_x \not\ll \sigma$ .

Hence, by denoting  $c := \frac{\text{Tr}[W_x^\alpha(\sigma^\perp)^{1-\alpha}]}{\text{Tr}[W_x^\alpha\sigma^{1-\alpha}]} > 0$ , Eq. (3.52) leads to

$$\lim_{t \rightarrow 0} P(x) \frac{\log \{(1-t)^{1-\alpha} + t^{1-\alpha}c\}}{t} \quad (3.57)$$

$$= \lim_{t \rightarrow 0} P(x) \frac{-(1-\alpha)(1-t)^{-\alpha} + (1-\alpha)t^{-\alpha}c}{(1-t)^{1-\alpha} + t^{1-\alpha}c} \quad (3.58)$$

$$= +\infty, \quad (3.59)$$

where Eq. (3.58) is by L'Hôpital's rule again. Combining Eqs. (3.56) and (3.59) concludes Eq. (3.50).

Next, we show the fixed-point property:  $\mathcal{M}_\alpha(\mathcal{H}) = \mathcal{F}_\alpha(\mathcal{H})$ , where  $\mathcal{F}_\alpha(\mathcal{H}) := \{\sigma \in \mathcal{S}_{>0}(\mathcal{H})\}$  denotes the fixed-points of the map:  $\mathsf{T}_{\alpha,P} : \mathcal{S}_{P,W}(\mathcal{H}) \rightarrow \mathcal{S}(\mathcal{H})$ . A necessary and sufficient condition for  $\sigma$  to be an optimizer is

$$\partial_\omega g_\alpha(\sigma) := \mathsf{D}g_\alpha(\sigma)[\omega - \sigma] = 0, \quad (3.60)$$

for all  $\omega \in \mathcal{S}(\mathcal{H})$ , where  $\mathsf{D}g_\alpha(\sigma)$  denotes the Fréchet derivative of the map  $g_\alpha$  (see e.g. [111, Appendix C]). Using the chain rule of Fréchet derivatives, it follows

$$\partial_\omega g_\alpha(\sigma) = \text{Tr} \left[ \sum_{x \in \mathcal{X}} P(x) \frac{W_x^\alpha}{\text{Tr}[W_x^\alpha\sigma^{1-\alpha}]} \partial_\omega \sigma^{1-\alpha} \right] \quad (3.61)$$

$$= \text{Tr} \left[ \sum_{x \in \mathcal{X}} P(x) \frac{\sigma^{\frac{-\alpha}{2}} W_x^\alpha \sigma^{\frac{-\alpha}{2}}}{\text{Tr}[W_x^\alpha\sigma^{1-\alpha}]} \sigma^{\frac{\alpha}{2}} \partial_\omega \sigma^{1-\alpha} \sigma^{\frac{\alpha}{2}} \right]. \quad (3.62)$$

We claim that the operators

$$\left\{ \Delta_\omega = \sigma^{\frac{\alpha}{2}} \partial_\omega \sigma^{1-\alpha} \sigma^{\frac{\alpha}{2}} : \omega \in \mathcal{S}(\mathcal{H}) \right\} \quad (3.63)$$

span the space of traceless Hermitian operators on  $\mathcal{S}(\mathcal{H})$ . Let  $\sigma = \sum_i \lambda_i |i\rangle\langle i|$  with  $\lambda_i > 0$  be the eigenvalue decomposition. One can verify [84, Theorem 3.25] that

$$\langle i | \Delta_\omega | j \rangle = \begin{cases} (\lambda_i \lambda_j)^{\frac{\alpha}{2}} \frac{\lambda_i^{1-\alpha} - \lambda_j^{1-\alpha}}{\lambda_i - \lambda_j} \langle i | \omega - \sigma | j \rangle, & \text{if } \lambda_i \neq \lambda_j \\ (1-\alpha) \langle i | \omega - \sigma | j \rangle, & \text{if } \lambda_i = \lambda_j \end{cases}. \quad (3.64)$$

Therefore,  $\Delta_\omega$  is Hermitian and  $\text{Tr}[\Delta_\omega] = 0$  for all  $\omega \in \mathcal{S}(\mathcal{H})$ . Moreover, the basis of the traceless Hermitian operators is given by the operators

$$\left\{ \Gamma_{ij} = |i\rangle\langle j| + |j\rangle\langle i|, \Gamma'_{ij} = i(|i\rangle\langle j| - |j\rangle\langle i|), \Gamma''_{ij} = |i\rangle\langle i| - |j\rangle\langle j| \right\}_{i \neq j}. \quad (3.65)$$

For every tuple  $(i, j)$  with  $i \neq j$  there exists an  $\varepsilon > 0$  such that the state  $\omega = \sigma + \varepsilon \Gamma_{ij}$  is still in  $\mathcal{S}(\mathcal{H})$ . For this state, we find that  $\Delta_\omega = \eta \Gamma_{ij}$  for some real  $\eta > 0$ . The similar argument applies to  $\Gamma'_{ij}$  and  $\Gamma''_{ij}$ . Hence, we have verified that the operators  $\{\Delta_\omega\}_{\omega \in \mathcal{S}(\mathcal{H})}$  span the space of traceless Hermitian operators.

Armed with the above discussion, the condition that  $\partial_\omega g_\alpha(\sigma) = 0$  for all  $\omega \in \mathcal{S}(\mathcal{H})$  is equivalent

to the condition that the operators

$$\sum_{x \in \mathcal{X}} P(x) \frac{\sigma^{\frac{-\alpha}{2}} W_x^\alpha \sigma^{\frac{-\alpha}{2}}}{\text{Tr}[W_x^\alpha \sigma^{1-\alpha}]} \quad (3.66)$$

must be proportional to the identity. Thus, the optimum must be a fixed point of the map  $\mathsf{T}_{\alpha,P}(\cdot)$ .

Lastly, to prove the uniqueness of the optimizer, it remains to show  $\partial_\omega^2 g_\alpha(\sigma) : \mathbb{D}^2 g_\alpha(\sigma)[\omega - \sigma, \omega - \sigma] < 0$  for all  $\omega \neq \sigma$  and  $\sigma > 0$ . Continuing on Eq. (3.61), we have

$$\partial_\omega^2 g_\alpha(\sigma) = -\text{Tr} \left[ \sum_{x \in \mathcal{X}} P(x) \frac{W_x^\alpha}{\text{Tr}^2[W_x^\alpha \sigma^{1-\alpha}]} \partial_\omega \sigma^{1-\alpha} \right] + \text{Tr} \left[ \sum_{x \in \mathcal{X}} P(x) \frac{W_x^\alpha}{\text{Tr}[W_x^\alpha \sigma^{1-\alpha}]} \partial_\omega^2 \sigma^{1-\alpha} \right] \quad (3.67)$$

$$< \text{Tr} \left[ \sum_{x \in \mathcal{X}} P(x) \frac{W_x^\alpha}{\text{Tr}[W_x^\alpha \sigma^{1-\alpha}]} \partial_\omega^2 \sigma^{1-\alpha} \right], \quad (3.68)$$

where Eq. (3.68) holds by noting that  $\partial_\omega \sigma^{1-\alpha} \neq 0$  for all  $\omega \neq \sigma$ . Further,  $\partial_\omega^2 \sigma^{1-\alpha} \leq 0$  since  $u \mapsto u^{1-\alpha}$  is operator concave. Thus,  $\partial_\omega^2 g_\alpha(\sigma) < 0$ , item (b) is proved.

- (3.2)-(c) Recall the definition given in Eq. (3.40). The assertion follows because the pointwise infimum of linear functions is concave.
- (3.2)-(d) This assertion was proved by Mosonyi and Ogawa [59, Corollary B.2].
- (3.2)-(e) The idea of the proof originate from Nakiboğlu [114, Lemmas 16, 17].

Recalling item (d), the map  $\alpha \mapsto \frac{1-\alpha}{\alpha} I_\alpha^{(2)}(P, \mathcal{W})$  is concave on  $(0, 1]$ . Since any concave function is continuous in its interior [117, Corollary 6.3.3], the map  $\alpha \mapsto I_\alpha^{(2)}(P, \mathcal{W})$  is continuous on  $(0, 1)$ . The continuity at  $\alpha = 0$  can be verified as follows. Let  $\sigma_{0,P} \in \mathcal{S}(\mathcal{H})$  be any state such that  $I_0^{(2)}(P, \mathcal{W}) = D_0(\mathcal{W} \| \sigma_{0,P} | P)$ . Then, the monotonicity in item (a) and the definition of  $I_\alpha^{(2)}$  given in Eq. (3.40) imply that

$$I_0^{(2)}(P, \mathcal{W}) \leq I_\alpha^{(2)}(P, \mathcal{W}) \leq D_\alpha(\mathcal{W} \| \sigma_{0,P} | P), \quad \forall \alpha \in (0, 1]. \quad (3.69)$$

The continuity of  $\alpha \mapsto D_\alpha$  on  $[0, 1]$ , Lemma 3.2-(a), thus implies  $\lim_{\alpha \downarrow 0} I_\alpha(P, \mathcal{W}) = I_0(P, \mathcal{W})$ .

It remains to show the continuity at  $\alpha = 1$ . We claim the following fact about the Augustin mean.

**Lemma 3.4.** Given  $\alpha \in (0, 1]$  and  $P \in \mathcal{P}(\mathcal{X})$ , we let  $\sigma_{\alpha,P} \in \mathcal{S}(\mathcal{H})$  be the Augustin mean, i.e.  $I_{\alpha}^{(2)}(P, \mathcal{W}) = D_{\alpha}(\mathcal{W} \parallel \sigma_{\alpha,P} | P)$ . The following hold.

- For any  $\alpha \in [1/2, 1]$ ,

$$D_{\alpha}(W_x \parallel \sigma_{\alpha,P}) \leq \log \frac{1}{P(x)}. \quad (3.70)$$

- For any  $\alpha \in [1/2, 1]$ ,

$$\sigma_{\alpha,P} \leq \left( \min_{x:P(x)>0} P(x) \right)^{\frac{\alpha-1}{\alpha}} \sigma_{1,P}. \quad (3.71)$$

Then, Eq. (3.71) and Lemma 3.2-(b) imply that

$$D_{\alpha}(\mathcal{W} \parallel \sigma_{\alpha,P} | P) \geq D_{\alpha}(\mathcal{W} \parallel \sigma_{1,P} | P) + \frac{1-\alpha}{\alpha} \log \left( \min_{x:P(x)>0} P(x) \right), \quad \forall \alpha \in [1/2, 1]. \quad (3.72)$$

Moreover, the fact  $D_{\alpha}(\mathcal{W} \parallel \sigma_{\alpha,P} | P) = I_{\alpha}^{(2)}(P, \mathcal{W})$  in item (b) and the monotonicity in item (a) show that

$$D_{\alpha}(\mathcal{W} \parallel \sigma_{1,P} | P) + \frac{1-\alpha}{\alpha} \log \left( \min_{x:P(x)>0} P(x) \right) \leq I_{\alpha}^{(2)}(P, \mathcal{W}) \leq I_1^{(2)}(P, \mathcal{W}), \quad \forall \alpha \in [1/2, 1]. \quad (3.73)$$

It is clearly that  $D_{\alpha}(\mathcal{W} \parallel \sigma_{1,P} | P) < +\infty$  by the fact that  $\sigma_{1,P} \gg W_x$  for all  $x \in \text{supp}(P)$ . Then, the continuity of  $\alpha \mapsto D_{\alpha}$  on  $[0, 1]$ , Lemma 3.2-(a), together with the fact  $D_1(\mathcal{W} \parallel \sigma_{1,P} | P) = I_1^{(2)}(P, \mathcal{W})$  imply the continuity of  $I_{\alpha}^{(2)}$  at  $\alpha = 1$ .

In the following, we prove Lemma 3.4 to complete the proof of item (e).

*Proof of Lemma 3.4.* Proposition 3.2 (b) implies that the Augustin mean satisfies

$$\sigma_{\alpha,P} = \left( \sum_{x \in \mathcal{X}} P(x) W_x^{\alpha} e^{(1-\alpha)D_{\alpha}(W_x \parallel \sigma_{\alpha,P})} \right)^{\frac{1}{\alpha}}. \quad (3.74)$$

Using the operator monotonicity of  $(\cdot)^{\frac{1-\alpha}{\alpha}}$  for  $\alpha \in [1/2, 1]$  (see e.g. [69, 84]), we have

$$\sigma_{\alpha,P}^{1-\alpha} \geq P(x)^{\frac{1-\alpha}{\alpha}} W_x^{1-\alpha} e^{\frac{(1-\alpha)^2}{\alpha} D_{\alpha}(W_x \parallel \sigma_{\alpha,P})}. \quad (3.75)$$

Then, Eq. (3.75) and Lemma 3.2-(b) imply that

$$D_{\alpha}(W_x \parallel \sigma_{\alpha,P}) = \frac{1}{\alpha-1} \log \text{Tr} [W_x^{\alpha} \sigma_{\alpha,P}^{1-\alpha}] \quad (3.76)$$

$$\leq -\log P(x)^{\frac{1}{\alpha}} - \frac{1-\alpha}{\alpha} D_{\alpha}(W_x \parallel \sigma_{\alpha,P}), \quad (3.77)$$

which proves the first claim.

For any  $\alpha \in [1/2, 1]$ , the map  $(\cdot)^{\frac{1}{\alpha}}$  is operator convex. Then, Eq. (3.74) yields

$$\sigma_{\alpha,P} \leq \sum_{x \in \mathcal{X}} P(x) W_x e^{\frac{1-\alpha}{\alpha} D_\alpha(W_x \| \sigma_{\alpha,P})}. \quad (3.78)$$

Note that  $P\mathcal{W} = \sigma_{1,P}$ . Applying Eq. (3.74) on (3.78) gives the desired result in Eq. (3.71).  $\square$

(3.2)-(f) To prove the equicontinuity, we need the following inequality:

$$I_\alpha^{(2)}(\alpha, P_\beta) \leq \beta I_\alpha^{(2)}(\alpha, P_1) + (1 - \beta) I_\alpha^{(2)}(\alpha, P_0) + H(\beta) \quad (3.79)$$

for any  $P_1, P_0 \in \mathcal{P}(\mathcal{X})$ ,  $P_\beta = \beta P_1 + (1 - \beta) P_0$ ,  $\beta \in (0, 1)$ ,  $\alpha \in [0, 1]$ ; and we shorthand  $H(\beta) := -\beta \log \beta - (1 - \beta) \log(1 - \beta)$  the binary entropy function.

Let  $\sigma_{\alpha,P} \in \mathcal{S}(\mathcal{H})$  be the Augustin mean<sup>3</sup> as in item (b) for  $\alpha \in [0, 1]$ . Lemma 3.2-(b) implies that, for every  $\alpha \in [0, 1]$ ,

$$\begin{aligned} & \sum_{x \in \mathcal{X}} P_\beta(x) D_\alpha(W_x \| \beta \sigma_{\alpha,P_1} + (1 - \beta) \sigma_{\alpha,P_0}) \\ &= \beta \sum_{x \in \mathcal{X}} P_1(x) D_\alpha(W_x \| \beta \sigma_{\alpha,P_1} + (1 - \beta) \sigma_{\alpha,P_0}) + (1 - \beta) \sum_{x \in \mathcal{X}} P_0(x) D_\alpha(W_x \| \beta \sigma_{\alpha,P_1} + (1 - \beta) \sigma_{\alpha,P_0}) \end{aligned} \quad (3.80)$$

$$\leq \beta \sum_{x \in \mathcal{X}} P_1(x) D_\alpha(W_x \| \sigma_{\alpha,P_1}) - \beta \log \beta + (1 - \beta) \sum_{x \in \mathcal{X}} P_0(W_x) D_\alpha(W_x \| \sigma_{\alpha,P_0}) - (1 - \beta) \log(1 - \beta) \quad (3.81)$$

$$= \beta I_\alpha^{(2)}(P_1, \mathcal{W}) + (1 - \beta) I_\alpha(P_0, \mathcal{W}) + H(\beta). \quad (3.82)$$

Let  $s_\wedge, s_1, s_0$  be

$$s_\wedge = \frac{P_1 \wedge P_0}{\|P_1 \wedge P_0\|_1}, \quad (3.83)$$

$$s_1 = \frac{P_1 - P_1 \wedge P_0}{1 - \|P_1 \wedge P_0\|_1}, \quad (3.84)$$

$$s_0 = \frac{P_0 - P_1 \wedge P_0}{1 - \|P_1 \wedge P_0\|_1}. \quad (3.85)$$

One can verify that.

$$P_1 = \left(1 - \frac{\|P_1 - P_0\|_1}{2}\right) s_\wedge + \frac{\|P_1 - P_0\|_1}{2} s_1, \quad (3.86)$$

$$P_0 = \left(1 - \frac{\|P_1 - P_0\|_1}{2}\right) s_\wedge + \frac{\|P_1 - P_0\|_1}{2} s_0. \quad (3.87)$$

---

<sup>3</sup>For  $\alpha = 1$ , the Augustin mean is not unique. We note that the proof of item (f) does not require the uniqueness.

Then, the concavity of  $P \mapsto I_\alpha^{(2)}(P, \mathcal{W})$  given in item (c) together with Eq. (3.79) yield

$$I_\alpha^{(2)}(P_0, \mathcal{W}) - I_\alpha^{(2)}(P_1, \mathcal{W}) \leq H\left(\frac{\|P_1 - P_0\|_1}{2}\right) + \frac{\|P_1 - P_0\|_1}{2} \left(I_\alpha^{(2)}(s_0, \mathcal{W}) - I_\alpha^{(2)}(s_1, \mathcal{W})\right) \quad (3.88)$$

$$\leq H\left(\frac{\|P_1 - P_0\|_1}{2}\right) + \frac{\|P_1 - P_0\|_1}{2} I_\alpha^{(2)}(s_0, \mathcal{W}) \quad (3.89)$$

for  $\alpha \geq 0$ . Thus,

$$\left|I_\alpha^{(2)}(P_0, \mathcal{W}) - I_\alpha^{(2)}(P_1, \mathcal{W})\right| \leq H\left(\frac{\|P_1 - P_0\|_1}{2}\right) + \frac{\|P_1 - P_0\|_1}{2} \log |\mathcal{X}| \quad (3.90)$$

since  $\alpha \mapsto I_\alpha^{(2)}$  is monotone increasing by item (a). The above inequality implies the desired equicontinuity.

The joint continuity of  $(\alpha, P) \mapsto I_\alpha^{(2)}(P, \mathcal{W})$  follows from the continuity of  $\alpha \mapsto I_\alpha^{(2)}(P, \mathcal{W})$  given in (e) and uniform equicontinuity.

- (3.2)-(g) Let  $(\alpha_k, P_k)_{k \in \mathbb{N}}$  be an arbitrary sequence such that  $\alpha_k \in (0, 1]$ ,  $P_k \in \mathcal{P}(\mathcal{X})$ , and  $\lim_{k \rightarrow +\infty} (\alpha_k, P_k) = (\alpha_0, P_0) \in (0, 1] \times \mathcal{P}(\mathcal{X})$ . Further, let  $(\sigma_{\alpha_k, P_k})_{k \in \mathbb{N}}$  be the sequence of the Augustin mean corresponding to  $(\alpha_k, P_k)$ . Since  $\mathcal{S}(\mathcal{H})$  is compact, there exists a convergent subsequence  $\{k_l\}_{l \in \mathbb{N}}$  such that  $\lim_{l \rightarrow +\infty} \sigma_{\alpha_{k_l}, P_{k_l}} = \sigma_0$  for some  $\sigma_0 \in \mathcal{S}(\mathcal{H})$ .

The joint continuity of  $(\alpha, P) \mapsto I_\alpha^{(2)}(P, \mathcal{W})$  in item (f) thus implies

$$\lim_{k \rightarrow +\infty} I_{\alpha_k}^{(2)}(P_k, \mathcal{W}) = D_{\alpha_0}(\mathcal{W} \| \sigma_0 | P_0) = I_{\alpha_0}^{(2)}(P_0, \mathcal{W}) = D_{\alpha_0}(\mathcal{W} \| \sigma_{\alpha_0, P_0} | P_0). \quad (3.91)$$

Then, the uniqueness of the minimizer  $\sigma_{\alpha, P}$  in item (b) guarantees that  $\sigma_0 = \sigma_{\alpha_0, P_0}$ . Hence,

$$\lim_{k \rightarrow +\infty} \sigma_{\alpha_k, \sigma_k} = \sigma_0 = \sigma_{\alpha_0, \sigma_0}, \quad (3.92)$$

which proves item (g).

- (3.2)-(h) Berge's maximum theorem [118, Section IV.3], [119, Lemma 3.1] shows that the continuous map  $(\alpha, P) \mapsto I_\alpha^{(2)}(P, \mathcal{W})$  maximized over the compact set  $P \in \mathcal{P}(\mathcal{X})$  is still continuous for  $\alpha \in [0, 1]$ .

□

## Chapter 4

# Quantum Hypothesis Testing

The goal of this chapter is to provide an introduction to quantum hypothesis testing. In Parts II and III later, our finite blocklength bounds heavily rely on the results in this chapter. In Sections 4.1 and 4.2 below, we present the error exponent analysis, while the moderate deviation analysis is given in Section 4.3.

The binary quantum hypothesis testing consists of a null hypothesis and an alternative hypothesis. The null hypothesis and the alternative hypothesis are described by the quantum states  $\rho \in \mathcal{S}(\mathcal{H})$  and  $\sigma \in \mathcal{S}(\mathcal{H})$ , respectively. Given any test  $0 \leq Q \leq \mathbf{1}$  that determines the outcome to be null hypothesis  $\rho$ , the *type-I error* and *type-II error* of the hypothesis testing are defined as follows:

$$\alpha(Q; \rho) := \text{Tr}[(\mathbf{1} - Q)\rho], \quad (4.1)$$

$$\beta(Q; \sigma) := \text{Tr}[Q\sigma]. \quad (4.2)$$

Unless  $\rho \perp \sigma$ , one cannot make both the type-I and type-II errors arbitrary small given the above definitions. Thus, we define the minimum type-I error when the type-II error is below  $\mu \in (0, 1)$  as

$$\widehat{\alpha}_\mu(\rho\|\sigma) := \min_{0 \leq Q \leq \mathbf{1}} \{\alpha(Q; \rho) : \beta(Q; \sigma) \leq \mu\}. \quad (4.3)$$

The following famous quantum Stein's lemma characterizes the trade-off relation between these two errors. That is, the quantum relative entropy  $D(\rho\|\sigma)$  serves as a benchmark to determine the asymptotic error behaviors of the optimal type-I error.

**Theorem 4.1** (Quantum Stein's Lemma [101], [58], [92]). *Given a binary hypotheses:  $\mathsf{H}_0 : \rho$  and  $\mathsf{H}_1 : \sigma$ , one has*

$$\lim_{n \rightarrow +\infty} \widehat{\alpha}_{\exp\{-nr\}}(\rho^{\otimes n}\|\sigma^{\otimes n}) = \begin{cases} 0, & r < D(\rho\|\sigma) \\ 1, & r > D(\rho\|\sigma) \end{cases}. \quad (4.4)$$

For an  $n$ -shot independent extension of the binary hypothesis:

$$\mathsf{H}_0 : \rho^n = \rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n, \quad (4.5)$$

$$\mathsf{H}_1 : \sigma^n = \sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n, \quad (4.6)$$

we define an error exponent function [92] by

$$\phi_n(r|\rho^n\|\sigma^n) := \sup_{\alpha \in (0,1]} \left\{ \frac{\alpha - 1}{\alpha} \left( r - \frac{1}{n} D_\alpha(\rho^n\|\sigma^n) \right) \right\}, \quad r \geq 0. \quad (4.7)$$

For the case  $\rho^n \ll \sigma^n$ , it is known that [92, Lemma 4]

$$\phi_n(r|\rho^n\|\sigma^n) = \begin{cases} +\infty, & r \in [0, -\frac{1}{n} \log \text{Tr}[(\rho^n)^0 \sigma^n]), \\ -\log \text{Tr}[\rho^n (\sigma^n)^0], & r \geq \frac{1}{n} D(\rho^n\|\sigma^n). \end{cases} \quad (4.8)$$

In the following Sections 4.1 and 4.2, we show that the exponent function  $\phi_n$  will determine how fast the optimal type-I error exponentially decay, i.e.

$$\lim_{n \rightarrow +\infty} -\frac{1}{n} \log \widehat{\alpha}_{\exp\{-nr\}}(\rho^{\otimes n}\|\sigma^{\otimes n}) = \phi_1(r|\rho\|\sigma) = \sup_{0 \leq \alpha \leq 1} \frac{1-\alpha}{\alpha} (D_\alpha(\rho\|\sigma) - r). \quad (4.9)$$

## 4.1 Achievability

Quantum Stein's lemma, given in Theorem 4.1, states that if the exponential decay of the type-II error is not faster than the relative entropy, i.e.  $r < D(\rho\|\sigma)$ , then the optimal type-I error vanishes asymptotically. The quantum Hoeffding bound makes a step further to investigate the non-asymptotics: how fast does the optimal type-I error decays? The achievability bound is then to give an exponential upper bound for it. This result was first proved by Hayashi [94], and the upper bound can be expressed as Petz's Rényi divergence. Together with the converse bound, discussed in Section 4.2 later, the error exponent for the optimal type-I error in quantum hypothesis testing was solved; see Eq. (4.9).

For the convenience of readers, we provide the proof of the achievability in Theorem 4.2 below.

**Theorem 4.2** (Achievability Hoeffding Bound [94], [92, Section 5.5]). *Given a binary hypotheses:  $H_0 : \rho$  and  $H_1 : \sigma$ , and rate  $r < D(\rho\|\sigma)$ , one has*

$$-\frac{1}{n} \log \widehat{\alpha}_{\exp\{-nr\}}(\rho^{\otimes n}\|\sigma^{\otimes n}) \geq \phi_1(r|\rho\|\sigma), \quad (4.10)$$

where  $\phi_n$  is defined in Eq. (4.7).

*Proof of Theorem 4.2.* Fix an  $n \in \mathbb{N}$ ,  $\alpha \in (0, 1)$ , and let

$$A = e^{-nx} \sigma^{\otimes n} \quad (4.11)$$

$$B = \rho^{\otimes n}, \quad (4.12)$$

where  $x$  will be determined later. Consider a sequence of test  $\{(1 - Q_n, Q_n)\}$  with  $Q_n := \{B - A \geq 0\}$ .

Then, Lemma 2.8 gives that

$$\beta(Q_n; \sigma^{\otimes n}) = \text{Tr} [Q_n \sigma^{\otimes n}] \quad (4.13)$$

$$= e^{nx} \text{Tr} [Q_n A] \quad (4.14)$$

$$\leq e^{nx\alpha} Q_\alpha (\rho^{\otimes n} \| \sigma^{\otimes n}) \quad (4.15)$$

$$= e^{nx\alpha} Q_\alpha (\rho \| \sigma)^n \quad (4.16)$$

$$\alpha(Q_n; \rho^{\otimes n}) = \text{Tr} [(\mathbb{1} - Q_n) \rho^{\otimes n}] \quad (4.17)$$

$$= e^{nx} \text{Tr} [(\mathbb{1} - Q_n) B] \quad (4.18)$$

$$\leq e^{-nx(1-\alpha)} Q_\alpha (\rho^{\otimes n} \| \sigma^{\otimes n}) \quad (4.19)$$

$$= e^{-nx(1-\alpha)} Q_\alpha (\rho \| \sigma)^n. \quad (4.20)$$

Now, choose  $x$  such that  $x\alpha + \log Q_\alpha (\rho \| \sigma) = -r$  to have

$$\beta(Q_n; \sigma^{\otimes n}) \leq \exp\{-nr\}. \quad (4.21)$$

Further, it is not hard to see that

$$\alpha(Q_n; \rho^{\otimes n}) \leq \exp\{-n\phi_1(r | \rho \| \sigma)\}. \quad (4.22)$$

□

## 4.2 Optimality

The optimality of the quantum Hoeffding bound means to provide a lower bound to the optimal type-I error. In other words, the performance of the hypothesis testing with any test cannot be improved. This problem was solved by Nagaoka [120]—he showed that asymptotically the error exponent of the optimal type-I error is upper bounded by  $\phi_1(\rho \| \sigma)$ ; see Theorem 4.3 below. Hence, together with the achievability bound in Theorem 4.2, the error exponent in Eq. (4.9) is fully characterized. The method employed by Nagaoka was introduced by Nussbaum and Szkoła [121], which is a crucial tool to translate a pair of quantum density operators to a pair of classical distributions. This thus plays a significant role in almost all the converse problems in quantum information theory. We provide the knowledge of the Nussbaum-Szkoła mapping in Section 4.2.1 below.

**Theorem 4.3** (Asymptotic Converse Hoeffding Bound [120], [92, Section 5.4]). *Given a binary hypotheses:  $H_0 : \rho$  and  $H_1 : \sigma$ , and rate  $r < D(\rho \| \sigma)$ , one has*

$$\lim_{n \rightarrow +\infty} -\frac{1}{n} \log \widehat{\alpha}_{\exp\{-nr\}} (\rho^{\otimes n} \| \sigma^{\otimes n}) \leq \phi_1(r | \rho \| \sigma), \quad (4.23)$$

where  $\phi_n$  is defined in Eq. (4.7).

Nagaoka's result in Theorem 4.3 is asymptotic, i.e. it holds when  $n \rightarrow +\infty$ . This motivates us to derive a finite blocklength converse bound. Moreover, we are interested in the tightest converse bound. In the following Theorem 4.4, we establish a sharp converse bound for quantum binary hypothesis testing, which serves as the fundamental tool to prove the sphere-packing bounds both in Slepian-Wolf

coding with QSI (Chapter 7) and classical-quantum channel coding (Chapter 11), and the converse bounds in moderate deviation analysis (see Chapters 8 and 12).

Before stating Theorem 4.4, we introduce some notation. Let

$$\mathsf{H}_0 : \rho^n = \rho_1 \otimes \cdots \otimes \rho_n; \quad (4.24)$$

$$\mathsf{H}_1 : \sigma^n = \sigma_1 \otimes \cdots \otimes \sigma_n, \quad (4.25)$$

where  $\rho_x, \sigma_x \in \mathcal{S}(\mathcal{H})$  for  $x \in [n]$ . Further, denote by  $(p_i, q_i)$  be the Nussbaum-Szkoła distribution of  $(\rho_i, \sigma_i)$  [121] that will be introduced very shortly in Section 4.2.1. For  $\alpha \in [0, 1]$ , define

$$B_\alpha(\rho^n \| \sigma^n) := \frac{1}{n} \sum_{x \in [n]} \mathbb{E}_{v_{x,\alpha}} \left[ \log \frac{p_x}{q_x} \right]; \quad (4.26)$$

$$V_\alpha(\rho^n \| \sigma^n) := \frac{1}{n} \sum_{x \in [n]} \mathbb{E}_{v_{x,\alpha}} \left[ \left| \log \frac{p_x}{q_x} - \mathbb{E}_{v_{\alpha,x}} \left[ \log \frac{p_x}{q_x} \right] \right|^2 \right]; \quad (4.27)$$

$$T_\alpha(\rho^n \| \sigma^n) := \frac{1}{n} \sum_{x \in [n]} \mathbb{E}_{v_{x,\alpha}} \left[ \left| \log \frac{p_x}{q_x} - \mathbb{E}_{v_{\alpha,x}} \left[ \log \frac{p_x}{q_x} \right] \right|^3 \right], \quad (4.28)$$

where  $(p_x, q_x)$  is the Nussbaum-Szkoła distribution of  $(\rho_x, \sigma_x)$  for  $x \in [n]$ , and the *tilted distribution* is

$$v_{x,\alpha}(i, j) := \frac{p_x^\alpha(i, j) q_x^{1-\alpha}(i, j)}{\sum_{i,j} p_x^\alpha(i, j) q_x^{1-\alpha}(i, j)}, \quad \alpha \in [0, 1]. \quad (4.29)$$

With the above notation, we have the following converse bound.

**Theorem 4.4** (Sharp Converse Hoeffding Bounds for Quantum Hypothesis Testing). *Consider a binary hypothesis testing:  $H_0 : \rho^n = \bigotimes_{i=1}^n \rho_i$  and  $H_1 : \sigma^n = \bigotimes_{i=1}^n \sigma_i$  given in Eq. (4.24) with  $\rho^n \ll \sigma^n$ . Let  $r \in \mathbb{R}$  be such that there exists an  $\alpha^* \in (0, 1]$  such that*

$$\phi_n(r|\rho^n\|\sigma^n) = \frac{1-\alpha^*}{\alpha^*} \left( \frac{1}{n} D_{\alpha^*}(\rho^n\|\sigma^n) - r \right). \quad (4.30)$$

*Then, we have the following: (i) for any test  $Q_n$ , either*

$$\alpha(Q^n; \rho^n) \geq \frac{1}{8} \exp \left\{ -n\phi_n(r|\rho^n\|\sigma^n) - \alpha^* \sqrt{2nV_{\alpha^*}(\rho^n\|\sigma^n)} \right\}, \quad (4.31)$$

*or*

$$\beta(Q^n; \sigma^n) \geq \frac{1}{8} \exp \left\{ -nr - (1-\alpha^*) \sqrt{2nV_{\alpha^*}(\rho^n\|\sigma^n)} \right\} \quad (4.32)$$

*holds; (ii) if  $\alpha^* \in (0, 1)$ , then for any test  $Q_n$ , either*

$$\alpha(Q^n; \rho^n) \geq e^{-n\phi_n(r|\rho^n\|\sigma^n)} \frac{e^{-K_n(\alpha^*)}}{2\sqrt{2n\pi V_{\alpha^*}(\rho^n\|\sigma^n)}} \left( 1 - \frac{1 + (1 + K_n(\alpha^*)^2)}{2\sqrt{nV_{\alpha^*}(\rho^n\|\sigma^n)}} \right), \quad (4.33)$$

*or*

$$\beta(Q^n; \sigma^n) \geq e^{-nr} \frac{e^{-K_n(\alpha^*)}}{2\sqrt{2n\pi V_{\alpha^*}(\rho^n\|\sigma^n)}} \left( 1 - \frac{1 + (1 + K_n(\alpha^*)^2)}{2\sqrt{nV_{\alpha^*}(\rho^n\|\sigma^n)}} \right) \quad (4.34)$$

*holds. Here,  $K_n(\alpha) := \frac{15\sqrt{2\pi}T_\alpha(\rho^n\|\sigma^n)}{V_\alpha(\rho^n\|\sigma^n)} \in \mathbb{R}_{>0}$  and  $V_{\alpha^*}(\rho^n\|\sigma^n) \in \mathbb{R}_{>0}$ .*

The proof is delayed to Section 4.2.2.

Thanks to Theorem 4.4, one can employ the Taylor's expansion of the  $\phi_n$  to obtain the following sharp converse Hoeffding bound, which is the finite blocklength improvement of Nagaoka's result in Theorem 4.3.

**Corollary 4.1** (Sharp Converse Hoeffding Bound (i.i.d states)). *Given a binary hypotheses:  $H_0 : \rho^n$  and  $H_1 : \sigma^n$  as in Eq. (4.24), and rate:*

$$\frac{1}{n} D_0(\rho^n\|\sigma^n) < r < \frac{1}{n} D(\rho^n\|\sigma^n), \quad (4.35)$$

*there exist  $K, N_0 \in \mathbb{N}$  such that for all  $n \geq N_0$ , the following holds*

$$-\log \widehat{\alpha}_{\exp\{-nr\}}(\rho^{\otimes n}\|\sigma^{\otimes n}) \leq n\phi_n(r|\rho^n\|\sigma^n) + \frac{1}{2} (1 + |\phi'_n(r|\rho^n\|\sigma^n)|) \log n + K. \quad (4.36)$$

*where  $\phi_n$  is defined in Eq. (4.7), and  $\phi'_n$  denotes the first-order derivative of  $\phi_n$ .*

### 4.2.1 Nussbaum-Szkoła Distributions

Assume the dimension of the Hilbert space  $\mathcal{H}$  is  $d$ . Given density operators  $\rho, \sigma \in \mathcal{S}(\mathcal{H})$  with spectral decompositions

$$\rho = \sum_{i \in [d]} \lambda_i |x_i\rangle\langle x_i|, \quad \text{and} \quad \sigma = \sum_{j \in [d]} \gamma_j |y_j\rangle\langle y_j|, \quad (4.37)$$

we define the *Nussbaum-Szkoła distributions* [121]  $p^{\rho, \sigma}, q^{\rho, \sigma}$  as

$$p^{\rho, \sigma}(i, j) := \lambda_i |\langle x_i | y_j \rangle|^2, \quad q^{\rho, \sigma}(i, j) := \gamma_j |\langle x_i | y_j \rangle|^2. \quad (4.38)$$

The distributions  $p^{\rho, \sigma}, q^{\rho, \sigma}$  have the same mathematical properties as the density operators  $\rho, \sigma$  in some cases, and thus are useful in the sequel. First, one can verify that [121, 16],

$$D_\alpha(\rho \| \sigma) = D_\alpha(p^{\rho, \sigma} \| q^{\rho, \sigma}), \quad \forall \alpha \in [0, 1]. \quad (4.39)$$

Second, for product states  $\rho_1 \otimes \rho_2$  and  $\sigma_1 \otimes \sigma_2$ , we have

$$p^{\rho_1 \otimes \rho_2, \sigma_1 \otimes \sigma_2} = p^{\rho_1, \sigma_1} \otimes p^{\rho_2, \sigma_2}, \quad \text{and} \quad q^{\rho_1 \otimes \rho_2, \sigma_1 \otimes \sigma_2} = q^{\rho_1, \sigma_1} \otimes q^{\rho_2, \sigma_2}. \quad (4.40)$$

Third,  $\rho \ll \sigma$  if and only if  $p^{\rho, \sigma} \ll q^{\rho, \sigma}$ . Moreover, we usually use  $\omega$  to represent the pair of indices  $(i, j)$  in Eq.(4.38), and the distributions  $p^{\rho, \sigma}, q^{\rho, \sigma}$  can be thought of as diagonalized matrices, e.g.  $\text{Tr}[p^{\rho, \sigma}] = \sum_{\omega \in [d] \times [d]} p^{\rho, \sigma}(\omega)$ .

### 4.2.2 Proofs of Theorem 4.4 and Corollary 4.1

The first claim directly follows from Dailai's result in [38, Theorem 4]. Before proceeding, we need to introduce some notation. Let  $\tilde{p}^n := \bigotimes_{i=1}^n \tilde{p}_i$  and  $\tilde{q}^n := \bigotimes_{i=1}^n \tilde{q}_i$ , where  $(\tilde{p}_i, \tilde{q}_i)$  are the Nussbaum-Szkoła distributions [121] of  $(\rho_i, \sigma_i)$  for  $i \in [n]$ . Since  $D_\alpha(\rho_i \| \sigma_i) = D_\alpha(\tilde{p}_i \| \tilde{q}_i)$ , for all  $\alpha \in (0, 1)$ , we shorthand

$$\phi_n(r) := \phi_n(r | \rho^n \| \sigma^n) = \phi_n(r | \tilde{p}^n \| \tilde{q}^n) \in \mathbb{R}_{>0}. \quad (4.41)$$

Applying Nagaoka's argument [120], for any  $0 \leq Q_n \leq 1$  with  $\delta = \exp\{nr - n\phi_n(r)\}$ , we have

$$\alpha(Q_n; \rho^n) + \delta \beta(Q_n; \sigma^n) \geq \frac{1}{2} \left( \alpha(\tilde{\mathcal{U}}; \tilde{p}^n) + e^{nr - n\phi_n(r)} \beta(\tilde{\mathcal{U}}; \tilde{q}^n) \right), \quad (4.42)$$

where  $\alpha(\tilde{\mathcal{U}}; \tilde{p}^n) := \sum_{\omega \notin \tilde{\mathcal{U}}} \tilde{p}^n(\omega)$ ,  $\beta(\tilde{\mathcal{U}}; \tilde{q}^n) := \sum_{\omega \in \tilde{\mathcal{U}}} \tilde{q}^n(\omega)$ , and

$$\tilde{\mathcal{U}} := \left\{ \omega : \tilde{p}^n(\omega) e^{n\phi_n(r)} > \tilde{q}^n(\omega) e^{nr} \right\}. \quad (4.43)$$

Now, we further define the non-normalized distributions  $p^n := \bigotimes_{i=1}^n p_i$  and  $q^n := \bigotimes_{i=1}^n q_i$ , where  $p_i := \tilde{p}_i q_i^0$ ,  $q_i := \tilde{q}_i p_i^0$ , for every  $i \in [n]$ . Namely, we restrict  $(p^n, q^n)$  to be in the joint support of  $\tilde{p}^n$  and  $\tilde{q}^n$ . Letting

$$\mathcal{U} := \left\{ \omega : p^n(\omega) e^{n\phi_n(r)} > q^n(\omega) e^{nr} \right\}, \quad (4.44)$$

it is not hard to see that

$$\alpha(\mathcal{U}; p^n) = \alpha(\tilde{\mathcal{U}}; \tilde{p}^n); \quad (4.45)$$

$$\beta(\mathcal{U}; q^n) = \beta(\tilde{\mathcal{U}}; \tilde{q}^n) \quad (4.46)$$

$$\phi_n(r) = \phi_n(r|p^n\|q^n). \quad (4.47)$$

Hence, we focus on the pair  $(p^n, q^n)$  and the decision region  $\mathcal{U}$  onwards.

Let

$$\begin{aligned} \Lambda_{0,n}(\alpha) &:= \frac{1}{n} \sum_{i \in [n]} \Lambda_{0,i}(\alpha), \quad \Lambda_{0,i}(\alpha) := \log \mathbb{E}_{p_i} \left[ e^{(1-\alpha) \log \frac{q_i}{p_i}} \right]; \\ \Lambda_{1,n}(\alpha) &:= \frac{1}{n} \sum_{i \in [n]} \Lambda_{1,i}(\alpha), \quad \Lambda_{1,i}(\alpha) := \log \mathbb{E}_{q_i} \left[ e^{(1-\alpha) \log \frac{p_i}{q_i}} \right]. \end{aligned} \quad (4.48)$$

Since  $p^n$  and  $q^n$  have the same support, both  $\Lambda_{0,n}(\alpha)$  and  $\Lambda_{1,n}(\alpha)$  are smooth functions in  $\alpha \in \mathbb{R}$ . One can calculate their derivatives as follows:

$$\Lambda'_{0,n}(\alpha) = \frac{1}{n} \sum_{i \in [n]} \mathbb{E}_{v_{i,\alpha}} \left[ \log \frac{p_i}{q_i} \right]; \quad \Lambda'_{1,n}(\alpha) = \frac{1}{n} \sum_{i \in [n]} \mathbb{E}_{v_{i,1-\alpha}} \left[ \log \frac{q_i}{p_i} \right] \quad (4.49)$$

$$\Lambda''_{0,n}(\alpha) = \frac{1}{n} \sum_{i \in [n]} \text{Var}_{v_{i,\alpha}} \left[ \log \frac{p_i}{q_i} \right]; \quad \Lambda''_{1,n}(\alpha) = \frac{1}{n} \sum_{i \in [n]} \text{Var}_{v_{i,1-\alpha}} \left[ \log \frac{q_i}{p_i} \right], \quad (4.50)$$

$$\begin{aligned} T_{0,n}(\alpha) &:= \frac{1}{n} \sum_{i \in [n]} \mathbb{E}_{v_{i,\alpha}} \left[ \left| \log \frac{p_i}{q_i} - \Lambda'_{0,n}(\alpha) \right|^3 \right]; \\ T_{1,n}(\alpha) &:= \frac{1}{n} \sum_{i \in [n]} \mathbb{E}_{v_{i,1-\alpha}} \left[ \left| \log \frac{q_i}{p_i} - \Lambda'_{1,n}(\alpha) \right|^3 \right], \end{aligned} \quad (4.51)$$

where we denote the tilted distribution by

$$v_{i,\alpha}(\omega) := \frac{p_i^\alpha(\omega) q_i^{1-\alpha}(\omega)}{\sum_{\bar{\omega}} p_i^\alpha(\bar{\omega}) q_i^{1-\alpha}(\bar{\omega})}, \quad \alpha \in [0, 1]. \quad (4.52)$$

Further, it is not hard to verify that for all  $\alpha \in [0, 1]$ .

$$\begin{aligned} \Lambda_{0,n}(\alpha) &= \Lambda_{1,n}(1-\alpha); \quad \Lambda'_{0,n}(\alpha) = -\Lambda'_{1,n}(1-\alpha); \\ \Lambda''_{0,n}(\alpha) &= \Lambda''_{1,n}(1-\alpha); \quad T_{0,n}(\alpha) = T_{1,n}(1-\alpha). \end{aligned} \quad (4.53)$$

Next, we define the *Lengendre-Fenchel transform*:

$$\Lambda_{j,n}^*(z) := \sup_{\alpha \in \mathbb{R}} \{(1-\alpha)z - \Lambda_{j,n}(\alpha)\}, \quad j \in \{0, 1\}. \quad (4.54)$$

The quantities  $\Lambda_{j,n}^*(z)$  would appear in the lower bounds of  $\alpha(Q^n; \rho^n)$  and  $\beta(Q^n; \sigma^n)$  as shown later.

Now, we are ready to show the first claim. Ref. [38, Theorem 4] states that for any test  $Q^n$ , either

$$\alpha(Q^n; \rho^n) \geq \frac{1}{8} \exp \left\{ -n [\alpha^* \Lambda'_{0,n}(\alpha^*) - \Lambda_{0,n}(\alpha^*)] - \alpha^* \sqrt{2nV_{\alpha^*}(\rho^n\|\sigma^n)} \right\}, \quad (4.55)$$

or

$$\beta(Q^n; \sigma^n) \geq \frac{1}{8} \exp \left\{ -n [-(1-\alpha^*)\Lambda'_{0,n}(\alpha^*) + \Lambda_{0,n}(\alpha^*)] - (1-\alpha^*)\sqrt{2nV_{\alpha^*}(\rho^n\|\sigma^n)} \right\}, \quad (4.56)$$

holds. By Eqs. (4.53), and (2.49), (2.51) in Section 2.2, we have

$$\phi_n(r) = \alpha^* \Lambda'_{0,n}(\alpha^*) - \Lambda_{0,n}(\alpha^*); \quad (4.57)$$

$$r = -(1-\alpha^*)\Lambda'_{0,n}(\alpha^*) + \Lambda_{0,n}(\alpha^*), \quad (4.58)$$

which proves the first claim.

To show the second claim, we will employ Bahadur-Ranga Rao's concentration inequality, Theorem 2.1, in Section 2.2, to further lower bound  $\alpha(\mathcal{U}; p^n)$  and  $\beta(\mathcal{U}; q^n)$ . Letting  $Z_i = \log \frac{q_i}{p_i}$  with probability measure  $\mu_i = p_i$ , and  $z = r - \phi_n(r)$  in Theorem 2.1, the Bahadur-Randga Rao's inequality gives

$$\alpha(\mathcal{U}; p^n) := \sum_{\omega \notin \mathcal{U}} p^n(\omega) \quad (4.59)$$

$$= \Pr \left\{ \frac{1}{n} \sum_{i=1}^n Z_i \geq \phi_n(r) - r \right\} \quad (4.60)$$

$$\geq \exp \left\{ -n \Lambda_{0,n}^*(\phi_n(r) - r) \right\} \frac{e^{-K_n(\alpha^*)}}{\sqrt{2\pi \Lambda''_n(\alpha^*)}} \left( 1 - \frac{1 + (1 + K_n(\alpha^*)^2)}{2\sqrt{\Lambda''_{0,n}(\alpha^*)}} \right), \quad (4.61)$$

where

$$K_n(\alpha) := 15\sqrt{2\pi} \frac{T_\alpha(\rho^n\|\sigma^n)}{V_\alpha(\rho^n\|\sigma^n)} = 15\sqrt{2} \frac{T_{0,n}(\alpha)}{\Lambda''_{0,n}(\alpha)}. \quad (4.62)$$

Moreover, Lemma 2.13 in Section 2.2 relates the Legendre-Fenchel transform  $\Lambda_{j,P_{\mathbf{x}^n}}^*(z)$  to the desired error exponent function  $\phi_n(r)$ :

$$\Lambda''_{0,n}(\alpha^*) > 0; \quad (4.63)$$

$$\Lambda_{0,n}^*(\phi_n(r) - r) = \phi_n(r); \quad (4.64)$$

$$\Lambda_{1,n}^*(r - \phi_n(r)) = r. \quad (4.65)$$

Hence, we have

$$\alpha(\mathcal{U}; p^n) \geq \exp \left\{ -n \phi_n(r) \right\} \frac{e^{-K_n(\alpha^*)}}{\sqrt{2\pi \Lambda''_{0,n}(\alpha^*)}} \left( 1 - \frac{1 + (1 + K_n(\alpha^*)^2)}{2\sqrt{\Lambda''_{0,n}(\alpha^*)}} \right). \quad (4.66)$$

Similarly, applying Theorem 2.1 with  $Z_i = \log \frac{p_i}{q_i}$ ,  $\mu_i = q_i$ , and  $z = \phi_n(r) - r$  yields

$$\beta(\mathcal{U}; q^n) := \sum_{\omega \in \mathcal{U}} q^n(\omega) \quad (4.67)$$

$$= \Pr \left\{ \frac{1}{n} \sum_{i=1}^n Z_i \geq \phi_n(r) - r \right\} \quad (4.68)$$

$$\geq \exp \left\{ -n\Lambda_{1,n}^*(r - \phi_n(r)) \right\} \frac{e^{-K_n(1-\alpha^*)}}{\sqrt{2\pi\Lambda_{1,n}''(1-\alpha^*)}} \left( 1 - \frac{1 + (1 + K_n(1-\alpha^*)^2)}{2\sqrt{\Lambda_{1,n}''(1-\alpha^*)}} \right) \quad (4.69)$$

$$= \exp \{-nr\} \frac{e^{-K_n(1-\alpha^*)}}{\sqrt{2\pi\Lambda_{1,n}''(1-\alpha^*)}} \left( 1 - \frac{1 + (1 + K_n(1-\alpha^*)^2)}{2\sqrt{\Lambda_{1,n}''(1-\alpha^*)}} \right) \quad (4.70)$$

$$= \exp \{-nr\} \frac{e^{-K_n(\alpha^*)}}{\sqrt{2\pi\Lambda_{0,n}''(\alpha^*)}} \left( 1 - \frac{1 + (1 + K_n(\alpha^*)^2)}{2\sqrt{\Lambda_{0,n}''(\alpha^*)}} \right), \quad (4.71)$$

where the last equality follows from Eq. (4.53). Hence, by Eqs. (4.42), (4.66), and (4.71), we conclude our claim.  $\square$

### 4.3 Moderate Deviation Analysis

In this section, we analyze quantum hypothesis testing in the moderate deviation regime. Specifically, we will show that the optimal type-I error asymptotically vanish when the exponential rate of type-II error approaches quantum relative entropy at a speed  $a_n$ . Here,  $(a_n)_{n \in \mathbb{N}}$  is any sequence satisfying

$$\begin{aligned} \text{(i)} \quad & \lim_{n \rightarrow +\infty} a_n = 0; \\ \text{(ii)} \quad & \lim_{n \rightarrow +\infty} a_n \sqrt{n} = +\infty. \end{aligned} \quad (4.72)$$

The achievability part is given in Theorem 4.5. In Section 4.3.1, we provide two proofs. The first one follows from the Theorem 4.2 in Section 4.1, and an asymptotic expansions of the exponent function  $\phi_n$ . The second proof relies on a concentration inequality for noncommutative martingales [122]. The converse part and its proof are provided in Theorem 4.6 and Section 4.3.2.

We remark that the moderate deviation analysis for classical hypothesis testing was studied by Sason [45], and by Watanabe and Hayashi [123]. Moreover, a recent work by Rouzé and Datta [124] formulated the quantum hypothesis problem into a martingale, which is similar to our approach for proving the achievability.

**Theorem 4.5** (Achievability). *Let  $\rho, \sigma \in \mathcal{S}(\mathcal{H})$  be the density operators with non-zero and finite information variance  $V := \mathbb{V}(\rho\|\sigma) > 0$ . For any sequence of real numbers  $\{a_n\}_{n \in \mathbb{N}}$  satisfying Eq. (12.1), there exists a sequence  $r_n := \mathbb{D}(\rho\|\sigma) - a_n$  such that*

$$\limsup_{n \rightarrow +\infty} \frac{1}{na_n^2} \log \hat{\alpha}_{\exp\{-nr_n\}}(\rho^{\otimes n}\|\sigma^{\otimes n}) \leq -\frac{1}{2V}. \quad (4.73)$$

The proof is provided in Section 4.3.1

**Theorem 4.6** (Converse). *Let  $\rho, \sigma \in \mathcal{S}(\mathcal{H})$  be the density operators with non-zero and finite information variance  $V := \mathbb{V}(\rho\|\sigma) > 0$ . For any sequence of real numbers  $\{a_n\}_{n \in \mathbb{N}}$  satisfying Eq. (12.1), there exists a sequence  $r_n := \mathbb{D}(\rho\|\sigma) - a_n$  such that*

$$\liminf_{n \rightarrow +\infty} \frac{1}{na_n^2} \log \widehat{\alpha}_{\exp\{-nr_n\}}(\rho^{\otimes n}\|\sigma^{\otimes n}) \geq -\frac{1}{2V}. \quad (4.74)$$

The proof is provided in Section 4.3.2

### 4.3.1 Proof of Theorem 4.5

In this section, we present two proofs of Theorem 4.5. The first one relies on the quantum Hoeffding bound [92] and the Taylor's expansion of the function  $E_h$ .

*The first proof of Theorem 4.5.* We start the proof from recalling Audenaet et al.'s achievability [92] of the quantum Hoeffding bound in Lemma 2.8:

$$\widehat{\alpha}_{\exp\{-nr\}}(\rho^{\otimes n}\|\sigma^{\otimes n}) \leq \exp \left\{ -n \left[ \sup_{0 < \alpha \leq 1} \left\{ \frac{\alpha - 1}{\alpha} (r - D_\alpha(\rho\|\sigma)) \right\} \right] \right\}. \quad (4.75)$$

Since  $\mathbb{D}(\rho\|\sigma) > 0$  (due to Eq. (3.4)), we have

$$\mathbb{D}(\rho\|\sigma) - a_n > 0 \quad (4.76)$$

for all sufficiently large  $n$ . Choose such  $n$  onwards. Then Eq. (4.75) implies that for all sufficiently large  $n$ , there exists  $r_n = D(\rho\|\sigma) - a_n$  and

$$\frac{1}{na_n^2} \log \widehat{\alpha}(\rho^{\otimes n}\|\sigma^{\otimes n}) \leq \frac{1}{na_n^2} - \frac{1}{a_n^2} \sup_{0 < \alpha \leq 1} \left\{ \frac{\alpha - 1}{\alpha} (r - D_\alpha(\rho\|\sigma)) \right\} \quad (4.77)$$

$$= \frac{1}{na_n^2} - \frac{1}{a_n^2} \sup_{s \geq 0} \{E_h(s) - sr_n\}, \quad (4.78)$$

where we substitute  $s = \frac{1-\alpha}{\alpha}$  and invoke Eq. (9.9):

$$E_h(s) := E_h(s, P) = sD_{\frac{1}{1+s}}(\rho\|\sigma). \quad (4.79)$$

with  $\mathcal{X} = \{x\}$  and  $W_x = \rho$ .

Therefore, we apply Taylor's theorem, along with items (c) and (e) in Proposition 9.3, to obtain

$$E_h(s) = s\mathbb{D}(\rho\|\sigma) - \frac{s^2}{2}V + \frac{s^3}{6} \frac{\partial^3 E_h(s)}{\partial s^3} \Big|_{s=\bar{s}} \quad (4.80)$$

for some  $\bar{s} \in [0, s]$  and all  $s \geq 0$ . Now let  $s_n = a_n/V$ , for all  $n \in \mathbb{N}$ . Then for all sufficiently large  $n$

and for some  $\bar{s}_n \in [0, s_n]$ , Eq. (4.80) yields

$$\sup_{s \geq 0} \{E_h(s) - sr_n\} \geq E_h(s_n) - s_n r_n \quad (4.81)$$

$$= \frac{a_n}{V} (\mathbb{D}(\rho\|\sigma) - r_n) - \frac{a_n^2}{2V} + \frac{a_n^3}{6V^2} \frac{\partial^3 E_h(s)}{\partial s^3} \Big|_{s=\bar{s}_n} \quad (4.82)$$

$$= \frac{a_n^2}{2V} + \frac{a_n^3}{6V^2} \frac{\partial^3 E_h(s)}{\partial s^3} \Big|_{s=\bar{s}_n}, \quad (4.83)$$

where we substitute  $r_n = D(\rho\|\sigma) - a_n$  in Eq. (4.83).

Note that  $s_n = a_n/V \leq 1$  for all sufficiently large  $n$  since  $\lim_{n \rightarrow \infty} a_n = 0$  in Eq. (12.1) and the assumption:  $V > 0$ . Define

$$\Upsilon := \max_{s \in [0, 1]} \left| \frac{\partial^3 E_h(s)}{\partial s^3} \right|, \quad (4.84)$$

From item (a) in Proposition 9.3,  $\frac{\partial^3 E_h(s)}{\partial s^3}$  is continuous over  $s \geq 0$ . Hence the maximum in Eq. (4.84) is well-defined and finite. Therefore, (4.83) leads to

$$\sup \{E_h(s) - sr_n\} \geq \frac{a_n^2}{2V} + \frac{a_n^3}{6V^2} \frac{\partial^3 E_h(s)}{\partial s^3} \Big|_{s=\bar{s}_n} \quad (4.85)$$

$$\geq \frac{a_n^2}{2V} - \frac{a_n^3}{6V^2} \left| \frac{\partial^3 E_h(s)}{\partial s^3} \right|_{s=\bar{s}_n} \quad (4.86)$$

$$\geq \frac{a_n^2}{2V} - \frac{a_n^3}{6V^2} \Upsilon \quad (4.87)$$

for all sufficiently large  $n$ .

Substituting Eq. (4.87) into Eq. (4.78) yields

$$\frac{1}{na_n^2} \log \widehat{\alpha}_{\exp\{-nr_n\}}(\rho\|\sigma) \leq \frac{1}{na_n^2} - \frac{1}{2V} \left(1 - \Upsilon \frac{a_n}{3V^2}\right), \quad (4.88)$$

which implies the desired achievability part:

$$\limsup_{n \rightarrow +\infty} \frac{1}{na_n^2} \log \widehat{\alpha}_{\exp\{-nr_n\}}(\rho\|\sigma) \leq -\frac{1}{2V}. \quad (4.89)$$

□

In the following, we give an alternative proof of Theorem 4.5 by employing a noncommutative Bennett inequality [122].

*The second proof of Theorem 4.5.* It is well-known that the Neyman-Pearson (likelihood-ratio) test achieves the optimum type-I error with the constraint of the type-II error. Hence, it suffices to prove that

$$\limsup_{n \rightarrow +\infty} \frac{1}{na_n^2} \log \widehat{\alpha}_{\exp\{-nr_n\}}(\rho\|\sigma) = \lim_{n \rightarrow \infty} \frac{1}{na_n^2} \log \alpha_n(\eta_n) \geq -\frac{1}{2V}, \quad (4.90)$$

where

$$\eta_n := \mathbb{D}(\rho\|\sigma) - a_n, \quad n \in \mathbb{N}. \quad (4.91)$$

For notational convenience, we first consider the non-identical case. Let the two hypotheses be

$$\mathsf{H}_0 : \rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n \quad (4.92)$$

$$\mathsf{H}_1 : \sigma_1 \otimes \sigma_2 \otimes \cdots \otimes \sigma_n, \quad (4.93)$$

where  $\rho_i, \sigma_i \in \mathcal{S}(\mathcal{H}_i)$ , for every  $i \in [n]$ . Define the operator

$$L_n := \log \bigotimes_{i=1}^n \rho_i - \log \bigotimes_{i=1}^n \sigma_i = \sum_{i=1}^k (\log \rho_i - \log \sigma_i), \quad (4.94)$$

which can be seen as the quantum generalization of the Neyman-Pearson log-likelihood ratio.

Next, we formulate the hypothesis testing problem in the noncommutative probability space [125, 126]. Let  $\mathfrak{M}_k$  be the von Neumann algebra on the Hilbert space  $\bigotimes_{i=1}^k \mathcal{H}_i$  with  $\mathfrak{M}_0 = \emptyset$ , and  $(\mathfrak{M}_k)_{k=0}^n$  forms a increasing filtration (see e.g. [127]). The *normal faithful tracial state*  $\tau : \mathfrak{M}_n \rightarrow \mathbb{C}$  on  $\mathfrak{M}_n$  is defined as  $\tau : X \mapsto \text{Tr} \left[ \bigotimes_{j=1}^n \rho_j X \right]$ . Let  $\mathbb{E}_{\bigotimes_{j=1}^n \rho_j} [\cdot | \mathfrak{M}_k] : \mathfrak{M}_n \rightarrow \mathfrak{M}_k$  be the conditional expectation of  $\mathfrak{M}_n$  with respect to  $\mathfrak{M}_k$ . For every  $k \in \{0, 1, \dots, n\}$ , we let

$$U_k := \mathbb{E}_{\bigotimes_{j=1}^n \rho_j} [L_n | \mathfrak{M}_k] \quad (4.95)$$

$$= \mathbb{E}_{\bigotimes_{j=1}^n \rho_j} \left[ \sum_{i=1}^n (\log \rho_i - \log \sigma_i) \middle| \mathfrak{M}_k \right] \quad (4.96)$$

$$= \sum_{i=1}^k (\log \rho_i - \log \sigma_i) + \sum_{i=k+1}^n \mathbb{E}_{\bigotimes_{j=1}^n \rho_j} [\log \rho_i - \log \sigma_i] \quad (4.97)$$

$$= \sum_{i=1}^k (\log \rho_i - \log \sigma_i) + \sum_{i=k+1}^n \text{Tr} \left[ \bigotimes_{j=1}^n \rho_j (\log \rho_i - \log \sigma_i) \right] \quad (4.98)$$

$$= \sum_{i=1}^k (\log \rho_i - \log \sigma_i) + \sum_{i=k+1}^n \mathbb{D}(\rho_i\|\sigma_i). \quad (4.99)$$

In particular, we have

$$U_0 = \sum_{i=1}^n \mathbb{D}(\rho_i\|\sigma_i) \quad (4.100)$$

$$U_n = \sum_{i=1}^n (\log \rho_i - \log \sigma_i) = L_n, \quad (4.101)$$

Hence,  $\{U_k - U_{k-1}\}_{k=1}^n$  forms a martingale:

$$U_k - U_{k-1} = \log \rho_k - \log \sigma_k - \mathbb{D}(\rho_k \| \sigma_k); \quad (4.102)$$

$$\mathbb{E}_{\bigotimes_{j=1}^n \rho_j} [U_k - U_{k-1} | \mathfrak{M}_{k-1}] = 0; \quad (4.103)$$

$$\mathbb{E}_{\bigotimes_{j=1}^n \rho_j} [(U_k - U_{k-1})^2 | \mathfrak{M}_{k-1}] = \mathbb{V}(\rho_k \| \sigma_k) =: v_k. \quad (4.104)$$

Denote by

$$b_k := \|\log \rho_k - \log \sigma_k - \mathbb{D}(\rho_k \| \sigma_k)\|_\infty, \quad (4.105)$$

where  $\|\cdot\|_\infty$  denotes the operator norm. The martingale is bounded by  $\|U_k - U_{k-1}\|_\infty \leq b_k$  for every  $k \in [n]$ .

Equipped with the notation above, the type-I error can be rephrased as:

$$\alpha_n(\eta_n) = \text{Tr} \left[ \left\{ \bigotimes_{i=1}^n \rho_i - e^{n\eta_n} \bigotimes_{i=1}^n \sigma_i \leq 0 \right\} \bigotimes_{i=1}^n \rho_i \right] \quad (4.106)$$

$$= \text{Tr} \left[ \bigotimes_{i=1}^n \rho_i \left\{ \sum_{i=1}^n (\log \rho_i - \log \sigma_i) \leq n\eta_n \right\} \right] \quad (4.107)$$

$$= \text{Tr} \left[ \bigotimes_{i=1}^n \rho_i \{U_n - U_0 \leq -na_n\} \right] \quad (4.108)$$

$$= \tau(\mathbf{1}_{(-\infty, -na_n)}(U_n - U_0)) \quad (4.109)$$

$$= \tau(\mathbf{1}_{(na_n, \infty)}(U_n - U_0)), \quad (4.110)$$

where the third equality (4.108) follows from the definition of  $\eta_n$  in Eq. (4.91) and Eqs. (4.100) and (4.101). The last line (4.110) is due to the symmetry of  $U_n - U_0$ , i.e.  $\mathbb{E}_{\bigotimes_{i=1}^n} [U_n - U_0] = 0$ .

In the following, we borrow the idea from Sason [45] to employ the noncommutative Bennett inequality to upper bound Eq. (4.110).

**Theorem 4.7** (Noncommutative Bennett Inequality [122, Theorem 0.1]). *Let  $(X_k)_{k=1}^n$  be a self-adjoint martingale with respect to the filtration  $(\mathfrak{M}_k)_{k=0}^n$  such that: (i)  $\mathbb{E}[X_k | \mathfrak{M}_{k-1}] = 0$ ; (ii)  $\mathbb{E}[X_k^2 | \mathfrak{M}_{k-1}] = v_k$ ; (iii)  $\|X_k\|_\infty \leq b_k$ . Then for any  $x > 0$ ,*

$$\tau \left( \mathbf{1}_{[x, \infty)} \left( \sum_{k=1}^n X_k \right) \right) \leq \exp \left\{ - \frac{\sum_{k=1}^n v_k}{\sup_{k \in [n]} b_k^2} \varphi \left( \frac{x \sup_{k \in [n]} b_k}{\sum_{k=1}^n v_k} \right) \right\}, \quad (4.111)$$

where  $\varphi(u) := (1+u) \log(1+u) - u$ .

By applying Theorem 4.7 to Eq. (4.110) with  $x = na$  and  $X_k = U_k - U_{k-1}$  for ever  $k \in [n]$ :

$$\alpha_n(\eta_n) \leq \exp \left\{ - \frac{\sum_{k=1}^n v_k}{\sup_{k \in [n]} b_k^2} \varphi \left( \frac{na \sup_{k \in [n]} b_k}{\sum_{k=1}^n v_k} \right) \right\} \quad (4.112)$$

$$= \exp \left\{ - \frac{n\bar{v}}{B^2} \varphi \left( \frac{ab}{\bar{v}} \right) \right\}, \quad (4.113)$$

where

$$b := \sup_{k \in [n]} b_k, \quad B^2 := \sup_{k \in [n]} b_k^2, \quad \bar{v} := \frac{\sum_{k=1}^n v_k}{n}. \quad (4.114)$$

By recalling  $\varphi(u) = (1+u)\log(1+u) - u$  and using a scalar inequality [45, Lemma 1]:

$$(1+u)\log(1+u) \geq u + \frac{u^2}{2} - \frac{u^3}{6}, \quad u \geq 0, \quad (4.115)$$

Eq. (4.113) leads to

$$\alpha_n(\eta_n) = \text{Tr} \left[ \left\{ \bigotimes_{i=1}^n \rho_i - e^{n\eta_n} \bigotimes_{i=1}^n \sigma_i \leq 0 \right\} \bigotimes_{i=1}^n \rho_i \right] \quad (4.116)$$

$$\leq \exp \left\{ -\frac{n\bar{v}}{B^2} \left[ \frac{(a_n b)^2}{2\bar{v}^2} - \frac{(a_n b)^3}{6\bar{v}^3} \right] \right\} \quad (4.117)$$

$$= \exp \left\{ -n \left[ \frac{a_n^2 b^2}{2\bar{v} B^2} \left( 1 - \frac{a_n b}{3\bar{v}^2} \right) \right] \right\}. \quad (4.118)$$

Now considering the identical case:

$$\bigotimes_{i=1}^n \rho_i = \rho^{\otimes n} \in \mathcal{S}(\mathcal{H}^{\otimes n}), \quad \text{and} \quad \bigotimes_{i=1}^n \sigma_i = \sigma^{\otimes n} \in \mathcal{S}(\mathcal{H}^{\otimes n}) \quad (4.119)$$

with  $\rho \ll \sigma$  (otherwise  $\alpha_n(\eta_n) = 0$  and Eq. (4.90) holds trivially), we have

$$\bar{v} = V, \quad (4.120)$$

$$b = B = \|\log \rho - \log \sigma - \mathbb{D}(\rho\|\sigma)\|_\infty < \infty, \quad (4.121)$$

where the finiteness of  $b$  comes from  $\rho \ll \sigma$  and the assumption that the Hilbert space  $\mathcal{H}$  is finite-dimensional. From Eq. (4.118), the type-I error is upper bounded by

$$\alpha_n(\eta_n) \leq \exp \left\{ -n \left[ \frac{a_n^2}{2V} \left( 1 - \frac{a_n b}{3V^2} \right) \right] \right\}. \quad (4.122)$$

Finally, recall that  $\lim_{n \rightarrow \infty} a_n = 0$  in Eq. (12.1). By letting  $n$  tend to infinity, we prove the achievability part:

$$\lim_{n \rightarrow +\infty} \frac{1}{na_n^2} \log \alpha_n(\eta_n) \leq -\frac{1}{2V}. \quad (4.123)$$

□

### 4.3.2 Proof of Theorem 4.6

The converse part is a direct consequence of the sharp converse Hoeffding bound, Theorem 4.3, in Section 4.2.

Let  $r_n := D(\rho\|\sigma) - a_n$ ,  $\mathcal{X} = \{x\}$  and  $W_x = \rho$ . We apply Theorem 4.3 with  $r = r_n$  to obtain

$$\widehat{\alpha}_{\exp\{-nr_n\}}(\rho^{\otimes n}\|\sigma^{\otimes n}) \geq \frac{A}{s_n^* \sqrt{n}} \exp \left\{ -n \left[ \sup_{0 < \alpha \leq 1} \frac{1-\alpha}{\alpha} (D_\alpha(\rho\|\sigma) - (r_n - c_n)) \right] \right\}, \quad (4.124)$$

for sufficiently large  $n \in \mathbb{N}$  and some constant  $A > 0$ . Here

$$s_n^* := \arg \max_{s \geq 0} \left\{ s D_{\frac{1}{1+s}}(\rho\|\sigma) - sr_n \right\}. \quad (4.125)$$

Now let

$$\delta_n := a_n + c_n, \quad \forall n \in \mathbb{N}, \quad (4.126)$$

and invoke Proposition 12.2 with  $W_x = \rho$ ,  $P(x) = 1$ , and substitute  $P^* \mathcal{W}$  with  $\sigma$  to obtain

$$\limsup_{n \rightarrow +\infty} \frac{\sup_{s \geq 0} \left\{ -s(D(\rho\|\sigma) - \delta_n) + s D_{\frac{1}{1+s}}(\rho\|\sigma) \right\}}{\delta_n^2} \leq \frac{1}{2V}. \quad (4.127)$$

Moreover, Eq. (12.46) in Proposition 12.2 in Section 12.2 gives that  $\lim_{n \rightarrow +\infty} \frac{s_n^*}{\delta_n} \leq 1/V$ . Here, we delay the proof of Proposition 12.2 to Section 12.3 for the reason that we unify the proofs for the exponent in quantum hypothesis testing and c-q channel coding there.

Combining Eqs. (4.124) and (4.127) concludes our claim:

$$\liminf_{n \rightarrow +\infty} \frac{\log \widehat{\alpha}_{\exp\{-nr_n\}}(\rho^{\otimes n}\|\sigma^{\otimes n})}{n \delta_n^2} \geq -\frac{1}{2V}. \quad (4.128)$$

□

## Part II

# Classical Information Storage with a Quantum Helper

## Chapter 5

# Error Exponent Functions (Source Coding)

In this chapter, we define different versions of the exponent functions and auxiliary functions for Slepian-Wolf coding with QSI. We prove a variational representation in Section 5.1. The properties of the auxiliary function and exponent functions are provided in Sections 5.2 and 5.3, respectively.

For  $t = \{\}, \{*\}$  or  $\{\flat\}$ , we define

$$E_r^t(R) := \max_{0 \leq s \leq 1} \{E_0^t(s) + sR\}; \quad (5.1)$$

$$E_{sp}^t(R) := \sup_{s \geq 0} \{E_0^t(s) + sR\}; \quad (5.2)$$

$$E_{sc}^t(R) := \sup_{-1 < s < 0} \{E_0^t(s) + sR\}; \quad (5.3)$$

$$E_0^t(s) := -sH_{\frac{1}{1+s}}^{t,\uparrow}(X|B)_\rho, \quad (5.4)$$

where  $H_\alpha^{t,\uparrow}$  is the Rényi conditional entropy defined in Section 3.2. For  $t = \{\}$ , i.e. the Petz's Rényi conditional entropy, quantum Sibson's identity given in Lemma 3.3 shows that the auxiliary function  $E_0(s)$  admits an closed-form:

$$E_0(s) = -\log \text{Tr} \left[ \left( \text{Tr}_X \rho_{XB}^{\frac{1}{1+s}} \right)^{1+s} \right] \quad (5.5)$$

We also define another version of the exponent function via  $H_\alpha^\downarrow$ :

$$E_r^\downarrow(R) := \max_{0 \leq s \leq 1} \{E_0^\downarrow(s) + sR\}, \quad (5.6)$$

$$E_0^\downarrow(s) := -sH_{1-s}^\downarrow(X|B)_\rho. \quad (5.7)$$

The Golden-Thompson inequality given in Lemma 2.7 implies that

$$E_{sp}(R) \leq E_{sp}^\flat(R) \quad (5.8)$$

$$E_r(R) \leq E_r^\flat(R). \quad (5.9)$$

Further, since  $H_\alpha^\uparrow(X|B)_\rho \leq H_{2-\frac{1}{\alpha}}^\downarrow(X|B)_\rho$  for  $\alpha \in [1/2, +\infty]$  [128, Corollary 4], [10, Corollary 5.3]. For  $R \in [H_1^\uparrow(X|B)_\rho, H_{1/2}^\uparrow(X|B)_\rho]$ , together with Proposition 5.3-(a) below, we have

$$E_r^\downarrow(R) \leq E_r(R) = E_{sp}(R) \leq E_{sp}^\flat(R) = E_r^\flat(R). \quad (5.10)$$

In Chapter 6 later, we obtain an achievability bound of the optimal error in terms of  $E_r^\downarrow$ . We conjecture that it can be further improved by  $E_r$ .

We also define an exponent that will yield bound to type-dependent sources in Section 6.2.

$$E_r^{(2),\downarrow}(R, P) := \sup_{0 \leq s \leq 1} s \left( \sum_{x \in \mathcal{X}} P(x) D_{1-s}(\rho_B^x \| \rho_B^P) - H(P) + R \right), \quad (5.11)$$

## 5.1 Variational Representations

In Theorem 5.1 below, we show that the exponent functions defined in terms of  $D^\flat$  admit the variational representations as introduced by Csiszár and J. Körner's [55, 56, 27].

**Theorem 5.1** (Variational Representations). *Let  $\rho_{XB}$  be a classical-quantum state. Then,*

$$E_r^\flat(R) = \min_{\sigma_{XB} \in \mathcal{S}(XB)} \{D(\sigma_{XB} \| \rho_{XB}) + |R - H(X|B)_\sigma|^+\}, \quad (5.12)$$

$$E_{sp}^\flat(R) = \min_{\sigma_{XB} \in \mathcal{S}(XB)} \{D(\sigma_{XB} \| \rho_{XB}) : R \leq H(X|B)_\sigma\}, \quad (5.13)$$

$$E_{sc}^\flat(R) = \min_{\sigma_{XB} \in \mathcal{S}(XB)} \{D(\sigma_{XB} \| \rho_{XB}) + |H(X|B)_\sigma - R|^+\}, \quad (5.14)$$

where we denote by  $|x|^+ := \max\{0, x\}$ .

*Proof of Theorem 5.1.* We only provide the proof for Eq (5.13) since Eqs. (5.12) and (5.14) follow similarly. The method of Lagrange multipliers gives that

$$\min_{\sigma_{XB} \in \mathcal{S}(XB)} \{D(\sigma_{XB} \| \rho_{XB}) : R \leq H(X|B)_\sigma\} \quad (5.15)$$

$$= \sup_{s \geq 0} \min_{\sigma_{XB} \in \mathcal{S}(XB)} \{D(\sigma_{XB} \| \rho_{XB}) + s[R - H(X|B)_\sigma]\} \quad (5.16)$$

$$= \sup_{s \geq 0} \min_{\sigma_{XB} \in \mathcal{S}(XB)} \left\{ D(\sigma_{XB} \| \rho_{XB}) + \min_{\tau_B \in \mathcal{S}(B)} sD(\sigma_{XB} \| \mathbb{1}_B \otimes \tau_B) + sR \right\} \quad (5.17)$$

$$= \sup_{s \geq 0} \min_{\tau_B \in \mathcal{S}(B)} \min_{\sigma_{XB} \in \mathcal{S}(XB)} \{D(\sigma_{XB} \| \rho_{XB}) + sD(\sigma_{XB} \| \mathbb{1}_B \otimes \tau_B) + sR\} \quad (5.18)$$

$$= \sup_{s \geq 0} \min_{\tau_B \in \mathcal{S}(B)} \left\{ sD_{\frac{1}{1+s}}^\flat(\rho_{XB} \| \mathbb{1}_B \otimes \tau_B) + sR \right\} \quad (5.19)$$

$$= \sup_{s \geq 0} \left\{ E_0^\flat(s, \rho_{XB}) + sR \right\}, \quad (5.20)$$

where we use the representation  $H(X|B)_\sigma = \max_{\tau_B \in \mathcal{S}(B)} -D(\sigma_{XB} \| \mathbb{1}_X \otimes \tau_B)$  in Eq. (5.17); Eq. (5.19) follows the Lemma 3.1 in Section 3.1, which was proved by Mosonyi and Ogawa [59]; in the last line (5.20) we recall the definition  $E_0^\flat(s, \rho_{XB}) := -sH_{\frac{1}{1+s}}^\flat(X|Y)_\rho$ .  $\square$

## 5.2 Properties of Auxiliary Functions

In the following, we collect some useful properties of the auxiliary functions  $E_0(s)$  and  $E_0^\downarrow(s)$ .

**Proposition 5.1** (Properties of  $E_0$ ). *Let  $\rho_{XB}$  be a classical-quantum state with  $H(X|Y)_\rho > 0$ , the auxiliary function  $E_0(s)$  defined in Eq. (5.5) admits the following properties.*

(a) (Continuity) *The function  $s \mapsto E_0(s)$  is smooth for all  $s \in (-1, +\infty)$ .*

(b) (Negativity)

$$E_0(s) \leq 0, \quad s \geq 0 \quad (5.21)$$

with  $E_0(0) = 0$ .

(c) (Concavity) *The function  $s \mapsto E_0(s)$  is concave in  $s$  for all  $s \in (-1, +\infty)$ .*

(d) (First-order Derivative)

$$\left. \frac{\partial E_0(s)}{\partial s} \right|_{s=0} = -H(X|B)_\rho. \quad (5.22)$$

(e) (Second-order Derivative)

$$\left. \frac{\partial^2 E_0(s)}{\partial s^2} \right|_{s=0} = -V(X|B)_\rho, \quad (5.23)$$

where  $V(X|B)_\rho$  is defined in Eq. (3.21).

The proof is provided in Section 5.2.1 below.

**Proposition 5.2** (Properties of  $E_0^\downarrow$ ). *Let  $\rho_{XB}$  be a classical-quantum state with  $H(X|Y)_\rho > 0$ , the auxiliary function  $E_0^\downarrow(s)$  defined in Eq. (5.7) admits the following properties.*

(a) (Continuity) *The function  $s \mapsto E_0(s)$  is smooth for all  $s \in [0, +\infty)$ .*

(b) (Negativity)

$$E_0^\downarrow(s) \leq 0, \quad s \geq 0 \quad (5.24)$$

with  $E_0^\downarrow(0) = 0$ .

(c) (Concavity) *The function  $s \mapsto E_0^\downarrow(s)$  is concave in  $s$  for all  $s \in (-1, +\infty)$ .*

(d) (First-order Derivative)

$$\left. \frac{\partial E_0^\downarrow(s)}{\partial s} \right|_{s=0} = -H(X|B)_\rho. \quad (5.25)$$

(e) (Second-order Derivative)

$$\left. \frac{\partial^2 E_0^\downarrow(s)}{\partial s^2} \right|_{s=0} = -V(X|B)_\rho. \quad (5.26)$$

The proof is provided in Section 5.2.2 below.

### 5.2.1 Proof of Proposition 5.1

*Proof of Proposition 5.1.*

(5.1)-(a) (Continuity) Since  $E_0(s)$  admits a closed-form

$$-\log \text{Tr} \left[ \text{Tr}_X \rho_{XB}^{\frac{1}{1+s}} \right]^{1+s}, \quad \forall s > -1. \quad (5.27)$$

It is clearly smooth for all  $s > -1$ .

(5.1)-(b) (Negativity) The negativity of  $E_0(s)$  directly follows from the non-negativity of the conditional Rényi entropy and the definition, Eq. (5.4).

(5.1)-(c) (Concavity) The concavity for  $s \geq 0$  can be proved with the geometric matrix means in [36]. Here, we present another proof by the following matrix inequality.

Let  $\rho_{XB} = \sum_{x \in \mathcal{X}} P(x)|x\rangle\langle x| \otimes W_x$ ,  $t = \gamma = 1$ ,  $i = x$ ,  $k = |\mathcal{X}|$ ,  $A_i = P(x)W_x$ , and  $Z_i = I_{n,m}$ . We obtain the log-convexity of the map by applying Lemma 2.12:

$$p \mapsto \text{Tr} \left( \sum_{x \in \mathcal{X}} (P(x)W_x)^{\frac{1}{p}} \right)^p, \quad \forall p > 0, \quad (5.28)$$

which is exactly the concavity of the map  $s \mapsto E_0(s)$  for all  $s > -1$ .

(5.1)-(d) (First-order derivative) By the definition of  $E_0(s)$ ,

$$\frac{\partial E_0(s)}{\partial s} \Big|_{s=0} = -H_{\frac{1}{1+s}}^{\uparrow}(X|B)_{\rho} - s \frac{\partial H_{\frac{1}{1+s}}^{\uparrow}(X|B)_{\rho}}{\partial s} \Big|_{s=0} = -H(X|B)_{\rho}. \quad (5.29)$$

(5.1)-(e) (Second-order derivative) Similar to Item (d), it follows that

$$\frac{\partial^2 E_0(s)}{\partial s^2} \Big|_{s=0} = -2 \frac{\partial H_{\frac{1}{1+s}}^{\uparrow}(X|B)_{\rho}}{\partial s} - s \frac{\partial^2 H_{\frac{1}{1+s}}^{\uparrow}(X|B)_{\rho}}{\partial s^2} \Big|_{s=0}. \quad (5.30)$$

The above equation indicates that we need to evaluate the first-order derivative of  $H_{\frac{1}{1+s}}^{\uparrow}(X|B)_{\rho}$  at 0. In the following, we directly deal with the closed-form expression, Eq. (5.5).

To ease the burden of derivations, we denote some notation:

$$f(s) := \text{Tr}_X \rho_{XB}^{1/(1+s)}, \quad (5.31)$$

$$g(s) := f(s)^{(1+s)}, \quad (5.32)$$

$$F(s) := \text{Tr}[g(s)], \quad (5.33)$$

Then,

$$\frac{\partial E_0(s)}{\partial s} = -\frac{F'(s)}{F(s)} \quad (5.34)$$

$$\frac{\partial^2 E_0(s)}{\partial s^2} = -\frac{F''(s)}{F(s)} - \left( \frac{\partial E_0(s)}{\partial s} \right)^2. \quad (5.35)$$

Direct calculation shows that

$$f'(s) = -\frac{1}{(1+s)^2} \text{Tr}_X \rho_{XB}^{1/(1+s)} \log \rho_{XB}, \quad (5.36)$$

$$f''(s) = \frac{1}{(1+s)^3} \text{Tr}_X \rho_{XB} \log \rho_{XB} \cdot \left[ 2 + \frac{\log \rho_{XB}}{(1+s)} \right]. \quad (5.37)$$

Note that<sup>1</sup>  $g(s) = e^{(1+s)\log f(s)}$ . By applying the chain rule of the Fréchet derivatives, one can show

$$g'(s) = D \exp[\log g(s)] ((1+s)D \log[f(s)] (f'(s)) + \log f(s)). \quad (5.38)$$

---

<sup>1</sup>Here, let's assume  $\rho_{XB}$  has full support on  $\mathcal{S}(XB)$  for brevity. The general case should hold with more technical derivations.

Further, we employ Lemma 2.11 and Eqs.(5.33), (5.38), to obtain

$$F'(s) = \text{Tr} [g'(s) ((1+s)\mathbb{D}\log[f(s)](f'(s)) + \log f(s))] , \quad (5.39)$$

$$\begin{aligned} F''(s)|_{s=0} &= \text{Tr} [g'(s) ((1+s)\mathbb{D}\log[f(s)](f'(s)) + \log f(s))]|_{s=0} \\ &\quad + \text{Tr} [g(s) (2\mathbb{D}\log[f(s)](f'(s)) + (1+s) \{\mathbb{D}\log[f(s)](f''(s)) \\ &\quad + \mathbb{D}^2\log[f(s)](f'(s))\})]|_{s=0}. \end{aligned} \quad (5.40)$$

Before evaluating  $F''(s)$  at  $s = 0$ , note that Eqs. (5.31), (5.32), (5.36), (5.37), and (5.38) yield

$$f(0) = g(0) = \rho_B, \quad (5.41)$$

$$f'(0) = -\text{Tr}_X \rho_{XB} \log \rho_{XB}, \quad (5.42)$$

$$f''(0) = 2\text{Tr}_X \rho_{XB} \log \rho_{XB} + \text{Tr}_X \rho_{XB} \log^2 \rho_{XB}, \quad (5.43)$$

$$g'(0) = \mathbb{D} \exp[\log g(0)] ((1+0)\mathbb{D}\log[f(0)](f'(0)) + \log f(0)) \quad (5.44)$$

$$= \mathbb{D} \exp[\log f(0)] (\mathbb{D}\log[f(0)](f'(0)) + \log f(0)) \quad (5.45)$$

$$= f'(0) + f(0) \log f(0) \quad (5.46)$$

$$= -\text{Tr}_X \rho_{XB} \log \rho_{XB} + \rho_B \log \rho_B. \quad (5.47)$$

From Eqs. (5.46), (5.39), the first term in Eq. (5.40) leads to

$$\text{Tr} [g'(0) ((1+0)\mathbb{D}\log[f(0)](f'(0)) + \log f(0))] \quad (5.48)$$

$$= \text{Tr} [f'(0)\mathbb{D}\log[f(0)](f'(0)) + 2f'(0)\log f(0) + f(0)\log^2 f(0)] \quad (5.49)$$

$$= \text{Tr} [f'(0)\mathbb{D}\log[f(0)](f'(0)) - 2\text{Tr}_X \rho_{XB} \log \rho_{XB} \cdot \log \rho_B + \rho_B \log^2 \rho_B] \quad (5.50)$$

Further, from Eqs. (5.37), (5.42), and (5.43), the second term in Eq. (5.40) leads to

$$\begin{aligned} &\text{Tr} [f(0) (2\mathbb{D}\log[f(0)](f'(0)) + \{\mathbb{D}\log[f(0)](f''(0)) \\ &\quad + \mathbb{D}^2\log[f(0)](f'(0))\})] \end{aligned} \quad (5.51)$$

$$= \text{Tr} [2f'(0) + f''(0) - f'(0)\mathbb{D}\log[f(0)](f'(0))] \quad (5.52)$$

$$= \text{Tr} [\text{Tr}_X \rho_{XB} \log^2 \rho_{XB} - f'(0)\mathbb{D}\log[f(0)](f'(0))]. \quad (5.53)$$

Combining Eqs. (5.40), (5.50), (5.53) gives

$$F''(0) = \text{Tr} [\rho_{XB} (\log \rho_{XB} - \log \mathbb{1}_X \otimes \rho_B)^2]. \quad (5.54)$$

Finally, Eqs. (5.35) and (5.54) conclude our result:

$$\frac{\partial E_0(s)}{\partial s} \Big|_{s=0} = -V(\rho_{XB} \| \mathbb{1}_X \otimes \rho_B) = -V(X|B)_\rho. \quad (5.55)$$

Moreover, Eq. (5.30) gives

$$\frac{\partial H_\alpha^\uparrow(X|B)_\rho}{\partial \alpha} \Big|_{\alpha=0} = \frac{1}{2} V(X|B)_\rho. \quad (5.56)$$

□

### 5.2.2 Proof of Proposition 5.2

*Proof of Proposition 5.2.*

(5.2)-(a) (Continuity) Since  $E_0^\downarrow(s) = -\log \text{Tr} [\rho_{XB}^{1-s} (\mathbb{1}_X \otimes \rho_B)^s]$

$$-\log \text{Tr} \left[ \left( \text{Tr}_X \rho_{XB}^{\frac{1}{1+s}} \right)^{1+s} \right], \quad \forall s > -1. \quad (5.57)$$

It is smooth for all  $s \geq 0$ .

(5.2)-(b) (Negativity) The negativity of  $E_0^\downarrow(s, \rho_{XB})$  directly follows from the non-negativity of the conditional Rényi entropy and the definition, Eq. (5.4).

(5.2)-(c) (Concavity) The claim follows from the concavity of the map  $s \mapsto sD_{1-s}(\cdot \| \cdot)$  (Lemma 3.2-(d)).

(5.2)-(d) (First-order derivative) One can verify that

$$\frac{\partial E_0^\downarrow(s, \rho_{XB})}{\partial s} \Big|_{s=0} = D_{1-s}(\rho_{XB} \| \mathbb{1}_X \otimes \rho_B) - sD'_{1-s}(\rho_{XB} \| \mathbb{1}_X \otimes \rho_B) \Big|_{s=0} \quad (5.58)$$

$$= D_{1-s}(\rho_{XB} \| \mathbb{1}_X \otimes \rho_B) \Big|_{s=0} \quad (5.59)$$

$$= D(\rho_{XB} \| \mathbb{1}_X \otimes \rho_B) \quad (5.60)$$

$$= -H(X|B)_\rho. \quad (5.61)$$

(5.2)-(e) (Second-order derivative) Continuing from item (d), one obtain

$$\frac{\partial^2 E_0^\downarrow(s)}{\partial s^2} \Big|_{s=0} = -2D'_{1-s}(\rho_{XB} \| \mathbb{1}_X \otimes \rho_B) + sD''_{1-s}(\rho_{XB} \| \mathbb{1}_X \otimes \rho_B) \Big|_{s=0} \quad (5.62)$$

$$= -2D'_{1-s}(\rho_{XB} \| \mathbb{1}_X \otimes \rho_B) \Big|_{s=0} \quad (5.63)$$

$$= -V(\rho_{XB} \| \mathbb{1}_X \otimes \rho_B) \quad (5.64)$$

$$= V(X|B)_\rho, \quad (5.65)$$

where in equality (5.64) we use the fact  $D'_{1/(1+s)}(\cdot \| \cdot)|_{s=0} = V(\cdot \| \cdot)/2$  [129, Theorem 2].

□

### 5.3 Properties of Error Exponent Functions and Saddle-Point

**Proposition 5.3** (Properties of the Exponent Function). *Let  $\rho_{XB}$  be a classical-quantum state with  $H(X|B)_\rho > 0$ , the following holds.*

(a)  $E_{\text{sp}}(\cdot)$  is convex, differentiable, and monotonically increasing on  $[0, +\infty]$ . Further,

$$E_{\text{sp}}(R) = \begin{cases} 0, & R \leq H_1^\uparrow(X|B)_\rho \\ E_r(R), & H_1^\uparrow(X|B)_\rho \leq R \leq H_{1/2}^\uparrow(X|B)_\rho \\ +\infty, & R > H_0^\uparrow(X|Y)_\rho \end{cases} \quad (5.66)$$

(b) Define

$$F_R(\alpha, \sigma_B) := \begin{cases} \frac{1-\alpha}{\alpha} (R + D_\alpha(\rho_{XB} \| \mathbb{1}_X \otimes \sigma_B)), & \alpha \in (0, 1), \\ 0, & \alpha = 1, \end{cases} \quad (5.67)$$

on  $(0, 1] \times \mathcal{S}(B)$ . For  $R \in (H_1^\uparrow(X|B)_\rho, H_0^\uparrow(X|B)_\rho)$ , there exists a unique saddle-point  $(\alpha^*, \sigma^*) \in (0, 1) \times \mathcal{S}(B)$  of  $F_R(\cdot, \cdot)$  such that

$$F_R(\alpha^*, \sigma^*) = \sup_{\alpha \in [0, 1]} \inf_{\sigma_B \in \mathcal{S}(B)} F_R(\alpha, \sigma_B) = \inf_{\sigma_B \in \mathcal{S}(B)} \sup_{\alpha \in [0, 1]} F_R(\alpha, \sigma_B) = E_{\text{sp}}(R). \quad (5.68)$$

(c) Any saddle-point  $(\alpha^*, \sigma^*)$  of  $F_R(\cdot, \cdot)$  satisfies

$$\mathbb{1}_X \otimes \sigma^* \gg \rho_{XB}. \quad (5.69)$$

*Proof of Proposition 5.3.*

(5.3)-(a) Item (a) in Proposition 3.1 shows that the map  $\alpha \mapsto H_\alpha^\uparrow(X|B)_\rho$  is monotonically decreasing on  $[0, 1]$ . Hence, from the definition:

$$E_{\text{sp}}(R) := \sup_{\alpha \in (0, 1]} \frac{1-\alpha}{\alpha} (R - H_\alpha^\uparrow(X|B)_\rho), \quad (5.70)$$

it is not hard to verify that  $E_{\text{sp}}(R) = +\infty$  for all  $R > H_0^\uparrow(H|B)_\rho$ ; finite for all  $R < H_0^\uparrow(H|B)_\rho$ ; and  $E_{\text{sp}}^{\text{SW}}(R) = 0$ , for all  $R \geq H_1^\uparrow(H|B)_\rho$ . Moreover,  $E_{\text{sp}}(R) = E_r(R)$  for  $R \in [H_1^\uparrow(X|Y)_\rho, H_{1/2}^\uparrow(X|Y)_\rho]$  by the definition in Eq. (5.1).

For every  $\alpha \in (0, 1]$ , the function  $\frac{1-\alpha}{\alpha}(R - H_\alpha^\uparrow(X|B)_\rho)$  is a non-decreasing, convex, and continuous function in  $R \in \mathbb{R}_{>0}$ . Since  $E_{\text{sp}}(R)$  is the pointwise supremum of the above function,  $E_{\text{sp}}(R)$  is non-decreasing, convex, and lower semi-continuous function for all  $R \geq 0$ . Furthermore, since a convex function is continuous on the interior of the interval if it is finite [117, Corollary 6.3.3], thus  $E_{\text{sp}}(R)$  is continuous for all  $R < H_0^\uparrow(X|B)_\rho$ , and continuous from the left at  $R = H_0^\uparrow(X|B)_\rho$ .

(5.3)-(b) Let

$$\mathcal{S}_\rho(B) := \{\sigma_B \in \mathcal{S}(B) : \rho_{XB} \not\perp \mathbb{1}_X \otimes \sigma_B\}. \quad (5.71)$$

Fix an arbitrary  $R \in (H_1^\uparrow(X|B)_\rho, H_0^\uparrow(X|B)_\rho)$ . In the following, we first prove the existence of a saddle-point of  $F_R(\cdot, \cdot)$  on  $(0, 1] \times \mathcal{S}_\rho(B)$ . Ref. [130, Lemma 36.2] states that  $(\alpha^*, \sigma^*)$  is a saddle point of  $F_R(\cdot, \cdot)$  if and only if the supremum in

$$\sup_{\alpha \in (0, 1]} \inf_{\sigma \in \mathcal{S}_\rho(B)} F_R(\alpha, \sigma) \quad (5.72)$$

is attained at  $\alpha^* \in (0, 1]$ , the infimum in

$$\inf_{\sigma \in \mathcal{S}_\rho(B)} \sup_{\alpha \in (0, 1]} F_R(\alpha, \sigma) \quad (5.73)$$

is attained at  $\sigma^* \in \mathcal{S}_\rho(B)$ , and the two extrema in Eqs. (9.152), (5.73) are equal and finite. We first claim that,  $\forall \alpha \in (0, 1]$ ,

$$\inf_{\sigma \in \mathcal{S}_\rho(B)} F_R(\alpha, \sigma) = \inf_{\sigma \in \mathcal{S}(B)} F_R(\alpha, \sigma). \quad (5.74)$$

To see this, observe that for any  $\alpha \in (0, 1)$ , Eqs. (3.5) yield

$$\forall \sigma \in \mathcal{S}(B) \setminus \mathcal{S}_\rho(B), \quad D_\alpha(\rho_{XB} \| \mathbb{1}_X \otimes \sigma) = +\infty, \quad (5.75)$$

which, in turn, implies

$$\forall \sigma \in \mathcal{S}(B) \setminus \mathcal{S}_\rho(B), \quad F_R(\alpha, \sigma) = +\infty. \quad (5.76)$$

Further, Eq. (5.74) holds trivially when  $\alpha = 1$ . Hence, Eq. (5.74) yields

$$\sup_{\alpha \in (0, 1]} \inf_{\sigma \in \mathcal{S}_\rho(B)} F_R(\alpha, \sigma) = \sup_{\alpha \in (0, 1]} \inf_{\sigma \in \mathcal{S}(B)} F_R(\alpha, \sigma) \quad (5.77)$$

Owing to the fact  $R < H_0^\uparrow(X|B)_\rho$  and Eq. (5.2), we have

$$E_{\text{sp}}(R) = \sup_{\alpha \in (0, 1]} \inf_{\sigma \in \mathcal{S}(B)} F_R(\alpha, \sigma) < +\infty, \quad (5.78)$$

which guarantees the supremum in the right-hand side of Eq. (5.78) is attained at some  $\alpha \in (0, 1]$ . Namely, there exists some  $\bar{\alpha}_R \in (0, 1]$  such that

$$\sup_{\alpha \in (0, 1]} \inf_{\sigma \in \mathcal{S}_\rho(B)} F_R(\alpha, \sigma) = \max_{\alpha \in [\bar{\alpha}_R, 1]} \inf_{\sigma \in \mathcal{S}(B)} F_R(\alpha, \sigma) < +\infty. \quad (5.79)$$

Thus, we complete our claim in Eq. (5.72). It remains to show that the infimum in Eq.(9.153) is attained at some  $\sigma^* \in \mathcal{S}_\rho(B)$  and the supremum and infimum are exchangeable. To achieve this, we will show that  $([\bar{\alpha}_R, 1], \mathcal{S}_\rho(B), F_R)$  is a closed saddle-element (see Definition 5.1 below) and employ the boundness of  $[\bar{\alpha}_R, 1] \times \mathcal{S}_\rho(B)$  to conclude our claim.

**Definition 5.1** (Closed Saddle-Element [130]). We denote by  $\text{ri}$  and  $\text{cl}$  the relative interior and the closure of a set, respectively. Let  $\mathcal{A}, \mathcal{B}$  be subsets of a real vector space, and  $F : \mathcal{A} \times \mathcal{B} \rightarrow \mathbb{R} \cup \{\pm\infty\}$ . The triple  $(\mathcal{A}, \mathcal{B}, F)$  is called a closed saddle-element if for any  $x \in \text{ri}(\mathcal{A})$  (resp.  $y \in \text{ri}(\mathcal{B})$ ),

- (i)  $\mathcal{B}$  (resp.  $\mathcal{A}$ ) is convex.
- (ii)  $F(x, \cdot)$  (resp.  $F(\cdot, y)$ ) is convex (resp. concave) and lower (resp. upper) semi-continuous.
- (iii) Any accumulation point of  $\mathcal{B}$  (resp.  $\mathcal{A}$ ) that does not belong to  $\mathcal{B}$  (resp.  $\mathcal{A}$ ), say  $y_o$  (resp.  $x_o$ ) satisfies  $\lim_{y \rightarrow y_o} F(x, y) = +\infty$  (resp.  $\lim_{x \rightarrow x_o} F(x, y) = -\infty$ ).

Fix an arbitrary  $\alpha \in \text{ri}([\bar{\alpha}_R, 1]) = (\bar{\alpha}_R, 1)$ . We check that  $(\mathcal{S}_\rho(B), F_R(\alpha, \cdot))$  fulfills the three items in Definition 9.1. (i) The set  $\mathcal{S}_\rho(B)$  is clearly convex. (ii) Lemma 3.2-(c) implies that  $\sigma \mapsto D_\alpha(W_x \|\sigma)$  is convex and lower semi-continuous. Since convex combination preserves the convexity and the lower semi-continuity, Eq. (5.67) yields that  $\sigma \mapsto F_R(\alpha, \sigma)$  is convex and lower semi-continuous on  $\mathcal{S}_\rho(B)$ . (iii) Due to the compactness of  $\mathcal{S}(B)$ , any accumulation point of  $\mathcal{S}_\rho(B)$  that does not belong to  $\mathcal{S}_\rho(B)$ , say  $\sigma_o$ , satisfies  $\sigma_o \in \mathcal{S}(B) \setminus \mathcal{S}_\rho(B)$ . Eqs. (5.75) and (5.76) then show that  $F_R(\alpha, \sigma_o) = +\infty$ .

Next, fix an arbitrary  $\sigma \in \text{ri}(\mathcal{S}_\rho(B))$ . Owing to the convexity of  $\mathcal{S}_\rho(B)$ , it follows that  $\text{ri}(\mathcal{S}_\rho(B)) = \text{ri}(\text{cl}(\mathcal{S}_\rho(B)))$  (see e.g. [131, Theorem 6.3]). We first claim  $\text{cl}(\mathcal{S}_\rho(B)) = \mathcal{S}(B)$ . To see this, observe that  $\mathcal{S}_{>0}(B) \subseteq \mathcal{S}_\rho(B)$  since a full-rank operator is not orthogonal with  $\rho_{XB}$ . Hence,

$$\mathcal{S}(B) = \text{cl}(\mathcal{S}_{>0}(B)) \subseteq \text{cl}(\mathcal{S}_\rho(B)). \quad (5.80)$$

On the other hand, the fact  $\mathcal{S}_\rho(B) \subseteq \mathcal{S}(B)$  leads to

$$\text{cl}(\mathcal{S}_\rho(B)) \subseteq \text{cl}(\mathcal{S}(B)) = \mathcal{S}(B). \quad (5.81)$$

By Eqs. (9.160) and (5.81), we deduce that

$$\text{ri}(\mathcal{S}_\rho(B)) = \text{ri}(\text{cl}(\mathcal{S}_\rho(B))) = \text{ri}(\mathcal{S}(B)) = \mathcal{S}_{>0}(B), \quad (5.82)$$

where the last equality in Eq. (5.82) follows from [132, Proposition 2.9]. Hence, we obtain

$$\forall \sigma \in \text{ri}(\mathcal{S}_\rho(B)) \quad \text{and} \quad \mathbb{1}_X \otimes \sigma \gg \rho_{XB}. \quad (5.83)$$

Now we verify that  $([\bar{\alpha}_R, 1], F_R(\cdot, \sigma))$  satisfies the three items in Definition 9.1. Fix an arbitrary  $\sigma \in \text{ri}(\mathcal{S}_\rho(B))$ . (i) The set  $(0, 1]$  is obviously convex. (ii) From Lemma 3.2-(a), the map  $\alpha \mapsto F_R(\alpha, \sigma)$  is continuous on  $(0, 1]$ . Further, it is not hard to verify that  $F_R(1, \sigma) = 0 = \lim_{\alpha \uparrow 1} F_R(\alpha, \sigma)$  from Eqs. (5.83), (9.143), and (3.5). Item (b) in Proposition 3.1 implies that  $\alpha \mapsto F_R(\alpha, \sigma)$  on  $[\bar{\alpha}_R, 1]$  is concave. Moreover, the continuity of  $\alpha \mapsto F_R(\alpha, \sigma)$  on  $[\bar{\alpha}_R, 1]$  guarantees the concavity of  $\alpha \mapsto F_R(\alpha, \sigma)$  on  $[\bar{\alpha}_R, 1]$ . (iii) Since  $[\bar{\alpha}_R, 1]$  is closed, there is no accumulation point of  $[\bar{\alpha}_R, 1]$  that does not belong to  $[\bar{\alpha}_R, 1]$ .

We are at the position to prove the saddle-point property. The closed saddle-element, along with the boundness of  $\mathcal{S}_\rho(B)$  and Rockafellar's saddle-point result [130, Theorem 8], [131, Theorem

37.3] imply that

$$-\infty < \sup_{\alpha \in [\bar{\alpha}_R, 1]} \inf_{\sigma \in \mathcal{S}_\rho(B)} F_R(s, \sigma) = \min_{\sigma \in \mathcal{S}_\rho(B)} \sup_{\alpha \in [\bar{\alpha}_R, 1]} F_R(s, \sigma). \quad (5.84)$$

Then Eqs. (9.159) and (5.84) lead to the existence of a saddle-point of  $F_R(\cdot, \cdot)$  on  $(0, 1] \times \mathcal{S}_\rho(B)$ .

Next, we prove the uniqueness. The rate  $R$  and item (a) in Proposition 5.3 shows that

$$\sup_{0 < \alpha \leq 1} \min_{\sigma \in \mathcal{S}(B)} F_R(\alpha, \sigma) \in \mathbb{R}_{>0}. \quad (5.85)$$

Note that  $\alpha^* = 1$  will not be a saddle point of  $F_{R,P}(\cdot, \sigma)$  because  $F_R(1, \sigma) = 0, \forall \sigma \in \mathcal{S}(B)$ , contradicting Eq. (5.85).

Now, fix  $\alpha^* \in (0, 1)$  to be a saddle-point of  $F_R(\cdot, \cdot)$ . Lemma 3.2-(c) implies that the map  $\sigma \mapsto D_{\alpha^*}(\rho_{XB} \| \mathbf{1}_X \otimes \sigma)$  is convex. Further, observing that  $\rho_X \ll \mathbf{1}_X$ , the convexity can be enhanced to the strict convexity (see e.g. [133, Appendix C]). Thus the minimizer of Eq. (5.85) is unique. Next, let  $\sigma^* \in \mathcal{S}_\rho(B)$  be a saddle-point of  $F_R(\cdot, \cdot)$ . Then,

$$F_R(\alpha, \sigma^*) = \frac{1-\alpha}{\alpha} \left( R - H_\alpha^\uparrow(X|B)_\rho \right). \quad (5.86)$$

Item (b) in Proposition 3.1 then shows that  $\frac{1-\alpha}{\alpha} H_\alpha^\uparrow(X|B)_\rho$  is strictly concave on  $(0, 1)$ , which in turn implies that  $F_R(\cdot, \sigma^*)$  is also strictly concave on  $(0, 1)$ . Hence, the maximizer of Eq. (9.165) is unique, which completes item (b) of Proposition 5.3.

(5.3)-(c) As shown in the proof of item (b),  $\alpha^* = 1$  is not a saddle point of  $F_R(\cdot, \cdot)$  for any  $R < H_0^\uparrow(X|B)_\rho$ . We assume  $(\alpha^*, \sigma^*)$  is a saddle-point of  $F_R(\cdot, \cdot)$  with  $\alpha^* \in (0, 1)$ , it holds that

$$F_R(\alpha^*, \sigma^*) = \min_{\sigma \in \mathcal{S}_\rho(B)} F_R(\alpha^*, \sigma) = \frac{1-\alpha^*}{\alpha^*} R + \frac{1-\alpha^*}{\alpha^*} \min_{\sigma \in \mathcal{S}(B)} D_{\alpha^*}(\rho_{XB} \| \mathbf{1}_X \otimes \sigma). \quad (5.87)$$

By quantum Sibson's identity given in Lemma 3.3 (see also [134], [128, Lemma 1], [10, Lemma 5.1]), the minimizer of Eq. (5.87) is

$$\sigma^* = \frac{(\text{Tr}_X [\rho_{XB}^{\alpha^*}])^{\frac{1}{\alpha^*}}}{\text{Tr} \left[ (\text{Tr}_X [\rho_{XB}^{\alpha^*}])^{\frac{1}{\alpha^*}} \right]}. \quad (5.88)$$

From this expression, it is clear that  $\mathbf{1}_X \otimes \sigma^* \gg \rho_{XB}$ , and thus item (c) is proved.  $\square$

## Chapter 6

# Achievability (Source Coding)

In the error exponent regime (i.e. large deviation regime), the achievability for Slepian-Wolf coding with QSI means that, given a fixed compression rate, there exists a coding strategy such that its error probability is upper bounded by a certain exponential decay, i.e.

$$\forall R > H(X|B)_\rho, \exists \mathcal{C}_n, E(R) > 0 \text{ such that } \varepsilon^*(n, R) \leq \varepsilon(\mathcal{C}_n) \leq \exp\{-nE(R) + o(n)\}. \quad (6.1)$$

The goal of this chapter is to prove a finite blocklength upper bounds for the optimal probability error for Slepian-Wolf coding with QSI. Specifically, we consider the sources generated from two ensembles. The first one is the *i.i.d. ensemble*:

$$\Pr(\mathbf{x}^n) = \prod_{i=1}^n P(x_i), \quad \text{for some } P \in \mathcal{P}(\mathcal{X}). \quad (6.2)$$

In the second scenario, sources are uniformly generated from some type class, i.e.

$$\Pr(\mathbf{x}^n) = \frac{1}{|T_P^n|} \mathbf{1}_{\mathbf{x}^n \in T_P^n}, \quad \text{for some } P \in \mathcal{P}_n(\mathcal{X}), \quad (6.3)$$

where  $T_P^n$  denotes the set of sequences  $\mathbf{x}^n$  with the same empirical distribution  $P$ , and  $\mathcal{P}_n(\mathcal{X})$  denotes the set of all possible types. We call this the *type-dependent sources*.

In Section 6.1 below, we show an achievability bound for the i.i.d. sources. The first order of the exponential error decaying is  $E_r^\downarrow(R)$  (see Eq. (5.6)), which is also termed the random coding exponent for i.i.d. source coding with QSI. In Section 6.2, we prove an achievability bound for the sources with fixed type  $P$ . The first order is  $E_r^{(2),\downarrow}(R, P)$  (see Eq. (5.11)). Via a type decomposition for any codes  $\mathcal{C}^n$  [27]:

$$P_e(\mathcal{C}^n) = \sum_{Q \in \mathcal{P}_n(\mathcal{X})} \Pr[\mathbf{x}^n \in T_Q^n] P_e(\mathcal{C}^n, Q), \quad (6.4)$$

we obtain a second bound for the i.i.d. sources:

$$\min_{Q \in \mathcal{P}(\mathcal{X})} \left\{ D(Q||\rho_X) + E_r^{(2),\downarrow}(R, Q) \right\}. \quad (6.5)$$

Preliminary analysis and simulation indicate that the above quantity is tighter than  $E_r^\downarrow(R)$ . The reason

is that the obtained exponents with ‘ $\downarrow$ ’ are not optimal. See Conjecture 6.1 in Section 6.1 below.

## 6.1 I.I.D. Sources

**Theorem 6.1** (Achievability of CQSI with I.I.D. Sources). *Consider a Slepian-Wolf coding with a joint classical-quantum state  $\rho_{XB} \in \mathcal{S}(XB)$  with  $H(X|B)_\rho > 0$ . Let  $R < H(X|B)_\rho$ . The following holds for every  $n \in \mathbb{N}$ ,*

$$-\frac{1}{n} \log \varepsilon^*(n, R) \geq E_r^\downarrow(R) - \frac{\log 4}{n}, \quad (6.6)$$

where

$$E_r^\downarrow(R) := \sup_{\frac{1}{2} \leq \alpha \leq 1} \frac{1-\alpha}{\alpha} \left( R - H_{2-\frac{1}{\alpha}}^\downarrow(X|B)_\rho \right), \quad (6.7)$$

and  $H_\alpha^\downarrow(X|B)_\rho := -D_\alpha(\rho_{XB} \| \mathbf{1}_X \otimes \rho_B)$  for  $D_\alpha$  being Petz's Rényi divergence, see Eq. (3.5).

*Proof.* Our technique it to use a random coding argument to prove Theorem 6.1. The idea originates from Gallager [57] and later studied by Renes and Renner [41].

We first present an one-shot achievability. It is not hard to extend to the  $n$ -tuple cases. Let  $f : \mathcal{X} \rightarrow \mathcal{I}$  be a random encoder that encodes every source  $x \in \mathcal{X}$  into some index  $i \in \mathcal{I}$  with equal probability  $1/M = 1/|\mathcal{I}|$ . Then, the optimal probability of error can be upper bounded by

$$\varepsilon^*(1, \log M) \leq \mathbb{E}_x \mathbb{E}_i [\varepsilon(x, i)], \quad (6.8)$$

$$= \mathbb{E}_x \mathbb{E}_i \text{Tr} \left[ \rho_B^{(x)} \left( \mathbf{1}_B - \Lambda_x^{(i)} \right) \right], \quad (6.9)$$

where we denote by  $\varepsilon(\mathbf{x}^n, i)$  the error probability conditioned on  $\mathbf{x}^n$  being the source and it is encoded into  $i$ . Here, the adopted decoder is a pretty good measurement:

$$\Lambda_x^{(i)} := \left( \sum_{\bar{x}: f(\bar{x})=i} \Pi_{\bar{x}} \right)^{-1/2} \Pi_x \left( \sum_{\bar{x}: f(\bar{x})=i} \Pi_{\bar{x}} \right)^{-1/2}, \quad (6.10)$$

where  $0 \preceq \Lambda_x^{(i)} \preceq \mathbf{1}_B$  for each  $i \in \mathcal{I}$ , and  $\Pi_x$  will be specified later. Applying the Hayashi-Nagaoka inequality [93, Lemma 2] to obtain

$$\mathbf{1}_X - \Lambda_x^{(i)} \preceq 2(\mathbf{1}_B - \Pi_x) + 4 \sum_{\bar{x} \neq x} \mathbf{1}_{f(\bar{x})=i} \Pi_{\bar{x}}, \quad (6.11)$$

where  $\mathbf{1}_{f(\bar{x})=i}$  denotes the indicator function when the event  $f(\bar{x}) = i$  is true. Combining Eqs. (6.9) and (6.11) gives

$$\varepsilon(x, i) \leq 2 \text{Tr} \left[ \rho_B^{(x)} (\mathbf{1}_B - \Pi_x) \right] + 4 \text{Tr} \left[ \rho_B^{(x)} \sum_{\bar{x} \neq x} \mathbf{1}_{f(\bar{x})=i} \Pi_{\bar{x}} \right]. \quad (6.12)$$

Taking average over  $i$  and using the assumption  $\Pr\{f(\bar{x}) = i\} = 1/M$  yield

$$\mathbb{E}_i [\varepsilon(x, i)] \leq 2 \text{Tr} \left[ \rho_B^{(x)} (\mathbb{1}_B - \Pi_x) \right] + 4 \Pr\{f(\bar{x}) = i\} \text{Tr} \left[ \rho_B^{(x)} \sum_{\bar{x} \neq x} \Pi_{\bar{x}} \right] \quad (6.13)$$

$$= 2 \text{Tr} \left[ \rho_B^{(x)} (\mathbb{1}_B - \Pi_x) \right] + \frac{4}{M} \text{Tr} \left[ \rho_B^{(x)} \sum_{\bar{x} \neq x} \Pi_{\bar{x}} \right] \quad (6.14)$$

$$\leq 2 \text{Tr} \left[ \rho_B^{(x)} (\mathbb{1}_B - \Pi_x) \right] + \frac{4}{M} \text{Tr} \left[ \rho_B^{(x)} \sum_{\bar{x} \in \mathcal{X}} \Pi_{\bar{x}} \right]. \quad (6.15)$$

By taking average over  $x$  we obtain

$$\varepsilon^*(1, \log M) \leq 2 \sum_{x \in \mathcal{X}} P(x) \text{Tr} \left[ \rho_B^{(x)} (\mathbb{1}_B - \Pi_x) \right] + \frac{4}{M} \text{Tr} \left[ \rho_B \sum_{\bar{x} \in \mathcal{X}} \Pi_{\bar{x}} \right], \quad (6.16)$$

$$= 2 \text{Tr} [\rho_{XB} (\mathbb{1}_{XB} - \Pi_{XB})] + \frac{4}{M} \text{Tr} [\mathbb{1}_X \otimes \rho_B \Pi_{XB}], \quad (6.17)$$

where  $\Pi_{XB} := \sum_{x \in \mathcal{X}} |x\rangle\langle x| \otimes \Pi_x$ . Next, we invoke Audenaert *et al.*'s inequality in Lemma 2.8: for every  $\mathbf{X}, \mathbf{Y} \succeq 0$  and  $s \in [0, 1]$ ,

$$\text{Tr} [\{\mathbf{X} - \mathbf{Y} \succeq 0\} \mathbf{Y} + \{\mathbf{Y} - \mathbf{X} \prec 0\} \mathbf{X}] \leq \text{Tr} [\mathbf{X}^{1-s} \mathbf{Y}^s]. \quad (6.18)$$

Letting  $\mathbf{X} = \rho_{XB}$ ,  $\mathbf{Y} = \frac{1}{M} \mathbb{1}_X \otimes \rho_B$ ,  $\Pi_{XB} = \{\rho_{XB} - \frac{1}{M} \mathbb{1}_X \otimes \rho_B \succeq 0\}$ , we have one-shot achievability:

$$\varepsilon^*(1, \log M) \leq 4 \min_{s \in [0, 1]} M^{-s} \text{Tr} [\rho_{XB}^{1-s} (\mathbb{1}_X \otimes \rho_B)^s]. \quad (6.19)$$

Finally, we consider the  $n$ -tuple case. Note that  $\rho_{X^n B^n} = \rho_{XB}^{\otimes n}$ , and let  $M = \exp\{nR\}$ . Eqs. (6.19) and (5.6) lead to

$$\varepsilon^*(n, R) \leq 4 \exp \left\{ -n E_r^\downarrow(R) \right\}, \quad (6.20)$$

which completes the proof □

**Conjecture 6.1** (Random Coding Bound for CQSW). *Consider a Slepian-Wolf coding with a joint classical-quantum state  $\rho_{XB} \in \mathcal{S}(XB)$  with  $H(X|B)_\rho > 0$ . Let  $R < H(X|B)_\rho$ . The following holds for every  $n \in \mathbb{N}$ ,*

$$-\frac{1}{n} \log \varepsilon^*(n, R) \geq E_r(R), \quad (6.21)$$

where

$$E_r(R) := \sup_{\frac{1}{2} \leq \alpha \leq 1} \frac{1-\alpha}{\alpha} \left( R - H_\alpha^\uparrow(X|B)_\rho \right), \quad (6.22)$$

and  $H_\alpha^\uparrow(X|B)_\rho := \max_{\sigma_B \in \mathcal{S}(B)} D_\alpha(\rho_{XB} \| \mathbb{1}_X \otimes \sigma_B)$  for  $D_\alpha$  being Petz's Rényi divergence, see Eq. (3.5).

## 6.2 Type-Dependent Sources

**Theorem 6.2** (Achievability of CQSI with Type-Dependent Sources). *For any  $n \geq 2$ , quantum side information  $\{\rho_B^x\}_{x \in \mathcal{X}}$ ,  $P \in \mathcal{P}_n(\mathcal{X})$ , there exist an  $n$ -blocklength channel code  $\mathcal{C}$  with fixed composition  $P$  and rate  $R$  such that the average error probability  $\text{P}_e(\mathcal{C})$  can be bounded by*

$$\log \text{P}_e(\mathcal{C}) \leq -nE_r^{(2),\downarrow}(R, P) + K \log n, \quad (6.23)$$

where  $K$  is a constant only depending on  $|\mathcal{X}|$ , and the entropic exponent function is defined by

$$E_r^{(2),\downarrow}(R, P) := \sup_{0 \leq s \leq 1} s \left( \sum_{x \in \mathcal{X}} P(x) D_{1-s}(\rho_B^x \| \rho_B^P) - H(P) + R \right), \quad (6.24)$$

where  $\rho_B^P := \sum_{x \in \mathcal{X}} P(x) \rho_B^x$ . In particular,

$$-\frac{1}{n} \log \varepsilon^*(n, R, P) \geq E_r^{(2),\downarrow}(R, P) - \frac{K \log n}{n}. \quad (6.25)$$

To prove Theorem 6.2, we will first prove a one-shot version given by the following proposition.

**Proposition 6.1** (One-shot Achievability of CQSI). *For any quantum side information  $\{\rho_B^x\}_{x \in \mathcal{X}}$ ,  $P \in \mathcal{P}(\mathcal{X})$ ,  $\mathcal{B} \subset \mathcal{X}$ , sources uniformly distributed from  $\mathcal{B}$ , an index set  $\mathcal{I}$ , and  $\alpha \in [1/2, 1]$ , there exists a code  $\mathcal{C}$  such that the average error probability  $\text{P}_e(\mathcal{C})$  can be bounded by*

$$\log \text{P}_e(\mathcal{C}) \leq -s \left[ \inf_{x \in \mathcal{B}} D_{1-s}(\rho_B^x \| \rho_B^P) - \log(|\mathcal{B}| - 1) + \log |\mathcal{I}| \right] + \log \frac{6}{P(\mathcal{B})}. \quad (6.26)$$

*Proof of Proposition 10.1.* We prove the existence of the source codes satisfying Eq. (6.26) by using a random coding argument. For any  $P \in \mathcal{P}(\mathcal{X})$  and  $\mathcal{B} \subset \mathcal{X}$  with  $P(\mathcal{B}) > 0$ , we define the conditional probability as

$$P_{\mathcal{B}}(x) := \frac{\mathbb{1}_{x \in \mathcal{B}} P(x)}{P(\mathcal{B})}. \quad (6.27)$$

We consider the ensemble of codes satisfying the following: the assignments of the sources  $x$  to the index  $\mathcal{E}(x) = i$  are jointly independent with probability  $\frac{1}{|\mathcal{I}|}$  for all  $i \in \mathcal{I}$ . The decoder is characterized by a family of POVMs  $\mathcal{F} = (\Pi_x^{(i)})_{x \in \mathcal{B}, i \in \mathcal{I}}$ :

$$\Pi_x^{(i)} := \left( \sum_{\bar{x} \in \mathcal{B}} \Lambda_{\bar{x}}^{(i)} \right)^{-1/2} \Lambda_x^{(i)} \left( \sum_{\bar{x} \in \mathcal{B}} \Lambda_{\bar{x}}^{(i)} \right)^{-1/2}, \quad (6.28)$$

$$\Lambda_x^{(i)} := \left\{ \rho_B^x \otimes |i\rangle\langle i| - \gamma \rho_B^{P_{\mathcal{B}}} \otimes \tau_{\mathcal{I}} > 0 \right\}, \quad (6.29)$$

where  $\gamma > 0$  will be chosen later, and  $\tau_{\mathcal{I}}$  means the uniform distribution on  $\mathcal{I}$ . Then, the average error probability of the code  $\mathcal{C} = (\mathcal{E}, \mathcal{F})$  is

$$\text{P}_e(\mathcal{C}) = \frac{1}{|\mathcal{B}|} \sum_{x \in \mathcal{B}} \text{Tr} \left[ \rho_B^x \otimes |i\rangle\langle i| \left( \mathbb{1} - \Pi_x^{(i)} \right) \right]. \quad (6.30)$$

Invoking the Hayashi-Nagaoka inequality in Lemma 2.9:

$$\mathbb{1} - \Pi_x^{(i)} \leq 2 \left( \mathbb{1} - \Lambda_x^{(i)} \right) + 4 \sum_{\bar{x} \neq x} \Lambda_{\bar{x}}^{(i)}, \quad (6.31)$$

we obtain

$$\begin{aligned} P_e(\mathcal{C}) &\leq \frac{2}{|\mathcal{B}|} \sum_{x \in \mathcal{B}} \text{Tr} \left[ \rho_B^x \otimes |i\rangle\langle i| \left\{ \rho_B^x |i\rangle\langle i| - \gamma \rho_B^{P_B} \otimes \tau_{\mathcal{I}} \leq 0 \right\} \right] \\ &\quad + \frac{4}{|\mathcal{B}|} \sum_{x \in \mathcal{B}} \sum_{\bar{x} \neq x} \text{Tr} \left[ \rho_B^x \otimes |i\rangle\langle i| \left\{ \rho_{\bar{x}}^{\bar{x}} \otimes |\bar{i}\rangle\langle \bar{i}| - \gamma \rho_B^{P_B} \otimes \tau_{\mathcal{I}} > 0 \right\} \right]. \end{aligned} \quad (6.32)$$

The expected value of  $P_e(\mathcal{C})$  over the ensemble is then

$$\begin{aligned} \mathbb{E}[P_e(\mathcal{C})] &\leq \frac{2}{|\mathcal{B}||\mathcal{I}|} \sum_{x \in \mathcal{B}} \sum_{i \in \mathcal{I}} \text{Tr} \left[ \rho_B^x \otimes |i\rangle\langle i| \left\{ \rho_B^x |i\rangle\langle i| - \gamma \rho_B^{P_B} \otimes \tau_{\mathcal{I}} \leq 0 \right\} \right] \\ &\quad + \frac{4}{|\mathcal{B}|} \sum_{i, \bar{i} \in \mathcal{I}} \Pr(i, \bar{i}) \sum_{x \in \mathcal{B}} \sum_{\bar{x} \neq x} \text{Tr} \left[ \rho_B^x \otimes |i\rangle\langle i| \left\{ \rho_{\bar{x}}^{\bar{x}} \otimes |\bar{i}\rangle\langle \bar{i}| - \gamma \rho_B^{P_B} \otimes \tau_{\mathcal{I}} > 0 \right\} \right] \\ &= \frac{2}{|\mathcal{B}||\mathcal{I}|} \sum_{x \in \mathcal{B}} \sum_{i \in \mathcal{I}} \text{Tr} \left[ \rho_B^x \otimes |i\rangle\langle i| \left\{ \rho_B^x |i\rangle\langle i| - \gamma \rho_B^{P_B} \otimes \tau_{\mathcal{I}} \leq 0 \right\} \right] \\ &\quad + \frac{4}{|\mathcal{B}|} \sum_{i \in \mathcal{I}} \Pr(i) \sum_{x \in \mathcal{B}} \sum_{\bar{x} \neq x} \text{Tr} \left[ \rho_B^x \otimes \tau_{\mathcal{I}} \left\{ \rho_{\bar{x}}^{\bar{x}} \otimes |i\rangle\langle i| - \gamma \rho_B^{P_B} \otimes \tau_{\mathcal{I}} > 0 \right\} \right] \\ &= \frac{2}{|\mathcal{B}||\mathcal{I}|} \sum_{x \in \mathcal{B}} \sum_{i \in \mathcal{I}} \text{Tr} \left[ \rho_B^x \otimes |i\rangle\langle i| \left\{ \rho_B^x |i\rangle\langle i| - \gamma \rho_B^{P_B} \otimes \tau_{\mathcal{I}} \leq 0 \right\} \right] \\ &\quad + 4(|\mathcal{B}| - 1) \sup_{x \in \mathcal{B}, i \in \mathcal{I}} \text{Tr} \left[ \rho_B^{P_B} \otimes \tau_{\mathcal{I}} \left\{ \rho_{\bar{x}}^{\bar{x}} \otimes |i\rangle\langle i| - \gamma \rho_B^{P_B} \otimes \tau_{\mathcal{I}} > 0 \right\} \right]. \end{aligned}$$

Next, we apply Audenaert *et al.*'s inequality in Lemma 2.8: for every  $A, B \geq 0$  and  $s \in [0, 1]$ ,

$$\text{Tr} [\{A - B \geq 0\} B + \{B - A \leq 0\} A] \leq \text{Tr} [A^{1-s} B^s]. \quad (6.33)$$

Letting  $A = \rho_B^x \otimes |i\rangle\langle i|$  and  $B = \gamma \rho_B^{P_B} \otimes \tau_{\mathcal{I}}$ , the first term on the right-hand side of Eq. (10.43) can be upper bounded by

$$\begin{aligned} &\frac{2}{|\mathcal{B}||\mathcal{I}|} \sum_{x \in \mathcal{B}} \sum_{i \in \mathcal{I}} \text{Tr} \left[ \rho_B^x \otimes |i\rangle\langle i| \left\{ \rho_B^x |i\rangle\langle i| - \gamma \rho_B^{P_B} \otimes \tau_{\mathcal{I}} \leq 0 \right\} \right] \\ &\leq \frac{2}{|\mathcal{B}||\mathcal{I}|} \sum_{x \in \mathcal{B}} \sum_{i \in \mathcal{I}} \gamma^s \text{Tr} \left[ (\rho_B^x \otimes |i\rangle\langle i|)^{1-s} \left( \rho_B^{P_B} \otimes \tau_{\mathcal{I}} \right)^s \right] \end{aligned} \quad (6.34)$$

$$\leq 2\gamma^s \exp \left\{ -s \inf_{x \in \mathcal{B}, i \in \mathcal{I}} D_{1-s} \left( \rho_B^x \otimes |i\rangle\langle i| \middle\| \rho_B^{P_B} \otimes \tau_{\mathcal{I}} \right) \right\} \quad (6.35)$$

$$= 2\gamma^s \exp \left\{ -s \left[ \inf_{x \in \mathcal{B}} D_{1-s} \left( \rho_B^x \middle\| \rho_B^{P_B} \right) + \log |\mathcal{I}| \right] \right\}, \quad (6.36)$$

for all  $s \in [0, 1]$ . Here, we use the additivity of  $D_\alpha$  in the last equality. Similarly, the second term on

the right-hand side of Eq. (10.43) can be upper bounded by

$$\begin{aligned} & 4(|\mathcal{B}| - 1) \sup_{x \in \mathcal{B}, i \in \mathcal{I}} \text{Tr} \left[ \rho_B^{P_{\mathcal{B}}} \otimes \tau_{\mathcal{I}} \left\{ \rho_B^{\bar{x}} \otimes |i\rangle\langle i| - \gamma \rho_B^{P_{\mathcal{B}}} \otimes \tau_{\mathcal{I}} > 0 \right\} \right] \\ & \leq 4(|\mathcal{B}| - 1) \gamma^{s-1} \sup_{x \in \mathcal{B}, i \in \mathcal{I}} \text{Tr} \left[ (\rho_B^x \otimes |i\rangle\langle i|)^{1-s} (\gamma \rho_B^P)^{1-t} \right] \end{aligned} \quad (6.37)$$

$$\leq 4(|\mathcal{B}| - 1) \gamma^{s-1} \exp \left\{ -s \left[ \inf_{x \in \mathcal{B}} D_{1-s} \left( \rho_B^x \| \rho_B^{P_{\mathcal{B}}} \right) + \log |\mathcal{I}| \right] \right\}. \quad (6.38)$$

By setting  $\gamma = |\mathcal{B}| - 1$ , Eqs. (6.33), (6.36), and (6.38) together yield

$$\mathbb{E} [\text{P}_e(\mathcal{C})] \leq 6 \exp \left\{ -s \left[ \inf_{x \in \mathcal{B}} D_{1-s} \left( \rho_B^x \| \rho_B^{P_{\mathcal{B}}} \right) - \log(|\mathcal{B}| - 1) + \log |\mathcal{I}| \right] \right\}. \quad (6.39)$$

Observe that

$$\rho_B^{P_{\mathcal{B}}} = \sum_x \frac{\mathbf{1}_{x \in \mathcal{B}} P(x) \rho_B^x}{P(\mathcal{B})} \leq \sum_x \frac{P(x) \rho_B^x}{P(\mathcal{B})} = \frac{\rho_B^x}{P(\mathcal{B})}. \quad (6.40)$$

Since Petz's Rényi divergence is non-increasing in its second argument [59, Lemma 3.24], we obtain

$$\mathbb{E} [\text{P}_e(\mathcal{C})] \leq 6 \exp \left\{ -s \left[ \inf_{x \in \mathcal{B}} D_{1-s} \left( \rho_B^x \| \rho_B^P \right) - \log(|\mathcal{B}| - 1) + \log |\mathcal{I}| + \log(P(\mathcal{B})) \right] \right\} \quad (6.41)$$

$$\leq \frac{6}{P(\mathcal{B})} \exp \left\{ -s \left[ \inf_{x \in \mathcal{B}} D_{1-s} \left( \rho_B^x \| \rho_B^P \right) - \log(|\mathcal{B}| - 1) + \log |\mathcal{I}| \right] \right\}. \quad (6.42)$$

Since there exists a channel coding with the average error probability less than or equal to  $\mathbb{E} [\text{P}_e(\mathcal{C})]$ , our claim is thus proven.  $\square$

By applying Proposition 6.1 with the type class  $T_P^n$  as the codeword space, we immediately arrive at the following achievability result for constant composition coding.

*Proof of Theorem 6.2.* First note that

$$\rho_{B^n}^{P^{\otimes n}} = \sum_{x^n \in \mathcal{X}^n} P^{\otimes n}(x^n) \rho_{B^n}^{x^n} = (\rho_B^P)^{\otimes n}. \quad (6.43)$$

The additivity of Rényi relative entropy implies that for all  $\mathbf{x} \in T_P^n$  and  $s \in [0, 1]$ ,

$$D_{1-s} \left( \rho_{B^n}^{x^n} \| \rho_{B^n}^{P^{\otimes n}} \right) = D_{1-s} \left( \rho_{B^n}^{x^n} \| (\rho_B^P)^{\otimes n} \right) \quad (6.44)$$

$$= n \sum_{x \in \mathcal{X}} P(x) D_{1-s} \left( \rho_B^x \| \rho_B^P \right). \quad (6.45)$$

Let  $\mathcal{B} = T_P^n$  in Proposition 6.1. By [27, p. 26], the probability of the set of all sequences with composition  $P$  under the i.i.d. distribution  $P$  is

$$P^{\otimes n} (T_P^n) = e^{-\xi \frac{|\text{supp}(P)|}{12 \log 2}} (2\pi n)^{-\frac{|\text{supp}(P)|-1}{2}} \sqrt{\prod_{x: P(x) > 0} \frac{1}{P(x)}} \quad (6.46)$$

for some  $\xi \in [0, 1]$ . Hence, Proposition 10.1 ensures that there exists an  $n$ -blocklength channel code  $\mathcal{C}$  with fixed composition  $P$  and rate  $R = \frac{\log |\mathcal{C}|}{n}$  such that

$$\log P_e(\mathcal{C}) \leq -nE_r^{(2),\downarrow}(R, P) + \frac{|\text{supp}(P)|}{12 \log 2} + \frac{|\text{supp}(P)| - 1}{2} \log(2\pi n) + \frac{1}{2} \sum_{x:P(x)>0} \log P(x) + \log 6. \quad (6.47)$$

Taking

$$K := \frac{|\mathcal{X}|}{12 \log 2} + \frac{|\mathcal{X}| - 1}{2} (1 + \log(2\pi)) + \log 6, \quad (6.48)$$

our result is proved for all  $n \geq 2$  such that  $\log n \geq 0$ .  $\square$

## Chapter 7

# Optimality (Source Coding)

The main result of this section is the finite blocklength converse bound for the optimal error probability—Theorem 7.1. We termed this the sphere-packing bound for Slepian-Wolf coding with QSI, as a counterpart of the sphere-packing bound in classical-quantum channel coding; see Chapter 11. The proof technique relies on an one-shot converse bound in Proposition 7.1 below, and a sharp  $n$ -shot converse bound, Theorem 4.3, given in Section 4.2.

**Theorem 7.1** (Sphere-Packing Bound for Slepian-Wolf Coding). *Consider a Slepian-Wolf coding with a joint classical-quantum state  $\rho_{XB} \in \mathcal{S}(XB)$  with  $H(X|B)_\rho > 0$ . Let  $R \in (H(X|B)_\rho, H_0^\uparrow(X|B)_\rho)$ . Then, there exist  $N_0, K \in \mathbb{N}$ , such that for all  $n \geq N_0$ , the following holds:*

$$-\frac{1}{n} \log \varepsilon^*(n, R) \leq E_{\text{sp}}(R) + \frac{1}{2} \left( 1 + \left| \frac{\partial E_{\text{sp}}(r)}{\partial r} \right|_{r=R} \right) \frac{\log n}{n} + \frac{K}{n}, \quad (7.1)$$

where

$$E_{\text{sp}}(R) := \sup_{0 \leq \alpha \leq 1} \frac{1-\alpha}{\alpha} \left( R - H_\alpha^\uparrow(X|B)_\rho \right), \quad (7.2)$$

and  $H_\alpha^\uparrow(X|B)_\rho := \max_{\sigma_B \in \mathcal{S}(B)} -D_\alpha(\rho_{XB} \| \mathbf{1}_X \otimes \sigma_B)$ .

The proof is provided in Section 7.2

### 7.1 One-Shot Converse Bound (Hypothesis Testing Reduction)

**Proposition 7.1** (One-Shot Converse Bound for Error). *Consider a Slepian-Wolf coding with a joint classical-quantum state  $\rho_{XB} \in \mathcal{S}(XB)$  and the index size  $M < |\mathcal{X}|$ . Then,*

$$-\log \varepsilon^*(1, \log M) \leq \min_{\sigma_B \in \mathcal{S}(B)} -\log \widehat{\alpha}_{\frac{M}{|\mathcal{X}|}}(\rho_{XB} \| \tau_X \otimes \sigma_B), \quad (7.3)$$

where  $\tau_X$  denotes the uniform distribution on the input alphabet  $\mathcal{X}$ ; and  $\widehat{\alpha}_\mu(\cdot \| \cdot)$  is defined in Eq. (4.3).

*Proof of Proposition 7.1.* We first claim that we can reduce to the case of deterministic encoders as follows. Assume for any deterministic encoder  $\mathcal{E} : \mathcal{X} \rightarrow \mathcal{W}$  with index size  $|\mathcal{W}| = M$ , any decoder  $\mathcal{D}$ ,

and any state  $\sigma_B \in \mathcal{S}(B)$ , we have

$$1 - \sum_{x \in \mathcal{X}} p(y) \text{Tr}[\Pi_y^{(\mathcal{E}(y))} \rho_B^y] \geq \hat{\alpha}_{\frac{M}{|\mathcal{X}|}}(\rho_{XB} \| \tau_X \otimes \sigma_B) \quad (7.4)$$

for  $\tau_X = \frac{1}{|\mathcal{X}|} \mathbb{1}_X$ . Then given a random encoding  $F$ , we may average over its constituent deterministic encoders to obtain

$$1 - \sum_{x \in \mathcal{X}} p(y) \sum_{j=1}^{|\mathcal{F}|} P_j \text{Tr}[\Pi_y^{(\mathcal{E}_j(y))} \rho_B^y] \geq \hat{\alpha}_{\frac{M}{|\mathcal{X}|}}(\rho_{XB} \| \tau_X \otimes \sigma_B) \quad (7.5)$$

using that (7.4) holds for each  $\mathcal{E}_j$ . Then, since the RHS does not depend on the encoding or decoding, we may minimize over random encodings  $F$  and decodings  $\mathcal{D}$  to find

$$\varepsilon^* \geq \hat{\alpha}_{\frac{M}{|\mathcal{X}|}}(\rho_{XB} \| \tau_X \otimes \sigma_B). \quad (7.6)$$

Thus

$$-\log \varepsilon^*(1, \log M) \leq -\log \hat{\alpha}_{\frac{M}{|\mathcal{X}|}}(\rho_{XB} \| \tau_X \otimes \sigma_B). \quad (7.7)$$

Since the LHS does not depend on  $\sigma$ , we may minimize over it, yielding

$$-\log \varepsilon^*(1, \log M) \leq \inf_{\sigma_B \in \mathcal{S}(B)} -\log \hat{\alpha}_{\frac{M}{|\mathcal{X}|}}(\rho_{XB} \| \tau_X \otimes \sigma_B) \quad (7.8)$$

which is the conjecture, (7.3).

Fix deterministic encoding  $\mathcal{E}$  and a decoding strategy, i.e. a collection of POVMs  $\{\mathcal{P}_w\}_{w \in \mathcal{W}}$ , given by  $\mathcal{P}_w = \{\Pi_{\hat{x}}^{(w)}\}_{\hat{x} \in \mathcal{X}}$ . Consider the map  $\Lambda : XB \rightarrow XB$  such that

$$\Lambda(|x\rangle\langle x| \otimes \sigma_B) = |x\rangle\langle x| \otimes \sum_{\hat{x}} \text{Tr}[\Pi_{\hat{x}}^{(\mathcal{E}(x))} \sigma_B] |\hat{x}\rangle\langle \hat{x}|. \quad (7.9)$$

This is the map that encodes in the second register the probability of each measurement outcome of the POVM  $\{\Pi_{\hat{x}}^{(\mathcal{E}(x))}\}_{\hat{x} \in \mathcal{X}}$ , when  $x$  is in the first register. To see that  $\Lambda$  is completely positive (CP), let us define for each  $x \in \mathcal{X}$  the measure-and-prepare map  $\Lambda^x : B \rightarrow B$  given by

$$\Lambda^x : \sigma_B \mapsto \sum_{\hat{x}} \text{Tr}[\Pi_{\hat{x}}^{(\mathcal{E}(x))} \sigma_B] |\hat{x}\rangle\langle \hat{x}|, \quad (7.10)$$

which is CP (see e.g. [50]). Then writing  $L_{|x\rangle\langle x|}$  for left-multiplication by the projector  $|x\rangle\langle x|$  and similarly  $R_{|x\rangle\langle x|}$  for right-multiplication, we have that

$$\Lambda = \sum_{x \in \mathcal{X}} L_{|x\rangle\langle x|} R_{|x\rangle\langle x|} \otimes \Lambda^x. \quad (7.11)$$

Since  $L_A R_A$  is CP for self-adjoint  $A$  (since  $A$  is its only Kraus operator), and the sum of CP maps is CP, we have that  $\Lambda$  is CP.

We define  $\hat{\alpha}_\varepsilon(\rho\|\sigma)$  as the minimum type I error for a binary test discriminating between  $\rho$  and  $\sigma$ , with type II error bounded by  $\varepsilon$ . The type I error of a test  $T$  here is  $\text{Tr}[(\mathbb{1} - T)\rho]$  and the type II error

is  $\text{Tr}[T\sigma]$ , and therefore

$$\hat{\alpha}_\varepsilon(\rho\|\sigma) = \inf_{\substack{T: 0 \leq T \leq \mathbb{1} \\ \text{Tr}[T\sigma] \leq \varepsilon}} \text{Tr}[(\mathbb{1} - T)\rho] \quad (7.12)$$

By writing the optimal type-I error into the hypothesis testing relative entropy [16],

$$-\log \hat{\alpha}_\varepsilon(\rho\|\sigma) = D_H^\varepsilon(\sigma\|\rho). \quad (7.13)$$

Since the hypothesis testing relative entropy satisfies the DPI, we have

$$D_H^\varepsilon(\rho\|\sigma) \geq D_H^\varepsilon(\Phi(\rho)\|\Phi(\sigma)) \quad (7.14)$$

for any CP map  $\Phi$ . Therefore,

$$\hat{\alpha}_\varepsilon(\rho\|\sigma) = \exp(-D_H^\varepsilon(\sigma\|\rho)) \leq \exp(-D_H^\varepsilon(\Phi(\sigma)\|\Phi(\rho))) = \hat{\alpha}_\varepsilon(\Phi(\rho)\|\Phi(\sigma)). \quad (7.15)$$

We set  $\tau_X = \frac{1}{|\mathcal{X}|} \mathbb{1}_X = \frac{1}{|\mathcal{X}|} \sum_{x \in \mathcal{X}} |x\rangle\langle x|$  as the completely mixed state on  $X$  and  $\sigma_B \in \mathcal{S}(B)$  arbitrary. Then for any  $\varepsilon > 0$ ,

$$\hat{\alpha}_\varepsilon(\rho_{XB}\|\tau_X \otimes \sigma_B) \leq \hat{\alpha}_\varepsilon(\Lambda(\rho_{XB})\|\Lambda(\tau_X \otimes \sigma_B)). \quad (7.16)$$

Let us consider these two states:

$$\Lambda(\tau_X \otimes \sigma_B) = \frac{1}{|\mathcal{X}|} \sum_{x \in \mathcal{X}} \Lambda(|x\rangle\langle x| \otimes \sigma_B) = \frac{1}{|\mathcal{X}|} \sum_{x \in \mathcal{X}} |x\rangle\langle x| \otimes \sum_{\hat{x}} \text{Tr}[\Pi_{\hat{x}}^{(\mathcal{E}(x))} \sigma_B] |\hat{x}\rangle\langle \hat{x}|, \quad (7.17)$$

and

$$\Lambda(\rho_{XB}) = \sum_{x \in \mathcal{X}} p(x) \Lambda(|x\rangle\langle x| \otimes \rho_B^x) = \sum_{x \in \mathcal{X}} p(x) |x\rangle\langle x| \otimes \sum_{\hat{x} \in \mathcal{X}} \text{Tr}[\Pi_{\hat{x}}^{(\mathcal{E}(x))} \rho_B^x] |\hat{x}\rangle\langle \hat{x}|. \quad (7.18)$$

Now, take a two element POVM (the test) as  $T = \sum_y |y\rangle\langle y| \otimes |y\rangle\langle y|$ . Then,

$$\text{Tr}[T\Lambda(\rho_{XB})] = \sum_y p(y) \text{Tr}[\Pi_y^{(\mathcal{E}(y))} \rho_B^y], \quad (7.19)$$

so this test has type I error of  $1 - \sum_y p(y) \text{Tr}[\Pi_y^{(\mathcal{E}(y))} \rho_B^y]$ .

On the other hand,

$$\text{Tr}[T\Lambda(\tau_X \otimes \sigma_B)] = \sum_y \frac{1}{|\mathcal{X}|} \text{Tr}[\Pi_y^{(\mathcal{E}(y))} \sigma_B] = \frac{1}{|\mathcal{X}|} \sum_{w \in \mathcal{W}} \sum_{y \in \mathcal{X}: \mathcal{E}(y)=w} \text{Tr}[\Pi_y^{(\mathcal{E}(y))} \sigma_B]. \quad (7.20)$$

Since

$$\sum_{y \in \mathcal{X}: \mathcal{E}(y)=w} \text{Tr}[\Pi_y^{(\mathcal{E}(y))} \sigma_B] \leq \sum_{y \in \mathcal{X}} \text{Tr}[\Pi_y^{(w)} \sigma_B] = \text{Tr}[\sigma_B] = 1, \quad (7.21)$$

we have

$$\text{Tr}[T\Lambda(\tau_X \otimes \sigma_B)] \leq \frac{M}{|\mathcal{X}|}. \quad (7.22)$$

That is, this test achieves type II error of  $\frac{M}{|\mathcal{X}|}$ . As the infimum over all such tests, we have that

$$1 - \sum_y p(y) \text{Tr}[\Pi_y^{(\mathcal{E}(y))} \rho_B^y] \geq \hat{\alpha}_{\frac{|\mathcal{W}|}{|\mathcal{X}|}}(\Lambda(\rho_{XB}) \| \Lambda(\tau_X \otimes \sigma_B)) \geq \hat{\alpha}_{\frac{|\mathcal{W}|}{|\mathcal{X}|}}(\rho_{XB} \| \tau_X \otimes \sigma_B) \quad (7.23)$$

where the second inequality is by (7.16). Then taking the infimum over  $\mathcal{E}$  and  $\mathcal{D}$ ,

$$\hat{\alpha}_{\frac{M}{|\mathcal{X}|}}(\rho_{XB} \| \tau_X \otimes \sigma_B) \leq \varepsilon^*(1, \log |\mathcal{W}|). \quad (7.24)$$

Thus,

$$-\log \varepsilon^*(1, \log M) \leq -\log \hat{\alpha}_{\frac{|\mathcal{W}|}{|\mathcal{X}|}}(\rho_{XB} \| \tau_X \otimes \sigma_B). \quad (7.25)$$

Since this holds independently of  $\sigma_B \in \mathcal{S}(B)$ , we may minimize over  $\sigma_B$  to find

$$-\log \varepsilon^*(1, \log M) \leq \min_{\sigma_B \in \mathcal{S}(B)} -\log \hat{\alpha}_{\frac{M}{|\mathcal{X}|}}(\rho_{XB} \| \tau_X \otimes \sigma_B),$$

which complete our claim.  $\square$

## 7.2 Proof of Main Result, Theorem 7.1

*Proof of Theorem 7.1.* The proof is split into two parts. We first invoke an one-shot converse bound in Proposition 7.1 to relate the optimal error of Slepian-Wolf coding to a binary hypothesis testing problem. Second, we employ a sharp converse Hoeffding bound in Theorem 4.3 to asymptotically expand the optimal type-I error, which yields the desired result in Eq. (7.1).

Applying Proposition 7.1 with an  $n$ -shot extension  $\rho_{X^n B^n}$  of the c-q state  $\rho_{XB}$ ,  $|\mathcal{W}| = \exp\{nR\}$ , and  $\tau_{X^n} = \frac{1}{|X^n|} \mathbb{1}_{X^n}$  gives

$$\log \left( \frac{1}{\varepsilon^*(n, R)} \right) \leq \min_{\sigma_B^n \in \mathcal{S}(B^n)} -\log \hat{\alpha}_{\frac{|\mathcal{W}|}{|X^n|}}(\rho_{X^n B^n} \| \tau_{X^n} \otimes \sigma_B^n) \quad (7.26)$$

$$\leq -\log \hat{\alpha}_{\frac{|\mathcal{W}|}{|X^n|}}(\rho_{X^n B^n} \| \tau_{X^n} \otimes (\sigma_B^\star)^{\otimes n}), \quad (7.27)$$

$$= -\log \hat{\alpha}_{\frac{|\mathcal{W}|}{|X^n|}}(\rho_{XB}^{\otimes n} \| (\tau_X \otimes \sigma_B^\star)^{\otimes n}), \quad (7.28)$$

where we invoke the saddle-point property in Proposition 5.3-(b) to denote by

$$\sigma_R^\star := \arg \min_{\sigma_B \in \mathcal{S}(B)} \sup_{\alpha \in [0, 1]} \frac{1 - \alpha}{\alpha} (R + D_\alpha(\rho_{XB} \| \mathbb{1}_X \otimes \sigma_B)). \quad (7.29)$$

Next, we show that the exponent  $\phi_n > 0$ , and thus we can exploit Theorem 4.3 to expand the right-hand side of Eq. (7.28). Let  $r = \log |\mathcal{X}| - R$ , and note that item (c) in Proposition 5.3 implies

$$\rho_{XB} \ll U_X \otimes \sigma_R^\star. \quad (7.30)$$

One can verify that

$$\phi_n(r|\rho_{XB}^{\otimes n}\| (U_X \otimes \sigma_R^*)^{\otimes n}) = \sup_{\alpha \in (0,1]} \frac{1-\alpha}{\alpha} (D_\alpha(\rho_{XB}\|U_X \otimes \sigma_R^*) - r) \quad (7.31)$$

$$= \sup_{\alpha \in (0,1]} \frac{1-\alpha}{\alpha} (D_\alpha(\rho_{XB}\|\mathbb{1}_X \otimes \sigma_R^*) - \log |\mathcal{X}| - r) \quad (7.32)$$

$$= E_{\text{sp}}(R) \quad (7.33)$$

$$> 0, \quad (7.34)$$

where  $\phi_n$  is defined in Eq. (2.27); equality (7.33) follows from the saddle-point property, item (b) in Proposition 5.3, and the definition of  $E_{\text{sp}}(R)$  in Eq. (5.2); the last inequality (7.34) is due to item (a) in Proposition 5.3 and the given range of  $R$ . Further, the positivity of  $\phi_n(r|\rho_{XB}^{\otimes n}\|(\tau_X \otimes \sigma_R^*)^{\otimes n})$  implies that  $r > D_0(\rho_{XB}\|\tau_X \otimes \sigma_R^*)$ . By choosing  $\varepsilon = r - D_0(\rho_{XB}\|\tau_X \otimes \sigma_R^*) > 0$ ,  $\rho = \rho_{XB}$  and  $\sigma = \tau_X \otimes \sigma_R^*$ , Eq. (7.31) guarantees the positivity of  $\phi_n$ . Hence, we apply Theorem 4.3 on Eq. (7.28) to obtain

$$\begin{aligned} & \log \left( \frac{1}{\varepsilon^*(n, R)} \right) \\ & \leq n \phi_n(r|\rho_{XB}^{\otimes n}\|(\tau_X \otimes \sigma_R^*)^{\otimes n}) + \frac{1}{2} \left( 1 + \left| \frac{\partial \phi_n(\tilde{r}|\rho_{XB}^{\otimes n}\|(\tau_X \otimes \sigma_R^*)^{\otimes n})}{\partial \tilde{r}} \right|_{\tilde{r}=r} \right) \log n + K, \end{aligned} \quad (7.35)$$

where  $K > 0$  is some finite constant independent of  $n$ . Finally, combining Eqs. (7.33) and (7.35) completes the proof.  $\square$

## Chapter 8

# Moderate Deviation Analysis (Source Coding)

In this chapter, we provide the moderate deviation analysis for Slepian-Wolf coding with QSI. As we have shown in Chapters 6 and 7, the optimal probability of error exponentially decay to zero as the compression rate is above the Slepian-Wolf limit  $H(X|B)_\rho$ . In Theorem 8.1 below, we consider the scenario that the compression rate approaches  $H(X|B)_\rho$  from above at a speed  $a_n$ , which satisfies

$$\begin{aligned} \text{(i)} \quad & \lim_{n \rightarrow +\infty} a_n = 0; \\ \text{(ii)} \quad & \lim_{n \rightarrow +\infty} a_n \sqrt{n} = +\infty. \end{aligned} \tag{8.1}$$

Then, the optimal probability of error still goes to zero asymptotically.

**Theorem 8.1** (Moderate deviations for the error). *theomodlarge Consider a Slepian-Wolf coding with a joint classical-quantum state  $\rho_{XB} \in \mathcal{S}(XB)$  and  $V(X|B)_\rho > 0$ . For any sequence  $(a_n)_{n \in \mathbb{N}}$  satisfying Eq. (1.7),*

$$\lim_{n \rightarrow +\infty} \frac{1}{na_n^2} \log \varepsilon^*(n, H(X|B)_\rho + a_n) = -\frac{1}{2V(X|B)_\rho}, \tag{8.2}$$

where the conditional information variance is defined by  $V(X|B)_\rho := V(\rho_{XB} \| \mathbf{1}_X \otimes \rho_B)$  and  $V(\rho \| \sigma) := \text{Tr}[\rho (\log \rho - \log \sigma)^2] - D(\rho \| \sigma)^2$ .

*Proof of Theorem 8.1.* We shorthand  $H = H(X|B)_\rho$ ,  $V = V(X|B)_\rho$  for notational convenience. We first show the achievability, i.e. the “ $\geq$ ” in Eq. (8.2). Let  $\{a_n\}_{n \geq 1}$  be any sequence of real numbers satisfying Eq. (8.1). For every  $n \in \mathbb{N}$ , Theorem 6.1 implies that there exists a sequence of  $n$ -block codes with rates  $R_n = H + a_n$  such that

$$\varepsilon^*(n, R_n) \leq 4 \exp \left\{ -n \left[ \max_{0 \leq s \leq 1} \left\{ E_0^\downarrow(s) + sR_n \right\} \right] \right\}. \tag{8.3}$$

Applying Taylor's theorem to  $E_0^\downarrow(s)$  at  $s = 0$  together with Proposition 5.2 gives

$$E_0^\downarrow(s) = -sH - \frac{s^2}{2}V + \frac{s^3}{6} \frac{\partial^3 E_0^\downarrow(s)}{\partial s^3} \Bigg|_{s=\bar{s}}, \tag{8.4}$$

for some  $\bar{s} \in [0, s]$ . Now, let  $s_n = a_n/V$ . Then,  $s_n \leq 1$  for all sufficiently large  $n$  by the assumption in Eq. (8.1) and  $V > 0$ . For all  $s_n \leq 1$ , Eq. (8.4) yields

$$\max_{0 \leq s \leq 1} \left\{ E_0^\downarrow(s) + sR_n \right\} \geq E_0^\downarrow(s_n) + s_n R_n \quad (8.5)$$

$$= \frac{a_n}{V} (-H + R_n) - \frac{a_n^2}{2V} + \frac{a_n^3}{6V^3} \left. \frac{\partial^3 E_0^\downarrow(s)}{\partial s^3} \right|_{s=\bar{s}_n} \quad (8.6)$$

$$= \frac{a_n^2}{2V} + \frac{a_n^3}{6V^3} \left. \frac{\partial^3 E_0^\downarrow(s)}{\partial s^3} \right|_{s=\bar{s}_n} \quad (8.7)$$

$$\geq \frac{a_n^2}{2V} - \frac{a_n^3}{6V^3} \left| \frac{\partial^3 E_0^\downarrow(s)}{\partial s^3} \right|_{s=\bar{s}_n} \quad (8.8)$$

$$\geq \frac{a_n^2}{2V} - \frac{a_n^3}{6V^3} \Upsilon, \quad (8.9)$$

where  $\bar{s}_n \in [0, s_n]$ ; Eq. (8.7) holds since  $R_n = H + a_n$ ; we denote by

$$\Upsilon = \max_{s \in [0, 1]} \left| \frac{\partial^3 E_0^\downarrow(s)}{\partial s^3} \right|. \quad (8.10)$$

This quantity is finite due to the compact set  $[0, 1]$  and the continuity, item (a) in Proposition 5.2. Therefore, substituting Eq. (8.9) into Eq. (8.3) gives for all sufficiently large  $n \in \mathbb{N}$ ,

$$\frac{1}{na_n^2} \log \left( \frac{1}{\varepsilon^*(n, R_n)} \right) \geq -\frac{\log 4}{na_n^2} + \frac{1}{2V} \left( 1 - \Upsilon \frac{a_n}{3V^2} \right). \quad (8.11)$$

Recall Eq. (1.7) and let  $n \rightarrow +\infty$ , which completes the achievability:

$$\liminf_{n \rightarrow +\infty} \frac{1}{na_n^2} \log \left( \frac{1}{\varepsilon^*(n, R_n)} \right) \geq \frac{1}{2V}. \quad (8.12)$$

We move on to show the converse, i.e. the " $\leq$ " in Eq. (8.2). Let  $N_1 \in \mathbb{N}$  be an integer such that  $R_n = H + a_n \in (H_1(X|B)_\rho, H_0(X|B)_\rho)$  for all  $n \in N_1$ . Invoke the one-shot converse bound, Proposition 7.1, with  $M = \exp\{nR_n\}$  to obtain for all  $n \geq N_1$ ,

$$\log \left( \frac{1}{\varepsilon^*(n, R_n)} \right) \leq \min_{\sigma_B^n \in \mathcal{S}(B^n)} -\log \widehat{\alpha}_{\frac{M}{|\mathcal{X}^n|}} (\rho_{X^n B^n} \| \tau_{X^n} \otimes \sigma_B^n) \quad (8.13)$$

$$\leq -\log \widehat{\alpha}_{\frac{M}{|\mathcal{X}^n|}} (\rho_{X^n B^n} \| \tau_{X^n} \otimes (\sigma_{R_n}^*)^{\otimes n}) \quad (8.14)$$

$$= -\log \widehat{\alpha}_{\frac{M}{|\mathcal{X}^n|}} (\rho_{X B}^{\otimes n} \| (\tau_X \otimes \sigma_{R_n}^*)^{\otimes n}), \quad (8.15)$$

where we denote by  $(\alpha_{R_n}^*, \sigma_{R_n}^*)$  the unique saddle-point of  $\frac{1-\alpha}{\alpha} (R_n - H_\alpha^\uparrow(X|B)_\rho)$ .

Next, we verify that we are able to employ Theorem 4.4 to asymptotically expand Eq. (8.15). Equation (8.27) in Proposition 8.1 below shows that  $\lim_{n \rightarrow +\infty} \alpha_{R_n} = 1$ . This together with the closed-

form expression of  $\sigma_{R_n}^*$  [134], [128, Lemma 1], [10, Lemma 5.1] shows that

$$\lim_{n \rightarrow +\infty} \sigma_{R_n}^* = \lim_{n \rightarrow +\infty} \frac{\left( \text{Tr}_X \left[ \rho_{XB}^{\alpha_{R_n}^*} \right] \right)^{\frac{1}{\alpha_{R_n}^*}}}{\text{Tr} \left[ \left( \text{Tr}_X \left[ \rho_{XB}^{\alpha_{R_n}^*} \right] \right)^{\frac{1}{\alpha_{R_n}^*}} \right]} = \rho_B. \quad (8.16)$$

Since  $V = V(\rho \| \mathbb{1}_X \otimes \rho_B) > 0$ , by the continuity of  $V(\cdot \| \cdot)$  (c.f. (3.34)), for every  $\kappa \in (0, 1)$  there exists  $N_2 \in \mathbb{N}$  such that for all  $n \geq N_2$ ,

$$V(\rho_{XB} \| \tau_X \otimes \sigma_{R_n}^*) = V(\rho_{XB} \| \mathbb{1}_X \otimes \sigma_{R_n}^*) \geq (1 - \kappa)V =: \nu > 0. \quad (8.17)$$

Hence, we apply Theorem 4.4 with  $r_n = \log |\mathcal{X}| - R_n$ ,  $\rho = \rho_{XB}$  and  $\sigma = \tau_X \otimes \sigma_{R_n}^*$  to obtain for all  $n \geq \max\{N_1, N_2\}$ ,

$$-\log \widehat{\alpha}_{\exp\{-nr_n\}}(\rho^{\otimes n} \| \sigma^{\otimes n}) \leq n \sup_{\alpha \in (0, 1]} \frac{1 - \alpha}{\alpha} (D_\alpha(\rho \| \sigma) - r_n + \gamma_n) + \log(s_n^* \sqrt{n}) + K, \quad (8.18)$$

$$= nE_{\text{sp}}(H + a_n + \gamma_n) + \log(s_n^* \sqrt{n}) + K, \quad (8.19)$$

for some constant  $K > 0$ , and  $s_n^* := (1 - \alpha_{R_n}^*)/\alpha_{R_n}^*$ . Now, let  $\delta_n := a_n + \gamma_n$ , and notice that  $\gamma_n = O(\frac{\log n}{n}) = o(a_n)$ . We invoke Proposition 8.1 below to have

$$\limsup_{n \rightarrow +\infty} \frac{E_{\text{sp}}(H(X|B)_\rho + \delta_n)}{a_n^2} = \limsup_{n \rightarrow +\infty} \frac{E_{\text{sp}}(H(X|B)_\rho + \delta_n)}{\delta_n^2} \leq \frac{1}{2V}. \quad (8.20)$$

Moreover, Eq. (8.27) in Proposition 8.1 gives that  $\lim_{n \rightarrow +\infty} \frac{s_n^*}{\delta_n} = 1/V$ . Combining Eqs. (1.7), (8.15), (8.19) and (8.20) to conclude our claim

$$\limsup_{n \rightarrow +\infty} \frac{1}{na_n^2} \log \left( \frac{1}{\varepsilon^*(n, R_n)} \right) \leq \limsup_{n \rightarrow +\infty} -\frac{\log \widehat{\alpha}_{\exp\{-nr_n\}}(\rho^{\otimes n} \| \sigma^{\otimes n})}{na_n^2} \quad (8.21)$$

$$\leq \frac{1}{2V} + \limsup_{n \rightarrow +\infty} \frac{\log(s_n^* \sqrt{n})}{na_n^2} \quad (8.22)$$

$$= \frac{1}{2V} + \limsup_{n \rightarrow +\infty} \frac{\log(s_n^* \sqrt{n})}{n\delta_n^2} \quad (8.23)$$

$$= \frac{1}{2V} + \limsup_{n \rightarrow +\infty} \frac{\frac{1}{2} \log(n\delta_n^2) - \log V}{n\delta_n^2} \quad (8.24)$$

$$= \frac{1}{2V}, \quad (8.25)$$

where the last line follows from  $\lim_{n \rightarrow +\infty} n\delta_n^2 = +\infty$ . Hence, Eq (8.12) together with Eq. (8.25) completes the proof.

**Proposition 8.1** (Error Exponent around Slepian-Wolf Limit). *Let  $(\delta_n)_{n \in \mathbb{N}}$  be a sequence of positive numbers with  $\lim_{n \rightarrow +\infty} \delta_n = 0$ . The following hold:*

$$\limsup_{n \rightarrow +\infty} \frac{E_{\text{sp}}(H(X|B)_\rho + \delta_n)}{\delta_n^2} \leq \frac{1}{2V(X|B)_\rho}; \quad (8.26)$$

$$\limsup_{n \rightarrow +\infty} \frac{s_n^*}{\delta_n} = \frac{1}{V(X|B)_\rho}, \quad (8.27)$$

where

$$s_n^* := \arg \max_{s \geq 0} \left\{ s(H(X|B)_\rho + \delta_n) - sH_{\frac{1}{1+s}}^\uparrow(X|B)_\rho \right\}. \quad (8.28)$$

The proof of Proposition 8.1 is provided in Section 8.1.

□

## 8.1 Asymptotic Expansion of Error Exponent around Slepian-Wolf Limit

*Proof of Proposition 8.1.* For notational convenience, we denote by  $H := H(X|B)_\rho$ ,  $V := V(X|B)_\rho$ . Thus,

$$E_{\text{sp}}(R) = \sup_{s \geq 0} \{sR + E_0(s)\}, \quad (8.29)$$

$$(8.30)$$

Let a *critical rate* to be

$$r_{\text{cr}} := \left. \frac{\partial E_0(s)}{\partial s} \right|_{s=1}. \quad (8.31)$$

Let  $N_0$  be the smallest integer such that  $H(X|B)_\rho + \delta_n < r_{\text{cr}}$ , for all  $n \geq N_0$ . Since the map  $r \mapsto E_{\text{sp}}(r)$  is non-increasing by item (a) in Proposition 5.3, the maximization over  $s$  in Eq. (8.29) can be restricted to the set  $[0, 1]$  for any rate below  $r_{\text{cr}}$ , i.e.,

$$E_{\text{sp}}(H + \delta_n) = \max_{0 \leq s \leq 1} \{s(H + \delta_n) + E_0(s)\}. \quad (8.32)$$

For every  $n \in \mathbb{N}$ , let  $s_n^*$  attain the maxima in Eq. (8.32) at a rate of  $H + \delta_n$ . It is not hard to observe that  $s_n^* > 0$  for all  $n \geq N_0$  since  $s_n^* = 0$  if and only if  $H + \delta_n < H$ , which violates the assumption of  $\delta_n > 0$  for finite  $n$ . Now, we will show Eq. (8.27) and

$$\lim_{n \rightarrow +\infty} s_n^* = 0. \quad (8.33)$$

Let  $(s_{n_k}^*)_{k \in \mathbb{N}}$  be arbitrary subsequences. Since  $[0, 1]$  are compact, we may assume that

$$\lim_{k \rightarrow \infty} s_{n_k}^* = s_o, \quad (8.34)$$

for some  $s_o \in [0, 1]$ .

Since  $s \mapsto E_0(s)$  is strictly concave from item (c) in Proposition 5.1, the maximizer  $s_n^*$  must satisfy

$$\frac{\partial E_0(s)}{\partial s} \Big|_{s=s_{n_k}^*} = -(H + \delta_{n_k}), \quad (8.35)$$

which together with item (a) in Proposition 5.1 implies

$$\lim_{k \rightarrow +\infty} \frac{\partial E_0(s)}{\partial s} \Big|_{s=s_{n_k}^*} = \frac{\partial E_0(s)}{\partial s} \Big|_{s=s_o} = -H. \quad (8.36)$$

On the other hand, item (d) in Proposition 5.1 gives

$$\frac{\partial E_0(s)}{\partial s} \Big|_{s=0} = -H. \quad (8.37)$$

Since item (d) in Proposition 5.1 guarantees

$$\frac{\partial^2 E_0(s)}{\partial s^2} \Big|_{s=0} = -V < 0, \quad (8.38)$$

which implies that the first-order derivative  $\partial E_0(s)/\partial s$  is strictly decreasing around  $s = 0$ . Hence, we conclude  $s_o = 0$ . Because the subsequence is arbitrary, Eq. (8.34) is shown.

Next, from Eqs. (8.35) and Eqs. (8.37), the mean value theorem states that there exists a number  $\hat{s}_{n_k} \in (0, s_{n_k}^*)$ , for each  $k \in \mathbb{N}$ , such that

$$-\frac{\partial^2 E_0(s)}{\partial s^2} \Big|_{s=\hat{s}_{n_k}} = \frac{-H + (H + \delta_{n_k})}{s_{n_k}^*} = \frac{\delta_{n_k}}{s_{n_k}^*}. \quad (8.39)$$

When  $k$  approaches infinity, items (a) and (e) in Proposition 5.1 give

$$\lim_{k \rightarrow +\infty} \frac{\partial^2 E_0(s)}{\partial s^2} \Big|_{s=\hat{s}_{n_k}} = \frac{\partial^2 E_0(s)}{\partial s^2} \Big|_{s=0} = -V. \quad (8.40)$$

Combining Eqs. (8.39) and (8.40) leads to

$$\lim_{k \rightarrow +\infty} \frac{s_{n_k}^*}{\delta_{n_k}} = \frac{1}{V}. \quad (8.41)$$

Since the subsequence was arbitrary, the above result establishes Eq. (8.27).

Finally, denote by

$$\Upsilon = \max_{s \in [0, 1]} \left| \frac{\partial^3 E_0(s)}{\partial s^3} \right| < +\infty. \quad (8.42)$$

For every sufficiently large  $n \geq N_0$ , we apply Taylor's theorem to the map  $s_n^* \mapsto E_0(s_n^*)$  at the original

point to obtain

$$E_{\text{sp}}(H + \delta_n) = s_n^*(H + \delta_n) + E_0(s_n^*) \quad (8.43)$$

$$= s_n^*\delta_n - \frac{(s_n^*)^2}{2}V + \frac{(s_n^*)^3}{6} \left. \frac{\partial^3 E_0(s, P_n)}{\partial s^3} \right|_{s=\bar{s}_n} \quad (8.44)$$

$$\leq s_n^*(H + \delta_n - H) - \frac{(s_n^*)^2}{2}V + \frac{(s_n^*)^3\Upsilon}{6} \quad (8.45)$$

$$\leq \sup_{s \geq 0} \left\{ s\delta_n - \frac{s^2}{2}V \right\} + \frac{(s_n^*)^3\Upsilon}{6} \quad (8.46)$$

$$= \frac{\delta_n^2}{2V} + \frac{(s_n^*)^3\Upsilon}{6}, \quad (8.47)$$

where  $\bar{s}_n$  is some number in  $[0, s_n^*]$ . Then, Eqs. (8.27), (8.34), (8.47), and the assumption  $\lim_{n \rightarrow +\infty} \delta_n = 0$  imply that the desired inequality

$$\limsup_{n \rightarrow +\infty} \frac{E_{\text{sp}}(H + \delta_n)}{\delta_n^2} \leq \frac{1}{2V}. \quad (8.48)$$

□

# Part III

## Classical Information Transmission over a Quantum Channel

## Chapter 9

# Error Exponent Functions (Channel Coding)

In this chapter, we introduce the auxiliary functions and the exponent functions for classical-quantum channel coding. Section 9.1 presents a variational representation for the entropic exponent defined via the log-Euclidean Rényi divergence  $D^b$ . Sections 9.2 and 9.3 provide major properties of the auxiliary functions and the introduced entropic exponent functions, respectively.

We defined the following exponents in terms of the Rényi and Augustin information defined in Section 3.3. For  $(t) \in \{\} \cup \{b\}$ , and  $R \geq 0$ , we define the following *auxiliary functions* [35, 2, 36, 59]

$$E_0^{(i),(t)}(s, P) := s I_{\frac{1}{1+s}}^{(i)}(P, \mathcal{W}) \quad i = \{1, 2\}, \quad (9.1)$$

and the *entropic exponent functions*:

$$E_r^{(i),(t)}(R, P) := \sup_{s \in [0, 1]} \left\{ E_0^{(i),(t)}(s, P) - sR \right\}, \quad (9.2)$$

$$E_{sp}^{(i),(t)}(R, P) := \sup_{s \geq 0} \left\{ E_0^{(i),(t)}(s, P) - sR \right\}. \quad (9.3)$$

In classical channel coding [30, 23, 135, 136, 27] and as will be shown later in Sections 10.1 and 10.2, the quantity with respective to ‘(1)’ can be connected to the codes i.i.d. ensemble, while ‘(2)’ corresponds to the constant composition codes.

By quantum Sibson’s identity given in Lemma 3.3, the auxiliary function  $E_0^{(1)}(s, P)$  of Petz’s version has a closed form expression and coincides the quantity introduced by Burnashev and Holevo [35, 2]:

$$E_0^{(1)}(s, P) = E_0(s, P) := -\log \text{Tr} \left[ \left( \sum_{x \in \mathcal{X}} P(x) \cdot W_x^{1/(1+s)} \right)^{1+s} \right]. \quad (9.4)$$

Proposition 3.2 and Eq. (3.42) imply that the two quantities of ‘(1)’ and ‘(2)’ are equal after

maximizing over the input distributions:

$$E_r^{(t)}(R) := \max_{P \in \mathcal{P}(\mathcal{X})} E_r^{(1),t}(R, P) = \max_{P \in \mathcal{P}(\mathcal{X})} E_r^{(2),t}(R, P), \quad (9.5)$$

$$E_{\text{sp}}^{(t)}(R) := \max_{P \in \mathcal{P}(\mathcal{X})} E_{\text{sp}}^{(1),t}(R, P) = \max_{P \in \mathcal{P}(\mathcal{X})} E_{\text{sp}}^{(2),t}(R, P). \quad (9.6)$$

Here,  $E_r^{(t)}(R)$  is called the *random coding exponent*, and  $E_{\text{sp}}^{(t)}(R)$  is the *sphere-packing exponent*.

In the following, we will require other variants of the above auxiliary function:  $\forall s \geq 0$  and  $\sigma \in \mathcal{S}(\mathcal{H})$ ,

$$E_0^{(1),\downarrow}(s, P, \sigma) := sD_{1-s}(P \circ \mathcal{W} \| P \otimes \sigma), \quad (9.7)$$

$$E_0^{(2),\downarrow}(s, P, \sigma) := sD_{1-s}(\mathcal{W} \| \sigma | P), \quad (9.8)$$

$$E_h(s, P, \sigma) := sD_{\frac{1}{1+s}}(\mathcal{W} \| \sigma | P), \quad (9.9)$$

$$E_h^{\flat}(s, P, \sigma) := sD_{\frac{1}{1+s}}^{\flat}(\mathcal{W} \| \sigma | P). \quad (9.10)$$

With this, we define another version fo the random coding exponent:

$$E_r^{(i),\downarrow}(R, P) := \sup_{0 \leq s \leq 1} \left\{ E_0^{(i),\downarrow}(s, P, P\mathcal{W}) - sR \right\}, \quad i \in \{1, 2\}. \quad (9.11)$$

This quantity will appear in the achievability (see Theorem 12.1 in Chapter 10), and Chapter 12.

We also define an sphere-packing exponents introduced by Haroutunian [32, 26], Blahut [33, 33], Csiszár-Körner [136, 27] in classical case, and by Winter [37] in the quantum case:

$$\tilde{E}_{\text{sp}}(R) := \max_{P \in \mathcal{P}(\mathcal{X})} \tilde{E}_{\text{sp}}(R, P), \quad (9.12)$$

where

$$\tilde{E}_{\text{sp}}(R, P) := \min_{\mathcal{V}: \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})} \{ D(\mathcal{V} \| \mathcal{W} | P) : I(P, \mathcal{V}) \leq R \}. \quad (9.13)$$

In the classical case,  $\tilde{E}_{\text{sp}}(R, P)$  is exactly the same as the exponent defined via Augustin information (9.3) [34, 27]. However, it is more involved in the quantum case [137]. In Theorem 5.1 of Section 9.1, we will show that

$$\tilde{E}_{\text{sp}}(R, P) = E_{\text{sp}}^{(2),\flat}(R, P). \quad (9.14)$$

To compare the above sphere-packing exponents, Jensen's inequality and Lemma (e) imply that

$$E_{\text{sp}}^{(1)}(R, P) \leq E_{\text{sp}}^{(2)}(R, P) \leq E_{\text{sp}}^{(2),\flat}(R, P) = \tilde{E}_{\text{sp}}(R, P). \quad (9.15)$$

In Section 11.2, we show a sphere-packing bound in terms of  $\tilde{E}_{\text{sp}}(R, P)$  via the dummy channel method; in Section 11.3, we prove a sphere-packing bound in terms of  $E_{\text{sp}}^{(2)}(R, P)$  for constant composition codes and  $E_{\text{sp}}(R)$  for general codes. It is generally believed that the Petz's version,  $E_{\text{sp}}(R)$ , is the optimal exponent for c-q channel coding. Hence, the exponent defined via the log-Euclidean Rényi divergence,  $D_{\alpha}^{\flat}$ , is weaker.

Similarly, [138], [128], [10, Corollary 5.3] give the relations between the random coding exponents:

$$E_r^{(1),\downarrow}(R, P) \leq E_r^{(2),\downarrow}(R, P) \wedge E_r^{(1)}(R, P) \leq E_r^{(2),\downarrow}(R, P) \vee E_r^{(1)}(R, P) \leq E_r^{(2)}(R, P) \leq E_r^{(2),\flat}(R, P). \quad (9.16)$$

The best existing achievability bound was proved by Hayashi [94] and Dalai [139] with  $E_r^{(1),\downarrow}(R, P)$  (see Section 10.1). In Section 10.2, we establish a tighter bound with  $E_r^{(2),\downarrow}(R, P)$ . As mentioned above, the Petz's version is conjectured to be the optimal error exponent at least for the hight rate regime ( $C_{1/2,W} \leq R \leq C_{1,W}$ ). Thus, we believe that the quantity  $E_r^{(2),\flat}(R, P)$  is too strong to hold for the achievability in c-q channel coding.

Lastly, we define

$$\tilde{E}_{\text{sp}}(R, P, \sigma) := \min_{\bar{\mathcal{W}}: \mathcal{X} \rightarrow \mathcal{S}_0} \{D(\bar{\mathcal{W}}\|\mathcal{W}|P) : D(\bar{\mathcal{W}}\|\sigma|P) \leq R\} \quad (9.17)$$

for all  $R > 0$ ,  $P \in \mathcal{P}(\mathcal{X})$ , and  $\sigma \in \mathcal{S}_{>0}(\mathcal{H})$ . From the definitions in Eq. (9.17), it is not hard to see that [92]

$$\tilde{E}_{\text{sp}}(R, P, \sigma) = 0, \quad \forall R \geq D(\mathcal{W}\|\sigma|P). \quad (9.18)$$

and

$$E_{\text{sp}}^{(2)}(R, P, \sigma) = \begin{cases} +\infty, & R < D_0(\mathcal{W}\|\sigma|P), \\ 0, & R \geq D(\mathcal{W}\|\sigma|P). \end{cases} \quad (9.19)$$

As we will show in Chapter 11, the quantity  $E_{\text{sp}}^{(2)}(R, P)$  plays a significant role in the connection between hypothesis testing and channel coding. Moreover, Proposition 9.5 in Section 9.3 below shows that the the minimizer in  $I_\alpha^{(2)}$  given in Eq. (3.40) and the maximizer in Eq. (9.3) forms a saddle-point.

Further, we define [27, p. 152], [38, Theorem 6]:

$$R_\infty := C_{0,W}. \quad (9.20)$$

From the definitions in Eqs. (3.33) and (9.20), it can be verified that  $R_\infty \leq C_W$  for all c-q channels  $\mathcal{W}$ . In Proposition 9.6 below, one has  $E_{\text{sp}}(R) = +\infty$  for  $R < R_\infty$ , and  $E_{\text{sp}}(R) = 0$  as  $R > C_W$ . Throughout this paper, we further assume that the considered c-q channel  $\mathcal{W}$  satisfies  $R_\infty < C_W$ .

## 9.1 Variational Representations

This section derives alternative formulations of the sphere-packing exponents of  $\tilde{E}_{\text{sp}}(R, P)$  and  $E_{\text{sp}}^{\flat}(R, P)$ , and provides a relation between these two exponents. As we will show later,  $\tilde{E}_{\text{sp}}(R, P)$  is an expression in the primal domain of an optimization problem, while  $E_{\text{sp}}^{\flat}(R, P)$  is in the dual domain.

We first consider the following convex optimization problem and then exploit it to establish variational formulations of the sphere-packing exponents. Let  $\rho, \tau \in \mathcal{S}(\mathcal{H})$  be two density operators.

Consider the following convex optimization problem:

$$(P) \quad e(r) := \inf_{\sigma \in \mathcal{S}(\mathcal{H})} D(\sigma \| \rho), \quad (9.21)$$

subject to  $D(\sigma \| \tau) \leq r.$

The above primal problem is interpreted as finding the optimal operator  $\sigma^*$  that achieves the minimum relative entropy  $e(r)$  to  $\rho$ , within  $r$ -radius to  $\tau$ . The following result shows the dual representation of problem (P) via Lagrangian duality.

**Lemma 9.1** ([99, Section 3.7], [120], [59, Theorem 3.6]). *The dual problem of (P) is given by*

$$(D) \quad \sup_{s \geq 0} \left\{ -(1+s) \log Q_{\frac{1}{1+s}}^\flat(\rho \| \tau) - sr \right\}. \quad (9.22)$$

*Proof.* By the method of Lagrange multipliers, the primal problem in Eq. (9.21) can be rewritten as

$$\sup_{s \geq 0} \inf_{\sigma \in \mathcal{S}(\mathcal{H})} \{D(\sigma \| \rho) + s(D(\sigma \| \tau) - r)\} \quad (9.23)$$

$$= \sup_{s \geq 0} \left\{ (1+s) \inf_{\sigma \in \mathcal{S}(\mathcal{H})} \left\{ \frac{1}{1+s} D(\sigma \| \rho) + \frac{s}{1+s} D(\sigma \| \tau) \right\} - sr \right\} \quad (9.24)$$

$$= \sup_{s \geq 0} \left\{ -(1+s) \log Q_{\frac{1}{1+s}}^\flat(\rho \| \tau) - sr \right\}, \quad (9.25)$$

where the last equality follows from Lemma 3.1.  $\square$

**Theorem 9.1** (Variational Representations of the Sphere-Packing Exponents). *Let  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  be a classical-quantum channel. For any  $R > R_\infty$ , we have*

$$\tilde{E}_{\text{sp}}(R, P) = \sup_{0 < \alpha \leq 1} \min_{\sigma \in \mathcal{S}(\mathcal{H})} \left\{ \frac{1-\alpha}{\alpha} (D_\alpha^\flat(\mathcal{W} \| \sigma | P) - R) \right\}, \quad \text{and} \quad (9.26)$$

$$E_{\text{sp}}(R, P) \leq \sup_{0 < \alpha \leq 1} \min_{\sigma \in \mathcal{S}(\mathcal{H})} \left\{ \frac{1-\alpha}{\alpha} (D_\alpha(\mathcal{W} \| \sigma | P) - R) \right\}, \quad (9.27)$$

where  $\tilde{E}_{\text{sp}}(R, P)$  and  $E_{\text{sp}}(R, P) := E_{\text{sp}}^{(1)}(R, P)$  are defined in Eqs. (9.17) and (9.3), respectively.

Moreover, equality in Eq. (9.27) is attained when maximizing over all prior distributions, i.e.,

$$E_{\text{sp}}(R) = \max_{P \in \mathcal{P}(\mathcal{X})} E_{\text{sp}}(R, P) = \max_{P \in \mathcal{P}(\mathcal{X})} \sup_{0 < \alpha \leq 1} \min_{\sigma \in \mathcal{S}(\mathcal{H})} \left\{ \frac{1-\alpha}{\alpha} (D_\alpha(\mathcal{W} \| \sigma | P) - R) \right\}. \quad (9.28)$$

*Proof.* We start with the proof of Eq. (9.26). Observe that

$$\min_{\sigma \in \mathcal{S}(\mathcal{H})} D(\mathcal{W} \| \sigma | P) = \min_{\sigma \in \mathcal{S}(\mathcal{H})} \sum_{x \in \mathcal{X}} P(x) \text{Tr}[V_x (\log V_x - \log \sigma)] \quad (9.29)$$

$$= I(P, \mathcal{V}). \quad (9.30)$$

We find

$$\tilde{E}_{\text{sp}}(R, P) = \min_{\mathcal{V}: \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})} \{D(\mathcal{V}\|\mathcal{W}|P) : I(P, \mathcal{V}) \leq R\} \quad (9.31)$$

$$= \min_{\mathcal{V}: \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})} \left\{ D(\mathcal{V}\|\mathcal{W}|P) : \min_{\sigma \in \mathcal{S}(\mathcal{H})} D(\mathcal{V}\|\sigma|P) \leq R \right\} \quad (9.32)$$

$$= \sup_{s \geq 0} \min_{\mathcal{V}: \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})} \left\{ D(\mathcal{V}\|\mathcal{W}|P) + s \left( \min_{\sigma \in \mathcal{S}(\mathcal{H})} D(\mathcal{V}\|\sigma|P) - R \right) \right\} \quad (9.33)$$

$$= \sup_{s \geq 0} \min_{\sigma \in \mathcal{S}(\mathcal{H})} \min_{\mathcal{V}: \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})} \left\{ -sR + \sum_{x \in \mathcal{X}} P(x) D(V_x\|W_x) + s \cdot D(V_x\|\sigma) \right\} \quad (9.34)$$

$$= \sup_{s \geq 0} \min_{\sigma \in \mathcal{S}(\mathcal{H})} \left\{ \sum_{x \in \mathcal{X}} P(x) \min_{V_x \in \mathcal{S}(\mathcal{H})} [D(V_x\|W_x) + s \cdot D(V_x\|\sigma) - sR] \right\} \quad (9.35)$$

$$= \min_{\sigma \in \mathcal{S}(\mathcal{H})} \left\{ \sum_{x \in \mathcal{X}} P(x) \min_{V_x \in \mathcal{S}(\mathcal{H})} \{D(V_x\|W_x) : D(V_x\|\sigma) \leq R\} \right\}. \quad (9.36)$$

In Eq. (9.33) we introduced the constraint into the objective function via the Lagrange multiplier  $s \geq 0$ ; and Eq. (9.35) follows from the linearity of the convex combination. By Lemma 9.1, the inner minimum over  $V_x \in \mathcal{S}(\mathcal{H})$  can be represented as its dual problem:

$$\tilde{E}_{\text{sp}}(R, P) = \min_{\sigma \in \mathcal{S}(\mathcal{H})} \sup_{s \geq 0} \left\{ -(1+s) \sum_{x \in \mathcal{X}} P(x) \log \left[ Q_{\frac{1}{1+s}}^{\flat}(W_x\|\sigma) \right] - sR \right\} \quad (9.37)$$

$$= \min_{\sigma \in \mathcal{S}(\mathcal{H})} \sup_{0 < \alpha \leq 1} \left\{ \frac{-\sum_{x \in \mathcal{X}} P(x) \log [Q_{\alpha}^{\flat}(W_x\|\sigma)] - (1-\alpha)R}{\alpha} \right\}, \quad (9.38)$$

where we substitute  $\alpha = 1/(1+s)$ . From Lemma 3.2, the numerator in the bracket of Eq. (9.38) is a concave-convex saddle function for every  $\sigma \in \mathcal{S}(\mathcal{H})$  and every  $\alpha \in (0, 1]$ . Hence, we invoke the minimax theorem, Lemma 9.2 below, to exchange the order of min-sup in Eq. (9.38):

$$\tilde{E}_{\text{sp}}(R, P) = \sup_{0 < \alpha \leq 1} \min_{\sigma \in \mathcal{S}(\mathcal{H})} \left\{ \frac{-\sum_{x \in \mathcal{X}} P(x) \log [Q_{\alpha}^{\flat}(W_x\|\sigma)] - (1-\alpha)R}{\alpha} \right\} \quad (9.39)$$

$$= \sup_{0 < \alpha \leq 1} \min_{\sigma \in \mathcal{S}(\mathcal{H})} \left\{ \frac{1-\alpha}{\alpha} (D_{\alpha}^{\flat}(\mathcal{W}\|\sigma|P) - R) \right\}, \quad (9.40)$$

where in (9.40) we recall the definition of the log-Euclidean  $\alpha$ -Rényi divergence, Eq. (3.6), and hence prove the first claim in Eq. (9.26).

Next, we will prove Eq. (9.27). From Jensen's inequality and the concavity of the logarithm, the

right-hand side of Eq. (9.27) implies that

$$\sup_{0 < \alpha \leq 1} \min_{\sigma \in \mathcal{S}(\mathcal{H})} \left\{ \frac{1-\alpha}{\alpha} \left( \sum_{x \in \mathcal{X}} P(x) D_\alpha(W_x \|\sigma) - R \right) \right\} \quad (9.41)$$

$$= \sup_{0 < \alpha \leq 1} \min_{\sigma \in \mathcal{S}(\mathcal{H})} \left\{ -\frac{1}{\alpha} \sum_{x \in \mathcal{X}} P(x) \log \text{Tr}[W_x^\alpha \sigma^{1-\alpha}] - \frac{1-\alpha}{\alpha} R \right\} \quad (9.42)$$

$$\geq \sup_{0 < \alpha \leq 1} \min_{\sigma \in \mathcal{S}(\mathcal{H})} \left\{ -\frac{1}{\alpha} \log \text{Tr} \left[ \sum_{x \in \mathcal{X}} P(x) [W_x^\alpha \sigma^{1-\alpha}] \right] - \frac{1-\alpha}{\alpha} R \right\} \quad (9.43)$$

$$= E_{\text{sp}}(R, P). \quad (9.44)$$

Finally, Eq. (9.28) follows from the following identity proved by Mosonyi and Ogawa [59, Proposition 4.2]:

$$\max_{P \in \mathcal{P}(\mathcal{X})} \min_{\sigma \in \mathcal{S}(\mathcal{H})} D_\alpha(\mathcal{W} \|\sigma|P) = \max_{P \in \mathcal{P}(\mathcal{X})} \min_{\sigma \in \mathcal{S}(\mathcal{H})} D_\alpha(P \circ \mathcal{W} \| P \otimes \sigma), \quad (9.45)$$

Note that the above relation also holds for  $D_\alpha^b$ .

**Lemma 9.2** ([111, Proposition 21]). *Let  $\mathcal{A} \subset \mathbb{R}_{\geq 0}$  be a convex set and let  $\mathcal{B}$  be a compact Hausdorff space. Further, let  $f : \mathcal{A} \times \mathcal{B} \rightarrow \mathbb{R}$  be concave on  $\mathcal{A}$  as well as convex on  $\mathcal{B}$ . Then*

$$\sup_{x \in \mathcal{A}} \inf_{y \in \mathcal{B}} \frac{f(x, y)}{x} = \inf_{y \in \mathcal{B}} \sup_{x \in \mathcal{A}} \frac{f(x, y)}{x}. \quad (9.46)$$

□

The following corollary is a simple consequence of the variational representations of the sphere-packing exponents in Theorem 9.1 and the Golden-Thompson inequality, Lemma 2.7.

**Corollary 9.1.** *For any classical-quantum channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$ ,  $R > R_\infty$ , and  $P \in \mathcal{P}(\mathcal{X})$ , it holds that*

$$E_{\text{sp}}(R, P) \leq \tilde{E}_{\text{sp}}(R, P). \quad (9.47)$$

## 9.2 Properties of Auxiliary Functions

In the following, we list the properties of the auxiliary functions  $E_0$ ,  $E_0^\downarrow$ ,  $E_h$ , and  $E_h^b$  in Propositions 9.1, 9.2, 9.3, and 9.4, respectively. Our ingredients come from properties of Petz's quantum Rényi divergence [60] (see also [140, 129, 10]) and the theory of matrix geometric means.

**Proposition 9.1** (Properties of  $E_0(s, P)$ ). *The auxiliary function  $E_0(s, P)$ , defined in Eq. (9.4), admits the following properties.*

- (a) *The partial derivatives  $\partial E_0(s, P)/\partial s$ ,  $\partial^2 E_0(s, P)/\partial s^2$ ,  $\partial^3 E_0(s, P)/\partial s^3$ , and  $E_0(s, P)$  are all continuous for  $(s, P) \in \mathbb{R}_{\geq 0} \times \mathcal{P}(\mathcal{X})$ .*
- (b) *For every  $P \in \mathcal{P}(\mathcal{X})$ , the function  $E_0(s, P)$  is concave in  $s$  for all  $s \in \mathbb{R}_{\geq 0}$ .*
- (c) *For every  $P \in \mathcal{P}(\mathcal{X})$ ,*

$$\left. \frac{\partial E_0(s, P)}{\partial s} \right|_{s=0} = I(P, \mathcal{W}). \quad (9.48)$$

- (d) *For every  $P \in \mathcal{P}(\mathcal{X})$ ,*

$$\lim_{s \rightarrow +\infty} \frac{\partial E_0(s, P)}{\partial s} \leq \frac{\partial E_0(s, P)}{\partial s} \leq I(P, \mathcal{W}), \quad \forall s \in \mathbb{R}_{\geq 0}. \quad (9.49)$$

- (e) *For every  $P \in \mathcal{P}(\mathcal{X})$ ,*

$$\left. \frac{\partial^2 E_0(s, P)}{\partial s^2} \right|_{s=0} = -V(P, \mathcal{W}). \quad (9.50)$$

The proof is provided in Section 9.2.1.

**Proposition 9.2** (Properties of  $E_0^\downarrow(s, P, \sigma)$ ). *Consider a classical-quantum channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$ , a distribution  $P \in \mathcal{P}(\mathcal{X})$ , and a state  $\sigma \in \mathcal{S}(\mathcal{H})$  with  $W_x \ll \sigma$  for all  $x \in \text{supp}(P)$ . Then  $E_0^\downarrow(s, P, \sigma)$  defined in Eq. (9.7) enjoys the following properties.*

- (a)  *$E_0^\downarrow(s, P, \sigma)$  and its partial derivatives  $\partial E_0^\downarrow(s, P, \sigma)/\partial s$ ,  $\partial^2 E_0^\downarrow(s, P, \sigma)/\partial s^2$ ,  $\partial^3 E_0^\downarrow(s, P, \sigma)/\partial s^3$  are all continuous in  $(s, P) \in \mathbb{R}_{\geq 0} \times \mathcal{P}(\mathcal{X})$ .*
- (b) *For every  $P \in \mathcal{P}(\mathcal{X})$ , the function  $E_0^\downarrow(s, P, \sigma)$  is concave in  $s \in \mathbb{R}_{\geq 0}$ .*
- (c) *For every  $P \in \mathcal{P}(\mathcal{X})$ ,*

$$\left. \frac{\partial E_0^\downarrow(s, P, \sigma)}{\partial s} \right|_{s=0} = D(P \circ \mathcal{W} \| P \otimes \sigma). \quad (9.51)$$

- (d) *For every  $P \in \mathcal{P}(\mathcal{X})$ ,*

$$\lim_{s \rightarrow +\infty} \frac{\partial E_0^\downarrow(s, P, \sigma)}{\partial s} \leq \frac{\partial E_0^\downarrow(s, P, \sigma)}{\partial s} \leq D(P \circ \mathcal{W} \| P \otimes \sigma), \quad \forall s \in \mathbb{R}_{\geq 0}. \quad (9.52)$$

- (e) *For every  $P \in \mathcal{P}(\mathcal{X})$ ,*

$$\left. \frac{\partial^2 E_0^\downarrow(s, P, \sigma)}{\partial s^2} \right|_{s=0} = -V(P \circ \mathcal{W} \| P \otimes \sigma). \quad (9.53)$$

The proof is provided in Section 9.2.2.

Properties of  $E_h$  and  $E_h^\downarrow$  will be crucial in the analysis of the converse part of our main result.

**Proposition 9.3** (Properties of  $E_h(s, P, \sigma)$ ). Consider a classical-quantum channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$ , a distribution  $P \in \mathcal{P}(\mathcal{X})$ , and a state  $\sigma \in \mathcal{S}(\mathcal{H})$  with  $W_x \ll \sigma$  for all  $x \in \text{supp}(P)$ . Then  $E_h(s, P, \sigma)$  defined in Eq. (9.9) enjoys the following properties.

- (a)  $E_h(s, P, \sigma)$  and its partial derivatives  $\partial E_h(s, P, \sigma)/\partial s$ ,  $\partial^2 E_h(s, P, \sigma)/\partial s^2$ ,  $\partial^3 E_h(s, P, \sigma)/\partial s^3$  are continuous for  $(s, P) \in \mathbb{R}_{\geq 0} \times \mathcal{P}(\mathcal{X})$ .
- (b) For every  $P \in \mathcal{P}(\mathcal{X})$ , the function  $E_h(s, P, \sigma)$  is concave in  $s$  for all  $s \in \mathbb{R}_{\geq 0}$ .
- (c) For every  $P \in \mathcal{P}(\mathcal{X})$ ,

$$\left. \frac{\partial E_h(s, P, \sigma)}{\partial s} \right|_{s=0} = D(\mathcal{W}\|\sigma|P). \quad (9.54)$$

- (d) For every  $P \in \mathcal{P}(\mathcal{X})$ ,

$$\lim_{s \rightarrow +\infty} \frac{\partial E_h(s, P, \sigma)}{\partial s} \leq \left. \frac{\partial E_h(s, P, \sigma)}{\partial s} \right|_{s=0} \leq D(\mathcal{W}\|\sigma|P), \quad \forall s \in \mathbb{R}_{\geq 0}. \quad (9.55)$$

- (e) For every  $P \in \mathcal{P}(\mathcal{X})$ ,

$$\left. \frac{\partial^2 E_h(s, P, \sigma)}{\partial s^2} \right|_{s=0} = -V(\mathcal{W}\|\sigma|P). \quad (9.56)$$

The proof is provided in Section 9.2.3.

**Proposition 9.4** (Properties of  $E_h^\flat(s, P, \sigma)$ ). Consider a classical-quantum channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$ , a distribution  $P \in \mathcal{P}(\mathcal{X})$ , and a state  $\sigma \in \mathcal{S}(\mathcal{H})$  with  $W_x \ll \sigma$  for all  $x \in \text{supp}(P)$ . Then  $E_h^\flat(s, P, \sigma)$  defined in Eq. (9.10) enjoys the following properties.

- (a)  $E_h^\flat(s, P, \sigma)$  and its partial derivatives  $\partial E_h^\flat(s, P, \sigma)/\partial s$ ,  $\partial^2 E_h^\flat(s, P, \sigma)/\partial s^2$ ,  $\partial^3 E_h^\flat(s, P, \sigma)/\partial s^3$  are all continuous for  $(s, P) \in \mathbb{R}_{\geq 0} \times \mathcal{P}(\mathcal{X})$ .
- (b) For every  $P \in \mathcal{P}(\mathcal{X})$ , the function  $E_h^\flat(s, P, \sigma)$  is concave in  $s$  for all  $s \in \mathbb{R}_{\geq 0}$ .
- (c) For every  $P \in \mathcal{P}(\mathcal{X})$ ,

$$\left. \frac{\partial E_h^\flat(s, P, \sigma)}{\partial s} \right|_{s=0} = D(\mathcal{W}\|\sigma|P). \quad (9.57)$$

- (d) For every  $P \in \mathcal{P}(\mathcal{X})$ ,

$$\lim_{s \rightarrow +\infty} \frac{\partial E_h^\flat(s, P, \sigma)}{\partial s} \leq \left. \frac{\partial E_h^\flat(s, P, \sigma)}{\partial s} \right|_{s=0} \leq D(\mathcal{W}\|\sigma|P), \quad \forall s \in \mathbb{R}_{\geq 0}. \quad (9.58)$$

- (e) For every  $P \in \mathcal{P}(\mathcal{X})$ ,

$$\left. \frac{\partial^2 E_h^\flat(s, P, \sigma)}{\partial s^2} \right|_{s=0} = -\tilde{V}(\mathcal{W}\|\sigma|P). \quad (9.59)$$

The proof is provided in Section 9.2.4.

### 9.2.1 Proof of Proposition 9.1

Fix any c-q channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$ . To ease the burden of derivations, we denote some notation:

$$f(s, P) := \sum_{x \in \mathcal{X}} P(x) W_x^{1/(1+s)} \in \mathcal{B}(\mathcal{H})_+, \quad (9.60)$$

$$g(s, P) := f(s, P)^{(1+s)} \in \mathcal{B}(\mathcal{H})_+, \quad (9.61)$$

$$F(s, P) := \text{Tr}[g(s, P)] \in \mathbb{R}_{\geq 0}, \quad (9.62)$$

for all  $(s, P) \in \mathbb{R}_{\geq 0} \times \mathcal{P}(\mathcal{X})$ . Clearly,  $f(\cdot, \cdot)$  is continuous on  $\mathbb{R}_{\geq 0} \times \mathcal{P}(\mathcal{X})$ . Direct calculation shows that

$$f'(s, P) := \frac{\partial f(s, P)}{\partial s} = -\frac{1}{(1+s)^2} \sum_{x \in \mathcal{X}} P(x) W_x^{1/(1+s)} \widehat{\log} W_x, \quad (9.63)$$

$$f''(s, P) := \frac{\partial^2 f(s, P)}{\partial s^2} = \frac{1}{(1+s)^3} \sum_{x \in \mathcal{X}} P(x) W_x^{1/(1+s)} \widehat{\log} W_x \left[ 2 + \frac{\widehat{\log} W_x}{(1+s)} \right], \quad (9.64)$$

$$f'''(s, P) := \frac{\partial^3 f(s, P)}{\partial s^3} = -\frac{1}{(1+s)^4} \sum_{x \in \mathcal{X}} P(x) W_x^{1/(1+s)} \widehat{\log} W_x \left[ 6 + \frac{6\widehat{\log} W_x}{(1+s)} + \frac{\widehat{\log}^2 W_x}{(1+s)^2} \right], \quad (9.65)$$

where we denote  $\widehat{\log}$  by

$$\widehat{\log} x = \begin{cases} \log x, & x > 0, \\ 0, & x = 0. \end{cases} \quad (9.66)$$

From Eqs. (9.63), (9.64), and (9.65), we infer that  $f'(s, P)$ ,  $f''(s, P)$ , and  $f'''(s, P)$  share the same support as  $f(s, P)$ , and are continuous for all  $(s, P) \in \mathbb{R}_{\geq 0} \times \mathcal{P}(\mathcal{X})$  (in the strong topology).

Observe that for all  $(s, P) \in \mathbb{R}_{\geq 0} \times \mathcal{P}(\mathcal{X})$ ,

$$g(s, P)^0 = f(s, P)^0. \quad (9.67)$$

Hence, the operator  $g(s, P)$  admit the expression:

$$g(s, P) = g(s, P)^0 e^{(1+s)\widehat{\log} f(s, P)} g(s, P)^0. \quad (9.68)$$

By applying the chain rule of the Fréchet derivatives, one can calculate that

$$\begin{aligned} g'(s, P) &:= \frac{\partial g(s, P)}{\partial s} \\ &= g(s, P)^0 D \exp \left[ \widehat{\log} g(s, P) \right] \left( (1+s) D \widehat{\log} [f(s, P)] (f'(s, P)) + \widehat{\log} f(s, P) \right) g(s, P)^0, \end{aligned} \quad (9.69)$$

$$\begin{aligned} g''(s, P) &:= \frac{\partial^2 g(s, P)}{\partial s^2} \\ &= g(s, P)^0 D^2 \exp \left[ \widehat{\log} g(s, P) \right] \left( (1+s) D \widehat{\log} [f(s, P)] (f'(s, P)) + \widehat{\log} f(s, P) \right) g(s, P)^0 \\ &\quad + g(s, P)^0 D \exp \left[ \widehat{\log} g(s, P) \right] \left( 2 D \widehat{\log} [f(s, P)] (f'(s, P)) + (1+s) \left\{ D \widehat{\log} [f(s, P)] (f''(s, P)) \right. \right. \\ &\quad \left. \left. + D^2 \widehat{\log} [f(s, P)] (f'(s, P)) \right\} \right) g(s, P)^0, \end{aligned} \quad (9.70)$$

where we use the following integral formulas (see e.g. [84, Example 3.22, Excercise 3.24])

$$\widehat{\text{Dlog}}[A](B) = \int_0^{+\infty} (t\mathbb{1} + A)^{-1} B (t\mathbb{1} + A)^{-1} dt, \quad (9.71)$$

$$\text{D}^2\widehat{\text{log}}[A](B) := \text{D}^2\widehat{\text{log}}[A](B, B) = -2 \int_0^{+\infty} (t\mathbb{1} + A)^{-1} B (t\mathbb{1} + A)^{-1} B (t\mathbb{1} + A)^{-1} dt \quad (9.72)$$

for all  $0 \leq B \ll A$ , and (see e.g. [84, Theorem 3.10])

$$\text{Dexp}[A](B) = \int_0^1 e^{(1-t)A} B e^{tA} dt, \quad (9.73)$$

$$\text{D}^2\text{exp}[A](B) := \text{D}^2\text{exp}[A](B, B) = 2 \int_0^1 \int_0^{t_1} e^{(1-t_1)A} B e^{(t_1-t_2)A} B e^{t_2 A} dt_2 dt_1 \quad (9.74)$$

for all self-adjoint operators  $A$  and  $B$ . Further, by [79, Theorem 3.5]  $\text{Dexp}[\cdot](\cdot)$ ,  $\text{D}^2\text{exp}[\cdot](\cdot)$  are continuous for all self-adjoint operators, and  $\widehat{\text{Dlog}}[A](B)$ ,  $\widehat{\text{D}^2\text{log}}[A](B)$  are continuous for all  $0 \leq B \ll A$ .

In the following, we will show that  $g'(s, P)$  is continuous for all  $(s, P) \in \mathbb{R}_{\geq 0} \times \mathcal{P}(\mathcal{X})$ . However, the operation  $\widehat{\text{Dlog}}[\cdot](\cdot)$  in Eq. (9.69) is only continuous for positive definite operators (see [71, Theorem 3.8]). We need to do little more work to circumvent this problem.

Let  $\{s_k, P_k\}_{k \geq 1}$  be an arbitrary sequence with limit  $(s_k, P_k) \rightarrow (s_o, P_o)$ . Observe that if  $f(s_k, P_k) \ll f(s_o, P_o)$  for some  $k \in \mathbb{N}$ , we can only focus on the support of  $f(s_o, P_o)$  and treat  $f(s_o, P_o)$  as a positive definite operator without loss of generality. Consider any subsequence  $\{s_{k_n}, P_{k_n}\}_{n \geq 1}$ . Suppose all but a finite number of  $(s_{k_n}, P_{k_n})$  satisfy

$$f(s_{k_n}, P_{k_n}) \ll f(s_o, P_o). \quad (9.75)$$

Then Eq. (9.69), and the continuity of  $f(\cdot, \cdot)$ ,  $f'(\cdot, \cdot)$ ,  $\widehat{\text{Dlog}}[f(\cdot, \cdot)](\cdot)$  (recall that it is continuous for positive definite operators), and  $\widehat{\text{Dexp}}[\log f(\cdot, \cdot)](\cdot)$  (see [71, Theorem 3.8], [79, Theorem 3.5]) imply that  $g'(\cdot, \cdot)$  is continuous at  $(s_o, P_o)$ . If this is not the case, we define

$$\omega_{\min} := \min_{x \in \mathcal{X}} \tilde{\lambda}_{\min}(W_x), \quad (9.76)$$

$$\omega_{\max} := \max_{x \in \mathcal{X}} \lambda_{\max}(W_x), \quad (9.77)$$

where  $\tilde{\lambda}_{\min}(X)$  denotes the minimum non-zero eigenvalue of an operator  $X$ . From Eqs. (9.60), (9.63), (9.76), and (9.77), one can verify that

$$f'(s, P) \leq \frac{f(s, P)}{(1+s)^2} \log \frac{1}{w_{\min}}, \quad (9.78)$$

$$f'(s, P) \geq \frac{f(s, P)}{(1+s)^2} \log \frac{1}{w_{\max}}. \quad (9.79)$$

Then for any subsequence that  $f(s_{k_n}, P_{k_n}) \ll f(s_o, P_o)$ , Eq.s (9.71), (9.78) and (9.79) imply

$$\begin{aligned} \mathbb{R}_{\geq 0} \ni \frac{1}{(1+s_o)^2} \log \frac{1}{\omega_{\max}} &\leq \liminf_{n \rightarrow +\infty} \widehat{\text{Dlog}}[f(s_{k_n}, P_{k_n})] (f'(s_{k_n}, P_{k_n})) \\ &\leq \limsup_{n \rightarrow +\infty} \widehat{\text{Dlog}}[f(s_{k_n}, P_{k_n})] (f'(s_{k_n}, P_{k_n})) \leq \frac{1}{(1+s_o)^2} \log \frac{1}{\omega_{\min}} \in \mathbb{R}_{\geq 0}. \end{aligned} \quad (9.80)$$

Invoking the continuity of  $f(\cdot, \cdot)$ ,  $g(\cdot, \cdot)^0$ , combined with Eqs. (9.69) and (9.80), we infer that<sup>1</sup>

$$\lim_{n \rightarrow +\infty} \left. \frac{\partial g(s, P_k)}{\partial s} \right|_{s=s_k} = g'(s_o, P_o). \quad (9.81)$$

Hence, we complete the claim of the continuity of  $g'(\cdot, \cdot)$ . By following the same approach, one can also verify the continuity of  $g''(\cdot, \cdot)$  and  $g'''(\cdot, \cdot)$ .

Recall the definition of  $E_0(s, P, W)$  in Eq. (9.4) and Eq. (9.62), we have  $E_0(s, P, W) = -\log F(s, P)$ . By denoting  $F'(s, P) := \partial F(s, P)/\partial s$ , direct calculation shows that

$$\frac{\partial E_0(s, P)}{\partial s} = -\frac{F'(s, P)}{F(s, P)} \quad (9.82)$$

$$\frac{\partial^2 E_0(s, P)}{\partial s^2} = -\frac{F''(s, P)}{F(s, P)} - \left( \frac{\partial E_0(s, P)}{\partial s} \right)^2, \quad (9.83)$$

$$\frac{\partial^3 E_0(s, P)}{\partial s^3} = -\frac{F'''(s, P)}{F(s, P)} + 3 \frac{\partial E_0(s, P)}{\partial s} \frac{\partial^2 E_0(s, P)}{\partial s^2} - \left( \frac{\partial E_0(s, P)}{\partial s} \right)^3. \quad (9.84)$$

Now we are at the position to prove Proposition 9.1:

- (9.1-(a)) Recalling from Eq. (9.61), the continuity of  $E_0(s, P)$ ,  $\partial E_0(s, P)/\partial s$ ,  $\partial^2 E_0(s, P)/\partial s^2$ , and  $\partial^3 E_0(s, P)/\partial s^3$  follow from the continuity of  $g(\cdot, \cdot)$ ,  $g'(\cdot, \cdot)$ ,  $g''(\cdot, \cdot)$ , and  $g'''(\cdot, \cdot)$ .
- (9.1-(b)) To prove the concavity of the map  $s \mapsto E_0(s, P)$  for  $s \geq 0$ , we first provide some useful lemmas and the definition of geometric means. Define the “ $s$ -weighted geometric mean” of positive definite matrices  $A$  and  $B$  by

$$A \#_s B := A^{1/2} \left( A^{-1/2} B A^{-1/2} \right)^s A^{1/2}. \quad (9.85)$$

It is known that the geometric mean is jointly concave in the matrix partial order (see e.g. [141]):

$$(\theta A + (1-\theta)B) \#_s (\theta C + (1-\theta)D) \succeq \theta (A \#_s C) + (1-\theta) (B \#_s D) \quad (9.86)$$

for all  $\theta, s \in [0, 1]$ .

Now we begin the proof of item (b). Since the geometric means, Eq. (9.85), are defined for positive definite matrices, we first present the proof that only works when all  $\{W_x\}_{x \in \mathcal{X}}$  are full rank. The proof can then be extended to include the non-invertible case.

---

<sup>1</sup>More precisely,  $f(s_{k_n}, P_{k_n})$  and  $f(s_o, P_o)$  share some disjoint support since  $f(s_{k_n}, P_{k_n}) \ll f(s_o, P_o)$ . However, owing to the finiteness of Eq. (9.80), the projection  $g(s_o, P_o)^0$  “nullifies” those disjoint support, and hence we can only consider the joint support of  $f(s_{k_n}, P_{k_n})$  and  $f(s_o, P_o)$ . The continuity of the operation  $\widehat{\text{Dlog}}[f(\cdot, \cdot)](\cdot)$  on the support of  $f(s_o, P_o)$  follows from the previous argument.

Let  $X$  be a random variable with the distribution  $P$ , and denote by  $\mathbb{E}_X$  the expectation with respect to  $P$ . Then it suffices to prove the convexity of the map:

$$f : t \mapsto \log \text{Tr} \left[ \left( \mathbb{E}_X W_X^{\frac{1}{t}} \right)^t \right] \quad (9.87)$$

for all  $t \geq 1$ .

Let  $l, r$ , and  $\theta$  be arbitrary numbers  $1 \leq l \leq r$ ,  $0 \leq \theta \leq 1$ , and define

$$t = \theta l + (1 - \theta)r. \quad (9.88)$$

Let  $t \equiv 1 + s \geq 1$ . Then we prove the convexity of the map  $f$  from Eq. (9.87), i.e.

$$f(t) \leq \theta f(l) + (1 - \theta)f(r). \quad (9.89)$$

Define the number  $\tau \in [0, 1]$  by

$$\tau = \frac{l\theta}{t}; \quad 1 - \tau = \frac{r(1 - \theta)}{t}. \quad (9.90)$$

Then it follows that

$$\frac{1}{t} = \frac{\theta}{t} + \frac{1 - \theta}{t} = \frac{\tau}{l} + \frac{1 - \tau}{r}. \quad (9.91)$$

The concavity of the geometric means (see Eq. (9.86)) implies that

$$\mathbb{E}_X \left[ W_X^{1/t} \right] = \mathbb{E}_X \left[ W_X^{\tau/l} W_X^{(1-\tau)/r} \right] \quad (9.92)$$

$$= \mathbb{E}_X \left[ W_X^{1/l} \#_{1-\tau} W_X^{1/r} \right] \quad (9.93)$$

$$\preceq \mathbb{E}_X \left[ W_X^{1/l} \right] \#_{1-\tau} \mathbb{E}_X \left[ W_X^{1/r} \right]. \quad (9.94)$$

Now let  $A \equiv \mathbb{E}_X \left[ W_X^{1/l} \right]$  and  $B \equiv \mathbb{E}_X \left[ W_X^{1/r} \right]$ . Since  $x \mapsto x^t$  for  $t \geq 1$  is a monotone function, Lemma 2.4 in Section 2.1 leads to

$$\text{Tr} \left[ \left( \mathbb{E}_X \left[ W_X^{1/t} \right] \right)^t \right] \leq \text{Tr} \left[ (A \#_{1-\tau} B)^t \right] \quad (9.95)$$

$$\leq \text{Tr} \left[ A^{t\tau} B^{t(1-\tau)} \right] \quad (9.96)$$

$$= \text{Tr} \left[ A^{l\theta} B^{r(1-\theta)} \right], \quad (9.97)$$

where Eq. (9.96) follows from Lemma 2.6. Finally, applying the matrix Hölder's inequality, Lemma 2.5, in Section 2.1 on the right-hand side of Eq. (9.97), we have

$$\begin{aligned} \text{Tr} \left[ \left( \mathbb{E}_X \left[ W_X^{1/t} \right] \right)^t \right] &\leq \left( \text{Tr} \left[ A^l \right] \right)^\theta (\text{Tr} [B^r])^{1-\theta} \\ &= \left( \text{Tr} \left( \mathbb{E}_X \left[ W_X^{1/l} \right] \right)^l \right)^\theta \left( \text{Tr} \left( \mathbb{E}_X \left[ W_X^{1/r} \right] \right)^r \right)^{1-\theta}. \end{aligned}$$

Taking the logarithm of the above inequality leads to  $f(t) \leq \theta f(l) + (1 - \theta)f(r)$ . This completes the proof for the special case of invertible channel outputs.

The above proof assumes that every realization of the density operator  $W_x$ ,  $x \in \mathcal{X}$ , is positive definite. Hence, each density operator  $W_x^{\tau/l} W_x^{(1-\tau)/r}$  can be expressed as a geometric mean  $W_x^{1/l} \#_{1-\tau} W_x^{1/r}$ . However, if  $W_x$  is not invertible for some  $x \in \mathcal{X}$ , then consider a sequence of positive definite operators  $W_{x,\varepsilon} := W_x + \varepsilon I$  that approximate  $W_x$ , i.e.,  $\lim_{\varepsilon \searrow 0} W_{x,\varepsilon} = W_x$ . The geometric mean of  $W_x^{1/l}$  and  $W_x^{1/r}$  is then defined by

$$\left(W_x^{1/l}\right) \#_s \left(W_x^{1/r}\right) := \lim_{\varepsilon \searrow 0} \left(W_{x,\varepsilon}^{1/l}\right) \#_s \left(W_{x,\varepsilon}^{1/r}\right), \quad (9.98)$$

by the continuity of the geometric means. Note that the concavity of the geometric means, and Lemmas 2.1 and 2.6 in Section 2.1 still hold if we use the definition in Eq. (9.98). We can thus obtain a complete the proof of item (b).

- (9.1-(c)) This item was discovered by Ogawa and Nagaoka [64, Eq. (12)]. For the sake of completeness, we provide the proof here. Note that

$$g(0, P) = f(0, P). \quad (9.99)$$

The continuity of  $g'(\cdot, \cdot)$  and Eq. (9.69) imply that

$$\begin{aligned} & g'(s, P) \Big|_{s=0} \\ &= g(0, P)^0 D \exp \left[ \widehat{\log} g(0, P) \right] \left( (1+0) D \widehat{\log} [f(0, P)] (f'(0, P)) + \widehat{\log} f(0, P) \right) g(0, P)^0 \\ &= D \exp \left[ \widehat{\log} f(0, P) \right] \left( D \widehat{\log} [f(0, P)] (f'(0, P)) + f(0, P) \widehat{\log} f(0, P) \right) \end{aligned} \quad (9.100)$$

$$= f'(s, P) + \widehat{\log} f(s, P) \Big|_{s=0} \quad (9.101)$$

$$= - \sum_{x \in \mathcal{X}} W_x \log W_x + W_P \widehat{\log} W_P. \quad (9.102)$$

Therefore,

$$\frac{\partial E_0(s, P, W)}{\partial s} \Big|_{s=0} = - \frac{F'(0, P)}{F(0, P)} = - \text{Tr} [g'(0, P)] = I(P, W). \quad (9.103)$$

- (9.1-(d)) The concavity of the map  $s \mapsto E(s, P)$  in item (b) ensures that  $\partial E(s, P)/\partial s$  is decreasing in  $s$ . Along with item (c) concludes Eq. (9.49).

- (9.1-(e)) By using Lemma 2.11 in Section 2.1, we have

$$\begin{aligned} F''(s, P) \Big|_{s=0} &= \text{Tr} \left[ g'(s, P) \left( (1+s) D \widehat{\log} [f(s, P)] (f'(s, P)) + \widehat{\log} f(s, P) \right) \right] \Big|_{s=0} \\ &+ \text{Tr} \left[ g(s, P) \left( 2 D \widehat{\log} [f(s, P)] (f'(s, P)) + (1+s) \left\{ D \widehat{\log} [f(s, P)] (f''(s, P)) \right. \right. \right. \\ &\quad \left. \left. \left. + D^2 \widehat{\log} [f(s, P)] (f'(s, P)) \right\} \right) \right] \Big|_{s=0}. \end{aligned} \quad (9.104)$$

From Eqs. (9.101), (9.102), the first term in Eq. (9.104) yields

$$\text{Tr} \left[ g'(0, P) \left( D\widehat{\log} [f(0, P)] (f'(0, P)) + \widehat{\log} f(0, P) \right) \right] \quad (9.105)$$

$$= \text{Tr} \left[ f'(0, P) D\widehat{\log} [f(0, P)] (f'(0, P)) + 2f'(0, P) \widehat{\log} f(0, P) + f(0, P) \widehat{\log}^2 f(0, P) \right]. \quad (9.106)$$

Similarly, from Eqs. (9.99),(9.64) the second term in Eq. (9.104) leads to

$$\begin{aligned} & \text{Tr} \left[ f(0, P) \left( 2D\widehat{\log} [f(0, P)] (f'(0, P)) + \left\{ D\widehat{\log} [f(0, P)] (f''(0, P)) \right. \right. \right. \\ & \quad \left. \left. \left. + D^2\widehat{\log} [f(0, P)] (f'(0, P)) \right\} \right) \right] \end{aligned} \quad (9.107)$$

$$= \text{Tr} \left[ \sum_{x \in \mathcal{X}} P(x) W_x \log^2 W_x - f'(0, P) D\widehat{\log} [f(0, P)] (f'(0, P)) \right]. \quad (9.108)$$

Equation (9.104) combined with Eqs. (9.106), (9.108) gives

$$F''(0, P) = \text{Tr} \left[ \sum_{x \in \mathcal{X}} W_x (\log W_x - \log W_P)^2 \right]. \quad (9.109)$$

Recalling Eq. (9.83) completes the proof.

□

### 9.2.2 Proof of Proposition 9.2

(9.2-(a)) The continuity can be proved by the standard approach of functional calculus (see e.g. [140, Lemma III.1] and [129, Section 4.2]). Let  $\tilde{F}(s) := \sum_{x \in \mathcal{X}} P(x) \text{Tr} [W_x^{1-s} \sigma^s]$ . Direct calculation shows that

$$\frac{\partial E_0^\downarrow(s, P, \sigma)}{\partial s} = -\frac{\tilde{F}'(s)}{\tilde{F}(s)}, \quad (9.110)$$

$$\frac{\partial^2 E_0^\downarrow(s, P, \sigma)}{\partial s^2} = -\frac{\tilde{F}''(s)}{\tilde{F}(s)} + \left( \frac{\partial E_0^\downarrow(s, P, \sigma)}{\partial s} \right)^2, \quad (9.111)$$

$$\frac{\partial^3 E_0^\downarrow(s, P, \sigma)}{\partial s^3} = -\frac{\tilde{F}'''(s, P)}{\tilde{F}(s, P)} + 3 \frac{\partial E_0^\downarrow(s, P, \sigma)}{\partial s} \frac{\partial^2 E_0^\downarrow(s, P, \sigma)}{\partial s^2} - \left( \frac{\partial E_0^\downarrow(s, P, \sigma)}{\partial s} \right)^3, \quad (9.112)$$

and

$$\tilde{F}'(s) = \sum_{x \in \mathcal{X}} P(x) \text{Tr} [-W_x^{1-s}(\log W_x)\sigma^s + W_x^{1-s}\sigma^s \log \sigma], \quad (9.113)$$

$$\begin{aligned} \tilde{F}''(s) &= \sum_{x \in \mathcal{X}} P(x) \text{Tr} [W_x^{1-s}(\log^2 W_x)\sigma^s - W_x^{1-s}(\log W_x)\sigma^s \log \sigma \\ &\quad - W_x^{1-s}(\log W_x)\sigma^s \log \sigma + W_x^{1-s}\sigma^s \log^2 \sigma], \end{aligned} \quad (9.114)$$

$$\begin{aligned} \tilde{F}'''(s) &= \sum_{x \in \mathcal{X}} P(x) \text{Tr} [-W_x^{1-s}(\log^3 W_x)\sigma^s + W_x^{1-s}(\log^2 W_x)\sigma^s \log \sigma \\ &\quad + 2W_x^{1-s}(\log^2 W_x)\sigma^s \log \sigma - 2W_x^{1-s}(\log W_x)\sigma^s \log^2 \sigma \\ &\quad - W_x^{1-s}(\log W_x)\sigma^s \log^2 \sigma + W_x^{1-s}\sigma^s \log^3 \sigma]. \end{aligned} \quad (9.115)$$

Since the matrix power function is continuous (with respect to the strong topology; see e.g. [71, Theorem 1.19]), we conclude the continuity of the partial derivatives Eqs. (9.110)-(9.112) in item (a).

- (9.2-(b)) The claim follows from the concavity of the map  $s \mapsto sD_{1-s}(\cdot \| \cdot)$  (Lemma 3.2-(d)).
- (9.2-(c)) The results can be derived from evaluating Eqs. (9.110) and (9.113) at  $s = 0$ . We provide an alternative proof here. One can verify

$$\frac{\partial E_0^\downarrow(s, P, \sigma)}{\partial s} \Big|_{s=0} = D_{1-s}(P \circ \mathcal{W} \| P \otimes \sigma) - sD'_{1-s}(P \circ \mathcal{W} \| P \otimes \sigma) \Big|_{s=0} \quad (9.116)$$

$$= D_{1-s}(P \circ \mathcal{W} \| P \otimes \sigma) \Big|_{s=0} \quad (9.117)$$

$$= D(P \circ \mathcal{W} \| P \otimes \sigma). \quad (9.118)$$

- (9.2-(d)) The concavity of the map  $s \mapsto E_0^\downarrow(s, P, \sigma)$  in item (b) ensures that  $\partial E_0^\downarrow(s, P, \sigma)/\partial s$  is non-increasing in  $s$ . Along with Eq. (9.118), we conclude Eq. (9.52).

- (9.2-(e)) Following from item (c), one obtain

$$\frac{\partial^2 E_0^\downarrow(s, P, \sigma)}{\partial s^2} \Big|_{s=0} = -2D'_{1-s}(P \circ \mathcal{W} \| P \otimes \sigma) + sD''_{1-s}(P \circ \mathcal{W} \| P \otimes \sigma) \Big|_{s=0} \quad (9.119)$$

$$= -2D'_{1-s}(P \circ \mathcal{W} \| P \otimes \sigma) \Big|_{s=0} \quad (9.120)$$

$$= -V(P \circ \mathcal{W} \| P \otimes \sigma), \quad (9.121)$$

where the last equality (9.121) follows from the fact  $D'_{1/1+s}(\cdot \| \cdot)|_{s=0} = V(\cdot \| \cdot)/2$  [129, Theorem 2].

□

### 9.2.3 Proof of Proposition 9.3

(9.3-(a)) Direct calculation yields that

$$\frac{\partial E_h(s, P, \sigma)}{\partial s} = D_{\frac{1}{1+s}}(\mathcal{W}\|\sigma|P) - \frac{s}{(1+s)^2} D'_{\frac{1}{1+s}}(\mathcal{W}\|\sigma|P) \quad (9.122)$$

$$\frac{\partial^2 E_h(s, P, \sigma)}{\partial s^2} = -\frac{2}{(1+s)^3} D'_{\frac{1}{1+s}}(\mathcal{W}\|\sigma|P) + \frac{s}{(1+s)^4} D''_{\frac{1}{1+s}}(\mathcal{W}\|\sigma|P) \quad (9.123)$$

$$\begin{aligned} \frac{\partial^3 E_h(s, P, \sigma)}{\partial s^3} &= \frac{6}{(1+s)^4} D'_{\frac{1}{1+s}}(\mathcal{W}\|\sigma|P) + \frac{3-3s}{(1+s)^5} D''_{\frac{1}{1+s}}(\mathcal{W}\|\sigma|P) \\ &\quad - \frac{s}{(1+s)^6} D'''_{\frac{1}{1+s}}(\mathcal{W}\|\sigma|P). \end{aligned} \quad (9.124)$$

From Eqs. (9.122)-(9.124) and the fact that  $D_{1/(1+s)}(\mathcal{W}\|\sigma|P)$ ,  $D'_{1/(1+s)}(\mathcal{W}\|\sigma|P)$ ,  $D''_{1/(1+s)}(\mathcal{W}\|\sigma|P)$ , and  $D'''_{1/(1+s)}(\mathcal{W}\|\sigma|P)$  are continuous for  $(s, P) \in \mathbb{R}_{\geq 0} \times \mathcal{P}(\mathcal{X})$ , we deduce the continuity property in item (a).

(9.3-(b)) The proof strategy follows closely with [59, Appendix B]. Let  $\psi(\alpha) = \sum_{x \in \mathcal{X}} P(x) \log \text{Tr}[W_x^\alpha \sigma^{1-\alpha}]$ . Since  $\alpha \mapsto \psi(\alpha)$  is convex for all  $\alpha \in (0, 1)$  (Lemma 3.2-(d)), it can be written as the supremum of affine functions, i.e.

$$\psi(\alpha) = \sup_{i \in \mathcal{I}} \{c_i \alpha + d_i\} \quad (9.125)$$

for some index set  $\mathcal{I}$ . Hence,

$$-E_h(s, P, \sigma) = (1+s)\psi\left(\frac{1}{1+s}\right) = \sup_{i \in \mathcal{I}} \{c_i + d_i(1+s)\}. \quad (9.126)$$

The right-hand side of Eq. (9.126), in turn, implies that the map  $s \mapsto E_h(s, P, \sigma)$  is concave for all  $s \in \mathbb{R}_{\geq 0}$ .

(9.3-(c)) From Eqs. (9.122), one finds

$$\left. \frac{\partial E_h(s, P, \sigma)}{\partial s} \right|_{s=0} = D(\mathcal{W}\|\sigma|P). \quad (9.127)$$

(9.3-(d)) The concavity of the map  $s \mapsto E_h(s, P, \sigma)$  in item (b) ensures that  $\partial E_h(s, P, \sigma)/\partial s$  is non-increasing in  $s$ . Along with Eq. (9.127) in item (c), we conclude Eq. (9.55).

(9.3-(e)) Applying  $D'_{1/(1+s)}(\cdot\|\cdot)|_{s=0} = V(\cdot\|\cdot)/2$  [129, Theorem 2], it holds that

$$\left. \frac{\partial^2 E_h(s, P, \sigma)}{\partial s^2} \right|_{s=0} = -V(\mathcal{W}\|\sigma|P). \quad (9.128)$$

□

### 9.2.4 Proof of Proposition 9.4

This proof follows similarly from Proposition 9.3.

(9.4-(a)) Direct calculation yields that

$$\frac{\partial E_h^\flat(s, P, \sigma)}{\partial s} = D_{\frac{1}{1+s}}^\flat(\mathcal{W}\|\sigma|P) - \frac{s}{(1+s)^2} D_{\frac{1}{1+s}}^{\flat\prime}(\mathcal{W}\|\sigma|P) \quad (9.129)$$

$$\frac{\partial^2 E_h^\flat(s, P, \sigma)}{\partial s^2} = -\frac{2}{(1+s)^3} D_{\frac{1}{1+s}}^{\flat\prime\prime}(\mathcal{W}\|\sigma|P) + \frac{s}{(1+s)^4} D_{\frac{1}{1+s}}^{\flat\prime\prime\prime}(\mathcal{W}\|\sigma|P) \quad (9.130)$$

$$\begin{aligned} \frac{\partial^3 E_h^\flat(s, P, \sigma)}{\partial s^3} &= \frac{6}{(1+s)^4} D_{\frac{1}{1+s}}^{\flat\prime\prime}(\mathcal{W}\|\sigma|P) + \frac{3-3s}{(1+s)^5} D_{\frac{1}{1+s}}^{\flat\prime\prime\prime}(\mathcal{W}\|\sigma|P) \\ &\quad - \frac{s}{(1+s)^6} D_{\frac{1}{1+s}}^{\flat\prime\prime\prime\prime}(\mathcal{W}\|\sigma|P). \end{aligned} \quad (9.131)$$

From Eqs. (9.129)-(9.131) and the fact that  $D_{1/(1+s)}^\flat(\mathcal{W}\|\sigma|P)$ ,  $D_{1/(1+s)}^{\flat\prime}(\mathcal{W}\|\sigma|P)$ ,  $D_{1/(1+s)}^{\flat\prime\prime}(\mathcal{W}\|\sigma|P)$ , and  $D_{1/(1+s)}^{\flat\prime\prime\prime}(\mathcal{W}\|\sigma|P)$  are continuous for  $(s, P) \in \mathbb{R}_{\geq 0} \times \mathcal{P}(\mathcal{X})$ , we deduce the continuity property in item (a).

(9.4-(b)) The proof strategy follows closely with [59, Appendix B]. Let

$$\tilde{\psi}(\alpha) = \sum_{x \in \mathcal{X}} P(x) \log \text{Tr} \left[ e^{\alpha \log W_x + (1-\alpha) \log \sigma} \right]. \quad (9.132)$$

Since  $\alpha \mapsto \tilde{\psi}(\alpha)$  is convex for all  $\alpha \in (0, 1]$  (Lemma 3.2-(d)), it can be written as the supremum of affine functions, i.e.

$$\tilde{\psi}(\alpha) = \sup_{i \in \mathcal{I}} \{c_i \alpha + d_i\} \quad (9.133)$$

for some index set  $\mathcal{I}$ . Hence,

$$-E_h^\flat(s, P, \sigma) = (1+s)\tilde{\psi}\left(\frac{1}{1+s}\right) = \sup_{i \in \mathcal{I}} \{c_i + d_i(1+s)\}. \quad (9.134)$$

The right-hand side of Eq. (9.134), in turn, implies that the map  $s \mapsto E_h^\flat(s, P, \sigma)$  is concave for all  $s \in \mathbb{R}_{\geq 0}$ .

(9.4-(c)) From Eqs. (9.129), one finds

$$\left. \frac{\partial E_h^\flat(s, P, \sigma)}{\partial s} \right|_{s=0} = D(\mathcal{W}\|\sigma|P). \quad (9.135)$$

(9.4-(d)) The concavity of the map  $s \mapsto E_h^\flat(s, P, \sigma)$  in item (b) ensures that  $\partial E_h^\flat(s, P, \sigma)/\partial s$  is non-increasing in  $s$ . Along with Eq. (9.135) in item (c), we conclude Eq. (9.58).

(9.4-(e)) Following similar steps in [129, Proposition 4], it can be verified that

$$D_\alpha^{\flat\prime}(\rho\|\sigma) \Big|_{\alpha=1} = \lim_{\alpha \uparrow 1} \frac{1}{2} \frac{d^2}{d\alpha^2} \log f(\alpha) = \frac{f(1)f''(1) - (f'(1))^2}{2(f(1))^2}, \quad (9.136)$$

where  $f(\alpha) := \text{Tr} [e^{\alpha \log \rho + (1-\alpha) \sigma}]$ . Further, the Fréchet derivative of the exponential (see e.g. [69,

Example X.4.2]) gives

$$f'(\alpha) = \text{Tr} \left[ e^{\alpha \log \rho + (1-\alpha) \log \sigma} (\log \rho - \log \sigma) \right], \quad (9.137)$$

$$f''(\alpha) = \int_0^1 dt \text{Tr} \left[ e^{t(\alpha \log \rho + (1-\alpha) \log \sigma)} (\log \rho - \log \sigma) e^{(1-t)(\alpha \log \rho + (1-\alpha) \log \sigma)} (\log \rho - \log \sigma) \right], \quad (9.138)$$

Therefore, Eq. (9.136) equals

$$D_\alpha^b(\rho\|\sigma) \Big|_{\alpha=1} = \frac{1}{2} \left( \int_0^1 dt \text{Tr} [\rho^{1-t} (\log \rho - \log \sigma) \rho^t (\log \rho - \log \sigma)] - D(\rho\|\sigma)^2 \right) \quad (9.139)$$

$$= \frac{1}{2} \tilde{V}(\rho\|\sigma). \quad (9.140)$$

Finally, combining with Eq. (9.130) yields

$$\frac{\partial^2 E_h^b(s, P, \sigma)}{\partial s^2} \Big|_{s=0} = -\tilde{V}(\mathcal{W}\|\sigma|P). \quad (9.141)$$

□

### 9.3 Properties of Error Exponent Functions and Saddle-Point

As we will show in Chapter 11, the quantity  $E_{sp}^{(2)}(R, P)$  plays a important role in the connection between hypothesis testing and channel coding. Moreover, in the last Section 9.1, we observe that the error-exponent functions can be represented as a sup-min formulation. In the following Proposition 9.5 we show that the pair of the optimizers in the error-exponent functions form a saddle-point.

**Proposition 9.5** (Saddle-Point). *Consider a classical-quantum channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$ , any  $R \in (C_{0,\mathcal{W}}, C_{\mathcal{W}})$ , and  $P \in \mathcal{P}(\mathcal{X})$ . Let<sup>a</sup>*

$$\mathcal{S}_{P,\mathcal{W}}(\mathcal{H}) := \{\sigma \in \mathcal{S}(\mathcal{H}) : \forall x \in \text{supp}(P), W_x \not\perp \sigma\}. \quad (9.142)$$

Define

$$F_{R,P}(\alpha, \sigma) := \begin{cases} \frac{1-\alpha}{\alpha} (D_\alpha(\mathcal{W}\|\sigma|P) - R), & \alpha \in (0, 1) \\ 0, & \alpha = 1 \end{cases}, \quad (9.143)$$

on  $(0, 1] \times \mathcal{S}(\mathcal{H})$ , and denote by

$$\mathcal{P}_R(\mathcal{X}) := \left\{ P \in \mathcal{P}(\mathcal{X}) : \sup_{0 < \alpha \leq 1} \inf_{\sigma \in \mathcal{S}(\mathcal{H})} F_{R,P}(\alpha, \sigma) \in \mathbb{R}_{>0} \right\}. \quad (9.144)$$

The following holds

(a) For any  $P \in \mathcal{P}(\mathcal{X})$ ,  $F_{R,P}(\cdot, \cdot)$  has a saddle-point on  $(0, 1] \times \mathcal{S}_{P,\mathcal{W}}(\mathcal{H})$  with the saddle-value:

$$\min_{\sigma \in \mathcal{S}(\mathcal{H})} \sup_{0 < \alpha \leq 1} F_{R,P}(\alpha, \sigma) = \sup_{0 < \alpha \leq 1} \min_{\sigma \in \mathcal{S}(\mathcal{H})} F_{R,P}(\alpha, \sigma) = E_{sp}^{(2)}(R, P). \quad (9.145)$$

(b) Fix  $P \in \mathcal{P}_R(\mathcal{X})$ . Any saddle-point  $(\alpha_{R,P}^*, \sigma_{R,P}^*)$  of  $F_{R,P}(\cdot, \cdot)$  satisfies  $\alpha_{R,P}^* \in (0, 1)$  and

$$\sigma_{R,P}^* \gg W_x, \quad \forall x \in \text{supp}(P). \quad (9.146)$$

(c) For  $P \in \mathcal{P}_R(\mathcal{X})$ , the saddle-point is unique.

(d) For any  $\underline{R} \in (C_{0,\mathcal{W}}, R]$ , both  $\alpha_{r,P}^*$  and  $\sigma_{r,P}^*$  are jointly continuous of  $(r, P)$  on  $[\underline{R}, R] \times \mathcal{P}(\mathcal{X})$ .

---

<sup>a</sup>For  $\alpha \in (0, 1]$ ,  $\mathcal{S}_{P,\mathcal{W}}(\mathcal{H})$  is the *effective domain* of  $F_{R,P}(\alpha, \cdot)$  [131]. Namely,  $F_{R,P}(\alpha, \sigma)$  is finite for all  $\sigma \in \mathcal{S}_{P,\mathcal{W}}(\mathcal{H})$ . Proposition 9.5 then aims to find the saddle-points within its domain  $(0, 1] \times \mathcal{S}_{P,\mathcal{W}}(\mathcal{H})$ . Otherwise, the saddle-point makes no sense.

The proof is provided in Section 9.3.1.

The following Proposition 9.6 discusses the continuity and differentiability of the error-exponent functions. The proof is shown in Section 9.3.2.

**Proposition 9.6** (Properties of Error-Exponent Functions). *Consider a classical-quantum channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  with  $C_{0,\mathcal{W}} < C_{\mathcal{W}}$ . We have*

- (a) *Given every  $P \in \mathcal{P}(\mathcal{X})$ ,  $E_{\text{sp}}^{(2)}(\cdot, P)$  is convex and non-increasing on  $[0, +\infty]$ , and continuous on  $[I_0^{(2)}(P, \mathcal{W}), +\infty]$ . For every  $R > C_{0,\mathcal{W}}$ ,  $E_{\text{sp}}^{(2)}(R, \cdot)$  is continuous on  $\mathcal{P}(\mathcal{X})$ . Further,*

$$E_{\text{sp}}^{(2)}(R, P) = \begin{cases} +\infty, & R < I_0^{(2)}(P, \mathcal{W}) \\ 0, & R \geq I_0^{(2)}(P, \mathcal{W}) \end{cases}. \quad (9.147)$$

- (b)  *$E_{\text{sp}}(\cdot)$  is convex and non-increasing on  $[0, +\infty]$ , and continuous on  $[C_{0,\mathcal{W}}, +\infty]$ . Further,*

$$E_{\text{sp}}(R) = \begin{cases} +\infty, & R < C_{0,\mathcal{W}} \\ 0, & R \geq C_{0,\mathcal{W}} \end{cases}. \quad (9.148)$$

- (c) *Consider any  $R \in (C_{0,\mathcal{W}}, C_{\mathcal{W}})$  and  $P \in \mathcal{P}_R(\mathcal{X})$  (see Eq. (9.144)). The function  $E_{\text{sp}}^{(2)}(\cdot, P)$  is differentiable with*

$$s_{R,P}^{\star} := \frac{1 - \alpha_{R,P}^{\star}}{\alpha_{R,P}^{\star}} = - \left. \frac{\partial E_{\text{sp}}^{(2)}(r, P)}{\partial r} \right|_{r=R} \in \mathbb{R}_{>0}, \quad (9.149)$$

where  $\alpha_{R,P}^{\star}$  is the optimizer in Eq. (9.3). Moreover,

$$I_{\alpha_{R,P}^{\star}}(P, \mathcal{W}) > R. \quad (9.150)$$

Given any  $R \in (R_{\infty}, C_{\mathcal{W}})$  and  $P \in \mathcal{P}_R(\mathcal{X})$ , we denote a *maximum absolute value subgradient* of the sphere-packing exponent at  $R$  by

$$|E'_{\text{sp}}(R)| := \max_{P: E_{\text{sp}}^{(2)}(R, P) = E_{\text{sp}}(R)} s_{R,P}^{\star}. \quad (9.151)$$

Note that the term  $|E'_{\text{sp}}(R)|$  in Eq. (9.151) is well-defined and finite by item (d) in Proposition 9.5.

Figure 9.1 below depicts different cases of the  $E_{\text{sp}}(R)$  over rate  $R$ .

### 9.3.1 Proof of Proposition 9.5

(9.5-(a)) Fix arbitrary  $R > C_{0,\mathcal{W}}$  and  $P \in \mathcal{P}(\mathcal{X})$ . In the following, we prove the existence of a saddle-point of  $F_{R,P}(\cdot, \cdot)$  on  $(0, 1] \times \mathcal{S}_{P,\mathcal{W}}(\mathcal{H})$ . Ref. [131, Lemma 36.2] states that  $(\alpha^{\star}, \sigma^{\star})$  is a saddle point of  $F_{R,P}(\cdot, \cdot)$  if and only if the supremum in

$$\sup_{\alpha \in (0, 1]} \inf_{\sigma \in \mathcal{S}_{P,\mathcal{W}}(\mathcal{H})} F_{R,P}(\alpha, \sigma) \quad (9.152)$$

is attained at  $\alpha^{\star} \in (0, 1]$ , the infimum in

$$\inf_{\sigma \in \mathcal{S}_{P,\mathcal{W}}(\mathcal{H})} \sup_{\alpha \in (0, 1]} F_{R,P}(\alpha, \sigma) \quad (9.153)$$

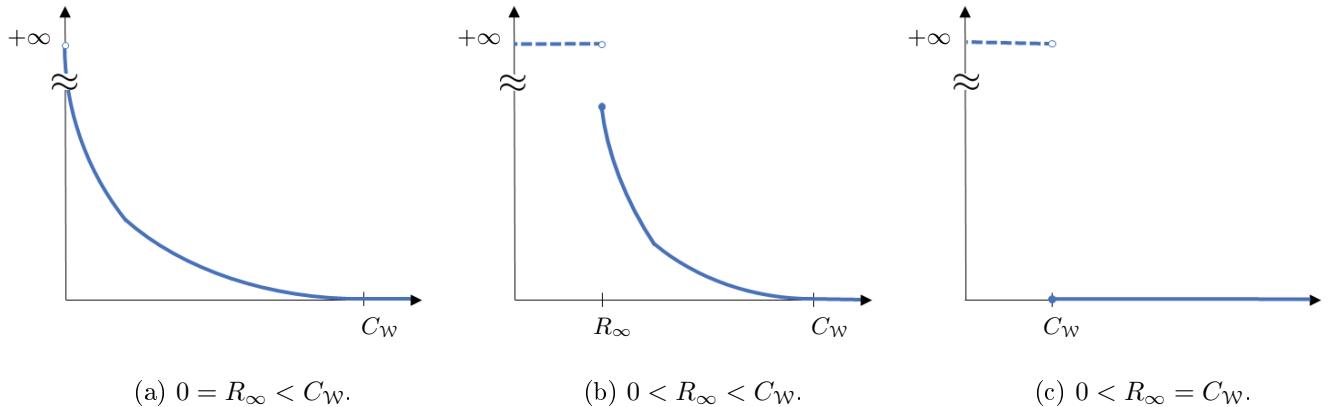


Figure 9.1: This figure illustrates three cases of the strong sphere-packing exponent  $E_{\text{sp}}(R)$  over  $R \geq 0$ . In the first case  $0 = R_\infty < C_W$  (the left figure),  $E_{\text{sp}}(R)$  is only infinite at  $R = 0$  and finite otherwise. In the second case  $0 < R_\infty < C_W$  (the central figure),  $E_{\text{sp}}(R) = +\infty$  for  $R < R_\infty$ , and  $E_{\text{sp}}(R) < +\infty$  for  $R \geq R_\infty$ . In the third case  $0 < R_\infty = C_W$  (the right figure),  $E_{\text{sp}}(R) = +\infty$  for  $R < C_W$ , and  $E_{\text{sp}}(R) = 0$  for  $R \geq C_W$ . Without loss of generality, we assume  $R_\infty < C_W$  to exclude the last case throughout this paper.

is attained at  $\sigma^* \in \mathcal{S}_{P,W}(\mathcal{H})$ , and the two extrema in Eqs. (9.152), (9.153) are equal and finite. We first claim that,  $\forall \alpha \in (0, 1]$ ,

$$\inf_{\sigma \in \mathcal{S}_{P,W}(\mathcal{H})} F_{R,P}(\alpha, \sigma) = \inf_{\sigma \in \mathcal{S}(\mathcal{H})} F_{R,P}(\alpha, \sigma). \quad (9.154)$$

To see this, observe that for any  $\alpha \in (0, 1)$ , Eqs. (3.5) and (3.16) yield

$$\forall \sigma \in \mathcal{S}(\mathcal{H}) \setminus \mathcal{S}_{P,W}(\mathcal{H}), \quad D_\alpha(\mathcal{W} \parallel \sigma | P) = +\infty, \quad (9.155)$$

which, in turn, implies

$$\forall \sigma \in \mathcal{S}(\mathcal{H}) \setminus \mathcal{S}_{P,W}(\mathcal{H}), \quad F_{R,P}(\alpha, \sigma) = +\infty. \quad (9.156)$$

Further, Eq. (9.154) holds trivially when  $\alpha = 1$ . Hence, Eq. (9.154) yields

$$\sup_{\alpha \in (0, 1]} \inf_{\sigma \in \mathcal{S}_{P,W}(\mathcal{H})} F_{R,P}(\alpha, \sigma) = \sup_{\alpha \in (0, 1]} \inf_{\sigma \in \mathcal{S}(\mathcal{H})} F_{R,P}(\alpha, \sigma) \quad (9.157)$$

Owing to the fact  $R > C_{0,W}$  and Eq. (9.3), we have

$$E_{\text{sp}}^{(2)}(R, P) = \sup_{\alpha \in (0, 1]} \inf_{\sigma \in \mathcal{S}(\mathcal{H})} F_{R,P}(\alpha, \sigma) < +\infty, \quad (9.158)$$

which guarantees the supremum in the right-hand side of Eq. (9.158) is attained at some  $\alpha \in (0, 1]$ . Namely, there exists some  $\bar{\alpha}_{R,P} \in (0, 1]$  such that

$$\sup_{\alpha \in (0, 1]} \inf_{\sigma \in \mathcal{S}_{P,W}(\mathcal{H})} F_{R,P}(\alpha, \sigma) = \max_{\alpha \in [\bar{\alpha}_{R,P}, 1]} \inf_{\sigma \in \mathcal{S}(\mathcal{H})} F_{R,P}(\alpha, \sigma) < +\infty. \quad (9.159)$$

Thus, we complete our claim in Eq. (9.152). It remains to show that the infimum in Eq.(9.153) is attained at some  $\sigma^* \in \mathcal{S}_{P,W}(\mathcal{H})$  and the supremum and infimum are exchangeable. To achieve this, we will show that  $([\bar{\alpha}_{R,P}, 1], \mathcal{S}_{P,W}(\mathcal{H}), F_{R,P})$  is a closed saddle-element (see Definition 9.1 below) and employ the boundness of  $[\bar{\alpha}_{R,P}, 1] \times \mathcal{S}_{P,W}(\mathcal{H})$  to conclude our claim.

**Definition 9.1** (Closed Saddle-Element [130]). We denote by  $\text{ri}$  and  $\text{cl}$  the relative interior and the closure of a set, respectively. Let  $\mathcal{A}, \mathcal{B}$  be subsets of a real vector space, and  $F : \mathcal{A} \times \mathcal{B} \rightarrow \mathbb{R} \cup \{\pm\infty\}$ . The triple  $(\mathcal{A}, \mathcal{B}, F)$  is called a closed saddle-element if for any  $x \in \text{ri}(\mathcal{A})$  (resp.  $y \in \text{ri}(\mathcal{B})$ ),

- (i)  $\mathcal{B}$  (resp.  $\mathcal{A}$ ) is convex.
- (ii)  $F(x, \cdot)$  (resp.  $F(\cdot, y)$ ) is convex (resp. concave) and lower (resp. upper) semi-continuous.
- (iii) Any accumulation point of  $\mathcal{B}$  (resp.  $\mathcal{A}$ ) that does not belong to  $\mathcal{B}$  (resp.  $\mathcal{A}$ ), say  $y_o$  (resp.  $x_o$ ) satisfies  $\lim_{y \rightarrow y_o} F(x, y) = +\infty$  (resp.  $\lim_{x \rightarrow x_o} F(x, y) = -\infty$ ).

Fix an arbitrary  $\alpha \in \text{ri}([\bar{\alpha}_{R,P}, 1]) = (\bar{\alpha}_{R,P}, 1)$ . We check that  $(\mathcal{S}_{P,W}(\mathcal{H}), F_{R,P}(\alpha, \cdot))$  fulfills the three items in Definition 9.1. (i) The set  $\mathcal{S}_{P,W}(\mathcal{H})$  is clearly convex. (ii) Recall Lemma 3.2-(c) that  $\sigma \mapsto D_\alpha(W_x \|\sigma)$  is convex and lower semi-continuous. Since convex combination preservers the convexity and the lower semi-continuity, Eq. (9.143) yields that  $\sigma \mapsto F_{R,P}(\alpha, \sigma)$  is convex and lower semi-continuous on  $\mathcal{S}_{P,W}(\mathcal{H})$ . (iii) Due to the compactness of  $\mathcal{S}(\mathcal{H})$ , any accumulation point of  $\mathcal{S}_{P,W}(\mathcal{H})$  that does not belong to  $\mathcal{S}_{P,W}(\mathcal{H})$ , say  $\sigma_o$ , satisfies  $\sigma_o \in \mathcal{S}(\mathcal{H}) \setminus \mathcal{S}_{P,W}(\mathcal{H})$ . Eqs. (9.155) and (9.156) then show that  $F_{R,P}(\alpha, \sigma_o) = +\infty$ .

Next, fix an arbitrary  $\sigma \in \text{ri}(\mathcal{S}_{P,W}(\mathcal{H}))$ . Owing to the convexity of  $\mathcal{S}_{P,W}(\mathcal{H})$ , it follows that  $\text{ri}(\mathcal{S}_{P,W}(\mathcal{H})) = \text{ri}(\text{cl}(\mathcal{S}_{P,W}(\mathcal{H})))$  (see e.g. [131, Theorem 6.3]). We first claim  $\text{cl}(\mathcal{S}_{P,W}(\mathcal{H})) = \mathcal{S}(\mathcal{H})$ . To see this, observe that  $\mathcal{S}_{>0}(\mathcal{H}) \subseteq \mathcal{S}_{P,W}(\mathcal{H})$  since a full-rank density operator is not orthogonal with every  $W_x$ ,  $x \in \mathcal{X}$ . Hence,

$$\mathcal{S}(\mathcal{H}) = \text{cl}(\mathcal{S}_{>0}(\mathcal{H})) \subseteq \text{cl}(\mathcal{S}_{P,W}(\mathcal{H})). \quad (9.160)$$

On the other hand, the fact  $\mathcal{S}_{P,W}(\mathcal{H}) \subseteq \mathcal{S}(\mathcal{H})$  leads to

$$\text{cl}(\mathcal{S}_{P,W}(\mathcal{H})) \subseteq \text{cl}(\mathcal{S}(\mathcal{H})) = \mathcal{S}(\mathcal{H}). \quad (9.161)$$

By Eqs. (9.160) and (9.161), we deduce that

$$\text{ri}(\mathcal{S}_{P,W}(\mathcal{H})) = \text{ri}(\text{cl}(\mathcal{S}_{P,W}(\mathcal{H}))) = \text{ri}(\mathcal{S}(\mathcal{H})) = \mathcal{S}_{>0}(\mathcal{H}), \quad (9.162)$$

where the last equality in Eq. (9.162) follows from [132, Proposition 2.9]. Hence, we obtain

$$\forall \sigma \in \text{ri}(\mathcal{S}_{P,W}(\mathcal{H})) \quad \text{and} \quad \forall x \in \mathcal{X}, \quad \sigma \gg W_x. \quad (9.163)$$

Now we verify that  $([\bar{\alpha}_{R,P}, 1], F_{R,P}(\cdot, \sigma))$  satisfies the three items in Definition 9.1. Fix an arbitrary  $\sigma \in \text{ri}(\mathcal{S}_{P,W}(\mathcal{H}))$ . (i) The set  $(0, 1]$  is obviously convex. (ii) From Lemma 3.2-(a), the map  $\alpha \mapsto F_{R,P}(\alpha, \sigma)$  is continuous on  $(0, 1)$ . Further, it is not hard to verify that

$F_{R,P}(1, \sigma) = 0 = \lim_{\alpha \uparrow 1} F_{R,P}(\alpha, \sigma)$  from Eqs. (9.163), (9.143), and (3.5). Item (d) in Proposition 3.2 and [59, Corollary B.2] implies that  $\alpha \mapsto F_{R,P}(\alpha, \sigma)$  on  $[\bar{\alpha}_R, 1]$  is concave. Moreover, the continuity of  $\alpha \mapsto F_{R,P}(\alpha, \sigma)$  on  $[\bar{\alpha}_{R,P}, 1]$  guarantees the concavity of  $\alpha \mapsto F_{R,P}(\alpha, \sigma)$  on  $[\bar{\alpha}_{R,P}, 1]$ . (iii) Since  $[\bar{\alpha}_{R,P}, 1]$  is closed, there is no accumulation point of  $[\bar{\alpha}_{R,P}, 1]$  that does not belong to  $[\bar{\alpha}_{R,P}, 1]$ .

We are at the position to prove item (a) of Proposition 9.5. The closed saddle-element, along with the boundness of  $\mathcal{S}_{P,W}(\mathcal{H})$  and Rockafellar's saddle-point result [130, Theorem 8], [131, Theorem 37.3] imply that

$$-\infty < \sup_{\alpha \in [\bar{\alpha}_{R,P}, 1]} \inf_{\sigma \in \mathcal{S}_{P,W}(\mathcal{H})} F_{R,P}(s, \sigma) = \min_{\sigma \in \mathcal{S}_{P,W}(\mathcal{H})} \sup_{\alpha \in [\bar{\alpha}_{R,P}, 1]} F_{R,P}(s, \sigma). \quad (9.164)$$

Then Eqs. (9.159) and (9.164) lead to the existence of a saddle-point of  $F_{R,P}(\cdot, \cdot)$  on  $(0, 1] \times \mathcal{S}_{P,W}(\mathcal{H})$ . Hence, item (a) is proved.

(9.5-(b)) Fix arbitrary  $R \in (C_{0,W}, C_W)$  and  $P \in \mathcal{P}_R(\mathcal{X})$ . We have

$$\sup_{0 < \alpha \leq 1} \min_{\sigma \in \mathcal{S}(\mathcal{H})} F_{R,P}(\alpha, \sigma) = \min_{\sigma \in \mathcal{S}(\mathcal{H})} \sup_{0 < \alpha \leq 1} F_{R,P}(\alpha, \sigma) \in \mathbb{R}_{>0} \quad (9.165)$$

by the saddle-point property in item (a) and the definition of  $\mathcal{P}_R(\mathcal{X})$  given in Eq. (9.144). First note that  $(1, \sigma)$  for any  $\sigma \in \mathcal{S}(\mathcal{H})$  will not be a saddle point of  $F_{R,P}(\cdot, \cdot)$  because  $F_{R,P}(1, \sigma) = 0, \forall \sigma \in \mathcal{S}(\mathcal{H})$ , contradicting Eq. (9.165).

Next, we assume  $(\alpha^*, \sigma^*)$  is a saddle-point of  $F_{R,P}(\cdot, \cdot)$  with  $\alpha^* \in (0, 1)$ , it holds that

$$F_{R,P}(\alpha^*, \sigma^*) = \min_{\sigma \in \mathcal{S}(\mathcal{H})} F_{R,P}(\alpha^*, \sigma) = \frac{\alpha^* - 1}{\alpha^*} R + \frac{1 - \alpha^*}{\alpha^*} \min_{\sigma \in \mathcal{S}(\mathcal{H})} D_{\alpha^*}(\mathcal{W} \parallel \sigma | P). \quad (9.166)$$

Since  $\sigma^*$  is the minimizer of  $\min_{\sigma \in \mathcal{S}(\mathcal{H})} D_{\alpha^*}(\mathcal{W} \parallel \sigma | P)$ , it is clear from Proposition 3.2-(b) that

$$\sigma^* \gg W_x, \quad \forall x \in \text{supp}(P), \quad (9.167)$$

and thus item (b) is proved.

(9.5-(c)) Continuing from item (b), we show the uniqueness of the saddle-point. Since  $(1, \sigma)$  for  $\sigma \in \mathcal{S}(\mathcal{H})$  will not be a saddle-point of  $F_{R,P}(\cdot, \cdot)$  as shown in item (b), we let  $\alpha^* \in (0, 1)$  attain the supremum in the left-hand side of Eq. (9.165). Proposition 3.2-(b) implies that the minimizer to the map  $\sigma \mapsto D_{\alpha^*}(\mathcal{W} \parallel \sigma | P)$  is unique, and thus it follows that the minimizer of Eq. (9.165) is unique as well.

Next, we will invoke Lemma 2.13 in Section 2.2 to show the uniqueness of the maximizer. Let  $\sigma^* \in \mathcal{S}(\mathcal{H})$  be the minimizer of right-hand side of the equality in Eq. (9.165), and let  $\mathbf{x}^n \in \mathcal{X}^n$  be an arbitrary sequence with an empirical distribution  $P$ . Denote by  $p^n, q^n$  be two distributions with  $(p_i, q_i)$  being the Nussbaum-Szkoła mapping of  $(W_{x_i}, \sigma^*)$ , where  $x_i$  is the  $i$ -th symbol of  $\mathbf{x}^n$  for  $i \in [n]$ . Further, item (b) guarantees that  $p^n \ll q^n$ .

Now, we let  $p^n$  and  $q^n$  to be the hypotheses described in Eq. (2.26). It is not hard to observe that  $\sup_{0 < \alpha \leq 1} F_{R,P}(\alpha, \sigma^*) = \phi_n(R)$  given in Eq. (2.27). Items (b) and (d) in Lemma 2.13 then

show that the optimizer  $\alpha^* \in (0, 1)$  of  $\sup_{0 < \alpha \leq 1} F_{R,P}(\alpha, \sigma^*)$  is unique, which completes the proof of item (c).

- (9.5-(d)) We first prove the joint continuity of  $(r, P) \mapsto \alpha_{r,P}^*$  on  $[\underline{R}, R] \times \mathcal{P}(\mathcal{X})$ . To that end, it suffices to show that  $P \mapsto \alpha_{r,P}^*$  is continuous on  $\mathcal{P}(\mathcal{X})$  for every  $r \in [\underline{R}, R]$ , and the family  $\{\alpha_{r,P}^*\}_{P \in \mathcal{P}(\mathcal{X})}$  is uniformly equicontinuous in  $r$  on  $[\underline{R}, R]$ . Moreover, it is equivalent to prove the joint continuity of  $(r, P) \mapsto s_{r,P}^*$  on  $[\underline{R}, R] \times \mathcal{P}(\mathcal{X})$  by using the substitution  $s_{r,P}^* := (1 - \alpha_{r,P}^*)/\alpha_{r,P}^*$ . This will ease the burden of notation.

In the following, we show the continuity of  $P \mapsto s_{r,P}^*$ . The proof idea of such continuity is similar to [98, Proposition 3.4]. Fix  $r \in [\underline{R}, R]$ , any  $P_0 \in \mathcal{P}(\mathcal{X})$  and consider arbitrary  $\{P_k\}_{k \in \mathbb{N}}$  such that  $P_k \in \mathcal{P}(\mathcal{X})$  for all  $k \in \mathbb{N}$ , and  $\lim_{n \rightarrow +\infty} P_k = P_0$ . Following from Proposition 9.6-(c) that will be proved later in Section 9.3.2, we have<sup>2</sup>

$$s_{r,P_k}^* = -\frac{\partial E_{\text{sp}}^{(2)}(r, P_k)}{\partial r} \in \mathbb{R}_{\geq 0}. \quad (9.168)$$

Since  $r \geq \underline{R} > C_{0,W}$ , the continuity of  $E_{\text{sp}}^{(2)}(r, \cdot)$  given in Proposition 9.6-(a) that will be proved later shows that

$$\lim_{k \rightarrow +\infty} E_{\text{sp}}^{(2)}(r, P_k) = E_{\text{sp}}^{(2)}(r, P_0). \quad (9.169)$$

Viewing  $(E_{\text{sp}}^{(2)}(r, P_k))_{k \in \mathbb{N}}$  as a sequence of functions that converges to  $E_{\text{sp}}^{(2)}(r, P_0)$ , Ref. [142, Corollary VI.6.2.8] proved that the sequence of first-order derivatives of differentiable convex functions converges to the first-order derivative of the limit. Indeed, Proposition 9.6-(a) guarantees that  $E_{\text{sp}}^{(2)}(\cdot, P)$  is convex. Therefore,

$$\lim_{k \rightarrow +\infty} s_{r,P_k}^* = \lim_{k \rightarrow +\infty} -\frac{\partial E_{\text{sp}}^{(2)}(r, P_k)}{\partial r} \Big|_{r=R} = -\frac{\partial E_{\text{sp}}^{(2)}(r, P_0)}{\partial r} \Big|_{r=R} = s_{R,P_0}^*, \quad (9.170)$$

which shows the continuity of  $P \mapsto s_{r,P}^*$  for every  $r \in [\underline{R}, R]$ .

Next, we prove the equicontinuity. Let  $R_1, R_2 \in [\underline{R}, R]$  be arbitrary. As will be shown later in Proposition 9.6-(a), for every  $P \in \mathcal{P}(\mathcal{X})$ ,  $E_{\text{sp}}^{(2)}(\cdot, P)$  is convex and non-increasing on  $[0, +\infty]$ . Using Eq. (9.168), the absolute value of the difference between the first-order derivative of  $E_{\text{sp}}^{(2)}(\cdot, P)$  at  $R_1$  and  $R_2$  can be calculated as follows

$$|s_{R_1,P}^* - s_{R_2,P}^*| \leq s_{R_1,P}^* \vee s_{R_2,P}^* = s_{R_1 \wedge R_2, W}^* \leq s_{\underline{R}, W}^*, \quad (9.171)$$

where  $s_{\underline{R}, P}^* = (1 - \alpha_{\underline{R}, P}^*)/\alpha_{\underline{R}, P}^*$  and  $\alpha_{\underline{R}, P}^*$  is the optimizer of  $E_{\text{sp}}^{(2)}(\underline{R}, P)$  given in Eq. (9.3).

For all  $P \in \mathcal{P}(\mathcal{X})$  such that  $\underline{R} \geq I_1(P, W)$ , the right-hand side of Eq. (9.171) is zero since  $E_{\text{sp}}^{(2)}(\underline{R}, P) = 0$  (see Proposition 9.6-(a) again). On the other hand, for all  $P \in \mathcal{P}(\mathcal{X})$  such that  $\underline{R} < I_1(P, W)$ , Proposition 9.6-(c) shows that

$$I_{\alpha_{\underline{R}, P}^*}^{(2)}(P, W) > \underline{R}. \quad (9.172)$$

---

<sup>2</sup>Here, for  $E_{\text{sp}}^{(2)}(r, P) = 0$ , we adopt  $(1, PW)$  as the saddle-point in Eq. (9.143), which means  $s_{r,P}^* = 0$ .

Further, since  $\underline{R} \in (C_{0,W}, C_{1,W})$ , the continuous monotone increase of the map  $\alpha \mapsto C_{\alpha,W}$  proved in Proposition 3.2-(h) guarantees that there exists a  $\alpha_{\underline{R}} \in (0, 1)$  such that

$$C_{\alpha_{\underline{R}}} = \underline{R}. \quad (9.173)$$

Then, from Eqs. (9.172), (9.173), and the definition of the Rényi information radius given in Eq. (3.42), we have

$$I_{\alpha_{\underline{R}}}^{(2)}(P, \mathcal{W}) \leq C_{\underline{R}, W} = \underline{R} < I_{\alpha_{\underline{R}, P}^*}^{(2)}(P, \mathcal{W}), \quad (9.174)$$

The above inequality (9.174) and the monotone increases of the map  $\alpha \mapsto I_{\alpha}^{(2)}(P, \mathcal{W})$  further imply that

$$\alpha_{\underline{R}} < \alpha_{\underline{R}, P}^*. \quad (9.175)$$

Both Eqs. (9.171) and (9.175) then yield

$$|s_{R_1, P}^* - s_{R_2, P}^*| \leq \frac{1 - \alpha_{\underline{R}}}{\alpha_{\underline{R}}} < \infty \quad (9.176)$$

for all  $P \in \mathcal{P}(\mathcal{X})$  such that  $\underline{R} < I_1(P, \mathcal{W})$ . This shows the equicontinuity of the family  $\{\alpha_{r, P}^*\}_{P \in \mathcal{P}(\mathcal{X})}$  on  $[\underline{R}, R]$ . Together with the continuity of  $P \mapsto s_{r, P}^*$  for all  $r \in [\underline{R}, R]$ , the joint continuity of  $(r, P) \mapsto s_{r, P}^*$  on  $[\underline{R}, R] \times \mathcal{P}(\mathcal{X})$  is proved.

Lastly, we move on to prove the continuity of  $(r, P) \mapsto \sigma_{r, P}^*$  on  $[\underline{R}, R] \times \mathcal{P}(\mathcal{X})$ . Let  $(R_k, P_k) \in [\underline{R}, R] \times \mathcal{P}(\mathcal{X})$  for all  $k \in \mathbb{N}$  be arbitrary such that  $\lim_{k \in \mathbb{N}} (R_k, P_k) = (R_0, P_0) \in [\underline{R}, R] \times \mathcal{P}(\mathcal{X})$ . From Eq. (9.166), the saddle-point property yields that

$$\sigma_{R_k, P_k}^* = \sigma_{\alpha_{R_k, P_k}^*, P_k}, \quad (9.177)$$

where in the right-hand side of the above equality we denote the Augustin mean by  $\sigma_{\alpha, P} := \min_{\sigma \in \mathcal{S}(\mathcal{H})} D_{\alpha}(\mathcal{W} \parallel \sigma | P)$ . Moreover, Proposition 3.2-(g) states that  $(\alpha, P) \mapsto \sigma_{\alpha, P}$  is jointly continuous on  $(0, 1] \times \mathcal{P}(\mathcal{X})$ . Hence, the joint continuity of  $(r, P) \mapsto \alpha_{r, P}^*$  proved above together with Eq. (9.177) show that

$$\lim_{k \rightarrow +\infty} \sigma_{R_k, P_k}^* = \lim_{k \rightarrow +\infty} \sigma_{\alpha_{R_k, P_k}^*, P_k} \quad (9.178)$$

$$= \sigma_{\lim_{k \rightarrow +\infty} \alpha_{R_k, P_k}^*, \lim_{k \rightarrow +\infty} P_k} \quad (9.179)$$

$$= \sigma_{\alpha_{\lim_{k \rightarrow +\infty} (R_k, P_k)}^*, \lim_{k \rightarrow +\infty} P_k} \quad (9.180)$$

$$= \sigma_{\alpha_{R_0, P_0}^*, P_0} \quad (9.181)$$

$$= \sigma_{R_0, P_0}^*, \quad (9.182)$$

which completes the proof of item (d). □

### 9.3.2 Proof of Proposition 9.6

(9.6-(a)) Fix any arbitrary  $P \in \mathcal{P}(\mathcal{X})$ . Item (a) in Proposition 3.2 shows that the map  $\alpha \mapsto I_\alpha^{(2)}(P, \mathcal{W})$  is monotone increasing on  $[0, 1]$ . Hence, from the definition in Eq. (9.3), it is not hard to verify that  $E_{\text{sp}}^{(2)}(R, P) = +\infty$  for all  $R \in (0, I_0^{(2)}(P, \mathcal{W}))$ ; finite for all  $R > I_0^{(2)}(P, \mathcal{W})$ ; and  $E_{\text{sp}}^{(2)}(R, P) = 0$ , for all  $R \geq I_1^{(2)}(P, \mathcal{W})$ .

For every  $\alpha \in (0, 1]$ , the function  $\frac{1-\alpha}{\alpha}(I_\alpha^{(2)}(P, \mathcal{W}) - R)$  in Eq. (9.3) is a non-increasing, convex, and continuous function in  $R \in \mathbb{R}_{>0}$ . Since  $E_{\text{sp}}^{(2)}(R, P)$  is the pointwise supremum of the above function,  $E_{\text{sp}}^{(2)}(R, P)$  is non-increasing, convex, and lower semi-continuous function for all  $R \geq 0$ . Furthermore, since a convex function is continuous on the interior of the interval if it is finite [117, Corollary 6.3.3], thus  $E_{\text{sp}}^{(2)}(R, P)$  is continuous for all  $R > I_0^{(2)}(P, \mathcal{W})$ , and continuous from the right at  $R = I_0^{(2)}(P, \mathcal{W})$ .

To establish the continuity of  $E_{\text{sp}}^{(2)}(R, P)$  in  $P \in \mathcal{P}(\mathcal{X})$ , we first claim that there exists some  $\bar{\alpha}_R \in (0, 1]$  such that for every  $P \in \mathcal{P}(\mathcal{X})$ ,

$$\sup_{\alpha \in (0, 1]} \frac{1-\alpha}{\alpha} (I_\alpha^{(2)}(P, \mathcal{W}) - R) = \sup_{\alpha \in [\bar{\alpha}_R, 1]} \frac{1-\alpha}{\alpha} (I_\alpha^{(2)}(P, \mathcal{W}) - R). \quad (9.183)$$

Recall that  $R > C_{0,\mathcal{W}} = \max_{P \in \mathcal{P}(\mathcal{X})} I_0^{(2)}(P, \mathcal{W})$ . The continuity, item (h) in Proposition 3.2, implies that there exists an  $\bar{\alpha}_R > 0$  such that

$$R \geq I_{\bar{\alpha}_R}^{(2)}(P, \mathcal{W}), \quad \forall P \in \mathcal{P}(\mathcal{X}). \quad (9.184)$$

Then, Eq. (9.184) and the monotone increases of the map  $\alpha \mapsto I_\alpha^{(2)}(P, \mathcal{W})$  yield that,

$$\frac{1-\alpha}{\alpha} (I_\alpha^{(2)}(P, \mathcal{W}) - R) < 0, \quad \forall P \in \mathcal{P}(\mathcal{X}), \text{ and } \alpha \in (0, \bar{\alpha}_R). \quad (9.185)$$

The non-negativity of  $E_{\text{sp}}^{(2)}(R, P) \geq 0$  ensures that the maximizer  $\alpha^*$  will not happen in the region  $(0, \bar{\alpha}_R)$ , and thus Eq. (9.183) is evident. Finally, Berge's maximum theorem [118, Section IV.3], [119, Lemma 3.1], the compactness of  $[\bar{\alpha}_R, 1]$ , and item (f) in Proposition 3.2 complete our claim:

$$P \mapsto E_{\text{sp}}^{(2)}(R, P) = \sup_{\alpha \in [\bar{\alpha}_R, 1]} \frac{1-\alpha}{\alpha} (I_\alpha^{(2)}(P, \mathcal{W}) - R) \text{ is continuous on } \mathcal{P}(\mathcal{X}). \quad (9.186)$$

(9.6-(b)) The statement follows since item (a) holds for any  $P \in \mathcal{P}(\mathcal{X})$  and we invoke the definition of  $C_{\alpha,\mathcal{W}}$  in Eq. (3.42).

(9.6-(c)) For any  $R \in (C_{0,\mathcal{W}}, C_{\mathcal{W}})$  and  $P \in \mathcal{P}_R(\mathcal{X})$ , item (c) in Proposition 9.5 shows that the optimizer  $\alpha_{R,P}^*$  is unique. Eq. (9.149) directly follows from item (d) in Lemma 2.13 in Section 2.2.

The saddle-point property in Proposition 9.5-(a) shows that

$$E_{\text{sp}}^{(2)}(R, P) = \frac{1 - \alpha_{R,P}^*}{\alpha_{R,P}^*} (I_{\alpha_{R,P}^*}^{(2)}(P, \mathcal{W}) - R). \quad (9.187)$$

Further, since  $E_{\text{sp}}^{(2)}(R, P) > 0$  and  $\alpha_{R,P}^* \in (0, 1)$  for  $P \in \mathcal{P}_R(\mathcal{X})$ , the above equality implies Eq. (9.150).

□

## Chapter 10

# Achievability (Channel Coding)

In the error exponent regime (i.e. large deviation regime), the achievability for channel coding means that, given a fixed transmission rate, there exists a coding strategy such that its error probability is upper bounded by a certain exponential decay, i.e.

$$\forall R < C_{\mathcal{W}}, \exists \mathcal{C}_n, E(R) > 0 \text{ such that } \varepsilon^*(n, R) \leq \varepsilon(\mathcal{C}_n) \leq \exp\{-nE(R) + o(n)\}. \quad (10.1)$$

To show such bounds, it is convenient to employ a *random coding argument*. In other words, the codewords  $\mathbf{x}^n$  are randomly chosen from some ensembles. If one can show that the average error probability over the ensemble achieves the desired upper bound, a good code thus exists. There are at least two useful ensembles for the random codes. The first one is the i.i.d. ensemble, where the  $n$ -blocklength codewords are i.i.d. generated from some probability distribution on the input alphabet, i.e.

$$\Pr(\mathbf{x}^n) = \prod_{i=1}^n P(x_i), \quad \text{for some } P \in \mathcal{P}(\mathcal{X}). \quad (10.2)$$

The second one is the constant composition ensemble, where the codewords are uniformly generated from some type class, i.e.

$$\Pr(\mathbf{x}^n) = \frac{1}{|T_P^n|} \mathbf{1}_{\mathbf{x}^n \in T_P^n}, \quad \text{for some } P \in \mathcal{P}_n(\mathcal{X}). \quad (10.3)$$

In the classical scenario, the achievable exponent for the i.i.d. ensemble was proved by Fano [24] and Gallager [30, 23] (see also [143, 144, 145]) in terms of the entropic exponent function defined via Rényi information:

$$E_r^{(1)}(R, P) = \sup_{\frac{1}{2} \leq \alpha \leq 1} \frac{1-\alpha}{\alpha} \left( I_\alpha^{(1)}(P, \mathcal{W} - R) \right). \quad (10.4)$$

On the other hand, the case for the i.i.d. ensemble was proved by Csiszár and Körner [136, 27], and Gallager [135] (see also [143, 144, 146]) in terms of the entropic exponent function defined via Augustin

information:

$$E_r^{(2)}(R, P) = \sup_{\frac{1}{2} \leq \alpha \leq 1} \frac{1-\alpha}{\alpha} \left( I_\alpha^{(2)}(P, \mathcal{W} - R) \right). \quad (10.5)$$

Jensen's inequality implies that the one with Augustin information is stronger  $E_r^{(1)}(R, P) \leq E_r^{(2)}(R, P)$ . Nevertheless, the two quantities coincide after optimizing the prior distribution, i.e.

$$E_r(R) = \sup_{\frac{1}{2} \leq \alpha \leq 1} \frac{1-\alpha}{\alpha} (C_{\alpha, \mathcal{W}} - R) = \sup_{P \in \mathcal{P}(\mathcal{X})} E_r^{(1)}(R, P) = \sup_{P \in \mathcal{P}(\mathcal{X})} E_r^{(2)}(R, P). \quad (10.6)$$

To our best knowledge, the exponents either  $E_r^{(1)}(R, P)$  or  $E_r^{(2)}(R, P)$  are not achievable in classical-quantum channel coding. The best result to date are the suboptimal quantity  $E_r^{(1), \downarrow}(R, P)$  proved by [94, 139], and  $E_r^{(2), \downarrow}(R, P)$  established by us. In the following Sections 10.1 and 10.2, we discuss the classical-quantum channel coding for the i.i.d. ensemble and constant composition ensemble, respectively.

## 10.1 Random Codes with I.I.D. Ensemble

The finite blocklength achievability bound for classical-quantum (c-q) channel exponent was first studied by Burnashev and Holevo [35, 2]. They introduced the following random coding exponent  $E_r(R)$  and the auxiliary function  $E_0(s, P)$  (see also Eqs. (9.2) and (9.4)):

$$E_r(R) = \sup_{0 \leq s \leq 1} \sup_{P \in \mathcal{P}(\mathcal{X})} \left\{ E_0^{(1)}(s, P) - sR \right\}; \quad (10.7)$$

$$E_0^{(1)}(s, P) = -\log \text{Tr} \left[ \left( \sum_{x \in \mathcal{X}} P(x) W_x^{\frac{1}{1+s}} \right)^{1+s} \right]. \quad (10.8)$$

By quantum Sibson's identity given in Lemma 3.3, it is easy to show that the random coding exponent can be expressed the Rényi capacity with Petz's version (see Eqs. (3.42) and (3.5)):

$$E_r(R) = \sup_{\frac{1}{2} \leq \alpha \leq 1} \frac{1-\alpha}{\alpha} (C_{\alpha, \mathcal{W}} - R). \quad (10.9)$$

Further, they showed that [35, 2] for pure-state c-q channels (i.e. the channel outputs are all rank-one density operators), there exists a random coding strategy and some decoder (POVM) such that the average error probability over the ensemble, denoted by  $\mathsf{P}_e(n, R)$ , can be upper bounded as

$$\mathsf{P}_e(n, R) \leq 4 \exp\{-nE_r(R)\}, \quad \forall R < C_{\mathcal{W}}, n \in \mathbb{N}. \quad (10.10)$$

However, for general c-q channels (i.e. the channel outputs are possibly non-rank-one density operators), the random coding bound by the exponent function in Eq. (10.9) is still open.

The slightly weaker achievability bound was later proven by Hayashi [93, 94, 147]:

$$\mathsf{P}_e(n, R) \leq 4 \exp\{-nE_r^{(1), \downarrow}(R, P)\}, \quad , n \in \mathbb{N}, \quad (10.11)$$

where  $P$  is the distribution of the i.i.d. ensemble. The above bound holds for all c-q channels. However, it can be shown that

$$E_r^{\downarrow,(1)}(R, P) \leq E_r^{(1)}(R, P), \quad \forall P \in \mathcal{P}(\mathcal{X}). \quad (10.12)$$

Recently, Dalai [139] proposed a method to prove Eqs. (10.9) and (10.11). For the sake of completeness, we provide the proof below.

**Theorem 10.1** (Dalai [139]). *Given any classical-quantum channels  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$ , and any random codes with size  $M$  and distribution  $P \in \mathcal{P}(\mathcal{X})$ , we have the one-shot bound:*

$$P_e(1, \log M) \leq 6(M-1)^s \exp \left\{ -E_0^{\downarrow}(s, P) \right\}, \quad \forall s \in [0, 1]. \quad (10.13)$$

Let the transmission rate be  $R := \frac{1}{n} \log M < C_{\mathcal{W}}$ . The  $n$ -shot bound is

$$P_e(n, R) \leq 6 \exp \left\{ -nE_r^{\downarrow}(R, P) \right\}, \quad \forall n \in \mathbb{N}. \quad (10.14)$$

For pure-state classical-quantum channels,

$$P_e(1, \log M) \leq 6(M-1)^s \exp \left\{ -E_0(s, P) \right\}, \quad \forall s \in [0, 1]. \quad (10.15)$$

*Proof of Theorem 10.1.* Assume the channel output of a random code is  $\{W_{x_1}, \dots, W_{x_M}\}$  where  $x_i$  has an i.i.d.  $P(x_i)$ . Construct a POVM  $\{\Pi_{x_i}\}_{i \in [M]}$  by

$$\Pi_{x_i} := \left( \sum_j \pi_{x_j} \right)^{-\frac{1}{2}} \pi_{x_i} \left( \sum_j \pi_{x_j} \right)^{-\frac{1}{2}}, \quad (10.16)$$

where

$$\pi_{x_i} := \left\{ W_{x_i}^{\alpha s} - \left( \sum_{j \neq i} W_{x_j}^{\alpha} \right)^s > 0 \right\}, \quad \alpha \in (0, 1], s \in (0, 1]. \quad (10.17)$$

Using Hayashi-Nagaoka inequality, Lemma 2.9, we have

$$\mathbb{1} - \Pi_{x_i} \leq 2(\mathbb{1} - \pi_{x_i}) + 4 \sum_{j \neq i} \pi_{x_j}. \quad (10.18)$$

Hence, the average probability of error given realizations  $(x_1, \dots, x_M)$  can be upper bounded as

$$\Pr \{ \text{error} | (x_1, \dots, x_M) \} = \frac{1}{M} \text{Tr} [W_{x_i} (\mathbb{1} - \Pi_{x_i})] \quad (10.19)$$

$$\begin{aligned} &\leq 2 \frac{1}{M} \sum_i \text{Tr} \left[ W_{x_i} \left\{ W_{x_i}^{\alpha s} - \left( \sum_{j \neq i} W_{x_j}^{\alpha} \right)^s \leq 0 \right\} \right] \\ &\quad + 2 \frac{1}{M} \sum_i \text{Tr} \left[ W_{x_i} \left\{ W_{x_i}^{\alpha s} - \left( \sum_{j \neq i} W_{x_j}^{\alpha} \right)^s > 0 \right\} \right]. \end{aligned} \quad (10.20)$$

For  $0 < \alpha \leq 1$  and  $0 < s \leq 1$ , using 2.10 to bound the first term in Eq. (10.20) as

$$\mathrm{Tr} \left[ W_{x_i} \left\{ W_{x_i}^{\alpha s} - \left( \sum_{j \neq i} W_{x_j}^\alpha \right)^s \leq 0 \right\} \right] \leq \mathrm{Tr} \left[ W_{x_i}^{1-\alpha s} \left( \sum_{j \neq i} W_{x_j}^\alpha \right)^s \right]. \quad (10.21)$$

Recalling the operator concavity of  $u \mapsto u^s$ , we take expectation of the random code to obtain

$$2\mathbb{E} \mathrm{Tr} \left[ W_{x_i}^{1-\alpha s} \left( \sum_{j \neq i} W_{x_j}^\alpha \right)^s \right] = 2 \mathrm{Tr} \left[ \mathbb{E}_x [W_x^{1-\alpha s}] \mathbb{E} \left[ \left( \sum_{j \neq i} W_{x_j}^\alpha \right)^s \right] \right] \quad (10.22)$$

$$\leq 2 \mathrm{Tr} \left[ \mathbb{E}_x [W_x^{1-\alpha s}] \left( \mathbb{E} \left[ \sum_{j \neq i} W_{x_j}^\alpha \right] \right)^s \right] \quad (10.23)$$

$$= 2(M-1)^s \mathrm{Tr} [\mathbb{E}_x [W_x^{1-\alpha s}] \mathbb{E}_x [W_x^\alpha]^s]. \quad (10.24)$$

For the second term in Eq. (10.20), we re-index it to have

$$4 \frac{1}{M} \sum_i \mathrm{Tr} \left[ \left( \sum_{j \neq i} W_{x_j} \right) \left\{ W_{x_i}^{\alpha s} \left( \sum_{j \neq i} W_{x_j}^\alpha \right)^s \right\} \right]. \quad (10.25)$$

Again, using Lemma 2.10 yields

$$\mathrm{Tr} \left[ \left( \sum_{j \neq i} W_{x_j} \right) \left\{ W_{x_i}^{\alpha s} \left( \sum_{j \neq i} W_{x_j}^\alpha \right)^s \right\} \right] \leq \mathrm{Tr} \left[ \left( \sum_{j \neq i} W_{x_j}^\alpha \right)^s W_{x_i}^{1-\alpha s} \right]. \quad (10.26)$$

Taking expectation and combining with Eq. (10.24), we have

$$\mathsf{P}_e(n, R) \leq 6(M-1)^s \mathrm{Tr} [\mathbb{E}_x [W_x^{1-\alpha s}] \mathbb{E}_x [W_x^\alpha]^s]. \quad (10.27)$$

Invoking the definition of  $E_r^\downarrow(R)$  and choosing  $\alpha = 1/(1+s)$ , we obtain Eq. (10.13).

For pure-state c-q channels, Eq. (10.27) can be rewritten as

$$\mathsf{P}_e(n, R) \leq 6(M-1)^s \mathrm{Tr} [\mathbb{E}_x [W_x]]^{1+s}, \quad (10.28)$$

because  $W_x^p = W_x$  for  $p \geq 0$  for pure-state c-q channels. The above expression equals to Eq. (10.15), which completes the proof.  $\square$

*Remark 10.1.* To obtain the Eq. (10.15) for general c-q channels, one possible way of the above method is to employ the inequality

$$\left( \sum_{j \neq i} W_{x_j} \right)^\alpha \leq \sum_{j \neq i} W_{x_j}^\alpha, \quad \forall \alpha \in [0, 1], \quad (10.29)$$

which in turn implies

$$\sum_{j \neq i} W_{x_j} \leq \left( \sum_{j \neq i} W_{x_j}^\alpha \right)^{\frac{1}{\alpha}}. \quad (10.30)$$

Unfortunately, the operator inequality in Eq. (10.29) does not hold for general density operators  $W_{x_i}$ . The inequality only holds under the weak majorization.  $\diamond$

Lastly, the following Conjecture 10.1 was posed by Holevo [2]. Note that to achieve the first order in Eq. (10.32), the right-hand side of Eq. (10.31) allows to have any sub-exponential prefactors  $\exp\{o(n)\}$ .

**Conjecture 10.1** (Random Coding Bound for Classical-Quantum Channels). *Given any classical-quantum channels  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$ , transmission rate  $R < C_{\mathcal{W}}$ , and random codes with distribution  $P \in \mathcal{P}(\mathcal{X})$ , one has*

$$P_e(n, R) \leq \exp\{-nE_r^{(1)}(R, P)\}, \quad \forall n \in \mathbb{N}. \quad (10.31)$$

In particular,

$$\varepsilon^*(n, R) \leq \exp\{-nE_r(R)\}, \quad \forall n \in \mathbb{N}. \quad (10.32)$$

## 10.2 Random Codes with Constant Composition Ensemble

To our best knowledge, the achievability bound of c-q channel coding has not been done before. In the following Theorem 10.2, we establish an achievability bound with the first-order term  $E_r^{(2),\downarrow}(R, P)$ . This quantity is stronger than  $E_r^{(1),\downarrow}(R, P)$  in Theorem 10.1.

**Theorem 10.2** (Achievability of Classical-Quantum Channel Coding with Fixed Composition). *For any  $n \geq 2$ ,  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{B})$ ,  $P \in \mathcal{P}_n(\mathcal{X})$ , there exist an  $n$ -blocklength channel code  $\mathcal{C}$  with fixed composition  $P$  and rate  $R$  such that the average error probability  $P_e(\mathcal{C})$  can be bounded by*

$$\log P_e(\mathcal{C}) \leq -nE_r^{(2),\downarrow}(R, P) + K \log n, \quad (10.33)$$

where  $K$  is a constant only depending on  $|\mathcal{X}|$ , and the entropic exponent function is defined by

$$E_r^{(2),\downarrow}(R, P) := \sup_{0 \leq s \leq 1} s \left( \sum_{x \in \mathcal{X}} P(x) D_{1-s}(W_x \| P\mathcal{W}) - R \right). \quad (10.34)$$

In particular,

$$-\frac{1}{n} \log \varepsilon^*(n, R, P) \geq E_r^{(2),\downarrow}(R, P) - \frac{K \log n}{n}. \quad (10.35)$$

To prove it, we will first prove a one-shot version given by the following proposition.

**Proposition 10.1** (One-shot Achievability of Classical-Quantum Channel Coding). *For any  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(B)$ ,  $P \in \mathcal{P}(\mathcal{X})$ ,  $\mathcal{B} \subset \mathcal{X}$ , and  $\alpha \in [1/2, 1]$ , there exists a channel code  $\mathcal{C}$  with codewords in  $\mathcal{B}$  and  $|\mathcal{C}| = M$  such that the average error probability  $P_e(\mathcal{C})$  can be bounded by*

$$\log P_e(\mathcal{C}) \leq -s \left[ \inf_{x \in \mathcal{B}} D_{1-s}(W_x \| P\mathcal{W}) - \log(M-1) \right] + \log \frac{6}{P(\mathcal{B})}, \quad (10.36)$$

where  $P\mathcal{W} = \sum_x P(x)W_x$ .

*Proof of Proposition 10.1.* We prove the existence of the channel codes satisfying Eq. (10.36) by using a random coding argument. For any  $P \in \mathcal{P}(\mathcal{X})$  and  $\mathcal{B} \subset \mathcal{X}$  with  $P(\mathcal{B}) > 0$ , let  $P_{\mathcal{B}} \in \mathcal{P}(\mathcal{X})$  be

$$P_{\mathcal{B}}(x) := \frac{\mathbb{1}_{x \in \mathcal{B}} P(x)}{P(\mathcal{B})}. \quad (10.37)$$

We consider the ensemble of codes satisfying the following: the assignments of the messages  $m$  to the code  $\mathcal{E}(m) = x$  are jointly independent with probability  $P_{\mathcal{B}}(x)$  for all  $m$  in the message set  $\mathcal{M}$ . The decoder is characterized by the POVM  $\mathcal{F} = (\Pi_m)_{m \in \mathcal{M}}$ :

$$\Pi_m := \left( \sum_{\bar{m} \in \mathcal{M}} \Lambda_{\bar{m}} \right)^{-1/2} \Lambda_m \left( \sum_{\bar{m} \in \mathcal{M}} \Lambda_{\bar{m}} \right)^{-1/2}, \quad (10.38)$$

$$\Lambda_m := \{W_{\mathcal{E}(m)} - \gamma P\mathcal{W} > 0\}, \quad (10.39)$$

where  $\gamma > 0$  will be chosen later. Then, the average error probability of the code  $\mathcal{C} = (\mathcal{E}, \mathcal{F})$  is

$$P_e(\mathcal{C}) = \frac{1}{M} \sum_{m \in \mathcal{M}} \text{Tr} [W_{\mathcal{E}(m)} (\mathbb{1} - \Pi_m)]. \quad (10.40)$$

Invoking the Hayashi-Nagaoka inequality in Lemma 2.9:

$$\mathbb{1} - \Pi_m \leq 2(\mathbb{1} - \Lambda_m) + 4 \sum_{\bar{m} \neq m} \Lambda_{\bar{m}}, \quad (10.41)$$

we obtain

$$P_e(\mathcal{C}) \leq \frac{2}{M} \sum_{m \in \mathcal{M}} \text{Tr} [W_{\mathcal{E}(m)} \{W_{\mathcal{E}(m)} - \gamma P\mathcal{W} \leq 0\}] + \frac{4}{M} \sum_{m \in \mathcal{M}} \sum_{\bar{m} \neq m} \text{Tr} [W_{\mathcal{E}(m)} \{W_{\mathcal{E}(\bar{m})} - \gamma P\mathcal{W} > 0\}]. \quad (10.42)$$

The expected value of  $P_e(\mathcal{C})$  over the ensemble is then

$$\mathbb{E}[P_e(\mathcal{C})] \leq 2 \sum_x P_{\mathcal{B}}(x) \text{Tr} [W_x \{W_x - \gamma P\mathcal{W} \leq 0\}] + 4(M-1) \sum_x P_{\mathcal{B}}(x) \text{Tr} [P_{\mathcal{B}}\mathcal{W} \{W_x - \gamma P\mathcal{W} > 0\}]. \quad (10.43)$$

Next, we apply Audenaert *et al.*'s inequality in Lemma 2.8: for every  $A, B \geq 0$  and  $s \in [0, 1]$ ,

$$\text{Tr} [\{A - B \geq 0\} B + \{B - A \leq 0\} A] \leq \text{Tr} [A^{1-s} B^s]. \quad (10.44)$$

Letting  $A = W_x$  and  $B = \gamma P\mathcal{W}$ , the first term on the right-hand side of Eq. (10.43) can be upper bounded by

$$2 \sum_x P_{\mathcal{B}}(x) \text{Tr} [W_x \{W_x - \gamma P\mathcal{W} \leq 0\}] \leq 2 \sum_x P_{\mathcal{B}}(x) \gamma^s \text{Tr} [W_x^{1-s} (P\mathcal{W})^s] \quad (10.45)$$

$$\leq 2\gamma^s \exp \left\{ -s \inf_{x \in \mathcal{B}} D_{1-s}(W_x \| P\mathcal{W}) \right\} \quad (10.46)$$

for all  $s \in [0, 1]$ . Similarly, the second term on the right-hand side of Eq. (10.43) can be upper bounded by

$$\begin{aligned} & 4(M-1) \sum_x P_{\mathcal{B}}(x) \text{Tr} [P_{\mathcal{B}}\mathcal{W} \{W_x - \gamma P\mathcal{W} > 0\}] \\ & \leq 4(M-1) \sum_x P_{\mathcal{B}}(x) \frac{1}{P(\mathcal{B})} \text{Tr} [P\mathcal{W} \{W_x - \gamma P\mathcal{W} > 0\}] \end{aligned} \quad (10.47)$$

$$\leq 4(M-1) \sum_x P_{\mathcal{B}}(x) \frac{1}{\gamma P(\mathcal{B})} \text{Tr} [W_x^{1-s} (\gamma P\mathcal{W})^s] \quad (10.48)$$

$$\leq 4(M-1) \frac{1}{\gamma^{s-1} P(\mathcal{B})} \exp \left\{ -s \inf_{x \in \mathcal{B}} D_{1-s}(W_x \| P\mathcal{W}) \right\}, \quad (10.49)$$

where Eq. (10.47) follows from below

$$P_{\mathcal{B}}\mathcal{W} = \sum_x \frac{\mathbf{1}_{x \in \mathcal{B}} P(x) W_x}{P(\mathcal{B})} \leq \sum_x \frac{P(x) W_x}{P(\mathcal{B})} = \frac{P\mathcal{W}}{P(\mathcal{B})}. \quad (10.50)$$

By setting  $\gamma = \frac{M-1}{P(\mathcal{B})}$ , Eqs. (10.43), (10.46), and (10.49) together yield

$$\mathbb{E} [\text{P}_e(\mathcal{C})] \leq \frac{6}{P(\mathcal{B})} \exp \left\{ -s \left[ \inf_{x \in \mathcal{B}} D_{1-s}(W_x \| P\mathcal{W}) - \log(M-1) \right] \right\} \quad (10.51)$$

for all  $s \in [0, 1]$ .

Since there exists a channel coding with the average error probability less than or equal to  $\mathbb{E} [\text{P}_e(\mathcal{C})]$ , our claim is thus proven.  $\square$

By applying Proposition 10.1 with the type class  $T_P^n$  as the codeword space, we immediately arrive at the following achievability result for constant composition coding.

*Proof of Theorem 10.2.* First note that

$$P^{\otimes n} \mathcal{W}^{\otimes n} = (P\mathcal{W})^{\otimes n}. \quad (10.52)$$

The additivity of Rényi relative entropy implies that for all  $\mathbf{x} \in T_P^n$  and  $s \in [0, 1]$ ,

$$D_{1-s}(W_{\mathbf{x}} \| P^{\otimes n} \mathcal{W}^{\otimes n}) = D_{1-s}(W_{\mathbf{x}} \| (P\mathcal{W})^{\otimes n}) \quad (10.53)$$

$$= n \sum_{x \in \mathcal{X}} P(x) D_{1-s}(W_x \| P\mathcal{W}). \quad (10.54)$$

Let  $\mathcal{B} = T_P^n$  in Proposition 10.1. By [27, p. 26], the probability of the set of all sequences with composition  $P$  under the i.i.d. distribution  $P$  is

$$P^{\otimes n}(T_P^n) = e^{-\xi \frac{|\text{supp}(P)|}{12 \log 2}} (2\pi n)^{-\frac{|\text{supp}(P)|-1}{2}} \sqrt{\prod_{x:P(x)>0} \frac{1}{P(x)}} \quad (10.55)$$

for some  $\xi \in [0, 1]$ . Hence, Proposition 10.1 ensures that there exists an  $n$ -blocklength channel code  $\mathcal{C}$  with fixed composition  $P$  and rate  $R = \frac{\log |\mathcal{C}|}{n}$  such that

$$\log P_e(\mathcal{C}) \leq -nE_r^{(2),\downarrow}(R, P) + \frac{|\text{supp}(P)|}{12 \log 2} + \frac{|\text{supp}(P)|-1}{2} \log(2\pi n) + \frac{1}{2} \sum_{x:P(x)>0} \log P(x) + \log 6. \quad (10.56)$$

Taking

$$K := \frac{|\mathcal{X}|}{12 \log 2} + \frac{|\mathcal{X}|-1}{2} (1 + \log(2\pi)) + \log 6, \quad (10.57)$$

our result is proved for all  $n \geq 2$  such that  $\log n \geq 0$ .  $\square$

## Chapter 11

# Optimality (Channel Coding)

In this chapter, we present the weak and strong sphere-packing bounds for c-q channels. In Section 11.1, we first review existing approaches of proving classical sphere-packing bound. In Section 11.2, we provide the proof of a weak sphere-packing bound by using Wolfowitz strong converse. This bound is new in the quantum scenario and will be used in the moderate deviation analysis in Section 12. In Section 11.3, we prove our main result of a finite blocklength strong sphere-packing bound for c-q channels, see Theorem 11.1 below, which improve Dalai's prefactor [38, 39] from the order of subexponential  $e^{O(\sqrt{n})}$  to polynomial. Lastly, in Section 11.4, we obtain exact asymptotics (i.e. exact prefactors) of the strong sphere-packing bound for a symmetric c-q channels, which can be seen as a generalization of classical symmetric channels [23].

**Theorem 11.1** (Finite Blocklength Strong Sphere-Packing Bound of Constant Composition Codes). *Consider a classical-quantum channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  and  $R \in (R_\infty, C_{\mathcal{W}})$ . For every  $\gamma > 0$ , there exist an  $N_0 \in \mathbb{N}$  and a constant  $A > 0$  such that for all constant composition codes  $\mathcal{C}_n$  of length  $n \geq N_0$  with message size  $|\mathcal{C}_n| \geq \exp\{nR\}$ , we have*

$$\bar{\varepsilon}(\mathcal{C}_n) \geq \frac{A}{n^{\frac{1}{2}(1+|E'_{\text{sp}}(R)|)+\gamma}} \exp\{-nE_{\text{sp}}(R)\}. \quad (11.1)$$

The following corollary generalizes the refined sphere-packing bound for constant composition codes to arbitrary codes by using the standard argument [31, p. 95]. We delay the proof to the end of Section 11.3.5.

**Corollary 11.1** (Finite Blocklength Strong Sphere-Packing Bound of General Codes). *Consider a classical-quantum channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  and  $R \in (R_\infty, C_{\mathcal{W}})$ . There exist some  $t > 1/2$  and  $N_0 \in \mathbb{N}$  such that for all codes of length  $n \geq N_0$ , we have*

$$\varepsilon^*(n, R) \geq n^{-t} \exp\{-nE_{\text{sp}}(R)\}. \quad (11.2)$$

Theorem 11.1 yields

$$\log \frac{1}{\bar{\varepsilon}(\mathcal{C}_n)} \leq nE_{\text{sp}}(R) + \frac{1}{2} (1 + |E'_{\text{sp}}(R)|) \log n + o(\log n), \quad (11.3)$$

where the term  $\frac{1}{2} (1 + |E'_{\text{sp}}(R)|)$  can be viewed as a second-order term (see the discussions in [20,

Section 4.4]). On the other hand, for the case of classical *non-singular* channels<sup>1</sup>, it was shown that [144, Theorem 3.6], for all constant composition codes  $\mathcal{C}_n$  and rate  $R \in (C_{1/2,W}, C_W)$ ,

$$\log \frac{1}{\varepsilon(\mathcal{C}_n)} \geq nE_r(R) + \frac{1}{2} (1 + |E'_r(R)|) \log n + \Omega(1), \quad (11.4)$$

where  $E_r(R)$  is the random coding exponent defined in Eq. (9.2), and note that  $E_r(R) = E_{sp}(R)$  for all  $R \geq C_{1/2,W}$  [23, p. 160], [36]. Hence our result, Theorem 11.1, matches the achievability up to the logarithmic order. We note that whether the third order  $o(\log n)$  in Eq. (11.3) can be improved to  $O(1)$  is still unknown even for the classical case.

## 11.1 Literature Review of Classical Sphere-Packing Bound

This section reviews existing proof approaches of classical sphere-packing bounds:

$$\varepsilon^*(n, R) \geq f(n) \exp \{-n [E_{sp}(R - g(n))] \}, \quad (11.5)$$

$$\varepsilon^*(n, R) \geq f(n) \exp \left\{ -n \left[ \tilde{E}_{sp}(R - g(n)) \right] \right\}, \quad (11.6)$$

where  $f(n)$  is the pre-factor of the bound, and  $g(n)$  is the back-off from the rate. We remark that  $E_{sp}$  coincides with  $\tilde{E}_{sp}$  in the classical case. The reason why we distinguish the notation  $E_{sp}$  and  $\tilde{E}_{sp}$  here is because of their possible quantum generalizations (recalling that they are not equal in the quantum case, i.e. Theorem 9.1 in Section 9.1). Table 11.1 below summarizes the comparisons of existing results.

Bounds\Settings	Finite blocklength	Composition dependent	Pre-factor $f(n)$	Rate back-off $g(n)$	Classical-quantum channels	Tightness
(a) Shannon-Gallager-Berlekamp [31]	No	Yes	$e^{-O(\sqrt{n})}$	$O\left(\frac{\log n}{n}\right)$	Dalai [38]	Strong
Haroutunian [32] (b) Omura [149] Csisár-Korner [27]	No	Yes	$e^{-o(n)}$	$o(1)$	Winter [37]	Weak
(c) Blahut [33]	No	No	$e^{-O(\sqrt{n})}$	$O\left(n^{-\frac{1}{2}}\right)$	Eqs. (11.130) & (11.135)	Strong
(d) Altuğ-Wagner [98]	Yes	Yes	$n^{-\frac{1}{2}(1+ E'_{sp}(R) +o(1))}$	0	Theorem 11.1	Strong
(e) Elkayam-Feder [150]	Yes	Yes	$O(n^{-t})$	$O\left(\frac{\log n}{n}\right)$	Unknown	Unknown
(f) Agustín-Nakiboğlu [151, 113, 112, 145, 114, 146]	Yes	No	$O(n^{-t})$	0	Unknown	Unknown

Table 11.1: Different sphere-packing bounds are compared by (i) the bound is finite blocklength or asymptotical; (ii) whether or not they are dependent on the constant composition codes; (iii) & (iv) the asymptotics of  $f(n)$  and  $g(n)$ ; (v) the corresponding c-q generalizations. The parameter  $t$  in rows (e) and (f) is some value in the range  $t > 1/2$ ; and (vi) whether their error exponent expressions for c-q channels are in the strong form (Eq. (1.4)) or weak form (Eq. (12.51)).

- (a) Shannon, Gallager and Berlekamp obtained the first classical sphere-packing bound Eq. (11.5),

<sup>1</sup>For classical *singular* channels, one has  $\log \frac{1}{\varepsilon(\mathcal{C}_n)} \geq nE_r(R) + \frac{1}{2} \log n + \Omega(1)$  [144]. Further, it was conjectured that [148] that  $\log \frac{1}{\varepsilon(\mathcal{C}_n)} \leq nE_{sp}(R) + \frac{1}{2} \log n + o(\log n)$ , for all asymmetric classical singular channels and constant composition codes. However, such a result remains open.

where [31, Theorem 5]

$$f(n) = e^{-O(\sqrt{n})}; \quad g(n) = O\left(\frac{\log n}{n}\right). \quad (11.7)$$

Their method is based on distinguishing two codewords, followed by Chebyshev's inequality. The works [152] and [153] further improved the coefficients in  $f(n)$  and  $g(n)$  for short to moderate blocklengths.

Remarkably, Shannon-Gallager-Berlekamp's result can be extended to c-q channels with almost the same asymptotics in Eq. (11.7) [38]. See also the result by Dalai and Winter for constant composition codes [39].

- (b) Haroutunian [32], Omura [149], Csiszár and Körner [27], Ahlswede [154] subsequently proposed a sphere-packing exponent using discrimination functions (i.e. the relative entropy function in Eq. (1.5)), and obtained the following classical sphere-packing bound for constant composition codes  $\mathcal{C}_n$ :

$$\bar{\varepsilon}(\mathcal{W}, \mathcal{C}_n) \geq \frac{1}{2} \exp \left\{ -n \tilde{E}_{\text{sp}}(R - \delta)(1 + \delta) \right\}, \quad (11.8)$$

for all  $\delta > 0$  and all sufficiently large  $n \in \mathbb{N}$ , and  $\bar{\varepsilon}(W, \mathcal{C}_n)$  denotes the average error of the code  $\mathcal{C}_n$ . The idea is to apply strong converse bounds [155, 156, 157, 149, 27] to a dummy channel, and then use a data-processing inequality for the discrimination function between the dummy and true channels. Recently, Altug and Wagner employed a particular strong converse result, Wolfowitz's strong converse result [158], and obtained a form of Eq. (11.6) with [43, Lemma 3]:

$$g(n) = O\left(\frac{1}{\sqrt{n}}\right). \quad (11.9)$$

Following the arguments in [154, Theorem 49], Winter proved a weak sphere-packing bound Eq. (11.8) for constant composition codes in c-q channels [37, Theorem II.20]. We remark that Altug and Wagner's result [43] can also be extended to a weak sphere-packing bound for c-q channels when combining Winter's approach [37] with Sharma and Warsi's strong converse result [134, Theorem 3].

- (c) Blahut related the channel coding problem to hypothesis testing [33, Theorem 20] (see also [25, Theorem 10.2.1]) and independently obtained a weak sphere-packing bound Eq. (11.6) with

$$f(n) = e^{-O(\sqrt{n})}; \quad g(n) = O\left(\frac{1}{\sqrt{n}}\right). \quad (11.10)$$

In Section 11.3, we generalize Blahut's result to a strong sphere-packing bound for c-q channels.

- (d) In Ref. [48], Altug and Wagner applied a sharp concentration inequality to refine the sphere-packing bound Eq. (11.7) with

$$f(n) = e^{-O(\sqrt{n})}; \quad g(n) = O\left(\frac{\log n}{n}\right), \quad (11.11)$$

for some  $t > 1/2$  and all sufficiently large  $n \in \mathbb{N}$ .

- (e) Elkayam and Feder [150] established a general expression for the error probability in terms of the cumulative distribution function [159, Theorem 6]. Combined with the method of types and Polyanskiy's minimax meta-converse [160, Theorem 3], they proved a classical sphere-packing bound for constant composition codes with

$$f(n) = \Theta(n^{-t}); \quad g(n) = O\left(\frac{\log n}{n}\right), \quad (11.12)$$

for some  $t > 1/2$ . This sphere-packing bound also had a polynomial pre-factor; however, it is unknown whether this method can be extended to c-q channels.

## 11.2 A Weak Sphere-Packing Bound via Wolfowitz Strong Converse

**Theorem 11.2** (Weak Converse Bound with Polynomial Prefactors). *Consider a classical-quantum channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  with  $\mathcal{S}_o := \overline{\text{im}(\mathcal{W})}$ , an arbitrary rate  $R \geq 0$ , and  $\sigma \in \mathcal{S}_{>0}(\mathcal{H})$ . For any  $\eta \in (0, \frac{1}{2})$  and  $c > 0$ , let  $N_0 \in \mathbb{N}$  such that for all  $n \geq N_0$ ,*

$$c \cdot e^{-\xi\sqrt{n}} \leq \frac{\eta}{2}, \quad (11.13)$$

where  $\xi = \sqrt{2A/\eta}$  and  $A := \max_{\rho \in \mathcal{S}_o} V(\rho\|\sigma)$ . Then, it holds that for all  $n \geq N_0$ ,

$$\widehat{\alpha}_{\exp\{-nR\}}(W_{\mathbf{x}^n}^{\otimes n} \|\sigma^{\otimes n}) \geq f(\eta) \exp\left\{-n \left[\frac{\widetilde{E}_{\text{sp}}\left(R - \frac{2\xi}{\sqrt{n}}, P_{\mathbf{x}^n}, \sigma\right)}{1-\eta}\right]\right\}, \quad (11.14)$$

where  $f(\eta) = \exp\left\{-\frac{h(1-\eta)}{1-\eta}\right\}$  and  $h(p) := -p \log p - (1-p) \log(1-p)$  is the binary entropy function.

*Remark 11.1.* Consider a constant composition code with common type  $P_{\mathbf{x}^n}$  on a finite input alphabet  $\mathcal{X}$ . Recall the definition of the weak sphere-packing exponent [37, 28]:

$$\widetilde{E}_{\text{sp}}(R, P_{\mathbf{x}^n}) := \min_{\bar{\mathcal{W}}: \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})} \{D(\bar{\mathcal{W}}\|\mathcal{W}|P_{\mathbf{x}^n}) : I(P_{\mathbf{x}^n}, \bar{\mathcal{W}}) \leq R\}. \quad (11.15)$$

Theorem 11.2, along with the one-shot converse bound (see Proposition 11.2 in Section 11.3.1 later), establishes a weak sphere-packing bound with polynomial prefactors, which generalizes Altug and Wagner's result [43, Lemma 3] to c-q channels: for any  $\eta \in (0, \frac{1}{2})$  and for all sufficiently large  $n$  such that Eq. (11.13) holds, we have

$$\varepsilon_{\max}(\mathcal{W}, P_{\mathbf{x}^n}) \geq \max_{\sigma \in \mathcal{S}(\mathcal{H})} \widehat{\alpha}_{\exp\{-nR\}}(W_{\mathbf{x}^n}^{\otimes n} \|\sigma^{\otimes n}) \quad (11.16)$$

$$\geq \widehat{\alpha}_{\exp\{-nR\}}(W_{\mathbf{x}^n}^{\otimes n} \|(\sigma^*)^{\otimes n}) \quad (11.17)$$

$$\geq f(\eta) \exp\left\{-n \left[\frac{\widetilde{E}_{\text{sp}}\left(R - \frac{2\xi}{\sqrt{n}}, P_{\mathbf{x}^n}\right)}{1-\eta}\right]\right\}, \quad (11.18)$$

where  $\sigma^* := P_{\mathbf{x}^n} \bar{\mathcal{W}}^*$  and  $\bar{\mathcal{W}}^*$  is an arbitrary minimizer in Eq. (11.15). Moreover, Eq. (11.18) im-

proves the prefactor of Winter's weak sphere-packing bound [37] from the order of subexponential to polynomial.  $\diamond$

*Proof of Theorem 11.2.* Consider an arbitrary sequence  $\mathbf{x}^n \in \mathcal{X}^n$  and a test  $Q_n$  on  $\mathcal{H}^{\otimes n}$ . For two c-q channels  $\bar{\mathcal{W}}, \mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}_o$ , the data-processing inequality implies that

$$D(\bar{W}_{\mathbf{x}^n}^{\otimes n} \| W_{\mathbf{x}^n}^{\otimes n}) \geq [1 - \alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n})] \log \frac{1 - \alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n})}{1 - \alpha(Q_n; W_{\mathbf{x}^n}^{\otimes n})} + \alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n}) \log \frac{\alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n})}{\alpha(Q_n; W_{\mathbf{x}^n}^{\otimes n})} \quad (11.19)$$

$$= -h(\alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n})) - \alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n}) \log \alpha(Q_n; W_{\mathbf{x}^n}^{\otimes n}) \\ - [1 - \alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n})] \log (1 - \alpha(Q_n; W_{\mathbf{x}^n}^{\otimes n})) \quad (11.20)$$

$$\geq -\alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n}) \log \alpha(Q_n; W_{\mathbf{x}^n}^{\otimes n}) - h(\alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n})), \quad (11.21)$$

where the last inequality (11.21) follows since the third term in (11.20) is non-negative. Continuing from Eq. (11.21), we have

$$\alpha(Q_n; W_{\mathbf{x}^n}^{\otimes n}) \geq \exp \left\{ -\frac{D(\bar{W}_{\mathbf{x}^n}^{\otimes n} \| W_{\mathbf{x}^n}^{\otimes n}) + h(\alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n}))}{\alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n})} \right\} \quad (11.22)$$

$$= \exp \left\{ -\frac{n D(\bar{\mathcal{W}} \| \mathcal{W} | P_{\mathbf{x}^n}) + h(\alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n}))}{\alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n})} \right\}, \quad (11.23)$$

where Eq. (11.23) follows from the additivity of the relative entropy and the empirical distribution  $P_{\mathbf{x}^n}$ .

The next step is to replace  $\alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n})$  with a lower bound that does not depend on the dummy channel  $\bar{W}$ , provided that  $\bar{W}$  satisfies certain conditions. This can be done using Proposition 11.1, Wolfowitz's strong converse bound. We delay its proof in Section 11.2.1 below.

**Proposition 11.1** (Wolfowitz's Strong Converse). *Let  $\mathcal{S}_o \subseteq \mathcal{S}(\mathcal{H})$  be closed and let  $\bar{\mathcal{W}} : \mathcal{X} \rightarrow \mathcal{S}_o$  be an arbitrary classical-quantum channel. Consider the binary hypothesis testing:*

$$\mathsf{H}_0 : \bar{W}_{\mathbf{x}^n}^{\otimes n}, \quad (11.24)$$

$$\mathsf{H}_1 : \sigma^{\otimes n}, \quad (11.25)$$

where  $\mathbf{x}^n \in \mathcal{X}^n$  and  $\sigma \in \mathcal{S}_{>0}(\mathcal{H})$ . For any test  $Q_n$  such that  $\beta(Q_n; \sigma^{\otimes n}) \leq e^{-nR}$  and  $D(\bar{W}_{\mathbf{x}^n}^{\otimes n} \| \sigma | P_{\mathbf{x}^n}) \leq R - 2\kappa$ , it holds that

$$\alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n}) > 1 - \frac{A}{n\kappa^2} - e^{-n\kappa}, \quad (11.26)$$

where  $A := \max_{\rho \in \mathcal{S}_o} V(\rho \| \sigma)$ .

Fix  $0 < \eta < \frac{1}{2}$ , and let  $\xi^2 := \frac{2A}{\eta}$ . Note that  $\xi^2$  is finite because  $A < +\infty$ . For all  $n \geq N_0$ , we have

$$c \cdot e^{-\xi\sqrt{n}} \leq \frac{\eta}{2} \quad (11.27)$$

by assumption in Theorem 11.2. Choose  $\kappa = \xi/\sqrt{n}$ . For any  $\bar{\mathcal{W}} : \mathcal{X} \rightarrow \mathcal{S}_o$  with  $D(\bar{\mathcal{W}} \| \sigma | P_{\mathbf{x}^n}) \leq R - \frac{2\xi}{\sqrt{n}}$  and any test  $Q_n$  such that  $\beta(Q_n; \sigma^{\otimes n}) \leq e^{-nR}$ , Proposition 11.1 gives a lower bound to the type-I

error:

$$\alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n}) \geq 1 - \frac{A}{n\kappa^2} - e^{-n\kappa} \geq 1 - \eta. \quad (11.28)$$

Hence, combining Eqs. (11.23) and (11.28) yields that, for any  $\beta(Q_n; \sigma^{\otimes n}) \leq ce^{-nR}$ ,

$$\alpha(Q_n; W_{\mathbf{x}^n}^{\otimes n}) \geq \max_{\bar{W}: D(\bar{W}\|\sigma|P_{\mathbf{x}^n}) \leq R - \frac{2\xi}{\sqrt{n}}} \exp \left\{ -\frac{n D(\bar{W}\|\mathcal{W}|P_{\mathbf{x}^n}) + h(1-\eta)}{1-\eta} \right\}, \quad (11.29)$$

$$= \exp \left\{ -\frac{h(1-\eta)}{1-\eta} \right\} \exp \left\{ -\frac{n \tilde{E}_{\text{sp}} \left( R - \frac{2\xi}{\sqrt{n}}, P_{\mathbf{x}^n}, \sigma \right)}{1-\eta} \right\}, \quad (11.30)$$

which concludes Theorem 11.2.  $\square$

### 11.2.1 Proof of Wolfowitz's Strong Converse, Proposition 11.1

This proof follows similar steps by Sharma and Warsi [134, Theorem 3], which uses generalized divergences to prove Wolfowitz's strong converse.

To prove our claim, we first introduce notation for generalized divergences. For any  $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ , and  $\gamma > 0$ , define the *hockey-stick divergence* by

$$\mathcal{D}_\gamma(\rho\|\sigma) := \text{Tr}[(\rho - \gamma\sigma)_+], \quad (11.31)$$

where  $A_+ := A\{A \geq 0\}$  denotes the positive part of  $A$ . This divergence satisfies the data-processing inequality (DPI):

$$\text{Tr}[(\rho - \gamma\varrho)_+] \geq \text{Tr}[(\mathcal{N}(\rho) - \gamma\mathcal{N}(\varrho))_+], \quad (11.32)$$

for any completely positive and trace-preserving map  $\mathcal{N} : \mathcal{S}(\mathcal{H}_{\text{in}}) \rightarrow \mathcal{S}(\mathcal{H}_{\text{out}})$  [134, Lemma 4]. Let

$$\rho_p := p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|, \quad \text{and} \quad \sigma_q := q|0\rangle\langle 0| + (1-q)|1\rangle\langle 1|, \quad (11.33)$$

for  $0 \leq p, q \leq 1$  and some orthonormal basis  $\{|0\rangle, |1\rangle\}$ , and define

$$d_\gamma(p\|q) := \mathcal{D}_\gamma(\rho_p\|\sigma_q). \quad (11.34)$$

Note that the quantity  $d_\gamma(p\|q)$  is independent of the choice of the basis  $\{|0\rangle, |1\rangle\}$ . Now we are ready to prove Proposition 11.1.

*Proof of Proposition 11.1.* Fix an arbitrary test  $Q_n$  on  $\mathcal{H}^{\otimes n}$ . For notational convenience, we shorthand  $\rho^n = \bar{W}_{\mathbf{x}^n}^{\otimes n}$ ,  $\tau^n = \sigma^{\otimes n}$ ,  $\alpha = \alpha(Q_n; \rho^n)$  and  $\beta = (Q_n; \tau^n)$ . Further, we assume  $\beta(Q_n; \tau^n) \leq e^{-nR}$ . From the definition of the classical divergence, Eqs. (11.31) and (11.34), and any  $\gamma > 0$ , we find

$$d_\gamma(1 - \alpha\|\beta) = (1 - \alpha - \gamma\beta)_+ + (\alpha - \gamma[1 - \beta])_+ \quad (11.35)$$

$$\geq 1 - \alpha - \gamma\beta \quad (11.36)$$

$$\geq 1 - \alpha - \gamma e^{-nR}. \quad (11.37)$$

On the other hand, DPI for the measurement map  $\text{Tr}[Q_n(\cdot)]|0\rangle\langle 0| + (1 - \text{Tr}[Q_n(\cdot)])|1\rangle\langle 1|$  implies that

$$\mathcal{D}_\gamma(\rho^n\|\tau^n) \geq d_\gamma(\text{Tr}[Q_n\rho^n]\|\text{Tr}[Q_n\tau^n]) = d_\gamma(1 - \alpha\|\beta). \quad (11.38)$$

Hence, Eqs. (11.37) and (11.38) lead to

$$\alpha \geq 1 - \mathcal{D}_\gamma(\rho^n\|\tau^n) - \gamma e^{-nR}. \quad (11.39)$$

Since

$$\mathcal{D}_\gamma(\rho^n\|\tau^n) = \text{Tr}[\{\rho^n - \gamma\tau^n \geq 0\}(\rho^n - \gamma\tau^n)] \quad (11.40)$$

$$\leq \text{Tr}[\{\rho^n - \gamma\tau^n \geq 0\}\rho^n], \quad (11.41)$$

Eq. (11.39) gives

$$\alpha \geq 1 - \text{Tr}[\{\rho^n - \gamma\tau^n \geq 0\}\rho^n] - \gamma e^{-nR}. \quad (11.42)$$

Next, invoking Lemma 11.1 below, for all  $\log \gamma > D(\rho^n\|\tau^n)$ , we have

$$\alpha \geq 1 - \frac{V(\rho^n\|\tau^n)}{[\log \gamma - D(\rho^n\|\tau^n)]^2} - \gamma e^{-nR} \quad (11.43)$$

$$= 1 - \frac{V(\bar{W}\|\sigma|P_{\mathbf{x}^n})}{n \left[ \frac{\log \gamma}{n} - D(\bar{W}\|\sigma|P_{\mathbf{x}^n}) \right]^2} - \gamma e^{-nR} \quad (11.44)$$

Finally, recall  $D(\bar{W}\|\sigma|P_{\mathbf{x}^n}) \leq R - 2\kappa$  and  $A := \max_{\rho \in \mathcal{S}_0} V(\rho\|\sigma)$  and choose  $\log \gamma = nD(\bar{W}\|\sigma|P_{\mathbf{x}^n}) + n\kappa$ . Then, Eq. (11.44) yields, for any test  $Q_n$  and  $\beta(Q_n; \sigma^{\otimes n}) \leq e^{-nR}$ ,

$$\alpha(Q_n; \bar{W}_{\mathbf{x}^n}^{\otimes n}) \geq 1 - \frac{V(\bar{W}\|\sigma|P_{\mathbf{x}^n})}{n\kappa^2} - e^{-n\kappa} \quad (11.45)$$

$$\geq 1 - \frac{A}{n\kappa^2} - e^{-n\kappa}, \quad (11.46)$$

which concludes the proof.

**Lemma 11.1** (Quantum Chebyshev's Inequality [115, Lemma 6]). *Let  $\rho, \sigma \in \mathcal{S}(\mathcal{H})$  and assume  $\log \gamma > D(\rho\|\sigma)$ . Then*

$$\text{Tr}[\rho \{\rho - \gamma\sigma \geq 0\}] \leq \frac{V(\rho\|\sigma)}{[\log \gamma - D(\rho\|\sigma)]^2}. \quad (11.47)$$

□

### 11.3 A Strong Sphere-Packing Bound

The goal the section is to prove Theorem 11.1, the strong sphere-packing bound for c-q channels with a polynomial pre-factor. To establish this result, we combine Blahut's insight of relating a channel coding problem to binary hypothesis testing [33, 25] with a sharp concentration inequality introduced in Section 2.2. Our proof consists of three major steps: (i) reduce the channel coding problem to

binary hypothesis testing (Proposition 11.2 in Section 11.3.1); (ii) bound its type-I error from below (Propositions 11.3 and 11.4 in Sections 11.3.2 and 11.3.3); (iii) employ Theorem 9.1 in Section 9.1 to relate the derived bound to the strong sphere-packing exponent. The proof of Theorem 11.1 and Corollary 11.1 will be given in Section 11.3.5.

### 11.3.1 One-Shot Converse Bound (Hypothesis Testing Reduction)

We first present a proof that relates the decoding error of a code to binary hypothesis testing. Proposition 11.2 below is similar to the meta-converse in Ref. [14]. However, the idea dates back to Fano [24], Shannon-Gallager-Berlekamp [31], and Blahut [33, 25].

**Proposition 11.2.** *For any classical-quantum channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  and any code  $\mathcal{C}$  with message size  $M$ , it follows that*

$$\epsilon_{\max}(\mathcal{C}) \geq \max_{\sigma \in \mathcal{S}(\mathcal{H})} \min_{x \in \mathcal{C}} \widehat{\alpha}_{\frac{1}{M}}(W_x \parallel \sigma). \quad (11.48)$$

*Proof.* Let  $x(m)$  be the codeword encoding the message  $m \in \{1, \dots, M\}$ . Define a binary hypothesis testing problem:

$$\mathsf{H}_0 : W_x, \quad (11.49)$$

$$\mathsf{H}_1 : \sigma, \quad (11.50)$$

where  $\sigma \in \mathcal{S}(\mathcal{H})$  can be viewed as a dummy channel output. Since  $\sum_{m=1}^M \beta(\Pi_m; \sigma) = 1$  for any POVM  $\Pi = \{\Pi_1, \dots, \Pi_M\}$ , and  $\beta(\Pi_m; \sigma) \geq 0$  for every  $m \in \mathcal{M}$ , there must exist a message  $m \in \mathcal{M}$  for any code  $\mathcal{C}$  such that  $\beta(\Pi_m; \sigma) \leq \frac{1}{M}$ . Fix such  $x := x(m)$ . Then

$$\epsilon_{\max}(\mathcal{C}) \geq \epsilon_m(\mathcal{C}) = \alpha(\Pi_m; W_x) \geq \widehat{\alpha}_{\frac{1}{M}}(W_x \parallel \sigma) \geq \min_{x \in \mathcal{C}} \widehat{\alpha}_{\frac{1}{M}}(W_x \parallel \sigma). \quad (11.51)$$

Since the above inequality (11.51) holds for every  $\sigma \in \mathcal{S}(\mathcal{H})$ , it follows that

$$\epsilon_{\max}(\mathcal{C}) \geq \max_{\sigma \in \mathcal{S}(\mathcal{H})} \min_{x \in \mathcal{C}} \widehat{\alpha}_{\frac{1}{M}}(W_x \parallel \sigma). \quad (11.52)$$

□

### 11.3.2 Chebyshev's Type Converse Bound

In the following Proposition, we generalize Blahut's one-shot converse Hoeffding bound [33, Theorem 10] to the quantum setting. This result is essentially a Chebyshev-type bound. We will employ it to lower bound the error of "bad sequences" that yield smaller error exponent in Section 11.3.5.

In the following Proposition, we will prove a finite blocklength bound of a composition via the hypothesis testing results—Eqs. (4.31) and (4.32) in Theorem 4.4. The difficulty of deriving a finite blocklength result is that one needs to obtain some universal coefficients independent of all possible compositions. Our core technique here is a uniform continuity property, Proposition 11.5, which will be presented in Appendix 11.3.4.

The following result is essentially a Chebyshev-type bound with prefactor  $\exp\{O(\sqrt{n})\}$ . We will employ it to lower bound the error of “bad sequences” that yield a inferior error exponent in Section 11.3.5.

**Proposition 11.3** (Chebyshev-Type Bound for a Fixed Composition). *Let  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  be a classical-quantum channel. Fix  $R \in (C_{0,\mathcal{W}}, C_{\mathcal{W}})$ . Consider a sequence  $\mathbf{x}^n \in \mathcal{X}^n$ . Then, for every  $c > 0$ , there exist a state  $\sigma^* \in \mathcal{S}(\mathcal{H})$ , an integer  $N_0 \in \mathbb{N}$ , independent of the sequences  $\mathbf{x}^n$  and  $\sigma$ , such that for all  $n \geq N_0$  we have*

$$\widehat{\alpha}_{c \exp\{-nR\}} (W_{\mathbf{x}^n}^{\otimes n} \| (\sigma^*)^{\otimes n}) \geq \exp \left\{ -A\sqrt{n} - nE_{\text{sp}}^{(2)}(R, P_{\mathbf{x}^n}) \right\}, \quad (11.53)$$

where  $A \in \mathbb{R}_{>0}$  is a finite positive constant depending on  $R$  and  $\mathcal{W}$ .

*Proof of Proposition 11.3.* Fix an arbitrary  $\underline{R} \in (C_{0,\mathcal{W}}, R)$ . Let  $\gamma_n := \frac{a\sqrt{n}}{2n} + \frac{\log 8 - \log c}{n}$  and  $R_n := R - \gamma_n$  for some  $a \in \mathbb{R}$ . The choice of  $a$  and the rate back-off term  $\gamma_n$  will become evident later. Let  $N_1 \in \mathbb{N}$  such that  $R_n \in [\underline{R}, R]$  for all  $n \geq N_1$ . Subsequently, we choose such  $n \geq N_1$  onwards.

We choose the optimal output state as

$$\sigma^* = \arg \min_{\sigma \in \mathcal{S}(\mathcal{H})} \sup_{0 < \alpha \leq 1} \frac{1 - \alpha}{\alpha} (D_\alpha(\mathcal{W} \| \sigma | P_{\mathbf{x}^n}) - R_n). \quad (11.54)$$

Let  $p^n := \bigotimes_{i=1}^n p_{x_i}$  and  $q^n := \bigotimes_{i=1}^n q_{x_i}$ , where  $(p_{x_i}, q_{x_i})$  are Nussbaum-Szkoła distributions [121] of  $(W_{x_i}, \sigma_{R,P}^*)$  for every  $i \in [n]$ . Since  $D_\alpha(W_{x_i} \| \sigma^*) = D_\alpha(p_{x_i} \| q_{x_i})$ , for  $\alpha \in (0, 1]$ , again we shorthand for all  $R_n \in [\underline{R}, R]$ ,

$$\phi_n(R_n) := \phi_n(R_n | W_{\mathbf{x}^n}^{\otimes n} \| (\sigma^*)^{\otimes n}) = \phi_n(R_n | p^n \| q^n) = E_{\text{sp}}^{(2)}(R_n, P_{\mathbf{x}^n}), \quad (11.55)$$

where the last equality in Eq. (11.55) follows from the saddle-point property, item (a) in Proposition 9.5. Moreover, item (b) in Proposition 9.5 implies that the state  $\sigma^*$  dominants all the states:  $\sigma^* \gg W_x$ , for all  $x \in \text{supp}(P_{\mathbf{x}^n})$ . Hence, we have  $p^n \ll q^n$ . This guarantees that  $V_\alpha(W_x \| \sigma^*)$  is finite for all  $\alpha \in [0, 1]$  and all  $x \in \text{supp}(P_{\mathbf{x}^n})$ .

Theorem 4.4 implies that for any test  $Q^n$  either

$$\alpha(Q^n; W_{\mathbf{x}^n}^{\otimes n}) \geq \frac{1}{8} \exp \left\{ -n\phi_n(R_n) - \alpha_{R_n, P_{\mathbf{x}^n}}^* \sqrt{2nV_{\alpha_{R_n, P_{\mathbf{x}^n}}^*}(P_{\mathbf{x}^n}, \mathcal{W})} \right\}, \quad (11.56)$$

or

$$\beta(Q^n; (\sigma^*)^{\otimes n}) \geq \frac{1}{8} \exp \left\{ -nR_n - (1 - \alpha_{R_n, P_{\mathbf{x}^n}}^*) \sqrt{2nV_{\alpha_{R_n, P_{\mathbf{x}^n}}^*}(P_{\mathbf{x}^n}, \mathcal{W})} \right\}, \quad (11.57)$$

where  $\alpha_{r, P_{\mathbf{x}^n}}^* \in (0, 1)$  satisfies, for all  $r \in [\underline{R}, R]$ ,

$$\phi_n(r) = \frac{1 - \alpha_{r, P_{\mathbf{x}^n}}^*}{\alpha_{r, P_{\mathbf{x}^n}}^*} \left( I_{\alpha_{r, P_{\mathbf{x}^n}}^*}^{(2)}(P_{\mathbf{x}^n}, \mathcal{W}) - r \right). \quad (11.58)$$

and we define

$$V_\alpha(P, \mathcal{W}) := \sum_{x \in \mathcal{X}} P(x) \mathbb{E}_{v_{x,\alpha}} \left[ \left| \log \frac{p_x}{q_x} - \mathbb{E}_{v_{x,\alpha}} \left[ \log \frac{p_x}{q_x} \right] \right|^2 \right], \quad (11.59)$$

$$v_{x,\alpha}(\omega) := \frac{p_x^\alpha(\omega) q_x^{1-\alpha}(\omega)}{\sum_{\bar{\omega}} p_x^\alpha(\bar{\omega}) q_x^{1-\alpha}(\bar{\omega})}. \quad (11.60)$$

Now, we will introduce a constant independent of  $\mathbf{x}^n$  to obtain a finite blocklength lower bound for  $\hat{\alpha}_{c \exp\{-nR\}}(W_{\mathbf{x}^n}^{\otimes n} \| (\sigma^*)^{\otimes n})$ . Let

$$V_{\max}(R) := \max_{(r,P) \in [\underline{R}, R] \times \mathcal{P}(\mathcal{X})} V_{\alpha_{r,P}^*}(P, \mathcal{W}). \quad (11.61)$$

Recall that  $V_\alpha(P_{\mathbf{x}^n}, \mathcal{W})$  is finite for all  $\alpha \in [0, 1]$ . Proposition 11.5 in Section 11.3.4 implies that  $V_{\alpha_{r,P}^*}(P, \mathcal{W})$  is joint continuous on  $[\underline{R}, R] \times \mathcal{P}(\mathcal{X})$ . Further, since  $\mathcal{P}(\mathcal{X})$  is compact, the quantity in Eq. (11.61) is well-defined and finite. Therefore,

$$\beta(Q^n; (\sigma^*)^{\otimes n}) \geq \frac{1}{8} \exp \left\{ -nR_n - (1 - \alpha_{R_n, P_{\mathbf{x}^n}}^*) \sqrt{2nV_{\alpha_{R_n, P_{\mathbf{x}^n}}^*}(P_{\mathbf{x}^n}, \mathcal{W})} \right\} \quad (11.62)$$

$$\geq \frac{1}{8} \exp \left\{ -nR_n - \sqrt{2nV_{\max}(R)} \right\} \quad (11.63)$$

$$= c \exp \{-nR\}, \quad (11.64)$$

where we choose  $a := \sqrt{2V_{\max}(R)}$  in the rate back-off term  $\gamma_n := \frac{a\sqrt{n}}{2n} + \frac{\log 8 - \log c}{n}$ .

Next, Eqs. (11.56) and (11.64) yield

$$\hat{\alpha}_{c \exp\{-nR\}}(W_{\mathbf{x}^n}^{\otimes n} \| (\sigma^*)^{\otimes n}) \geq \frac{1}{8} \exp \left\{ -n\phi_n(R_n) - \alpha_{R_n, P_{\mathbf{x}^n}}^* \sqrt{2nV_{\alpha_{R_n, P_{\mathbf{x}^n}}^*}(P_{\mathbf{x}^n}, \mathcal{W})} \right\} \quad (11.65)$$

$$\geq \frac{1}{8} \exp \left\{ -\sqrt{2nV_{\max}(R)} - nE_{\text{sp}}^{(2)}(R - \gamma_n, P_{\mathbf{x}^n}) \right\}. \quad (11.66)$$

Further, the convexity and the monotone decreases of  $r \mapsto E_{\text{sp}}^{(2)}(r, P)$  given in Proposition 9.6-(a) shows that

$$E_{\text{sp}}^{(2)}(R - \gamma_n, P_{\mathbf{x}^n}) \leq E_{\text{sp}}^{(2)}(R, P_{\mathbf{x}^n}) - \gamma_n \left. \frac{\partial E_{\text{sp}}^{(2)}(r, P_{\mathbf{x}^n})}{\partial r} \right|_{r=R}, \quad (11.67)$$

$$\leq E_{\text{sp}}^{(2)}(R, P_{\mathbf{x}^n}) - \gamma_n \left. \frac{\partial E_{\text{sp}}^{(2)}(r, P_{\mathbf{x}^n})}{\partial r} \right|_{r=\underline{R}}. \quad (11.68)$$

Next, we denote

$$\Upsilon := \max_{P \in \mathcal{P}(\mathcal{X})} \left| \left. \frac{\partial E_{\text{sp}}^{(2)}(r, P)}{\partial r} \right|_{r=\underline{R}} \right|. \quad (11.69)$$

Observe that  $\Upsilon \in \mathbb{R}_{\geq 0}$  due to  $\underline{R} > C_{0,W}$  and item (d) of Proposition 9.5. Then, Eqs. (11.66), (11.68),

and (11.69) lead to

$$\widehat{\alpha}_{c \exp\{-nR\}} (W_{\mathbf{x}^n}^{\otimes n} \| (\sigma^*)^{\otimes n}) \geq \exp \left\{ -\log 8 - \sqrt{2nV_{\max}(R)} - \gamma_n \Upsilon - nE_{\text{sp}}^{(2)}(R, P_{\mathbf{x}^n}) \right\}. \quad (11.70)$$

Since  $\gamma_n = O(1/\sqrt{n})$ , for any  $A > \sqrt{2V_{\max}(R)}$ , there exists a sufficiently large  $N_2 \in \mathbb{N}$  such that for all  $n \geq N_2$ ,

$$\log 8 + \sqrt{2nV_{\max}(R)} + \gamma_n \Upsilon \leq A\sqrt{n}. \quad (11.71)$$

By letting  $N_0 := \max\{N_1, N_2\}$  completes the proof.  $\square$

### 11.3.3 A Sharp Converse Bound

The following Proposition 11.4 is a sharp converse bound with polynomial prefactors obtained from Eqs. (4.33) and (4.34) in Theorem 4.4, which in turn were proved by employing Bahadur-Ranga Rao's inequality (see Section 2.2). Similar to Proposition 11.3 presented before, we will employ the uniform continuity, Proposition 11.5, given in Section 11.3.4 to prove Proposition 11.4. In Section 11.3.5, we will exploit this result to bound the error of "good sequences" with a polynomial prefactor.

**Proposition 11.4** (Sharp Converse Bound for a Fixed Composition). *Let  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  be a classical-quantum channel Fix  $R \in (C_{0,\mathcal{W}}, C_{\mathcal{W}})$ . Consider a sequence  $\mathbf{x}^n \in \mathcal{X}^n$  satisfying*

$$E_{\text{sp}}^{(2)}(R, P_{\mathbf{x}^n}) \in [\nu, +\infty) \quad (11.72)$$

for some constant  $\nu > 0$ . Then, for every  $c > 0$ , there exist a state  $\sigma^* \in \mathcal{S}(\mathcal{H})$ , an integer  $N_0 \in \mathbb{N}$ , independent of the sequences  $\mathbf{x}^n$  and  $\sigma$ , such that for all  $n \geq N_0$  we have

$$\widehat{\alpha}_{c \exp\{-nR\}} (W_{\mathbf{x}^n}^{\otimes n} \| (\sigma^*)^{\otimes n}) \geq \frac{A}{n^{\frac{1}{2}(1+s_{R,P_{\mathbf{x}^n}}^*)}} \exp \left\{ -nE_{\text{sp}}^{(2)}(R, P_{\mathbf{x}^n}) \right\}, \quad (11.73)$$

where  $s_{R,P}^* := -\left. \frac{\partial E_{\text{sp}}^{(2)}(r,P)}{\partial r} \right|_{r=R}$ , and  $A \in \mathbb{R}_{>0}$  is a finite positive constant depending on  $R, \nu$  and  $\mathcal{W}$ .

*Proof of Proposition 11.4.* Fix an arbitrary  $\underline{R} \in (C_{0,\mathcal{W}}, R)$ . Let  $\gamma_n := \frac{\log n}{2n} + \frac{x}{n}$  and  $R_n := R - \gamma_n$  for some  $x \in \mathbb{R}$ . The choice of  $x$  and the rate back-off term  $\gamma_n$  will become evident later. Let  $N_1 \in \mathbb{N}$  such that  $R_n \in [\underline{R}, R]$  for all  $n \geq N_1$ . Subsequently, we choose such  $n \geq N_1$  onwards.

We choose the optimal output state as

$$\sigma^* = \arg \min_{\sigma \in \mathcal{S}(\mathcal{H})} \sup_{0 < \alpha \leq 1} \frac{1-\alpha}{\alpha} (D_\alpha(\mathcal{W}\|\sigma|P_{\mathbf{x}^n}) - R_n). \quad (11.74)$$

as in the proof of Proposition 11.3. Let  $p^n := \bigotimes_{i=1}^n p_{x_i}$  and  $q^n := \bigotimes_{i=1}^n q_{x_i}$ , where  $(p_{x_i}, q_{x_i})$  are Nussbaum-Szkoła distributions [121] of  $(W_{x_i}, \sigma^*)$  for every  $i \in [n]$ . Since  $D_\alpha(W_{x_i}\|\sigma^*) = D_\alpha(p_{x_i}\|q_{x_i})$ , for  $\alpha \in (0, 1]$ , again we shorthand for all  $R_n \in [\underline{R}, R]$ ,

$$\phi_n(R_n) := \phi_n(R_n | W_{\mathbf{x}^n}^{\otimes n} \| (\sigma^*)^{\otimes n}) = \phi_n(R_n | p^n \| q^n) = E_{\text{sp}}^{(2)}(R_n, P_{\mathbf{x}^n}), \quad (11.75)$$

where the last equality in Eq. (11.75) follows from the saddle-point property, item (a) in Proposition 9.5. Moreover, item (b) in Proposition 9.5 implies that the state  $\sigma^*$  dominants all the states:  $\sigma^* \gg W_x$ , for all  $x \in \text{supp}(P_{\mathbf{x}^n})$ . Hence, we have  $p^n \ll q^n$ . Without loss of generality, we set zero all elements of  $q_{x_i}$  that do not lie in the support of  $p_{x_i}$ , i.e.  $q_{x_i}(\omega) = 0$ ,  $\omega \notin \text{supp}(p_{x_i})$ ,  $i \in [n]$ , because those elements do not contribute in  $\phi_n(R_n)$ .

Next, we define

$$V_\alpha(P, \mathcal{W}) := \sum_{x \in \mathcal{X}} P(x) \mathbb{E}_{v_{x,\alpha}} \left[ \left| \log \frac{p_x}{q_x} - \mathbb{E}_{v_{x,\alpha}} \left[ \log \frac{p_x}{q_x} \right] \right|^2 \right]; \quad (11.76)$$

$$T_\alpha(P, \mathcal{W}) := \sum_{x \in \mathcal{X}} P(x) \mathbb{E}_{v_{x,\alpha}} \left[ \left| \log \frac{p_x}{q_x} - \mathbb{E}_{v_{x,\alpha}} \left[ \log \frac{p_x}{q_x} \right] \right|^3 \right], \quad (11.77)$$

$$v_{x,\alpha}(\omega) := \frac{p_x^\alpha(\omega) q_x^{1-\alpha}(\omega)}{\sum_{\bar{\omega}} p_x^\alpha(\bar{\omega}) q_x^{1-\alpha}(\bar{\omega})}, \quad (11.78)$$

Applying Theorem 4.4, we have for any test  $Q^n$ ,

$$\alpha(Q^n; W_{\mathbf{x}^n}^{\otimes n}) \geq e^{-n\phi_n(R_n)} \frac{e^{-K_n(\alpha_{R_n, P_{\mathbf{x}^n}}^*)}}{2\sqrt{2n\pi V_{\alpha_{R_n, P_{\mathbf{x}^n}}^*}(P_{\mathbf{x}^n}, \mathcal{W})}} \left( 1 - \frac{1 + (1 + K_n(\alpha_{R_n, P_{\mathbf{x}^n}}^*)^2)}{2\sqrt{nV_{\alpha_{R_n, P_{\mathbf{x}^n}}^*}(P_{\mathbf{x}^n}, \mathcal{W})}} \right) \quad (11.79)$$

$$\beta(Q^n; (\sigma^*)^{\otimes n}) \geq e^{-nR_n} \frac{e^{-K_n(\alpha_{R_n, P_{\mathbf{x}^n}}^*)}}{2\sqrt{2n\pi V_{\alpha_{R_n, P_{\mathbf{x}^n}}^*}(P_{\mathbf{x}^n}, \mathcal{W})}} \left( 1 - \frac{1 + (1 + K_n(\alpha_{R_n, P_{\mathbf{x}^n}}^*)^2)}{2\sqrt{nV_{\alpha_{R_n, P_{\mathbf{x}^n}}^*}(P_{\mathbf{x}^n}, \mathcal{W})}} \right), \quad (11.80)$$

where  $K_n(\alpha) := 15\sqrt{2} \frac{T_\alpha(P_{\mathbf{x}^n}, \mathcal{W})}{V_\alpha(P_{\mathbf{x}^n}, \mathcal{W})}$ , and  $\alpha_{r, P_{\mathbf{x}^n}}^* \in (0, 1)$  satisfies, for all  $r \in [\underline{R}, R]$ ,

$$\phi_n(r) = \frac{1 - \alpha_{r, P_{\mathbf{x}^n}}^*}{\alpha_{r, P_{\mathbf{x}^n}}^*} \left( I_{\alpha_{r, P_{\mathbf{x}^n}}^*}^{(2)}(P_{\mathbf{x}^n}, \mathcal{W}) - r \right). \quad (11.81)$$

In the following, we will remove the dependency of  $R_n$  and  $P_{\mathbf{x}^n}$  in  $V_{(\cdot)}(\cdot)$  and  $K_n(\cdot)$ . Define the following quantities:

$$V_{\max}(R, \nu) := \max_{(r, P) \in [\underline{R}, R] \times \mathcal{P}_{R, \nu}(\mathcal{X})} V_{\alpha_{r, P}^*}(P, \mathcal{W}); \quad (11.82)$$

$$V_{\min}(R, \nu) := \min_{(r, P) \in [\underline{R}, R] \times \mathcal{P}_{R, \nu}(\mathcal{X})} V_{\alpha_{r, P}^*}(P, \mathcal{W}); \quad (11.83)$$

$$K_{\max}(R, \nu) := 15\sqrt{2\pi} \max_{(r, P) \in [\underline{R}, R] \times \mathcal{P}_{R, \nu}(\mathcal{X})} \frac{T_{\alpha_{r, P}^*}(P, \mathcal{W})}{V_{\alpha_{r, P}^*}(P, \mathcal{W})}, \quad (11.84)$$

where

$$\mathcal{P}_{R, \nu}(\mathcal{X}) := \left\{ P \in \mathcal{P}(\mathcal{X}) : \nu \leq E_{\text{sp}}^{(2)}(R, P_{\mathbf{x}^n}) \leq E_{\text{sp}}(R) < +\infty \right\} \quad (11.85)$$

is a compact set owing to the continuity of  $r \mapsto E_{\text{sp}}^{(2)}(r, P)$  given in Proposition 9.6. Also, Proposition 11.5 in Section 11.3.4 shows that the objective functions in Eqs. (11.82), (11.83), and (11.84) are continuous functions on  $\mathcal{P}(\mathcal{X})$ , which guarantees the maximization and minimization in the above definitions are well-defined and finite. Further, the quantity  $V_{\min}(R, \nu)$  is bounded away from zero

because of the positivity given in Theorem 4.4.

Now, we are ready to derive the lower bounds for  $\widehat{\alpha}_{c \exp\{-nR\}}(W_{\mathbf{x}^n}^{\otimes n} \| (\sigma^\star)^{\otimes n})$ . Let  $N_2 \in \mathbb{N}$  be sufficiently large such that for all  $n \geq N_2$ ,

$$\sqrt{n} \geq \frac{1 + (1 + K_{\max}(R, \nu))^2}{\sqrt{V_{\min}(R, \nu)}}. \quad (11.86)$$

Then, Eqs. (11.79) and (11.80) give

$$\alpha(Q^n; W_{\mathbf{x}^n}^{\otimes n}) \geq \frac{A(R, \nu)}{\sqrt{n}} \exp\{-n\phi_n(R_n)\}; \quad (11.87)$$

$$\beta(Q^n; (\sigma^\star)^{\otimes n}) \geq \frac{A(R, \nu)}{\sqrt{n}} \exp\{-nR_n\}, \quad (11.88)$$

where

$$A(R, \nu) := \frac{e^{-K_{\max}(R, \nu)}}{4\sqrt{2\pi V_{\max}(R, \nu)}}. \quad (11.89)$$

Choosing  $x = -\log A(R, \nu) + \log c$  in the rate back-off term  $\gamma_n = \frac{\log n}{2n} + \frac{x}{n}$ , we have

$$\beta(Q^n; (\sigma^\star)^{\otimes n}) \geq c \exp\{-nR\}. \quad (11.90)$$

Combining Eqs. (11.79) and (11.90) then yields

$$\widehat{\alpha}_{c \exp\{-nR\}}(W_{\mathbf{x}^n}^{\otimes n} \| (\sigma^\star)^{\otimes n}) \geq \frac{A(R, \nu)}{\sqrt{n}} \exp\{-n\phi_n(R_n)\} = \frac{A(R, \nu)}{\sqrt{n}} \exp\left\{-nE_{\text{sp}}^{(2)}(R - \gamma_n, P_{\mathbf{x}^n})\right\}. \quad (11.91)$$

It remains to remove the rate back-off term  $\gamma_n$  in Eq. (11.91). By Taylor's theorem, one has

$$E_{\text{sp}}^{(2)}(R - \gamma_n, P_{\mathbf{x}^n}) = E_{\text{sp}}^{(2)}(R, P_{\mathbf{x}^n}) - \gamma_n \left. \frac{\partial E_{\text{sp}}^{(2)}(r, P_{\mathbf{x}^n})}{\partial r} \right|_{r=R} + \frac{\gamma_n^2}{2} \left. \frac{\partial^2 E_{\text{sp}}^{(2)}(r, P_{\mathbf{x}^n})}{\partial r^2} \right|_{r=\bar{R}}, \quad (11.92)$$

for some  $\bar{R} \in (\underline{R}, R)$ . Recalling item (d) in Lemma 2.13, one can show that

$$\begin{aligned} - \left. \frac{\partial E_{\text{sp}}^{(2)}(r, P_{\mathbf{x}^n})}{\partial r} \right|_{r=R} &= s_{R, P_{\mathbf{x}^n}}^\star = \frac{1 - \alpha_{R, P_{\mathbf{x}^n}}^\star}{\alpha_{R, P_{\mathbf{x}^n}}^\star} \in \mathbb{R}_{>0}, \\ \left. \frac{\partial^2 E_{\text{sp}}^{(2)}(r, P_{\mathbf{x}^n})}{\partial r^2} \right|_{r=\bar{R}} &= \frac{(1 + \bar{s})^3}{V_{\alpha_{\bar{R}, P_{\mathbf{x}^n}}^\star}(P_{\mathbf{x}^n}, \mathcal{W})} \leq \frac{(1 + s_0)^3}{V_{\min}(R, \nu)} =: \Upsilon \in \mathbb{R}_{>0}, \end{aligned} \quad (11.93)$$

where

$$\bar{s} := - \left. \frac{\partial E_{\text{sp}}^{(2)}(r, P_{\mathbf{x}^n})}{\partial r} \right|_{r=\bar{R}} \leq - \left. \frac{\partial E_{\text{sp}}^{(2)}(r, P_{\mathbf{x}^n})}{\partial r} \right|_{r=R} =: s_0 \in \mathbb{R}_{>0} \quad (11.94)$$

by the monotone decreases of  $r \mapsto E_{\text{sp}}^{(2)}(r, P)$ . Then, Eqs. (11.91), (11.92) and (11.93) lead to

$$\widehat{\alpha}_{c \exp\{-nR\}}(W_{\mathbf{x}^n}^{\otimes n} \| (\sigma^*)^{\otimes n}) \geq \frac{A(R, \nu)}{\sqrt{n}} \exp\left\{-nE_{\text{sp}}^{(2)}(R, P_{\mathbf{x}^n}) - n\left[\gamma_n\left(s_{R, P_{\mathbf{x}^n}}^* + \frac{\gamma_n}{2}\Upsilon\right)\right]\right\} \quad (11.95)$$

$$= \frac{A(R, \nu)}{n^{\frac{1}{2}(1+s_{R, P_{\mathbf{x}^n}}^*)}} \exp\left\{-nE_{\text{sp}}^{(2)}(R, P_{\mathbf{x}^n}) - \ell_n\right\}, \quad (11.96)$$

where we denote by

$$\ell_n := -\left(s_{R, P_{\mathbf{x}^n}}^* + \frac{\gamma_n}{2}\Upsilon\right) \log A(R, \nu) + \frac{\gamma_n\Upsilon}{4} \log n. \quad (11.97)$$

Since  $s_{R, P_{\mathbf{x}^n}}^* \in \mathbb{R}_{>0}$  and  $\gamma_n \log n = o(1)$ , we choose a constant  $L \in \mathbb{R}_{>0}$  and  $N_3 \in \mathbb{N}$  such that

$$\ell_n \leq L, \quad \forall N \geq N_3. \quad (11.98)$$

Hence, Eqs. (11.96) and (11.98) lead to

$$\widehat{\alpha}_{c \exp\{-nR\}}(W_{\mathbf{x}^n}^{\otimes n} \| (\sigma^*)^{\otimes n}) = \frac{A(R, \nu) \exp\{-L\}}{n^{\frac{1}{2}(1+s_{R, P_{\mathbf{x}^n}}^*)}} \exp\left\{-nE_{\text{sp}}^{(2)}(R, P_{\mathbf{x}^n})\right\}. \quad (11.99)$$

By letting  $N_0 := \max\{N_1, N_2, N_3\}$  and  $A' := A(R, \nu) \exp\{-L\}$ , we conclude the proof.  $\square$

### 11.3.4 Uniform Continuity

The goal of this section is to present various uniform continuity properties, which play a significant role in proving finite blocklength converse bounds (see Propositions 11.3 and 11.4). Let  $r \in (C_{0,W}, C_{1,W})$  throughout this section. For any  $P \in \mathcal{P}_r(\mathcal{X}) := \{P \in \mathcal{P}(\mathcal{X}) : E_{\text{sp}}^{(2)}(r, P) > 0\}$ , we denote by  $(\alpha_{r,P}^*, \sigma_{r,P}^*) \in (0, 1) \times \mathcal{S}(\mathcal{H})$  the unique saddle-point of  $F(r, P)$  (see Proposition 9.5-(c)). For  $P \notin \mathcal{P}_r(\mathcal{X})$ , note that  $(1, \sigma)$  is a saddle-point of  $F(r, P)$  for all  $\sigma \in \mathcal{S}(\mathcal{H})$ . We thus choose  $(1, P\mathcal{W})$  to be the saddle-point of  $F(r, P)$  for  $P \notin \mathcal{P}_r(\mathcal{X})$ , subsequently. Define

$$B_r(P, \mathcal{W}) := \sum_{x \in \mathcal{X}} P(x) \mathbb{E}_{v_{x, \alpha_{r,P}^*}} \left[ \log \frac{p_x}{q_x} \right]; \quad (11.100)$$

$$V_r(P, \mathcal{W}) := \sum_{x \in \mathcal{X}} P(x) \mathbb{E}_{v_{x, \alpha_{r,P}^*}} \left[ \left| \log \frac{p_x}{q_x} - \mathbb{E}_{v_{x, \alpha_{r,P}^*}} \left[ \log \frac{p_x}{q_x} \right] \right|^2 \right]; \quad (11.101)$$

$$T_r(P, \mathcal{W}) := \sum_{x \in \mathcal{X}} P(x) \mathbb{E}_{v_{x, \alpha_{r,P}^*}} \left[ \left| \log \frac{p_x}{q_x} - \mathbb{E}_{v_{x, \alpha_{r,P}^*}} \left[ \log \frac{p_x}{q_x} \right] \right|^3 \right], \quad (11.102)$$

where  $(p_x, q_x)$  is the Nussbaum-Szkoła distribution [121] of  $(W_x, \sigma_{r,P}^*)$ , and the *tilted distribution* is

$$v_{x,\alpha}(i, j) := \frac{p_x^\alpha(i, j) q_x^{1-\alpha}(i, j)}{\sum_{\iota, j} p_x^\alpha(\iota, j) q_x^{1-\alpha}(\iota, j)}, \quad \alpha \in [0, 1]. \quad (11.103)$$

Inspired by Ref. [14, Lemma 62], we show the following continuity property, which are crucial for establishing the large deviation bounds in finite blocklength regime.

**Proposition 11.5** (Uniform Continuity). Fix  $R \in (C_{0,W}, C_{1,W})$ . For every  $\underline{R} \in (C_{0,W}, R]$ ,  $B_r(P, \mathcal{W})$ ,  $V_r(P, \mathcal{W})$ , and  $T_r(P, \mathcal{W})$  are jointly continuous functions of  $(r, P)$  on  $[\underline{R}, R] \times \mathcal{P}(\mathcal{X})$ .

*Remark 11.2.* When  $R \geq I_1^{(2)}(P, \mathcal{W}) = I(P, \mathcal{W})$ , Proposition 9.6-(a) implies that  $(\alpha_{R,P}^*, \sigma_{R,P}^*) = (1, P\mathcal{W})$ . In this case,  $V_R(P, \mathcal{W})$  equals to the *information variance*  $V(P)$  introduced by Tomamichel and Tan [18, Appendix B.3], and so does  $T_R(P, \mathcal{W}) = T(P)$ . The established Proposition 11.5 covers the special case of the continuities of  $V(P)$  and  $T(P)$  in  $P$ , and provides a rigorous proof for [18, Lemma 29]. We emphasize that such a continuity property is a critical step to ensure that the third-order term in the asymptotic expansion of coding rate (see e.g. [14], [18]) independent of all codeword sequences.

*Proof of Proposition 11.5.* Inspecting the definitions given in Eqs. (11.100), (11.101), and (11.102). it is not hard to see that the quantities  $B_r(P, \mathcal{W})$ ,  $V_r(P, \mathcal{W})$ , and  $T_r(P, \mathcal{W})$  are sums of finitely many terms. We thus prove that each term is a continuous function in  $P$ . In the following, we first show the continuity of  $B_r(P, \mathcal{W})$ . The proof for  $V_r(P, \mathcal{W})$  and  $T_r(P, \mathcal{W})$  follow similarly.

Fix an arbitrary  $x \in \mathcal{X}$  onwards. Let  $(R_k, P_k)_{k \in \mathbb{N}}$  be an arbitrary sequence such that  $(R_k, P_k) \in [\underline{R}, R] \times \mathcal{P}(\mathcal{X})$ , and  $\lim_{k \rightarrow +\infty} (R_k, P_k) = (R_0, P_0) \in [\underline{R}, R] \times \mathcal{P}(\mathcal{X})$ . To ease the burden of notation, we let

$$\alpha_k := \alpha_{R_k, P_k}^*, \text{ and } \sigma_k := \sigma_{R_k, P_k}^*, \quad \forall k \in \mathbb{N}. \quad (11.104)$$

Note that the joint continuity proved in Proposition 9.5-(d) guarantees that

$$\begin{aligned} \lim_{k \rightarrow +\infty} \alpha_k &= \alpha_{R_0, P_0}^* =: \alpha_0, \\ \lim_{k \rightarrow +\infty} \sigma_k &= \sigma_{R_0, P_0}^* =: \sigma_0. \end{aligned} \quad (11.105)$$

Given the eigenvalue decompositions  $W_x = \sum_i \lambda_i |e_i\rangle \langle e_i|$  and  $\sigma_k = \sum_j \mu_j(\sigma_k) |f_j^k\rangle \langle f_j^k|$ , Nussbaum-Szkoła distributions are  $p_x(i, j) = \lambda_i |\langle e_i | f_j^k \rangle|^2$  and  $q_x(i, j) = \mu_j(\sigma_{R_k, P_k}^*) |\langle e_i | f_j^k \rangle|^2$ . Here, we write  $f_j^k$  and  $\mu_j(\sigma_k)$  to emphasize the dependence on  $P_k$ . To prove the continuity of  $B_r(P, \mathcal{W})$ , it suffices to show

$$\begin{aligned} P_k(x) &\frac{\lambda_i^{\alpha_k} \mu_j^{1-\alpha_k}(\sigma_k) |\langle e_i | f_j^k \rangle|^2}{\sum_{i,j} \lambda_i^{\alpha_k} \mu_j^{1-\alpha_k}(\sigma_k) |\langle e_i | f_j^k \rangle|^2} \log \frac{\lambda_i}{\mu_j(\sigma_k)} \\ &\longrightarrow P_0(x) \frac{\lambda_i^{\alpha_0} \mu_j^{1-\alpha_0}(\sigma_0) |\langle e_i | f_j^0 \rangle|^2}{\sum_{i,j} \lambda_i^{\alpha_0} \mu_j^{1-\alpha_0}(\sigma_0) |\langle e_i | f_j^0 \rangle|^2} \log \frac{\lambda_i}{\mu_j(\sigma_0)}. \end{aligned} \quad (11.106)$$

In the following, we first exclude some trivial cases. If  $\lambda_i = 0$ , then the convergence is obvious (recalling that the power function is only acting on the support). We assume  $\lambda_i > 0$  onwards. If  $P_k(x) > 0$  only for finite number of  $k$ , then the convergence in Eq. (11.106) is also trivial. We may assume  $P_k(x) > 0$  for all  $k \in \mathbb{N}$  (switching to a subsequence if necessary). Further, Proposition 9.5-(b) implies that  $W_x \ll \sigma_k$  for all  $k \in \mathbb{N}$ . We have  $\lambda_i |\langle e_i | f_j^k \rangle|^2 = 0$  whenever  $\mu_j(\sigma_k) |\langle e_i | f_j^k \rangle|^2 = 0$  by the absolute continuity, which in turn implies the convergence of Eq. (11.106). We may assume  $\mu_j(\sigma_k) |\langle e_i | f_j^k \rangle|^2 > 0$  for all  $k \in \mathbb{N}$ .

With the above assumptions, we study two cases:  $P_0(x) = 0$  or not, separately. If  $P_0(x) > 0$ , then

$W_x \ll \sigma_0$ . The absolute continuity again implies that  $\mu_j(\sigma_0) > 0$  by the previous argument. Hence, we can deduce that  $\mu_j(\sigma_k)$  is bounded away from zero. Using the continuity given in Eqs. (11.105) and the continuity of logarithm,  $\log \lambda_i / \mu_j(\sigma_k)$  tends to  $\log \lambda_i / \mu_j(\sigma_0)$ , which shows the convergence in Eq. (11.106).

It remains to show the case of  $P_0(x) = 0$ . Observe that the convergence in Eq. (11.106) holds when  $\mu_j(\sigma_k) \not\rightarrow 0$ . We thus consider the circumstance that  $\mu_j(\sigma_k) \rightarrow 0$ . To achieve our goal, we will show that the log-likelihood ratio  $\log \frac{\lambda_i}{\mu_j(\sigma_k)}$  does not diverge too fast.

In what follows we inspect the eigenvalue  $\mu_j(\sigma_k)$ . The saddle-point property given in Proposition 9.5-(a) and Proposition 3.2-(b) indicate that  $\sigma_k$  must satisfy

$$\sigma_k = \left( \sum_{\bar{x} \in \mathcal{X}} P_k(\bar{x}) \frac{W_{\bar{x}}^{\alpha_k}}{\text{Tr}[W_{\bar{x}}^{\alpha_k}(\sigma_k)^{1-\alpha_k}]} \right)^{\frac{1}{\alpha_k}}. \quad (11.107)$$

Further, since  $\alpha_{r,P}^* \in (0, 1]$  for all  $(r, P) \in (C_{0,W}, \infty] \times \mathcal{P}(\mathcal{X})$ , the continuity of  $P \mapsto \alpha_{r,P}^*$  given in Proposition 9.5-(d) and the compactness of  $\mathcal{P}(\mathcal{X})$  imply that

$$\underline{\alpha_R} := \min_{P \in \mathcal{P}(\mathcal{X})} \alpha_{R,P}^* > 0 \quad (11.108)$$

By the convexity of  $r \mapsto E_{sp}^{(2)}(r, P)$  and Proposition 9.6-(c), we have  $\alpha_k \in [\underline{\alpha_R}, 1]$  for all  $k \in \{0\} \cup \mathbb{N}$ .

Therefore,

$$\mu_j(\sigma_k) = \langle f_j^k | \sigma_k | f_j^k \rangle \quad (11.109)$$

$$= \left( \sum_{\bar{x}} P_k(\bar{x}) \frac{\langle f_j^k | W_{\bar{x}}^{\alpha_k} | f_j^k \rangle}{\text{Tr}[W_{\bar{x}}^{\alpha_k}(\sigma_k)^{1-\alpha_k}]} \right)^{\frac{1}{\alpha_k}} \quad (11.110)$$

$$\geq \left( P_k(x) \frac{\langle f_j^k | W_x^{\alpha_k} | f_j^k \rangle}{\text{Tr}[W_x^{\alpha_k}(\sigma_k)^{1-\alpha_k}]} \right)^{\frac{1}{\alpha_k}} \quad (11.111)$$

$$= \left( P_k(x) \frac{\sum_i \lambda_i^{\alpha_k} |\langle e_i | f_j^k \rangle|^2}{\sum_{i,j} \lambda_i^{\alpha_k} \mu_j^{1-\alpha_k}(\sigma_k) |\langle e_i | f_j^k \rangle|^2} \right)^{\frac{1}{\alpha_k}} \quad (11.112)$$

$$\geq \left( P_k(x) \frac{\lambda_i^{\alpha_k} |\langle e_i | f_j^k \rangle|^2}{\sum_{i,j} \lambda_i^{\alpha_k} \mu_j^{1-\alpha_k}(\sigma_k) |\langle e_i | f_j^k \rangle|^2} \right)^{\frac{1}{\alpha_k}} \quad (11.113)$$

$$\geq \lambda_i c_k^{\frac{1}{\alpha_R}}, \quad (11.114)$$

where we denote by  $c_k := P_k(x) \frac{|\langle e_i | f_j^k \rangle|^2}{\sum_{i,j} \lambda_i^{\alpha_k} \mu_j^{1-\alpha_k}(\sigma_k) |\langle e_i | f_j^k \rangle|^2}$  in the last line. Note that  $\mu_j(\sigma_k) \leq 1$ . Eq. (11.114) then implies

$$\left| \log \frac{\lambda_i}{\mu_j(\sigma_k)} \right| \leq \log \frac{1}{\lambda_i} - \log \left( \lambda_i c_k^{\frac{1}{\alpha_R}} \right) \quad (11.115)$$

$$= 2 \log \frac{1}{\lambda_i} - \frac{1}{\alpha_R} \log c_k. \quad (11.116)$$

Since we assume  $\mu_j(\sigma_k) \rightarrow 0$  and  $\lambda_i > 0$ , Eq. (11.114) guarantees that

$$c_k \rightarrow 0. \quad (11.117)$$

Using Eqs. (11.108), (11.116), (11.117), and the fact that  $\lambda_i^{\alpha_k} \mu_j^{1-\alpha_k}(\sigma_k) \in [0, 1]$  for all  $k \in \mathbb{N}$ , we are able show that the left-hand side of Eq. (11.106) converges to 0:

$$P_k(x) \frac{\lambda_i^{\alpha_k} \mu_j^{1-\alpha_k}(\sigma_k) |\langle e_i | f_j^k \rangle|^2}{\sum_{i,j} \lambda_i^{\alpha_k} \mu_j^{1-\alpha_k}(\sigma_k) |\langle e_i | f_j^k \rangle|^2} \left| \log \frac{\lambda_i}{\mu_j(\sigma_k)} \right| \quad (11.118)$$

$$\leq c_k \left| \log \frac{\lambda_i}{\mu_j(\sigma_k)} \right| \quad (11.119)$$

$$\leq 2c_k \log \frac{1}{\lambda_i} - \frac{1}{\alpha_R} c_k \log c_k \quad (11.120)$$

$$\rightarrow 0, \quad (11.121)$$

which proves the joint continuity of  $(r, P) \mapsto B_r(P, \mathcal{W})$ .

Next, we show the continuity of  $V_r(P, \mathcal{W})$  and  $T_r(P, \mathcal{W})$ . Denote by  $B_r(W_x \| \sigma_k) := \mathbb{E}_{v_{x,\alpha_k}} [\log p_x / q_x]$  for convenience. For  $P_0(x) > 0$ ,  $\mu_j(\sigma_k)$  is bounded away from zero. Then,  $\log \lambda_i / \mu_j(\sigma_k)$  tends to  $\log \lambda_i / \mu_j(\sigma_0)$ , and it is not hard to see that  $B_{R_k}(W_x \| \sigma_k) \rightarrow B_{R_k}(W_x \| \sigma_0)$ . It suffices to prove the convergence when  $P_k(x) \rightarrow 0$  and  $\mu_j(\sigma_k) \rightarrow 0$  as mentioned before. Eq. (11.116) immediately implies that

$$B_{R_k}(W_x \| \sigma_k) = \sum_{i,j} \frac{\lambda_i^{\alpha_k} \mu_j^{1-\alpha_k}(\sigma_k) |\langle e_i | f_j^k \rangle|^2}{\sum_{i,j} \lambda_i^{\alpha_k} \mu_j^{1-\alpha_k}(\sigma_k) |\langle e_i | f_j^k \rangle|^2} \log \frac{\lambda_i}{\mu_j(\sigma_k)} \quad (11.122)$$

$$\leq 2 \log \frac{1}{\lambda_i} - \frac{1}{\alpha_R} \log c_k. \quad (11.123)$$

Using the inequality  $|a + b|^2 \leq 2(|a|^2 + |b|^2)$ , we obtain

$$P_k(x) \frac{\lambda_i^{\alpha_k} \mu_j^{1-\alpha_k}(\sigma_k) |\langle e_i | f_j^k \rangle|^2}{\sum_{i,j} \lambda_i^{\alpha_k} \mu_j^{1-\alpha_k}(\sigma_k) |\langle e_i | f_j^k \rangle|^2} \left| \log \frac{\lambda_i}{\mu_j(\sigma_k)} - B_{R_k}(W_x \| \sigma_k) \right|^2$$

$$\leq 2c_k \left| \log \frac{\lambda_i}{\mu_j(\sigma_k)} \right|^2 + 2c_k B_{R_k}^2(W_x \| \sigma_k). \quad (11.124)$$

Combining Eqs. (11.116), (11.117), (11.123), and (11.124), we prove the continuity of  $V_r(P, \mathcal{W})$ .

Similarly, using the inequality  $|a + b|^3 \leq 4(|a|^3 + |b|^3)$  gives

$$P_k(x) \frac{\lambda_i^{\alpha_k} \mu_j^{1-\alpha_k}(\sigma_k) |\langle e_i | f_j^k \rangle|^2}{\sum_{i,j} \lambda_i^{\alpha_k} \mu_j^{1-\alpha_k}(\sigma_k) |\langle e_i | f_j^k \rangle|^2} \left| \log \frac{\lambda_i}{\mu_j(\sigma_k)} - B_{\alpha_k}(W_x \| \sigma_k) \right|^3$$

$$\leq 4c_k \left| \log \frac{\lambda_i}{\mu_j(\sigma_k)} \right|^3 + 4c_k B_{R_k}^3(W_x \| \sigma_k). \quad (11.125)$$

Further, Eq. (11.116) implies

$$\left| \log \frac{\lambda_i}{\mu_j(\sigma_k)} \right|^3 \leq -4 \log^3 \lambda_i - \frac{4}{\alpha_R} \log^3 c_k. \quad (11.126)$$

Combining Eqs. (11.117), (11.123), (11.125), and (11.126), proves the continuity of  $T_r(P, \mathcal{W})$ .  $\square$

### 11.3.5 Proofs of Main Result, Theorem 11.1 and Corollary 11.1

We are ready to prove our main result—the refined strong sphere-packing bound in Theorem 11.1 for constant composition codes and Corollary 11.1 for general codes.

*Proof of Theorem 11.1.* Fix any rate  $C_{0,\mathcal{W}} < R < C_{\mathcal{W}}$ . First note that by Ref. [36, Proposition 10], we find

$$E_{\text{sp}}(R) \in \mathbb{R}_{>0}. \quad (11.127)$$

By Proposition 11.2 and the standard expurgation method (see e.g. [31, p. 96], [33, Theorem 20], [25, p. 395]), it holds for every constant composition code  $\mathcal{C}_n$  with a common composition  $P_{\mathbf{x}^n}$  that

$$\bar{\varepsilon}(\mathcal{C}_n) \geq \frac{1}{2}\varepsilon_{\max}(\mathcal{C}'_n) \geq \max_{\sigma \in \mathcal{S}(\mathcal{H})} \frac{1}{2}\widehat{\alpha}_{1/|\mathcal{C}'_n|}(W_{\mathbf{x}^n}^{\otimes n} \parallel \sigma^{\otimes n}) \quad (11.128)$$

$$\geq \max_{\sigma \in \mathcal{S}(\mathcal{H})} \frac{1}{2}\widehat{\alpha}_{2 \exp\{-nR\}}(W_{\mathbf{x}^n}^{\otimes n} \parallel \sigma^{\otimes n}) \quad (11.129)$$

$$\geq \frac{1}{2}\widehat{\alpha}_{2 \exp\{-nR\}}(W_{\mathbf{x}^n}^{\otimes n} \parallel (\sigma^*)^{\otimes n}), \quad (11.130)$$

where  $\mathcal{C}'_n$  is an expurgated code with message size  $|\mathcal{C}'_n| = \lceil |\mathcal{C}_n|/2 \rceil \geq \frac{1}{2} \exp\{nR\}$ . Inequality (11.129) holds because the map  $\mu \mapsto \widehat{\alpha}_\mu$  is monotone decreasing. In the last line (11.130) we denote by

$$\sigma^* = \sigma_{R, P_{\mathbf{x}^n}}^* := \arg \min_{\sigma \in \mathcal{S}(\mathcal{H})} \sup_{0 < \alpha \leq 1} \left\{ \frac{1-\alpha}{\alpha} (D_\alpha(\mathcal{W} \parallel \sigma | P_{\mathbf{x}^n}) - R) \right\} \quad (11.131)$$

a channel output state that depends on the coding rate  $R$  and the composition  $P_{\mathbf{x}^n}$ .

In the following, we deal with sequences of inputs that will yield different lower bounds. Fix an arbitrary  $\delta \in (0, E_{\text{sp}}(R))$ . Let  $\nu := E_{\text{sp}}(R) - \delta > 0$ , and define:

$$\mathcal{P}_{R,\nu}(\mathcal{X}) := \left\{ P_{\mathbf{x}^n} \in \mathcal{P}(\mathcal{X}) : \nu \leq E_{\text{sp}}^{(2)}(R, P_{\mathbf{x}^n}) \leq E_{\text{sp}}(R) < +\infty \right\}. \quad (11.132)$$

The set  $\mathcal{P}_{R,\nu}(\mathcal{X})$  ensures that the error exponents of the input sequences  $\mathbf{x}^n$  with composition  $P_{\mathbf{x}^n} \in \mathcal{P}_{R,\nu}(\mathcal{X})$  are close to the sphere-packing exponent  $E_{\text{sp}}(R)$ .

For sequences  $\mathbf{x}^n$  with  $P_{\mathbf{x}^n} \notin \mathcal{P}_{R,\nu}(\mathcal{X})$ , we infer that

$$E_{\text{sp}}(R) - E_{\text{sp}}^{(2)}(R, P_{\mathbf{x}^n}) = \delta > 0. \quad (11.133)$$

We then apply the Chebyshev-type bound, Proposition 11.3, with  $c = 2$  to obtain,  $\forall P_{\mathbf{x}^n} \notin \mathcal{P}_{R,\nu}(\mathcal{X})$ ,

$$\widehat{\alpha}_{2 \exp\{-nR\}}(W_{\mathbf{x}^n}^{\otimes n} \parallel (\sigma^*)^{\otimes n}) \geq \kappa_1 \exp\left\{-\kappa_2 \sqrt{n} - n E_{\text{sp}}^{(2)}(R, P_{\mathbf{x}^n})\right\}, \quad (11.134)$$

$$\geq \kappa_1 \exp\left\{-\kappa_2 \sqrt{n} - n [E_{\text{sp}}(R) - \delta]\right\}, \quad (11.135)$$

for all sufficiently large  $n$ , say  $n \geq N_1 \in \mathbb{N}$ . The equality in Eq. (11.134) follows from the saddle-point property, item (a) in Proposition 9.5, and the constants  $\kappa_1, \kappa_2$  are positive and finite constants.

Next, we consider sequences  $\mathbf{x}^n$  with  $P_{\mathbf{x}^n} \in \mathcal{P}_{R,\nu}(\mathcal{X})$ . Since such sequences satisfy Eq. (11.72), we apply the sharp lower bound, Proposition 11.4, with  $c = 2$  to obtain,  $\forall P_{\mathbf{x}^n} \in \mathcal{P}_{R,\nu}(\mathcal{X})$ ,

$$\widehat{\alpha}_{2 \exp\{-nR\}} (W_{\mathbf{x}^n}^{\otimes n} \| (\sigma^*)^{\otimes n}) \geq \frac{2A}{n^{\frac{1}{2}(1+s_{R,P_{\mathbf{x}^n}}^*)}} \exp\left\{-nE_{\text{sp}}^{(2)}(R, P_{\mathbf{x}^n})\right\}, \quad (11.136)$$

for all sufficiently large  $n$ , say  $n \geq N_2 \in \mathbb{N}$ , and some  $A \in \mathbb{R}_{>0}$ . In the following, we will relate the term  $s_{R,P_{\mathbf{x}^n}}^*$  in Eq. (11.136) to  $|E'_{\text{sp}}(R)|$ . The idea follows similar from [98, Eqs. (111)–(114)]. Let

$$\mathcal{P}_R^*(\mathcal{X}) := \left\{ P \in \mathcal{P}(\mathcal{X}) : E_{\text{sp}}^{(2)}(R, P) = E_{\text{sp}}(R) \right\}, \quad (11.137)$$

$$\mathcal{P}_\theta(\mathcal{X}) := \left\{ P \in \mathcal{P}_{R,\nu}(\mathcal{X}) : \min_{Q \in \mathcal{P}_R^*(\mathcal{X})} \|P - Q\|_1 \geq \theta \right\}. \quad (11.138)$$

Since  $s_{R,(\cdot)}^*$  is uniformly continuous on the compact set  $P \in \mathcal{P}_{R,\nu}(\mathcal{X})$  (see item (d) of Proposition 9.5), one has

$$\forall \gamma \in \mathbb{R}_{>0}, \exists f(\gamma) \in \mathbb{R}_{>0}, \text{ such that } \forall P, Q \in \mathcal{P}_{R,\nu}(\mathcal{X}), \|P - Q\|_1 < f(\gamma) \Rightarrow |s_{R,P}^* - s_{R,Q}^*| < \gamma. \quad (11.139)$$

By choosing  $\gamma \in \mathbb{R}_{>0}$  that satisfies Eq. (11.139), it follows that

$$s_{R,P_{\mathbf{x}^n}}^* \leq |E'_{\text{sp}}(R)| + \gamma, \quad \forall P_{\mathbf{x}^n} \in \mathcal{P}_{R,\nu}(\mathcal{X}) \setminus \mathcal{P}_{f(\gamma)}(\mathcal{X}). \quad (11.140)$$

Hence, Eqs. (11.136) and (11.140) further lead to,  $\forall P_{\mathbf{x}^n} \in \mathcal{P}_{R,\nu}(\mathcal{X}) \setminus \mathcal{P}_{f(\gamma)}(\mathcal{X})$ ,

$$\widehat{\alpha}_{2 \exp\{-nR\}} (W_{\mathbf{x}^n}^{\otimes n} \| (\sigma^*)^{\otimes n}) \geq \frac{2A}{n^{\frac{1}{2}(1+|E'_{\text{sp}}(R)|+\gamma)}} \exp\{-nE_{\text{sp}}(R)\}. \quad (11.141)$$

For the case  $P_{\mathbf{x}^n} \in \mathcal{P}_{R,\nu}(\mathcal{X}) \cap \mathcal{P}_{f(\gamma)}(\mathcal{X})$ , we have

$$E_{\text{sp}}(R) - \max_{P \in \mathcal{P}_{f(\gamma)}(\mathcal{X})} E_{\text{sp}}^{(2)}(R, P_{\mathbf{x}^n}) =: \delta' > 0. \quad (11.142)$$

Then, Eqs. (11.136) and (11.142) give,  $\forall P_{\mathbf{x}^n} \in \mathcal{P}_{R,\nu}(\mathcal{X}) \cap \mathcal{P}_{f(\gamma)}(\mathcal{X})$ ,

$$\widehat{\alpha}_{2 \exp\{-nR\}} (W_{\mathbf{x}^n}^{\otimes n} \| (\sigma^*)^{\otimes n}) \geq \frac{2A}{n^{\frac{1}{2}(1+s_{R,P_{\mathbf{x}^n}}^*)}} \exp\{-n[E_{\text{sp}}(R) - \delta']\}. \quad (11.143)$$

Finally, by comparing the bounds in Eqs. (11.135), (11.141) and (11.143), the first-order leading term in the right-hand side of Eq. (11.141) decays faster than that of Eqs. (11.135) and (11.143). Thus, for sufficiently large  $n$ , say  $n \geq N_3 \in \mathbb{N}$ , we combine the bounds to obtain, for all compositions  $P_{\mathbf{x}^n} \in \mathcal{P}(\mathcal{X})$ ,

$$\widehat{\alpha}_{2 \exp\{-nR\}} (W_{\mathbf{x}^n}^{\otimes n} \| (\sigma^*)^{\otimes n}) \geq \frac{2A}{n^{\frac{1}{2}(1+|E'_{\text{sp}}(R)|+\gamma)}} \exp\{-nE_{\text{sp}}(R)\}. \quad (11.144)$$

By combining Eqs. (11.130), (11.144), we conclude our result: for any  $\gamma > 0$  and every  $n$ -blocklength

constant composition code  $\mathcal{C}_n$ ,

$$\bar{\varepsilon}(\mathcal{C}_n) \geq \frac{A}{n^{\frac{1}{2}(1+|E'_{\text{sp}}(R)|+\gamma)}} \exp \{-nE_{\text{sp}}(R)\}, \quad (11.145)$$

for all sufficiently large  $n \geq N_0 := \max \{N_1, N_2, N_3\}$ .  $\square$

*Proof of Corollary 11.1.* For an  $n$ -blocklength code, there are at most  $\binom{n+|\mathcal{X}|-1}{|\mathcal{X}|-1} < n^{|\mathcal{X}|}$  different compositions. Hence, for any code with  $M = \exp\{nR\}$  codewords, there exists some codewords  $M'$  of the same composition such that  $M' \geq M/n^{|\mathcal{X}|}$ . Denote by  $\mathcal{C}'_n$  such constant composition codes with composition  $P_{\mathbf{x}^n}$ .

Fix an arbitrary  $R_0 \in (R_\infty, R)$ , and choose  $N_1$  be an integer such that  $R - \frac{|\mathcal{X}|}{n} \log n \geq R_0$  for all  $n \geq N_1$ . Consider such  $n \geq N_1$  onwards. By following the similar steps in Theorem 11.1, we obtain

$$\varepsilon^*(n, R) \geq \bar{\varepsilon}(\mathcal{C}'_n) \geq \frac{A}{n^{\frac{1}{2}(1+s_{R, P_{\mathbf{x}^n}}^*)}} \exp \left\{ -nE_{\text{sp}}^{(2)} \left( R - \frac{|\mathcal{X}|}{n} \log n, P_{\mathbf{x}^n} \right) \right\}, \quad (11.146)$$

for all sufficiently large  $n$ , say  $n \geq N_2 \in \mathbb{N}$ , and some  $s_{R, P_{\mathbf{x}^n}}^* \in \mathbb{R}_{>0}$ . Let

$$\Upsilon := \max_{P \in \mathcal{P}(\mathcal{X}): E_{\text{sp}}^{(2)}(\bar{R}, P) = E_{\text{sp}}(\bar{R})} \left| \frac{\partial E_{\text{sp}}^{(2)}(r, P)}{\partial r} \right|_{r=R_0}. \quad (11.147)$$

Then, item (a) in Proposition 9.6 implies that

$$E_{\text{sp}}^{(2)} \left( R - \frac{|\mathcal{X}|}{n} \log n, P_{\mathbf{x}^n} \right) \leq E_{\text{sp}}^{(2)}(R, P_{\mathbf{x}^n}) + \Upsilon \cdot \frac{|\mathcal{X}|}{n} \log n \quad (11.148)$$

$$\leq E_{\text{sp}}(R) + \Upsilon \cdot \frac{|\mathcal{X}|}{n} \log n, \quad \forall n \geq N_2 \quad (11.149)$$

Combining Eqs. (11.146) and (11.149) gives

$$\varepsilon^*(n, R) \geq \frac{A}{n^{\frac{1}{2}(1+s_{R, P_{\mathbf{x}^n}}^*)+\Upsilon|\mathcal{X}|}} \exp \{-nE_{\text{sp}}(R)\}, \quad \forall n \geq \max\{N_1, N_2\}. \quad (11.150)$$

By choosing  $t \in \mathbb{R}_{>0}$  such that  $n^{-t} \leq An^{-\frac{1}{2}(1+s_{R, P_{\mathbf{x}^n}}^*)-\Upsilon|\mathcal{X}|}$ , and letting  $N_0 := \max\{N_1, N_2\}$ , we conclude our claim.  $\square$

## 11.4 Symmetric Classical-Quantum Channels

In this section, we consider a symmetric c-q channels. By using the symmetric property of the channels, we show that the uniform distribution, denoted by  $U_{\mathcal{X}}$ , achieves the maximum of  $E_{\text{sp}}^{(1)}(R, \cdot)$  and  $E_{\text{sp}}^{(2)}(R, \cdot)$ . Then, by choosing the optimal output state  $\sigma_R^* = \sigma_{R, U_{\mathcal{X}}}^*$ , every input sequence in the codebook is a good codeword and attains the sphere-packing exponent  $E_{\text{sp}}(R)$ . Hence, we can remove the assumption of constant composition codes and apply Theorem 11.1 to obtain the exact pre-factor for the sphere-packing bound (Theorem 11.3).

A c-q channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  is *symmetric* if it satisfies

$$W_x := V^{x-1} W_1 (V^\dagger)^{x-1}, \quad \forall x \in \mathcal{X}, \quad (11.151)$$

where  $W_1 \in \mathcal{S}(\mathcal{H})$  is an arbitrary density operator, and  $V$  satisfies  $V^\dagger V = VV^\dagger = V^{|\mathcal{X}|} = \mathbb{1}_{\mathcal{H}}$ .

**Theorem 11.3** (Exact Sphere-packing Bound for Symmetric Classical-Quantum Channels). *For any rate  $R \in (R_\infty, C_{\mathcal{W}})$ , there exist  $A > 0$  and  $N_0 \in \mathbb{N}$  such that for all codes  $\mathcal{C}_n$  of length  $n \geq N_0$  with message size  $|\mathcal{C}_n| \geq \exp\{nR\}$ , we have*

$$\varepsilon_{\max}(\mathcal{C}_n) \geq \frac{A}{n^{\frac{1}{2}(1+|E'_{\text{sp}}(R)|)}} \exp\{-nE_{\text{sp}}(R)\}. \quad (11.152)$$

*Proof of Theorem 11.3.* The proof consists of the following steps. First, we show that the distribution  $U_{\mathcal{X}}$  satisfies  $E_{\text{sp}}^{(1)}(R, U_{\mathcal{X}}) = E_{\text{sp}}^{(2)}(R, U_{\mathcal{X}}) = E_{\text{sp}}(R)$ . Second, we show that  $E_{\text{sp}}^{(2)}(R, P) = E_{\text{sp}}(R)$  for all  $P \in \mathcal{P}(\mathcal{X})$ , which means that any codeword attains the sphere-packing exponent. Finally, we follow Theorem 11.1 to complete the proof.

Fix any  $R \in (C_{0,\mathcal{W}}, C_{\mathcal{W}})$ . From the definition of the symmetric channels in Eq. (11.151), it is not hard to verify that  $U_{\mathcal{X}} \mathcal{W}^\alpha = V U_{\mathcal{X}} \mathcal{W}^\alpha V^\dagger$  for all  $\alpha \in (0, 1]$ , where we denote by  $P \mathcal{W}^\alpha := \sum_{x \in \mathcal{X}} P(x) W_x^\alpha$  for all  $\alpha \in (0, 1]$ . Hence, it follows that

$$\text{Tr}[W_x^\alpha (U_{\mathcal{X}} \mathcal{W}^\alpha)^{\frac{1-\alpha}{\alpha}}] = \text{Tr}[V^{x-1} W_1^\alpha V^{\dagger x-1} (U_{\mathcal{X}} \mathcal{W}^\alpha)^{\frac{1-\alpha}{\alpha}}] \quad (11.153)$$

$$= \text{Tr}[W_1^\alpha (U_{\mathcal{X}} \mathcal{W}^\alpha)^{\frac{1-\alpha}{\alpha}}] \quad (11.154)$$

for all  $x \in \mathcal{X}$  and  $\alpha \in (0, 1]$ . Summing Eq. (11.154) over all  $x \in \mathcal{X}$  and dividing by  $M$  yields

$$\text{Tr}[W_x^\alpha (U_{\mathcal{X}} \mathcal{W}^\alpha)^{\frac{1-\alpha}{\alpha}}] = \text{Tr}[(U_{\mathcal{X}} \mathcal{W}^\alpha)^{\frac{1}{\alpha}}], \quad (11.155)$$

for all  $x \in \mathcal{X}$  and  $\alpha \in (0, 1]$ . Recalling Proposition 11.6 below, the above equation shows that the distribution  $U_{\mathcal{X}}$  indeed maximizes  $E_0(s, P)$ ,  $\forall s \in \mathbb{R}_{\geq 0}$ . Then we have

$$E_{\text{sp}}^{(1)}(R, U_{\mathcal{X}}) = \sup_{s \geq 0} \left\{ \max_{P \in \mathcal{P}(\mathcal{X})} E_0(s, P) - sR \right\} = E_{\text{sp}}(R).$$

Further, Jensen's inequality shows that  $E_{\text{sp}}^{(2)}(R, U_{\mathcal{X}}) \geq E_{\text{sp}}^{(1)}(R, U_{\mathcal{X}}) = E_{\text{sp}}(R)$ , and thus,  $E_{\text{sp}}^{(2)}(R, U_{\mathcal{X}}) = E_{\text{sp}}(R)$ .

Next, let  $(\alpha_R^*, \sigma_R^*)$  be the saddle-point of  $F_{R, U_{\mathcal{X}}}(\cdot, \cdot)$  (see Eq. (9.143)). One can observe from the definition of  $E_{\text{sp}}^{(2)}$  and Eq. (11.155) that all the quantities  $D_{\alpha_R^*}(W_x \| \sigma_R^*)$ ,  $x \in \mathcal{X}$ , are equal. Hence, quantum Sibson's identity given in Lemma 3.3 shows that

$$\sigma_R^* = \frac{(U_{\mathcal{X}} \mathcal{W}^{\alpha_R^*})^{1/\alpha_R^*}}{\text{Tr}[(U_{\mathcal{X}} \mathcal{W}^{\alpha_R^*})^{1/\alpha_R^*}]}, \quad (11.156)$$

which, in turn, implies that

$$E_{\text{sp}}^{(2)}(R, P) = \sup_{\alpha \in (0, 1]} F_{R, P}(\alpha, \sigma_R^*) = \sup_{s \geq 0} \{E_0(s, U_{\mathcal{X}}) - sR\} = E_{\text{sp}}(R), \quad \forall P \in \mathcal{P}(\mathcal{X}). \quad (11.157)$$

Further, we have

$$|E'_{\text{sp}}(R)| = \frac{1 - \alpha_R^*}{\alpha_R^*} = \left| \frac{\partial E_{\text{sp}}^{(2)}(R, P)}{\partial R} \right|, \quad \forall P \in \mathcal{P}(\mathcal{X}). \quad (11.158)$$

Since Eqs. (11.157) and (11.158) indicates that every input sequence attains the sphere-packing exponent, we apply the same arguments in the proof of Theorem 11.1 to conclude this theorem.

**Proposition 11.6** ([2, Eq. (38)]). *Let  $s \in \mathbb{R}_{\geq 0}$  be arbitrary. The Necessary and sufficient condition for the distribution  $P^*$  to maximize  $E_0(s, P)$  is*

$$\text{Tr} \left[ W_x^{1/(1+s)} \cdot \left( \sum_{x \in \mathcal{X}} P^*(x) W_x^{1/(1+s)} \right)^s \right] \geq \text{Tr} \left[ \left( \sum_{x \in \mathcal{X}} P^*(x) W_x^{1/(1+s)} \right)^{1+s} \right], \quad \forall x \in \mathcal{X} \quad (11.159)$$

with equality if  $P^*(x) \neq 0$ .

□

## Chapter 12

# Moderate Deviation Analysis (Channel Coding)

This section presents our main results—the error performance of classical-quantum channels satisfies the moderate deviation property, Eq. (1.6). The achievability part is stated in Theorem 12.1, and its proof is given in Section 12.1. Our proof strategy employs Hayashi’s bound [94] and the properties of the modified auxiliary function (Proposition 9.2). Theorem 12.2 contains the converse part, and is proved in Section 12.2. The proof involves a weak sphere-packing bound (Theorem 11.2), a sharp converse lower bound (Theorem 11.1), and an approximation of the error-exponent function around capacity (Proposition 12.2).

Let  $(a_n)_{n \in \mathbb{N}}$  be a sequence of real numbers satisfying

$$\begin{aligned} \text{(i)} \quad & a_n \rightarrow 0, \quad \text{as } n \rightarrow +\infty, \\ \text{(ii)} \quad & a_n \sqrt{n} \rightarrow +\infty, \quad \text{as } n \rightarrow +\infty. \end{aligned} \tag{12.1}$$

Unlike our proof techniques relying on error exponent analysis (the LDP regime), a recent and independent paper [161] obtained the same result, but proceeds from the second-order analysis (the CLT regime). Their achievability proof follows from the one-shot capacity by Hayashi and Nagaoka [93] (see also Hayashi [94], and Wang and Renner [162]); while the converse part reduces channel coding to hypothesis testing [163, 93, 44], followed by Strassen’s Gaussian approximation [13] and a powerful inequality in probability [164] to the quantum scenario.

**Theorem 12.1** (Achievability). *For any  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  with  $V_{\mathcal{W}} > 0$  and any sequence  $(a_n)_{n \geq 1}$  satisfying Eq. (12.1), there exists a sequence of codes  $\{\mathcal{C}_n\}_{n \geq 1}$  with rates  $R_n = C_{\mathcal{W}} - a_n$  so that*

$$\limsup_{n \rightarrow +\infty} \frac{1}{na_n^2} \log \bar{\varepsilon}(\mathcal{W}, \mathcal{C}_n) \leq -\frac{1}{2V_{\mathcal{W}}}, \tag{12.2}$$

where  $C_{\mathcal{W}}$  and  $V_{\mathcal{W}}$  are defined in Eqs. (3.33) and (3.36).

The proof is given in Section 12.1.

**Theorem 12.2** (Converse). *For any  $W \in \mathcal{W}(\mathcal{X})$  with  $V(W) > 0$ , any sequence  $\{a_n\}_{n \geq 1}$  satisfying Eq. (12.1), and any sequence of codes  $\{\mathcal{C}_n\}_{n \geq 1}$  with rates  $R_n = C(W) - a_n$ , it holds that*

$$\liminf_{n \rightarrow +\infty} \frac{1}{na_n^2} \log \bar{\varepsilon}(W, \mathcal{C}_n) \geq -\frac{1}{2V(W)}. \quad (12.3)$$

The proof is given in Section 12.2.

*Remark 12.1.* Altug and Wagner [43] proved Theorem 12.2 for discrete classical channels by a weak sphere-packing bound with the expression of  $\tilde{E}_{\text{sp}}$ . Although such a weak sphere-packing bound indeed holds for c-q channels (as we have shown in Theorem 11.2 and Remark 11.1 in Section 11.2), Proposition 12.2 in Section 12.2 shows that it will lead to

$$\limsup_{n \rightarrow +\infty} \frac{1}{na_n^2} \log \bar{\varepsilon}(\mathcal{W}, \mathcal{C}_n) \geq -\frac{1}{2\tilde{V}_{\mathcal{W}}}, \quad (12.4)$$

where  $\tilde{V}_{\mathcal{W}}$  is defined in Eq. (3.37). Since  $\tilde{V}(\rho\|\sigma) \leq V(\rho\|\sigma)$  [165, Theorem 1.2], it holds that  $\tilde{V}_{\mathcal{W}} \leq V_{\mathcal{W}}$  and the equality happens if and only if the channel reduces to classical. Hence, Altug and Wagner's method yields a weaker result in quantum regime; namely, a gap between the achievability and the converse. In Section 12.2, we will employ a sharp converse bound from strong large deviation theory to achieve our result, Theorem 12.2.

## 12.1 Proof of Achievability, Theorem 12.1

Let  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  satisfy  $V_{\mathcal{W}} > 0$ . Let  $\{a_n\}_{n \geq 1}$  be any sequence of real numbers satisfying Eq. (12.1). Since  $V_{\mathcal{W}} > 0$ , Eq. (3.38) in Section 3.3 shows that  $C_{\mathcal{W}} > 0$ . Hence, we have  $C_{\mathcal{W}} - a_n > 0$ , for all sufficiently large  $n$ . Fix such an integer  $n$  onwards. The achievability bound, Theorem 10.1, in Chapter 10 implies that there exists a code  $\mathcal{C}_n$  with  $R_n = C_{\mathcal{W}} - a_n$  so that

$$\bar{\varepsilon}(\mathcal{W}, \mathcal{C}_n) \leq 6 \exp \left\{ -n \left[ \max_{0 \leq s \leq 1} \left\{ E_0^{\downarrow}(s, P, P\mathcal{W}) - sR_n \right\} \right] \right\}, \quad (12.5)$$

for all  $P \in \mathcal{P}(\mathcal{X})$ . In the following, we denote by  $E_0^{\downarrow}(s, P) := E_0^{\downarrow}(s, P, P\mathcal{W})$  for notational convenience. Simple algebra yields

$$\frac{1}{na_n^2} \log \bar{\varepsilon}(\mathcal{W}, \mathcal{C}_n) \leq \frac{\log 6}{na_n^2} - \frac{1}{a_n^2} \max_{0 \leq s \leq 1} \left\{ E_0^{\downarrow}(s, P) - sR_n \right\}, \quad (12.6)$$

for all sufficiently large  $n$  and any  $P \in \mathcal{P}(\mathcal{X})$ .

Let  $\tilde{\mathcal{P}}(\mathcal{X})$  be the set of distributions that achieve the minimum in Eq. (3.36), and let  $\tilde{P} \in \tilde{\mathcal{P}}(\mathcal{X})$ . Note that Ref. [18, Lemma 3] implies that  $\tilde{\mathcal{P}}(\mathcal{X})$  is compact. Applying Taylor's theorem to  $E_0^{\downarrow}(s, \tilde{P})$  at  $s = 0$  together with Proposition 9.2 gives

$$E_0^{\downarrow}(s, \tilde{P}) = sC_{\mathcal{W}} - \frac{s^2}{2}V_{\mathcal{W}} + \left. \frac{s^3}{6} \frac{\partial^3 E_0^{\downarrow}(s, \tilde{P})}{\partial s^3} \right|_{s=\bar{s}}, \quad (12.7)$$

for some  $\bar{s} \in [0, s]$ . Let  $s_n = a_n/V_{\mathcal{W}}$ . Then  $s_n \leq 1$  for all sufficiently large  $n$  by the assumption in

Eq. (12.1) and  $V_{\mathcal{W}} > 0$ . For all  $s_n \leq 1$ , Eq. (12.7) yields

$$\max_{0 \leq s \leq 1} \left\{ E_0^\downarrow(s, \tilde{P}) - sR_n \right\} \geq E_0^\downarrow(s_n, \tilde{P}) - s_n R_n \quad (12.8)$$

$$= \frac{a_n}{V_{\mathcal{W}}} (C_{\mathcal{W}} - R_n) - \frac{a_n^2}{2V_{\mathcal{W}}} + \frac{a_n^3}{6V_{\mathcal{W}}^3} \left. \frac{\partial^3 E_0^\downarrow(s, \tilde{P})}{\partial s^3} \right|_{s=\bar{s}_n} \quad (12.9)$$

$$= \frac{a_n^2}{2V_{\mathcal{W}}} + \frac{a_n^3}{6V_{\mathcal{W}}^3} \left. \frac{\partial^3 E_0^\downarrow(s, \tilde{P})}{\partial s^3} \right|_{s=\bar{s}_n}, \quad (12.10)$$

where  $\bar{s}_n \in [0, s_n]$  and Eq. (12.10) holds since  $R_n = C_{\mathcal{W}} - a_n$ .

Define

$$\Upsilon = \max_{(s, P) \in [0, 1] \times \tilde{\mathcal{P}}(\mathcal{X})} \left| \frac{\partial^3 E_0^\downarrow(s, P)}{\partial s^3} \right|, \quad (12.11)$$

which is finite due to the compact set  $[0, 1] \times \tilde{\mathcal{P}}(\mathcal{X})$  and item (a) in Proposition 9.2. Therefore, Eq. (12.10) implies that

$$\max_{0 \leq s \leq 1} \left\{ E_0^\downarrow(s, \tilde{P}) - sR_n \right\} \geq \frac{a_n^2}{2V_{\mathcal{W}}} + \frac{a_n^3}{6V_{\mathcal{W}}^3} \left. \frac{\partial^3 E_0^\downarrow(s, \tilde{P})}{\partial s^3} \right|_{s=\bar{s}_n} \quad (12.12)$$

$$\geq \frac{a_n^2}{2V_{\mathcal{W}}} - \frac{a_n^3 \left| \frac{\partial^3 E_0^\downarrow(s, \tilde{P})}{\partial s^3} \right|_{s=\bar{s}_n}}{6V_{\mathcal{W}}^3} \quad (12.13)$$

$$\geq \frac{a_n^2}{2V_{\mathcal{W}}} - \frac{a_n^3 \Upsilon}{6V_{\mathcal{W}}^3}, \quad (12.14)$$

for all sufficiently large  $n$ .

Substituting Eq. (12.14) into Eq. (12.6) gives

$$\frac{1}{na_n^2} \log \bar{\varepsilon}(\mathcal{W}, \mathcal{C}_n) \leq \frac{\log 4}{na_n^2} - \frac{1}{2V_{\mathcal{W}}} \left( 1 - \frac{a_n \Upsilon}{3V_{\mathcal{W}}^2} \right). \quad (12.15)$$

Recall Eq. (12.1) and let  $n \rightarrow +\infty$ , which completes the proof:

$$\limsup_{n \rightarrow +\infty} \frac{1}{na_n^2} \log \bar{\varepsilon}(\mathcal{W}, \mathcal{C}_n) \leq -\frac{1}{2V_{\mathcal{W}}}. \quad (12.16)$$

□

## 12.2 Proof of Optimality, Theorem 12.2

Our strategy consists of the following steps. First, we claim that it suffices to prove Eq. (12.3) for the maximal error probability of any code  $\mathcal{C}_n$ , i.e.  $\varepsilon_{\max}(\mathcal{W}, \mathcal{C}_n)$ . Recall the standard expurgation method (see e.g. [31, p. 96], [33, Theorem 20], [25, p. 395]): by removing half codewords with highest error probability to arrive at  $\bar{\varepsilon}(\mathcal{W}, \mathcal{C}_n) \geq \frac{1}{2}\varepsilon_{\max}(\mathcal{W}, \mathcal{C}'_n)$  with  $|\mathcal{C}'_n| = \lceil |\mathcal{C}_n|/2 \rceil \geq \frac{1}{2}\exp\{nR_n\} = \exp\{n(R_n -$

$\frac{1}{n} \log 2) \}.$  Since the induced rate back-off is only  $\frac{1}{n} \log 2 = o(a_n)$ , one might define another sequence  $a'_n := a_n - \frac{1}{n} \log 2$  satisfying Eq. (12.1). Hence, without loss of generality, we only need to prove the converse part for  $\varepsilon_{\max}$ .

Second, we employ the method of Ref. [28, Lemma 16] to relate the error probability  $\varepsilon_{\max}$  to the minimum type-I error:

$$\frac{\log \varepsilon_{\max}(\mathcal{W}, \mathcal{C}_n)}{na_n^2} \geq \max_{\sigma^n \in \mathcal{S}(\mathcal{H}^{\otimes n})} \min_{\mathbf{x}^n \in \mathcal{X}^n} \frac{\log \widehat{\alpha}_{\exp\{-nR_n\}}(W_{\mathbf{x}^n}^{\otimes n} \| \sigma^n)}{na_n^2} \quad (12.17)$$

$$\geq \min_{\mathbf{x}^n \in \mathcal{X}^n} \frac{\log \widehat{\alpha}_{\exp\{-nR_n\}}(W_{\mathbf{x}^n}^{\otimes n} \| (P^* \mathcal{W})^{\otimes n})}{na_n^2}, \quad (12.18)$$

where  $P^* \in \mathcal{P}(\mathcal{X})$  is an arbitrary capacity-achieving distribution, i.e.  $I(P^*, \mathcal{W}) = C_{\mathcal{W}}$ .

Third, we divide the set of codewords into two groups. Fix an arbitrary  $\eta \in (0, \frac{1}{2})$ . Let  $A := \max_{\rho \in \mathcal{S}_0} V(\rho \| P^* \mathcal{W})$  and let  $\xi = \sqrt{2A/\eta}$ . Define:

$$\Omega_{\text{good}} := \{\mathbf{x}^n \in \mathcal{X}^n : D(\mathcal{W} \| P^* \mathcal{W} | P_{\mathbf{x}^n}) > R_n\}; \quad (12.19)$$

$$\Omega_{\text{bad}} := \mathcal{X}^n \setminus \Omega_{\text{good}}. \quad (12.20)$$

For the codes in  $\Omega_{\text{bad}}$ , we employ a weak converse bound in Theorem 11.2, and apply a sharp converse bound, Proposition 12.1 below, for  $\Omega_{\text{good}}$ . Furthermore, we can assume  $a_n > 0$  for all sufficiently large  $n \in \mathbb{N}$  owing to the assumption  $\lim_{n \rightarrow +\infty} a_n \sqrt{n} = +\infty$ . Subsequently, we will consider such  $n$  onwards. We remark that Proposition 12.1 follows the same argument as Proposition 11.4 in Section 11.3.3, and Chaganty-Sethuraman's concentration inequality, Theorem 2.2 in Section 2.2. Thus, we skip the proof.

*Proof of Theorem 12.2.* We start the proof with the case  $\Omega_{\text{bad}}$ , and further consider two different cases:

$$\Omega_{\text{bad}}^{(1)} := \left\{ \mathbf{x}^n \in \mathcal{X}^n : D(\mathcal{W} \| P^* \mathcal{W} | P_{\mathbf{x}^n}) \leq R_n - \frac{2\xi}{\sqrt{n}} \right\}; \quad (12.21)$$

$$\Omega_{\text{bad}}^{(2)} := \left\{ \mathbf{x}^n \in \mathcal{X}^n : R_n - \frac{2\xi}{\sqrt{n}} < D(\mathcal{W} \| P^* \mathcal{W} | P_{\mathbf{x}^n}) \leq R_n \right\}. \quad (12.22)$$

We apply the weak converse bound, Theorem 11.2, in Section 11.2 with  $\sigma = P^* \mathcal{W}$  to further lower bound the right-hand side of Eq. (12.18).

Let  $\eta$  and  $\xi$  be defined as above, and let  $N_1$  be an integer satisfying Eq. (11.13). Then Eq. (11.14) gives, for all  $n \geq N_1$ ,

$$\frac{\log \widehat{\alpha}_{\exp\{-nR_n\}}(W_{\mathbf{x}^n}^{\otimes n} \| (P^* \mathcal{W})^{\otimes n})}{na_n^2} \geq -\frac{\widetilde{E}_{\text{sp}}\left(R_n - \frac{2\xi}{\sqrt{n}}, P_{\mathbf{x}^n}, P^* \mathcal{W}\right)}{a_n^2(1-\eta)} + \frac{\log f(\eta)}{na_n^2}. \quad (12.23)$$

Further, Eq. (9.18) implies that for all  $\mathbf{x}^n \in \Omega_{\text{bad}}^{(1)}$ ,

$$\widetilde{E}_{\text{sp}}\left(R_n - \frac{2\xi}{\sqrt{n}}, P_{\mathbf{x}^n}, P^* \mathcal{W}\right) = 0. \quad (12.24)$$

Hence, we have for all  $\mathbf{x}^n \in \Omega_{\text{bad}}^{(1)}$ ,

$$\frac{\log \widehat{\alpha}_{\exp\{-nR_n\}}(W_{\mathbf{x}^n}^{\otimes n} \|(P^* \mathcal{W})^{\otimes n})}{na_n^2} \geq \frac{\log f(\eta)}{na_n^2} \quad (12.25)$$

$$\geq -\frac{1}{2V_{\mathcal{W}}} + \frac{\log f(\eta)}{na_n^2}, \quad (12.26)$$

where the last inequality follows from  $V_{\mathcal{W}} > 0$ . Since  $f(\eta) < +\infty$ , taking the infimum limit of  $n \rightarrow +\infty$  and using Eq. (12.1) give, for all  $\mathbf{x}^n \in \Omega_{\text{bad}}^{(1)}$ ,

$$\liminf_{n \rightarrow +\infty} \frac{\log \widehat{\alpha}_{\exp\{-nR_n\}}(W_{\mathbf{x}^n}^{\otimes n} \|(P^* \mathcal{W})^{\otimes n})}{na_n^2} \geq -\frac{1}{2V_{\mathcal{W}}}. \quad (12.27)$$

Next, we move on to  $\mathbf{x}^n \in \Omega_{\text{bad}}^{(2)}$ . In this case,  $\widetilde{E}_{\text{sp}}$  in Eq. (12.23) is not equal to zero for any finite  $n$ , we employ Eq. (12.45) in Proposition 12.2 below with  $\delta_n = a_n + 2\xi/\sqrt{n}$  and  $b_n = a_n$  to arrive at

$$\liminf_{n \rightarrow +\infty} \frac{\log \widehat{\alpha}_{\exp\{-nR_n\}}(W_{\mathbf{x}^n}^{\otimes n} \|(P^* \mathcal{W})^{\otimes n})}{na_n^2} \geq -\lim_{n \rightarrow +\infty} \frac{4\xi^2}{n \left(a_n + \frac{2\xi}{\sqrt{n}}\right)^2} \cdot \frac{1}{2\widetilde{V}_{\mathcal{W}}(1-\eta)} \quad (12.28)$$

$$= 0 \quad (12.29)$$

$$\geq -\frac{1}{2V_{\mathcal{W}}}, \quad (12.30)$$

where the equality follows since  $\lim_{n \rightarrow +\infty} na_n^2 = +\infty$ .

In the last case of  $\mathbf{x}^n \in \Omega_{\text{good}}$ , we employ a tighter bound, Proposition 12.1, to lower bound the right-hand side of Eq. (12.18).

**Proposition 12.1** (A Sharp Converse Bound). *Consider a classical-quantum channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  and a state  $\sigma \in \mathcal{S}(\mathcal{H})$ . Suppose the sequence  $\mathbf{x}^n \in \mathcal{X}^n$  satisfies*

$$\nu \leq V(\mathcal{W} \|\sigma|P_{\mathbf{x}^n}) < +\infty \quad (12.31)$$

for some  $\nu > 0$ , and suppose the sequence of rates  $(R_n)_{n \in \mathbb{N}}$  satisfies<sup>a</sup>  $D_0(\mathcal{W} \|\sigma|P_{\mathbf{x}^n}) < R_n < D(\mathcal{W} \|\sigma|P_{\mathbf{x}^n})$ . Then, there exists an  $N_0 \in \mathbb{N}$  such that, for all  $n \geq N_0$ ,

$$\widehat{\alpha}_{\exp\{-nR_n\}}(W_{\mathbf{x}^n}^{\otimes n} \|\sigma^{\otimes n}) \geq \frac{A}{s_n^* \sqrt{n}} \exp \left\{ -nE_{\text{sp}}^{(2)}(R_n - c_n, P_{\mathbf{x}^n}, \sigma) \right\}, \quad (12.32)$$

where  $c_n = \frac{K \log n}{n}$  and  $A, K > 0$  are finite constants independent of the sequence  $\mathbf{x}^n$ , and

$$s_n^* := \arg \max_{s \geq 0} \{E_{\text{h}}(s, P_{\mathbf{x}^n}, \sigma) - sR_n\}. \quad (12.33)$$

<sup>a</sup>Note that  $D_0(\mathcal{W} \|\sigma|P) = D(\mathcal{W} \|\sigma|P)$  implies  $W_x = \sigma$  for all  $x \in \text{supp}(P)$  [10, Corollary 4.1]. This further gives  $V(\mathcal{W} \|\sigma|P) = 0$ . However, the assumption in Eq. (12.31) ensures that  $\liminf_{n \in \mathbb{N}} D(\mathcal{W} \|\sigma|P_{\mathbf{x}^n}) - D_0(\mathcal{W} \|\sigma|P_{\mathbf{x}^n}) > 0$ . Hence, the intervals  $[D_0(\mathcal{W} \|\sigma|P_{\mathbf{x}^n}), D(\mathcal{W} \|\sigma|P_{\mathbf{x}^n})]$  for all  $\mathbf{x}^n$  satisfying Eq. (12.31) are not measure zero.

Before applying Proposition 12.1, we verify that the condition, Eq. (12.31), is satisfied. Define

$$v(\delta) := \min_{P \in \mathcal{P}(\mathcal{X})} \{V(\mathcal{W} \|P^* \mathcal{W}|P) : D(\mathcal{W} \|P^* \mathcal{W}|P) \geq C_{\mathcal{W}} - \delta\}. \quad (12.34)$$

Note that the map  $\delta \mapsto v(\delta)$  is monotone decreasing and continuous at 0 from above, i.e.  $\lim_{\delta \downarrow 0} v(\delta) = v(0) = V_W$  [18, Lemma 22]. For any  $\kappa \in (0, 1)$ , we can choose a sufficiently small  $\gamma > 0$  independent of the sequence  $\mathbf{x}^n$  such that  $v(\gamma) \geq (1 - \kappa)V_W =: \nu > 0$ . Further, let  $N_2 \in \mathbb{N}$  such that  $a_n \leq \gamma$  for all  $n \geq N_2$ . Then, one finds, for all  $\mathbf{x}^n \in \Omega_{\text{good}}$  and  $n \geq N_2$ ,

$$V(W \| P^* W | P_{\mathbf{x}^n}) \geq v(\gamma) \geq \nu > 0. \quad (12.35)$$

Moreover, since  $V_W > 0$  implies that  $C_W = \max_{P \in \mathcal{P}(\mathcal{X})} D(W \| P^* W | P) > \max_{P \in \mathcal{P}} D_0(W \| P^* W | P)$ , one can choose a sufficiently large  $n$ , say  $N_3 \in \mathbb{N}$ , such that  $R_n > D_0(W \| P^* W | P_{\mathbf{x}^n})$  for all  $n \geq N_3$ . Now, we have for all  $\mathbf{x}^n \in \Omega_{\text{good}}$  and  $n \geq \max\{N_2, N_3\}$  that

$$\max_{P \in \mathcal{P}(\mathcal{X})} D_0(W \| P^* W | P) < R_n < D(W \| P^* W | P_{\mathbf{x}^n}); \quad (12.36)$$

$$0 < \nu \leq V(W \| P^* W | P_{\mathbf{x}^n}). \quad (12.37)$$

Together with Eqs. (12.18) and (12.35) and letting  $\sigma = P^* W$ , Proposition 12.1 yields, for all  $\mathbf{x}^n \in \Omega_{\text{good}}$  and all sufficiently large  $n$ , say  $n \geq N_4 \in \mathbb{N}$ ,

$$\frac{\log \hat{\alpha}_{\exp\{-nR_n\}}(W_{\mathbf{x}^n}^{\otimes n} \| (P^* W)^{\otimes n})}{na_n^2} \geq -\frac{E_{\text{sp}}^{(2)}(R_n - c_n, P_{\mathbf{x}^n}, P^* W)}{a_n^2} - \frac{\log s_n^* \sqrt{n}}{na_n^2} + \frac{\log A}{na_n^2}. \quad (12.38)$$

Recall Eq. (12.46) in Proposition 12.2 below with  $b_n = 0$  and  $\delta_n = a_n + c_n$  that  $\limsup_{n \rightarrow +\infty} \frac{s_n^*}{a_n + c_n} \leq \frac{1}{V_W}$ . Hence, one can fix an arbitrary  $\zeta > 0$  and there exists an  $N_5 \in \mathbb{N}$  such that  $\frac{s_n^* \sqrt{n}}{(a_n + c_n)\sqrt{n}} \leq \frac{1}{V_W} + \zeta$  for all  $n \geq N_5$ . This then leads to for all sufficiently large  $n \geq \max\{N_2, N_3, N_4, N_5\}$  and all  $\mathbf{x}^n \in \Omega_{\text{good}}$ ,

$$\frac{\log \hat{\alpha}_{\exp\{-nR_n\}}(W_{\mathbf{x}^n}^{\otimes n} \| (P^* W)^{\otimes n})}{na_n^2} \geq -\frac{E_{\text{sp}}^{(2)}(R_n - c_n, P_{\mathbf{x}^n}, P^* W)}{a_n^2} - \frac{\log(a_n + c_n)\sqrt{n}}{na_n^2} + \frac{\log \frac{A}{V_W} + \zeta}{na_n^2}. \quad (12.39)$$

Taking  $n \rightarrow +\infty$ , the second and the third terms on the right-hand side of Eq. (12.39) vanish since  $c_n = K \frac{\log n}{n} = o(a_n)$  and the assumption  $\lim_{n \rightarrow +\infty} a_n \sqrt{n} = +\infty$ .

Next, we apply Eq. (12.44) in Proposition 12.2 again to bound the error-exponent function  $E_{\text{sp}}^{(2)}$  in Eq. (12.38): for all  $\mathbf{x}^n \in \Omega^{(3)}$

$$\liminf_{n \rightarrow +\infty} \frac{\log \hat{\alpha}_{\exp\{-nR_n\}}(W_{\mathbf{x}^n}^{\otimes n} \| (P^* W)^{\otimes n})}{na_n^2} \geq -\limsup_{n \rightarrow +\infty} \frac{E_{\text{sp}}^{(2)}(C_W - \delta_n, P_{\mathbf{x}^n}, P^* W)}{a_n^2} \quad (12.40)$$

$$= -\limsup_{n \rightarrow +\infty} \frac{E_{\text{sp}}^{(2)}(C_W - \delta_n, P_{\mathbf{x}^n}, P^* W)}{\delta_n^2} \quad (12.41)$$

$$\geq -\frac{1}{2V_W}. \quad (12.42)$$

Finally, combining Eqs. (12.18), (12.27), (12.30) and (12.42) concludes the desired Eq. (12.3).

**Proposition 12.2** (Error Exponent around Capacity). *Let  $(b_n)_{n \in \mathbb{N}}$  be a sequence of real numbers with  $\lim_{n \rightarrow +\infty} b_n = 0$  and let  $(\delta_n)_{n \in \mathbb{N}}$  be a sequence of positive numbers with  $\lim_{n \rightarrow +\infty} \delta_n = 0$ . Suppose the sequence of distributions  $(P_n)_{n \in \mathbb{N}}$  satisfies*

$$C_{\mathcal{W}} - \delta_n < D(\mathcal{W} \| P^* \mathcal{W} | P_n) \leq C_{\mathcal{W}} - b_n. \quad (12.43)$$

The following hold:

$$\limsup_{n \rightarrow +\infty} \frac{E_{\text{sp}}^{(2)}(C_{\mathcal{W}} - \delta_n, P_n, P^* \mathcal{W})}{\delta_n^2} \leq \limsup_{n \rightarrow +\infty} \frac{(\delta_n - b_n)^2}{2V_{\mathcal{W}} \delta_n^2}; \quad (12.44)$$

$$\limsup_{n \rightarrow +\infty} \frac{\tilde{E}_{\text{sp}}(C_{\mathcal{W}} - \delta_n, P_n, P^* \mathcal{W})}{\delta_n^2} \leq \limsup_{n \rightarrow +\infty} \frac{(\delta_n - b_n)^2}{2\tilde{V}_{\mathcal{W}} \delta_n^2}; \quad (12.45)$$

$$\limsup_{n \rightarrow +\infty} \frac{s_n^*}{\delta_n} \leq \frac{1}{V_{\mathcal{W}}}, \quad (12.46)$$

where

$$s_n^* := \arg \max_{s \geq 0} \{E_h(s, P_n, P^* \mathcal{W}) - s(C_{\mathcal{W}} - \delta_n)\}. \quad (12.47)$$

The proof of Proposition 12.2 is provided in Section 12.3 below.  $\square$

### 12.3 Asymptotic Expansions of Error-Exponent around Capacity

*Proof of Proposition 12.2.* We only prove Eqs. (12.44) and (12.46), since Eq. (12.45) follows from the same argument and Proposition 9.4.

Recall the error-exponent function  $E_{\text{sp}}^{(2)}$ :

$$E_{\text{sp}}^{(2)}(C_{\mathcal{W}} - \delta_n, P, P^* \mathcal{W}) = \sup_{s \geq 0} \{-s(C_{\mathcal{W}} - \delta_n) + E_h(s, P, P^* \mathcal{W})\}. \quad (12.48)$$

In the following, we fix  $\sigma = P^* \mathcal{W}$  in the definition of  $E_h$  (Eq. (9.9)) and denote by

$$E_h(s, P) := E_h(s, P, P^* \mathcal{W}) = sD_{\frac{1}{1+s}}(\mathcal{W} \| P^* \mathcal{W} | P). \quad (12.49)$$

for notational convenience. We define a *critical rate* for a c-q channel  $\mathcal{W}$  to be

$$r_{\text{cr}} := \max_{P \in \mathcal{P}(\mathcal{X})} \left. \frac{\partial E_h(s, P)}{\partial s} \right|_{s=1}. \quad (12.50)$$

Let  $N_0$  be the smallest integer such that  $C_{\mathcal{W}} - \delta_n > r_{\text{cr}}, \forall n \geq N_0$ . Since the map  $r \mapsto E_{\text{sp}}^{(2)}(r, \cdot, \cdot)$  is non-increasing [92, Section 5], the maximization over  $s$  in Eq. (12.48) can be restricted to the set  $[0, 1]$  for any rate above  $r_{\text{cr}}$ , i.e.,

$$E_{\text{sp}}^{(2)}(C_{\mathcal{W}} - \delta_n, P_n, P^* \mathcal{W}) = \max_{0 \leq s \leq 1} \{-s(C_{\mathcal{W}} - \delta_n) + E_h(s, P_n)\}. \quad (12.51)$$

For every  $n \in \mathbb{N}$ , let  $s_n^*$  attain the maxima in Eq. (12.51) at a rate of  $C_{\mathcal{W}} - \delta_n \geq 0$ . In the following lemma, we discuss the asymptotic behavior of  $\{s_n^*\}_{n \in \mathbb{N}}$ .

**Lemma 12.1.** Let  $s_n^*$  attain the maxima in Eq. (12.51) and  $P_n$  satisfy Eq. (12.43). We have

- (a) The limit point of  $\{P_n\}_{n \in \mathbb{N}}$  is capacity achieving.
- (b)  $s_n^* > 0$  for all  $n \in \mathbb{N}$  and  $\lim_{n \rightarrow +\infty} s_n^* = 0$ .

*Proof of Lemma 12.1.* Let  $(P_{n_k})_{k \in \mathbb{N}}$  and  $(s_{n_k}^*)_{k \in \mathbb{N}}$  be arbitrary subsequences. Since  $\mathcal{P}(\mathcal{X})$  and  $[0, 1]$  are compact, we may assume that

$$\lim_{k \rightarrow +\infty} P_{n_k} = P_o, \quad \lim_{k \rightarrow \infty} s_{n_k}^* = s_o, \quad (12.52)$$

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

(12.1-(a)) Let  $k \rightarrow +\infty$ . Eq. (12.43) implies that

$$D(\mathcal{W} \| P^* \mathcal{W} | P_o) = C_{\mathcal{W}}, \quad (12.53)$$

which guarantees that  $P_o$  is capacity-achieving by the dual representation of the information radius, see e.g. [166], [19, Theorem 2].

(12.1-(b)) One can observe from Eq. (12.51) that  $s_n^* = 0$  if and only if  $C_{\mathcal{W}} - \delta_n \geq D(\mathcal{W} \| P^* \mathcal{W} | P_n)$ . However, this violates the assumption in Eq. (12.43). Hence, we have  $s_n^* > 0$  for all  $n \in \mathbb{N}$ .

Since  $P_o$  is capacity achieving, the uniqueness of the divergence center implies that  $P_o \mathcal{W} = P^* \mathcal{W}$ . Item (c) in Proposition 9.3 shows that

$$\frac{\partial^2 E_h(s, P_o)}{\partial s^2} \Big|_{s=0} = -V(\mathcal{W} \| P^* \mathcal{W} | P_o) = -V(P_o, \mathcal{W}) \leq -V_{\mathcal{W}} < 0, \quad (12.54)$$

where the last inequality follows since  $V_{\mathcal{W}} > 0$ . Then, Eq. (12.54) implies that the first-order derivative  $\partial E_h(s, P_o) / \partial s$  is strictly decreasing around  $s = 0$ . Moreover, item (d) in Proposition 9.3 gives

$$\frac{\partial E_h(s, P_o)}{\partial s} \Big|_{s=s_o} \leq D(\mathcal{W} \| P^* \mathcal{W} | P_o) = C_{\mathcal{W}}, \quad (12.55)$$

This, together with items (b) and (c) in Proposition 9.3, shows that the first inequality in Eq. (12.55) becomes an equality if and only if  $s_o = 0$ . Since the subsequence was arbitrary, item (b) is shown. □

Now we are ready to prove this proposition. We start with proving Eq. (12.46). Since  $s \mapsto E_h(s, \cdot)$  is concave from item (b) in Proposition 9.3, the maximizer  $s_n^*$  must satisfy

$$\frac{\partial E_h(s, P_{n_k})}{\partial s} \Big|_{s=s_{n_k}^*} = C_{\mathcal{W}} - \delta_{n_k}. \quad (12.56)$$

Further, item (c) in Proposition 9.3 gives

$$\left. \frac{\partial E_h(s, P_{n_k}^*)}{\partial s} \right|_{s=0} = D(\mathcal{W} \| P^* \mathcal{W} | P_{n_k}^*). \quad (12.57)$$

The mean value theorem states that there exists a number  $\hat{s}_{n_k} \in (0, s_{n_k}^*)$ , for each  $k \in \mathbb{N}$ , such that

$$\left. -\frac{\partial^2 E_h(s, P_{n_k})}{\partial s^2} \right|_{s=\hat{s}_{n_k}} = \frac{D(\mathcal{W} \| P^* \mathcal{W} | P_{n_k}) - C_{\mathcal{W}} + \delta_{n_k}}{s_{n_k}^*} \quad (12.58)$$

$$\leq \frac{\delta_{n_k}}{s_{n_k}^*}, \quad (12.59)$$

where the last inequality is again due to  $D(\mathcal{W} \| P^* \mathcal{W} | P_{n_k}^*) \leq C_{\mathcal{W}}$ . When  $k$  approaches infinity, items (a) and (e) in Proposition 9.3 give

$$\lim_{k \rightarrow +\infty} \left. \frac{\partial^2 E_h(s, P_{n_k})}{\partial s^2} \right|_{s=\hat{s}_{n_k}} = \left. \frac{\partial^2 E_h(s, P_o)}{\partial s^2} \right|_{s=0} = -V(P_o, \mathcal{W}) \leq -V_{\mathcal{W}}. \quad (12.60)$$

Combining Eqs. (12.59) and (12.60) leads to

$$\limsup_{k \rightarrow +\infty} \frac{s_{n_k}^*}{\delta_{n_k}} \leq \frac{1}{V_{\mathcal{W}}}. \quad (12.61)$$

Since the subsequence was arbitrary, the above result establishes Eq. (12.46).

Next, for any sufficiently large  $n \geq N_0$ , we apply Taylor's theorem to the map  $s_n^* \mapsto E_h(s_n^*, P_n)$  at the original point to obtain

$$\begin{aligned} & E_{\text{sp}}^{(2)}(C_{\mathcal{W}} - \delta_n, P_n, P^* \mathcal{W}) \\ &= -s_n^*(C_{\mathcal{W}} - \delta_n) + E_h(s_n^*, P_n) \end{aligned} \quad (12.62)$$

$$= s_n^*(\delta_n + D(\mathcal{W} \| P^* \mathcal{W} | P_n) - C_{\mathcal{W}}) - \frac{(s_n^*)^2}{2} V(P_n, \mathcal{W}) + \frac{(s_n^*)^3}{6} \left. \frac{\partial^3 E_h(s, P_n)}{\partial s^3} \right|_{s=\bar{s}_n} \quad (12.63)$$

for some  $\bar{s}_n \in [0, s_n^*]$ . Let

$$\Upsilon = \max_{(s, P) \in [0, 1] \times \mathcal{P}(\mathcal{X})} \left| \frac{\partial^3 E_h(s, P)}{\partial s^3} \right|. \quad (12.64)$$

Continuing from Eq. (12.63) gives

$$E_{\text{sp}}^{(2)}(C_{\mathcal{W}} - \delta_n, P_n, P^* \mathcal{W}) \leq s_n^*(\delta_n - b_n) - \frac{(s_n^*)^2}{2} V(P_n, \mathcal{W}) + \frac{(s_n^*)^3 \Upsilon}{6} \quad (12.65)$$

$$\leq \sup_{s \geq 0} \left\{ s(\delta_n - b_n) - \frac{s^2}{2} V(P_n, \mathcal{W}) \right\} + \frac{(s_n^*)^3 \Upsilon}{6} \quad (12.66)$$

$$= \frac{(\delta_n - b_n)^2}{2V(P_n, \mathcal{W})} + \frac{(s_n^*)^3 \Upsilon}{6}, \quad (12.67)$$

where the first line follows from the assumption  $D(\mathcal{W} \| P^* \mathcal{W} | P_n) \leq C_{\mathcal{W}} - b_n$  in Eq. (12.43) and

Eq. (12.64). Finally, Eq. (12.67), along with item (b) in Lemma 12.1 and Eq. (12.61), implies that

$$\limsup_{n \rightarrow +\infty} \frac{E_{\text{SP}}^{(2)}(C_{\mathcal{W}} - \delta_n, P_n, P^* \mathcal{W})}{\delta_n^2} \leq \limsup_{n \rightarrow +\infty} \frac{(\delta_n - b_n)^2}{2V(P_n, \mathcal{W})\delta_n^2} \quad (12.68)$$

$$\leq \limsup_{n \rightarrow +\infty} \frac{(\delta_n - b_n)^2}{2V_{\mathcal{W}}\delta_n^2}, \quad (12.69)$$

where the last inequality follows from the continuity of  $V(\cdot, \mathcal{W})$  on  $\mathcal{P}(\mathcal{X})$  (Eq. (3.34)); the fact that  $\{P_n\}_{n \in \mathbb{N}}$  is capacity achieving (item (a) in Lemma 12.1); and the definition of  $V_{\mathcal{W}}$  in Eq. (3.36).

□

# Chapter 13

## Conclusions and Open problems

This thesis targets at characterizing the decoding error probability as a function of the coding blocklength. We study two fundamental quantum information processing protocols—the classical data compression (i.e. Slepian-Wolf coding) with quantum side information, and the classical-quantum channel coding. We have proven varieties of properties for the error exponent functions, which enables us to better understand the error behaviors of these information tasks. Then, we established numerous finite blocklength bounds for the optimal probability of error. Our results are not only of theoretical interests but also of practical values—they serve as the performance benchmark for designing the next generation quantum information technology. Lastly, we extend the derived finite blocklength results in the large deviation regime to the moderate deviation regime. We show that the optimal probability error vanishes asymptotically as the rate approaches the Slepian-Wolf limit/channel capacity slowly.

It is interesting to observe that there is an elegant duality between the two tasks when expressing the error exponent functions as conditional Rényi entropy and Rényi capacity. By exploiting this duality, we are able to unify the technical proofs these two tasks under the same framework of quantum hypothesis testing. Finally, we illustrate such relationship in Table 13.1 below, and depict the error exponent functions in Figure 13.1.

Bounds\Settings	Slepian-Wolf Coding with Quantum Side Information	Classical-Quantum Channel Coding
Achievability $(R < C_W \text{ or } R > H(X B)_\rho)$	$E_r(R) := \max_{0 \leq s \leq 1} \{E_0(s) - sR\}$ $= \max_{1/2 \leq \alpha \leq 1} \left\{ \frac{1-\alpha}{\alpha} (R - H_\alpha^\uparrow(X Y)_\rho) \right\}$	$E_r(R) := \max_{0 \leq s \leq 1} \left\{ \max_{P \in \mathcal{P}(\mathcal{X})} E_0(s, P) - sR \right\}$ $= \max_{1/2 \leq \alpha \leq 1} \left\{ \frac{1-\alpha}{\alpha} (C_{\alpha,W} - R) \right\}$
Optimality $(R < C_W \text{ or } R > H(X B)_\rho)$	$E_{sp}(R) := \sup_{s \leq 0} \{E_0(s) - sR\}$ $= \sup_{0 \leq \alpha \leq 1} \left\{ \frac{1-\alpha}{\alpha} (R - H_\alpha^\uparrow(X Y)_\rho) \right\}$	$E_{sp}(R) := \sup_{s \leq 0} \left\{ \max_{P \in \mathcal{P}(\mathcal{X})} E_0(s, P) - sR \right\}$ $= \sup_{0 \leq \alpha \leq 1} \left\{ \frac{1-\alpha}{\alpha} (C_{\alpha,W} - R) \right\}$
Strong Converse $(R > C_W \text{ or } R < H(X B)_\rho)$	$E_{sc}^*(R) := \sup_{-1 < s < 0} \{E_0^*(s) - sR\}$ $= \sup_{\alpha > 1} \left\{ \frac{1-\alpha}{\alpha} (R - H_\alpha^{*,\uparrow}(X Y)_\rho) \right\}$	$E_{sc}^*(R) := \sup_{-1 < s < 0} \left\{ \max_{P \in \mathcal{P}(\mathcal{X})} E_0^*(s, P) - sR \right\}$ $= \sup_{\alpha > 1} \left\{ \frac{1-\alpha}{\alpha} (C_{\alpha,W}^* - R) \right\}$
Auxiliary Function	$E_0(s) := -\log \text{Tr}_B \left[ \left( \text{Tr}_X (\rho_{XB})^{1/(1+s)} \right)^{1+s} \right]$	$E_0(s, P) := -\log \text{Tr} \left[ \left( \sum_{x \in \mathcal{X}} P(x) \cdot W_x^{1/(1+s)} \right)^{1+s} \right]$

Table 13.1: The comparison of the error exponent analysis for Slepian-Wolf coding with quantum side information and classical-quantum channel coding. We note that we only obtained suboptimal achievability results (i.e. with the exponent  $E_r^\downarrow(R)$  instead of  $E_r(R)$ ).

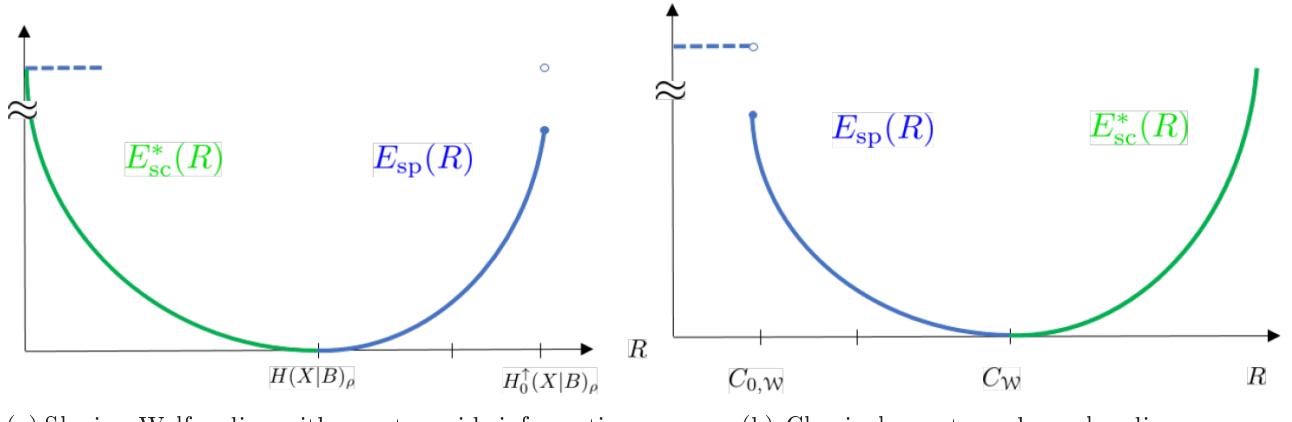


Figure 13.1: Sphere-packing exponents in two quantum information processing protocols.

## 13.1 Open Problems

There are still many open problems in the error exponent analysis. We divide them into the following categories: (a) Properties of the error exponent functions and auxiliary functions; (b) Random coding bound; (c) Sphere-packing bound; and (d) Moderate Deviation Analysis.

### 13.1.1 Properties of Error Exponent Functions and Auxiliary Functions

**Problem 1** (Concavity). *For any classical-quantum channel  $W : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$ , define the sandwiched auxiliary function:*

$$E_0^*(s, P) := \min_{\sigma \in \mathcal{S}(\mathcal{H})} s D_{\frac{1}{1+s}}^*(P \circ W \| P \otimes \sigma), \quad (s, P) \in (-1, +\infty) \times \mathcal{P}(\mathcal{X}), \quad (13.1)$$

where we denote by

$$D_\alpha(\rho \| \sigma) := \frac{1}{\alpha - 1} \log \text{Tr} \left[ \left( \sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}} \right)^\alpha \right], \quad \forall \alpha \geq 0 \quad (13.2)$$

the sandwiched  $\alpha$ -Rényi divergence [167, 65, 10].

Then, the map  $s \mapsto E_0^*(s, P)$  is concave for all  $s \in (-1, 0)$ .

*Remark 13.1.* We are able to show that the map  $s \mapsto E_0(s, P)$  is concave for all  $s \in (-1, 0)$ , where  $E_0(s, P)$  is defined via Petz's Rényi divergence. However, the sandwiched  $\alpha$ -Rényi divergence has been shown the tightest entropic quantity in the strong converse domain [65, 59]. Hence, the concavity of the sandwiched auxiliary function is the most relevant.  $\diamond$

**Problem 2** (Continuity of the Sphere-Packing Exponent). *Let  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  be a classical-quantum channel, and fix  $R \in (C_{0,W}, C_{1,W})$ . For every  $\nu > 0$ , there exists a constant  $c > 0$  such that for all  $P \in \mathcal{P}(\mathcal{X})$  with  $E_{\text{sp}}(R, P) \geq \nu$  and,*

$$E_{\text{sp}}^{(2)}(R, P) \leq E_{\text{sp}}(R) - c \|\sigma_{\alpha_{R,P}, P} - \sigma_{\alpha_R, \mathcal{W}}\|_1^2, \quad (13.3)$$

where

$$E_{\text{sp}}^{(2)}(R, P) := \sup_{0 \leq \alpha \leq 1} \frac{1-\alpha}{\alpha} \left( I_{\alpha}^{(2)}(P, \mathcal{W}) - R \right); \quad (13.4)$$

$$I_{\alpha}^{(2)}(P, \mathcal{W}) := \inf_{\sigma \in \mathcal{S}(\mathcal{H})} D_{\alpha}(\mathcal{W} \|\sigma|P); \quad (13.5)$$

and  $\sigma_{\alpha,P}$ ,  $\sigma_{\alpha,\mathcal{W}}$ ,  $\alpha_{R,P}$ ,  $\alpha_R$  are the optimizers such that

$$I_{\alpha}^{(2)}(P, \mathcal{W}) = D_{\alpha}(\mathcal{W} \|\sigma_{\alpha,P}|P); \quad (13.6)$$

$$C_{\alpha,\mathcal{W}} = \sup_{P \in \mathcal{P}(\mathcal{X})} D_{\alpha}(\mathcal{W} \|\sigma_{\alpha,\mathcal{W}}|P); \quad (13.7)$$

$$E_{\text{sp}}^{(2)}(R, P) = \frac{1-\alpha_{R,P}}{\alpha_{R,P}} \left( I_{\alpha_{R,P}}^{(2)}(P, \mathcal{W}) - R \right); \quad (13.8)$$

$$E_{\text{sp}}(R) = \frac{1-\alpha_R}{\alpha_R} (C_{\alpha_R,\mathcal{W}} - R). \quad (13.9)$$

### 13.1.2 Achievability: Random Coding Bound

We shorthand  $P_{\text{RC}}(n) := \mathbb{E}_{\mathcal{C}_n}[\bar{\varepsilon}(\mathcal{W}, \mathcal{C}_n)]$  the average probability of error for a  $n$ -blocklength random codes with distribution  $P \in \mathcal{P}(\mathcal{X})$  on the input alphabet  $\mathcal{X}$ . Moreover, the following conditional Rényi entropies and Rényi divergences are defined via Petz's version [60]; see Eq. (3.5).

**Problem 3** (Random Coding Bound for Slepian-Wolf Coding with Quantum Side Information). *Consider a Slepian-Wolf coding with a joint classical-quantum state  $\rho_{XB} \in \mathcal{S}(XB)$  with  $H(X|B)_{\rho} > 0$ . Let  $R < H(X|B)_{\rho}$ . The following holds for every  $n \in \mathbb{N}$ ,*

$$\varepsilon^*(n, R) \leq e^{-nE_r(R)}, \quad (13.10)$$

where

$$E_r(R) := \sup_{\frac{1}{2} \leq \alpha \leq 1} \frac{1-\alpha}{\alpha} \left( R - H_{\alpha}^{\uparrow}(X|B)_{\rho} \right); \quad (13.11)$$

$$H_{\alpha}^{\uparrow}(X|B)_{\rho} := \sup_{\sigma_B \in \mathcal{S}(B)} -D_{\alpha}(\rho_{XB} \|\mathbb{1}_X \otimes \sigma_B). \quad (13.12)$$

**Problem 4** (Random Coding Bound for Classical-Quantum Channels). *For any classical-quantum channel  $\mathcal{W} : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$ , rate  $R < C_{\mathcal{W}}$ , and any  $n \in \mathbb{N}$ ,*

$$P_{\text{RC}}(n) \leq e^{-nE_r(R,P)}, \quad (13.13)$$

where

$$E_r(R, P) := \sup_{\frac{1}{2} \leq \alpha \leq 1} \frac{1-\alpha}{\alpha} \left( I_{\alpha}^{(1)}(P, \mathcal{W}) - R \right); \quad (13.14)$$

$$I_{\alpha}^{(1)}(P, \mathcal{W}) := \inf_{\sigma \in \mathcal{S}(\mathcal{H})} D_{\alpha}(P \circ \mathcal{W} \| P \otimes \sigma). \quad (13.15)$$

Moreover, the optimal probability of error can be upper bounded as

$$\varepsilon^*(n, R) \leq e^{-nE_r(R)}, \quad (13.16)$$

where  $E_r(R) := \sup_{P \in \mathcal{P}(\mathcal{X})} E_r(R, P)$ .

**Problem 5** (Exact Asymptotics of Random Coding Bound for Classical-Quantum Channels). *For any classical-quantum channel  $W : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  and any  $n$ -blocklength block codes,*

$$P_{RC}(n) = \frac{1 + o(1)}{\sqrt{n}} e^{-nE_r(R, P)}, \quad R \leq C_{1/2, W} \quad (13.17)$$

$$P_{RC}(n) = \frac{1 + o(1)}{n^{\frac{1}{2}\left(1+\left|\frac{\partial E_r(R, P)}{\partial R}\right|\right)}} e^{-nE_r(R, P)}, \quad C_{1/2, W} < R < C_W. \quad (13.18)$$

**Problem 6** (Random Coding Bound for Entanglement-Assisted Codes). *Let  $\mathcal{N} : \mathcal{S}(\mathcal{A}) \rightarrow \mathcal{S}(\mathcal{B})$  be a quantum channel. Fix any rate below the entanglement-assisted classical capacity, i.e.  $R < C_{ea}(\mathcal{N})$ . The optimal probability of error over all  $n$ -blocklength entanglement-assisted codes can be upper bounded as*

$$\varepsilon_{ea}^*(n, R) \leq e^{-nE_{r, ea}(R)}, \quad (13.19)$$

where

$$E_{r, ea}(R) := \sup_{\frac{1}{2} \leq \alpha \leq 1} \sup_{\psi_{AA'}} \inf_{\sigma_B \in \mathcal{S}(B)} \frac{1 - \alpha}{\alpha} (D_\alpha (\mathcal{N}_{A \rightarrow B}(\psi_{AA'}) \| \rho_{A'} \otimes \sigma_B) - R), \quad (13.20)$$

and  $\psi_{AA'}$  denotes the purification of  $\rho_A$ .

### 13.1.3 Optimality: Sphere-Packing Bound

We remark that the exact asymptotics of the sphere-packing for general codes in classical channels is still open. We do believe that the following Eq. (13.21) holds for both classical and c-q channels.

**Problem 7** (Exact Asymptotics of Sphere-Packing Bound for Classical-Quantum Channels). *For any classical-quantum channel  $W : \mathcal{X} \rightarrow \mathcal{S}(\mathcal{H})$  and any  $n$ -block codes (not necessary constant composition codes)<sup>1</sup>,*

$$\varepsilon^*(n, R) \geq \frac{1}{n^{\frac{1}{2}\left(1+\left|\frac{\partial E_{sp}(R)}{\partial R}\right|\right)}} e^{-nE_{sp}(R)}, \quad \forall R < C. \quad (13.21)$$

where,

$$E_{sp}(R) := \sup_{0 \leq \alpha \leq 1} \frac{1 - \alpha}{\alpha} (C_{\alpha, W} - R). \quad (13.22)$$

The sphere-packing bound beyond c-q channels are still unknown. We conjecture that it holds for an *entanglement-breaking channel*  $\mathcal{N}_{EB}$ , whose classical capacity is additive, i.e  $C(\mathcal{N}_{EB}^{\otimes n}) = nC(\mathcal{N}_{EB})$  [65, Theorem 18]. For general quantum channels, we might need regularized Rényi capacity.

---

<sup>1</sup>We note that the sphere-packing exponent is not necessarily differentiable. Throughout this section, we write  $\partial E_{sp}(R)/\partial R$  to be the left derivative.

**Problem 8** (Sphere-Packing Bound beyond Classical-Quantum Channels). *For any entanglement-breaking channel  $\mathcal{N}_{\text{EB}}$ , and any  $n$ -block codes*

$$\varepsilon^*(n, R) \geq \frac{1}{n^{\frac{1}{2}\left(1+\left|\frac{\partial E_{\text{sp}}(R)}{\partial R}\right|\right)}} e^{-nE_{\text{sp}}(R)}, \quad \forall R < C, \quad (13.23)$$

where

$$E_{\text{sp}}(R) := \sup_{0 \leq \alpha \leq 1} \frac{1-\alpha}{\alpha} (C_\alpha(\mathcal{N}_{\text{EB}}) - R). \quad (13.24)$$

Moreover, for any quantum channel  $\mathcal{N}$ , and any  $n$ -block codes

$$\varepsilon^*(n, R) \geq \frac{1}{n^{\frac{1}{2}\left(1+\left|\frac{\partial E_{\text{sp}}^\infty(R)}{\partial R}\right|\right)}} e^{-nE_{\text{sp}}^\infty(R)}, \quad \forall R < C, \quad (13.25)$$

where

$$E_{\text{sp}}^\infty(R) := \sup_{0 \leq \alpha \leq 1} \frac{1-\alpha}{\alpha} \left( \lim_{n \rightarrow +\infty} \frac{1}{n} C_\alpha(\mathcal{N}^{\otimes n}) - R \right). \quad (13.26)$$

**Problem 9** (Sphere-Packing Bound for Entanglement-Assisted Codes). *Let  $\mathcal{N} : \mathcal{S}(\mathcal{A}) \rightarrow \mathcal{S}(\mathcal{B})$  be a quantum channel. Fix any rate below the entanglement-assisted classical capacity, i.e.  $R < C_{\text{ea}}(\mathcal{N})$ . Then for any  $n$ -block codes*

$$\varepsilon_{\text{ea}}^*(n, R) \geq \frac{1}{n^{\frac{1}{2}\left(1+\left|\frac{\partial E_{\text{sp},\text{ea}}(R)}{\partial R}\right|\right)}} e^{-nE_{\text{sp},\text{ea}}(R)}, \quad \forall R < C, \quad (13.27)$$

where

$$E_{\text{sp},\text{ea}}(R) := \sup_{0 \leq \alpha \leq 1} \sup_{\psi_{AA'}} \inf_{\sigma_B \in \mathcal{S}(B)} \frac{1-\alpha}{\alpha} (D_\alpha(\mathcal{N}_{A \rightarrow B}(\psi_{AA'}) \| \rho_{A'} \otimes \sigma_B) - R), \quad (13.28)$$

### 13.1.4 Moderate Deviation Analysis

**Problem 10** (Moderate Deviation Analysis for Entanglement-Breaking Channels). *Prove that any quantum entanglement-breaking channel  $\mathcal{N}_{\text{EB}}$  satisfies moderate deviation principle, i.e.*

$$\lim_{n \rightarrow +\infty} \frac{1}{na_n^2} \log \varepsilon^*(n, R) = -\frac{1}{2V(\mathcal{N}_{\text{EB}})}, \quad (13.29)$$

where the sequence  $(a_n)_{n \in \mathbb{N}}$  satisfy Eq. (12.1).

# Bibliography

- [1] A. Dembo and O. Zeitouni, *Large Deviations Techniques and Applications*. Springer, 1998.
- [2] A. Holevo, “Reliability function of general classical-quantum channel,” *IEEE Transaction on Information Theory*, vol. 46, no. 6, pp. 2256–2261, 2000.
- [3] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, 1984.
- [4] C. H. Bennett, “. quantum cryptography using any two nonorthogonal states,” *Physical Review Letters*, vol. 68, p. 3121–3124, 1992.
- [5] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels,” *Physical Review Letters*, vol. 70, p. 1895, 1993.
- [6] D. Gottesman and I. L. Chuang, “Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations,” *Nature*, vol. 402, p. 390, 1999.
- [7] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, 2009.
- [8] E. Gibney, “Chinese satellite is one giant step for the quantum internet,” *Nature*, vol. 535, no. 7613, pp. 478–479, jul 2016.
- [9] M. Tomamichel, M. Berta, and J. M. Renes, “Quantum coding with finite resources,” *Nature Communications*, vol. 7, p. 11419, may 2016.
- [10] M. Tomamichel, *Quantum Information Processing with Finite Resources*. Springer International Publishing, 2016.
- [11] C. E. Shannon, “A mathematical theory of communication,” *The Bell System Technical Journal*, vol. 27, pp. 379–423, 1948.
- [12] D. Slepian and J. Wolf, “Noiseless coding of correlated information sources,” *IEEE Transactions on Information Theory*, vol. 19, no. 4, pp. 471–480, jul 1973.
- [13] V. Strassen, “Asymptotische abschätzungen in Shannon’s informationstheorie,” *Transactions of the Third Prague Conference on Information Theory*, pp. 689–723, 1962.

- [14] Y. Polyanskiy, H. V. Poor, and S. Verdu, “Channel coding rate in the finite blocklength regime,” *IEEE Trans. Inform. Theory*, vol. 56, no. 5, pp. 2307–2359, may 2010.
- [15] M. Hayashi, “Information spectrum approach to second-order coding rate in channel coding,” *IEEE Transactions on Information Theory*, vol. 55, no. 11, pp. 4947–4966, nov 2009.
- [16] M. Tomamichel and M. Hayashi, “A hierarchy of information quantities for finite block length analysis of quantum tasks,” *IEEE Transactions on Information Theory*, vol. 59, no. 11, pp. 7693–7710, nov 2013.
- [17] K. Li, “Second-order asymptotics for quantum hypothesis testing,” *The Annals of Statistics*, vol. 42, no. 1, pp. 171–189, feb 2014.
- [18] M. Tomamichel and V. Y. F. Tan, “Second-order asymptotics for the classical capacity of image-additive quantum channels,” *Communications in Mathematical Physics*, vol. 338, no. 1, pp. 103–137, may 2015.
- [19] ——, “A tight upper bound for the third-order asymptotics for most discrete memoryless channels,” *IEEE Transactions on Information Theory*, vol. 59, no. 11, pp. 7041–7051, nov 2013.
- [20] V. Y. F. Tan, “Asymptotic estimates in information theory with non-vanishing error probabilities,” *Foundations and Trends® in Communications and Information Theory*, vol. 10, no. 4, pp. 1–184, 2014.
- [21] V. Y. F. Tan and M. Tomamichel, “The third-order term in the normal approximation for the AWGN channel,” *IEEE Transactions on Information Theory*, vol. 61, no. 5, pp. 2430–2438, may 2015.
- [22] C. E. Shannon, “Probability of error for optimal codes in a Gaussian channel,” *Bell System Technical Journal*, vol. 38, no. 3, pp. 611–656, may 1959.
- [23] R. Gallager, *Information Theory and Reliable Communication*. Wiley, 1968. [Online]. Available: <http://as.wiley.com/WileyCDA/WileyTitle/productCd-0471290483.html>
- [24] R. M. Fano, *Transmission of Information, A Statistical Theory of Communications*. The MIT Press, 1961.
- [25] R. E. Blahut, *Principles and practice of information theory*. Addison-Wesley, 1987.
- [26] E. A. Haroutunian, M. E. Haroutunian, and A. N. Harutyunyan, “Reliability criteria in information theory and in statistical hypothesis testing,” *Foundations and Trends® in Communications and Information Theory*, vol. 4, no. 2–3, pp. 97–263, 2007.
- [27] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Cambridge University Press (CUP), 2011.
- [28] H.-C. Cheng, M.-H. Hsieh, and M. Tomamichel, “Quantum sphere-packing bounds with polynomial prefactors,” 2017.

- [29] A. Feinstein, "Error bounds in noisy channels without memory," *IEEE Transactions on Information Theory*, vol. 1, no. 2, pp. 13–14, sep 1955.
- [30] R. Gallager, "A simple derivation of the coding theorem and some applications," *IEEE Transaction on Information Theory*, vol. 11, no. 1, pp. 3–18, jan 1965.
- [31] C. Shannon, R. Gallager, and E. Berlekamp, "Lower bounds to error probability for coding on discrete memoryless channels. I," *Information and Control*, vol. 10, no. 1, pp. 65–103, jan 1967.
- [32] E. A. Haroutunian, "Estimates of the error exponents for the semicontinuous memoryless channel," *Problemy Peredachi Informatsii*, vol. 4, no. 4, pp. 37–48, 1968, (in Russian). [Online]. Available: <http://mi.mathnet.ru/eng/ppi1871>
- [33] R. E. Blahut, "Hypothesis testing and information theory," *IEEE Transaction on Information Theory*, vol. 20, no. 4, pp. 405–417, jul 1974.
- [34] A. Ben-Tal, M. Teboulle, and A. Charnes, "The role of duality in optimization problems involving entropy functionals with applications to information theory," *Journal of Optimization Theory and Applications*, vol. 58, no. 2, pp. 209–223, aug 1988.
- [35] M. V. Burnashev and A. S. Holevo, "On the reliability function for a quantum communication channel," *Problems of information transmission*, vol. 34, no. 2, pp. 97–107, 1998.
- [36] H.-C. Cheng and M.-H. Hsieh, "Concavity of the auxiliary function for classical-quantum channels," *IEEE Transactions on Information Theory*, vol. 62, no. 10, pp. 5960 – 5965, 2016.
- [37] A. Winter, "Coding theorems of quantum information theory," 1999, (PhD Thesis, Universität Bielefeld).
- [38] M. Dalai, "Lower bounds on the probability of error for classical and classical-quantum channels," *IEEE Transactions on Information Theory*, vol. 59, no. 12, pp. 8027–8056, dec 2013.
- [39] M. Dalai and A. Winter, "Constant compositions in the sphere packing bound for classical-quantum channels," *IEEE Transactions on Information Theory*, pp. 1–1, 2017.
- [40] I. Devetak and A. Winter, "Classical data compression with quantum side information," *Physical Review A*, vol. 68, no. 4, oct 2003.
- [41] J. M. Renes and R. Renner, "One-shot classical data compression with quantum side information and the distillation of common randomness or secret keys," *IEEE Transactions on Information Theory*, vol. 58, no. 3, pp. 1985–1991, mar 2012.
- [42] Y. Altug and A. B. Wagner, "Moderate deviation analysis of channel coding: Discrete memoryless case," in *2010 IEEE International Symposium on Information Theory*. Institute of Electrical & Electronics Engineers (IEEE), jun 2010.
- [43] ——, "Moderate deviations in channel coding," *IEEE Transactions on Information Theory*, vol. 60, no. 8, pp. 4417–4426, aug 2014.

- [44] Y. Polyanskiy and S. Verdu, "Channel dispersion and moderate deviations limits for memoryless channels," in *2010 48th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. Institute of Electrical & Electronics Engineers (IEEE), sep 2010.
- [45] I. Sason, "Moderate deviations analysis of binary hypothesis testing," in *2012 IEEE International Symposium on Information Theory Proceedings*. Institute of Electrical & Electronics Engineers (IEEE), jul 2012.
- [46] ——, "On refined versions of the Azuma-Hoeffding inequality with applications in information theory," 2011.
- [47] M. Raginsky and I. Sason, "Concentration of measure inequalities in information theory, communications, and coding," *Foundations and Trends® in Communications and Information Theory*, vol. 10, no. 1-2, pp. 1–247, 2013.
- [48] R. R. Bahadur and R. R. Rao, "On deviations of the sample mean," *The Annals of Mathematical Statistics*, vol. 31, no. 4, pp. 1015–1027, dec 1960.
- [49] N. R. Chaganty and J. Sethuraman, "Strong large deviation and local limit theorems," *The Annals of Probability*, vol. 21, no. 3, pp. 1671–1690, jul 1993.
- [50] M. M. Wilde, *Quantum Information Theory*. Cambridge University Press, 2016.
- [51] T. Heinosaari and M. Ziman, *The Mathematical language of Quantum Theory*. Cambridge University Press, 2009.
- [52] H.-C. Cheng and M.-H. Hsieh, "Moderate deviation analysis for classical-quantum channels and quantum hypothesis testing," 2017.
- [53] H.-C. Cheng, E. P. Hanson, N. Datta, and M.-H. Hsieh, "Non-asymptotic classical data compression with quantum side informations," 2018.
- [54] ——, "Duality between source coding with quantum side information and c-q channel coding," 2018.
- [55] I. Csiszár and J. Körner, "Towards a general theory of source networks," *IEEE Transactions on Information Theory*, vol. 26, no. 2, pp. 155–165, mar 1980.
- [56] I. Csiszár, "Linear codes for sources and source networks: Error exponents, universal coding," *IEEE Transactions on Information Theory*, vol. 28, no. 4, pp. 585–592, jul 1982.
- [57] R. G. Gallager, "Source coding with side information and universal coding," 1976, technical Report. [Online]. Available: <http://web.mit.edu/gallager/www/papers/paper5.pdf>
- [58] T. Ogawa and H. Nagaoka, "Strong converse and Stein's lemma in quantum hypothesis testing," *IEEE Transaction on Information Theory*, vol. 46, no. 7, pp. 2428–2433, 2000.
- [59] M. Mosonyi and T. Ogawa, "Strong converse exponent for classical-quantum channel coding," *Communications in Mathematical Physics*, vol. 355, no. 1, pp. 373–426, jun 2017.

- [60] D. Petz, “Quasi-entropies for finite quantum systems,” *Reports on Mathematical Physics*, vol. 23, no. 1, pp. 57–65, feb 1986.
- [61] S. Golden, “Lower bounds for the Helmholtz function,” *Physical Review*, vol. 137, no. 4B, pp. B1127–B1128, feb 1965.
- [62] C. J. Thompson, “Inequality with applications in statistical mechanics,” *Journal of Mathematical Physics*, vol. 6, no. 11, p. 1812, 1965.
- [63] A. Winter, “Coding theorem and strong converse for quantum channels,” *IEEE Transaction on Information Theory*, vol. 45, no. 7, pp. 2481–2485, 1999. [Online]. Available: <http://dx.doi.org/10.1109/18.796385>
- [64] T. Ogawa and H. Nagaoka, “Strong converse to the quantum channel coding theorem,” *IEEE Transaction on Information Theory*, vol. 45, no. 7, pp. 2486–2489, 1999.
- [65] M. M. Wilde, A. Winter, and D. Yang, “Strong converse for the classical capacity of entanglement-breaking and Hadamard channels via a sandwiched Rényi relative entropy,” *Communications in Mathematical Physics*, vol. 331, no. 2, pp. 593–622, jul 2014.
- [66] H.-C. Cheng, E. P. Hanson, N. Datta, and M.-H. Hsieh, “Non-asymptotic joint source-channel coding with quantum side informations,” (*in preparation*).
- [67] M. S. Berger, *Nonlinearity and Functional Analysis*. Academic Press, 1977.
- [68] L. V. Kantorovich and G. P. Akilov, *Functional Analysis in Normed Spaces*. Pergamon Press, New York, 1982.
- [69] R. Bhatia, *Matrix Analysis*. Springer New York, 1997.
- [70] K. Atkinson and W. Han, *Theoretical Numerical Analysis: A Functional Analysis Framework*. Springer International Publishing, 2009.
- [71] N. J. Higham, *Functions of Matrices: Theory and Computation*. Society for Industrial & Applied Mathematics (SIAM), Jan 2008. [Online]. Available: <http://dx.doi.org/10.1137/1.9780898717778>
- [72] V. V. Peller, “Hankel operators in the perturbation theory of unitary and self-adjoint operators,” *Functional Analysis and Its Applications*, vol. 19, no. 2, pp. 111–123, 1985. [Online]. Available: <http://dx.doi.org/10.1007/bf01078390>
- [73] K. Bickel, “Differentiating matrix functions,” *Operators and Matrices*, no. 1, pp. 71–90, 2007. [Online]. Available: <http://dx.doi.org/10.7153/oam-07-03>
- [74] M. Z. Nashed, “Some remarks on variations and differentials,” *The American Mathematical Monthly*, vol. 73, no. 4, p. 63, Apr 1966. [Online]. Available: <http://dx.doi.org/10.2307/2313752>
- [75] F. Hiai, “Matrix analysis: Matrix monotone functions, matrix means, and majorization,” *Interdisciplinary Information Sciences*, vol. 16, no. 2, pp. 139–246, 2010. [Online]. Available: <http://dx.doi.org/10.4036/iis.2010.139>

- [76] L. M. Graves, “Riemann integration and Taylor’s theorem in general analysis,” *Transactions of the American Mathematical Society*, vol. 29, no. 1, pp. 163–163, Jan 1927.
- [77] K. Makherjea, *Differential Calculus in Normed Linear Spaces*, 2nd ed. Hindustan Book Agency, New Delhi, India, 2007.
- [78] J. Dieudonne, *Foundations of Modern Analysis*, 2nd ed. Academic Press, New York, 1969.
- [79] N. J. Higham and S. D. Relton, “Higher order fréchet derivatives of matrix functions and the level-2 condition number,” *SIAM Journal on Matrix Analysis and Applications*, vol. 35, no. 3, pp. 1019–1037, Jan 2014. [Online]. Available: <http://dx.doi.org/10.1137/130945259>
- [80] F. Hansen, “Operator convex functions of several variables,” *Publications of the Research Institute for Mathematical Sciences*, vol. 33, no. 3, pp. 443–463, 1997. [Online]. Available: <http://dx.doi.org/10.2977/prims/1195145324>
- [81] J. R. Rice, “A theory of condition,” *SIAM Journal on Numerical Analysis*, vol. 3, no. 2, pp. 287–310, Jun 1966. [Online]. Available: <http://dx.doi.org/10.1137/0703023>
- [82] N. J. Higham and S. D. Relton, “Estimating the condition number of the fréchet derivative of a matrix function,” *SIAM Journal on Scientific Computing*, vol. 36, no. 6, pp. C617–C634, Jan 2014. [Online]. Available: <http://dx.doi.org/10.1137/130950082>
- [83] E. Carlen, “Trace inequalities and quantum entropy: an introductory course,” in *Contemporary Mathematics*. American Mathematical Society (AMS), 2010, vol. 529, pp. 73–140. [Online]. Available: <http://dx.doi.org/10.1090/conm/529/10428>
- [84] F. Hiai and D. Petz, *Introduction to Matrix Analysis and Applications*. Springer International Publishing, 2014.
- [85] W. Pusz and S. Woronowicz, “Functional calculus for sesquilinear forms and the purification map,” *Reports on Mathematical Physics*, vol. 8, no. 2, pp. 159–170, oct 1975.
- [86] F. Kubo and T. Ando, “Means of positive linear operators,” *Mathematische Annalen*, vol. 246, no. 3, pp. 205–224, oct 1980.
- [87] R. Bhatia, *Positive Definite Matrices*. Princeton University Press, jan 2007.
- [88] J. S. Matharu and J. S. Aujla, “Some inequalities for unitarily invariant norms,” *Linear Algebra and its Applications*, vol. 436, pp. 1623–1631, 2012.
- [89] H. Araki, “On an inequality of Lieb and Thirring,” *Letters in Mathematical Physics*, vol. 19, no. 2, pp. 167–170, feb 1990.
- [90] K. Symanzik, “Proof and refinements of an inequality of Feynman,” *Journal of Mathematical Physics*, vol. 6, no. 7, pp. 1155–1156, jul 1965.
- [91] K. M. R. Audenaert, J. Calsamiglia, R. Muñoz-Tapia, E. Bagan, L. Masanes, A. Acin, and F. Verstraete, “Discriminating states: The quantum Chernoff bound,” *Physical Review Letters*, vol. 98, p. 160501, apr 2007.

- [92] K. M. R. Audenaert, M. Nussbaum, A. Szkoła, and F. Verstraete, “Asymptotic error rates in quantum hypothesis testing,” *Communications in Mathematical Physics*, vol. 279, no. 1, pp. 251–283, feb 2008.
- [93] M. Hayashi and H. Nagaoka, “General formulas for capacity of classical-quantum channels,” *IEEE Transaction on Information Theory*, vol. 49, no. 7, pp. 1753–1768, Jul 2003.
- [94] M. Hayashi, “Error exponent in asymmetric quantum hypothesis testing and its application to classical-quantum channel coding,” *Physical Review A*, vol. 76, no. 6, dec 2007.
- [95] J.-C. Bourin and E.-Y. Lee, “Matrix inequalities from a two variables functional,” *International Journal of Mathematics*, vol. 27, no. 09, p. 1650071, aug 2016.
- [96] A. Rényi, “On measures of entropy and information,” *Proc. 4th Berkeley Symp. on Math. Statist. Probability*, vol. 1, pp. 547–561, 1962.
- [97] T. van Erven and P. Harremoes, “Rényi divergence and kullback-leibler divergence,” *IEEE Transactions on Information Theory*, vol. 60, no. 7, pp. 3797–3820, jul 2014.
- [98] Y. Altuğ and A. B. Wagner, “Refinement of the sphere-packing bound: Asymmetric channels,” *IEEE Transactions on Information Theory*, vol. 60, no. 3, pp. 1592–1614, mar 2014.
- [99] M. Hayashi, *Quantum Information: An Introduction*. Springer.
- [100] H. Umegaki, “Conditional expectation in an operator algebra. IV. entropy and information,” *Kodai Mathematical Seminar Reports*, vol. 14, no. 2, pp. 59–85, 1962.
- [101] F. Hiai and D. Petz, “The proper formula for relative entropy and its asymptotics in quantum probability,” *Communications in Mathematical Physics*, vol. 143, no. 1, pp. 99–114, dec 1991.
- [102] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. John Wiley & Sons, Inc., apr 2005.
- [103] E. Hellinger, “Neue begründung der theorie quadratischer formen von unendlichvielen veränderlichen,” *Journal für die reine und angewandte Mathematik*, vol. 1909, no. 136, 1909.
- [104] L. L. Cam and G. L. Yang, *Asymptotics in Statistics*. Springer US, 1990.
- [105] E. H. Lieb, “Convex trace functions and the Wigner-Yanase-Dyson conjecture,” *Advances in Mathematics*, vol. 11, no. 3, pp. 267–288, dec 1973.
- [106] F. Hiai, “Concavity of certain matrix trace and norm functions. II,” *Linear Algebra and its Applications*, vol. 496, pp. 193–220, may 2016.
- [107] T. Ando, “Concavity of certain maps on positive definite matrices and applications to Hadamard products,” *Linear Algebra and its Applications*, vol. 26, pp. 203–241, aug 1979.
- [108] A. Holevo, “Bounds for the quantity of information transmitted by a quantum communication channel,” *Problems of Information Transmission*, vol. 9, no. 3, pp. 177–183, 1973.

- [109] ——, “Problems in the mathematical theory of quantum communication channels,” *Reports on Mathematical Physics*, vol. 12, no. 2, pp. 273–278, oct 1977.
- [110] ——, “The capacity of the quantum channel with general signal states,” *IEEE Transaction on Information Theory*, vol. 44, no. 1, pp. 269–273, 1998.
- [111] M. Hayashi and M. Tomamichel, “Correlation detection and an operational interpretation of the Rényi mutual information,” 2014.
- [112] B. Nakiboğlu, “The Renyi capacity and center.”
- [113] U. Augustin, “Noisy channels,” 1978, habilitation thesis, Universitat Erlangen.
- [114] B. Nakiboğlu, “The Augustin capacity and center.”
- [115] N. Sharma and N. A. Warsi, “On the strong converses for the quantum channel capacity theorems,” 2012.
- [116] A. N. Kolmogorov and S. V. Fomin, *Introductory Real Analysis*. Dover Publications, New York, 1975.
- [117] R. M. Dudley, *Real Analysis and Probability*. Cambridge University Press (CUP), 2002.
- [118] C. Berge, *Topological Spaces*. Oliver & Boyd, 1963.
- [119] B. Pshenichnyi, *Necessary Conditions for an Extremum Pshenichnyi*. CRC Press, 1971.
- [120] H. Nagaoka, “The converse part of the theorem for quantum Hoeffding bound,” 2006.
- [121] M. Nussbaum and A. Szkoła, “The Chernoff lower bound for symmetric quantum hypothesis testing,” *Annals of Statistics*, vol. 37, no. 2, pp. 1040–1057, apr 2009.
- [122] M. Junge and Q. Zeng, “Noncommutative Bennett and Rosenthal inequalities,” *The Annals of Probability*, vol. 41, no. 6, pp. 4287–4316, nov 2013.
- [123] S. Watanabe and M. Hayashi, “Finite-length analysis on tail probability for markov chain and application to simple hypothesis testing,” *The Annals of Applied Probability*, vol. 27, no. 2, pp. 811–845, apr 2017.
- [124] C. Rouzé and N. Datta, “Finite blocklength and moderate deviation analysis of hypothesis testing of correlated quantum states and application to classical-quantum channels with memory,” 2016.
- [125] D. V. Voiculescu, K. J. Dykema, and A. Nica, *Free random variables*. American Mathematical Society, 1992.
- [126] F. Hiai and D. Petz, *The Semicircle Law, Free Random Variables and Entropy*. American Mathematical Society, mar 2006.
- [127] G. Pisier and Q. Xu, “Non-commutative martingale inequalities,” *Communications in Mathematical Physics*, vol. 189, no. 3, pp. 667–698, nov 1997.

- [128] M. Tomamichel, M. Berta, and M. Hayashi, “Relating different quantum generalizations of the conditional rényi entropy,” *Journal of Mathematical Physics*, vol. 55, no. 8, p. 082206, aug 2014.
- [129] S. M. Lin and M. Tomamichel, “Investigating properties of a family of quantum rényi divergences,” *Quantum Information Processing*, vol. 14, no. 4, pp. 1501–1512, feb 2015.
- [130] R. T. Rockafellar, “Minimax theorems and conjugate saddle-functions.” *Mathematica Scandinavica*, vol. 14, p. 151, jun 1964.
- [131] ——, *Convex Analysis*. Walter de Gruyter GmbH, jan 1970.
- [132] S. Weis, “Quantum convex support,” *Linear Algebra and its Applications*, vol. 435, no. 12, pp. 3168–3188, dec 2011.
- [133] M. Hayashi and M. Tomamichel, “Correlation detection and an operational interpretation of the Rényi mutual information,” 2014.
- [134] N. Sharma and N. A. Warsi, “Fundamental bound on the reliability of quantum information transmission,” *Physical Review Letters*, vol. 110, no. 8, feb 2013.
- [135] R. G. Gallager, “Fixed composition arguments and lower bounds to error probability,” (unpublished) 1994. [Online]. Available: <http://web.mit.edu/gallager/www/notes/notes5.pdf>
- [136] I. Csiszár and J. Körner, “Graph decomposition: A new key to coding theorems,” *IEEE Transactions on Information Theory*, vol. 27, no. 1, pp. 5–12, Jan 1981.
- [137] M. Dalai, “Some remarks on classical and classical-quantum sphere packing bounds: Rényi vs. Kullback-Leibler,” *Entropy*, vol. 19, no. 7, p. 355, jul 2017.
- [138] M. Hayashi, “Gallager bound of classical-quantum channel coding,” 2006.
- [139] M. Dalai, “A note on random coding bounds for classical-quantum channels,” *Problems of Information Transmission*, vol. 53, no. 3, pp. 222–228, apr 2017.
- [140] M. Mosonyi and T. Ogawa, “Two approaches to obtain the strong converse exponent of quantum hypothesis testing for general sequences of quantum states,” *IEEE Transactions on Information Theory*, vol. 61, no. 12, pp. 6975–6994, dec 2015.
- [141] R. Bhatia and J. Holbrook, “Riemannian geometry and matrix geometric means,” *Linear Algebra and its Applications*, vol. 413, no. 2-3, pp. 594–618, mar 2006.
- [142] J.-B. Hiriart-Urruty and C. Lemaréchal, *Fundamentals of Convex Analysis*. Springer Nature, 2001.
- [143] J. Scarlett, A. Martínez, and A. Guillén i Fàbregas, “Mismatched decoding: Error exponents, second-order rates and saddlepoint approximations,” *IEEE Transactions on Information Theory*, vol. 60, no. 5, pp. 2647–2666, may 2014.
- [144] J. Scarlett, “Reliable communication under mismatched decoding,” 2014, phD thesis (University of Cambridge).

- [145] B. Nakiboğlu, "The sphere packing bound via Augustin's method."
- [146] ——, "The sphere packing bound for memoryless channels."
- [147] M. Hayashi, "Universal coding for classical-quantum channel," *Communications in Mathematical Physics*, vol. 289, no. 3, pp. 1087–1098, may 2009.
- [148] Y. Altug and A. B. Wagner, "The third-order term in the normal approximation for singular channels," in *2014 IEEE International Symposium on Information Theory*. Institute of Electrical and Electronics Engineers (IEEE), jun 2014.
- [149] J. K. Omura, "A lower bounding method for channel and source coding probabilities," *Information and Control*, vol. 27, no. 2, pp. 148–177, feb 1975.
- [150] N. Elkayam and M. Feder, "Sphere packing bound for constant composition," 2016, (in preparation). [Online]. Available: [http://www.eng.tau.ac.il/~elkayam/SPB\\_Abstract.pdf](http://www.eng.tau.ac.il/~elkayam/SPB_Abstract.pdf)
- [151] U. Augustin, "Error estimates for low rate codes," *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete*, vol. 14, no. 1, pp. 61–88, 1969.
- [152] A. Valembois and M. P. Fossorier, "Sphere-packing bounds revisited for moderate block lengths," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 2998–3014, dec 2004.
- [153] G. Wiechman and I. Sason, "An improved sphere-packing bound for finite-length codes over symmetric memoryless channels," in *2008 Information Theory and Applications Workshop*. Institute of Electrical & Electronics Engineers (IEEE), jan 2008.
- [154] R. Ahlswede, *Storing and Transmitting Data*, A. Ahlswede, I. Althöfer, C. Deppe, and U. Tamm, Eds. Springer International Publishing, 2014.
- [155] J. H. B. Kemperman, "Studies in coding theory I. technical report," *University of Rochester, NY*, 1962.
- [156] ——, "On the optimum rate of transmitting information," *The Annals of Mathematical Statistics*, vol. 40, no. 6, pp. 2156–2177, dec 1969.
- [157] U. Augustin, "Gedächtnisfreie kanäle für diskrete zeit," *Zeitschrift für Wahrscheinlichkeitstheorie und Verwandte Gebiete*, vol. 6, no. 1, pp. 10–61, 1966.
- [158] J. Wolfowitz, "The coding of messages subject to chance errors," *Illinois Journal of Mathematics*, vol. 1, no. 4, pp. 591–606, 1957. [Online]. Available: <http://projecteuclid.org/euclid.ijm/1255380682>
- [159] N. Elkayam and M. Feder, "Achievable and converse bounds over a general channel and general decoding metric," in *2015 IEEE Information Theory Workshop (ITW)*. Institute of Electrical & Electronics Engineers (IEEE), apr 2015.
- [160] Y. Polyanskiy, "Saddle point in the minimax converse for channel coding," *IEEE Transactions on Information Theory*, vol. 59, no. 5, pp. 2576–2595, may 2013.

- [161] C. T. Chubb, V. Y. F. Tan, and M. Tomamichel, “Moderate deviation analysis for classical communication over quantum channels,” *Communications in Mathematical Physics*, vol. 355, no. 3, pp. 1283–1315, Nov 2017.
- [162] L. Wang and R. Renner, “One-shot classical-quantum capacity and hypothesis testing,” *Physical Review Letters*, vol. 108, no. 20, may 2012.
- [163] H. Nagaoka, “Strong converse theorems in quantum information theory,” 2001, p. 33.
- [164] L. V. Rozovsky, “Estimate from below for large-deviation probabilities of a sum of independent random variables with finite variances,” *Journal of Mathematical Sciences*, vol. 109, pp. 2192–2209, 2002.
- [165] J.-C. Bourin, “Matrix versions of some classical inequalities,” *Linear Algebra and its Applications*, vol. 416, no. 2-3, pp. 890–907, jul 2006.
- [166] B. Schumacher and M. D. Westmoreland, “Optimal signal ensembles,” *Physical Review A*, vol. 63, no. 2, jan 2001.
- [167] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel, “On quantum Rényi entropies: A new generalization and some properties,” *Journal of Mathematical Physics*, vol. 54, no. 12, p. 122203, 2013.