

Marco Tomamichel

Quantum  
Information  
Processing with  
Finite Resources  
Mathematical  
Foundations



Springer

# **SpringerBriefs in Mathematical Physics**

Volume 5

## **Series editors**

Nathanaël Berestycki, Cambridge, UK

Mihalis Dafermos, Cambridge, UK

Tohru Eguchi, Tokyo, Japan

Atsuo Kuniba, Tokyo, Japan

Matilde Marcolli, Pasadena, USA

Bruno Nachtergaele, Davis, USA

More information about this series at <http://www.springer.com/series/11953>

Marco Tomamichel

# Quantum Information Processing with Finite Resources

Mathematical Foundations

 Springer

Marco Tomamichel  
School of Physics  
The University of Sydney  
Sydney  
Australia

ISSN 2197-1757 ISSN 2197-1765 (electronic)  
SpringerBriefs in Mathematical Physics  
ISBN 978-3-319-21890-8 ISBN 978-3-319-21891-5 (eBook)  
DOI 10.1007/978-3-319-21891-5

Library of Congress Control Number: 2015950017

Springer Cham Heidelberg New York Dordrecht London  
© The Author(s) 2016

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media  
([www.springer.com](http://www.springer.com))

# Acknowledgments

I was introduced to quantum information theory during my PhD studies in Renato Renner's group at ETH Zurich. It is from him that I learned most of what I know about quantum cryptography and smooth entropies. Renato also got me interested more generally in finite resource information theory as well as the entropies and other information measures that come along with it. He shaped my views on the topic and gave me all the tools I needed to follow my own ideas, and I am immensely grateful for that. A particular question that grew out of my PhD studies was whether one can understand smooth entropies in a broader framework of quantum Rényi entropies. This book now accomplishes this.

Joining Stephanie Wehner's group at the Centre for Quantum Technologies in Singapore for my postdoctoral studies was probably the best thing I could have done. I profited tremendously from interactions with Stephanie and her group about many of the topics covered in this book. On top of that, I was also given the freedom to follow my own interests and collaborate with great researchers in Singapore. In particular I want to thank Masahito Hayashi for sharing a small part of his profound knowledge of quantum statistics and quantum information theory with me. On the other hand, Vincent Y.F. Tan taught me much of what I know about classical information theory, and I greatly enjoyed talking to him about finite resource effects.

Renato Renner, Mark M. Wilde, and Andreas Winter encouraged me to write this book. It is my pleasure to thank Christopher T. Chubb and Mark M. Wilde for carefully reading the manuscript and spotting many typos. I also want to thank Rupert L. Frank, Elliott H. Lieb, Milán Mosonyi, and Renato Renner for many insightful comments and suggestions on an earlier draft. While writing I also greatly enjoyed and profited from scientific discussions with Mario Berta, Frédéric Dupuis, Anthony Leverrier, and Volkher B. Scholz about different aspects of this book. I also want to acknowledge support from a University of Sydney Postdoctoral Fellowship as well as the Centre of Excellence for Engineered Quantum Systems in Australia.

Last but not least, I want to thank my wife Thanh Nguyệt for supporting me during this time, even when the writing continued long after the office hours ended. I dedicate this book to the memory of my grandfathers, Franz Wagenbach and Giuseppe B. Tomamichel, the engineers in the family.

Sydney

Marco Tomamichel

# Contents

<b>1</b>	<b>Introduction</b> . . . . .	1
1.1	Finite Resource Information Theory . . . . .	2
1.2	Motivating Example: Source Compression . . . . .	4
1.3	Outline of the Book . . . . .	7
<b>2</b>	<b>Modeling Quantum Information</b> . . . . .	11
2.1	General Remarks on Notation . . . . .	11
2.2	Linear Operators and Events . . . . .	13
2.2.1	Hilbert Spaces and Linear Operators . . . . .	13
2.2.2	Events and Measures . . . . .	17
2.3	Functionals and States . . . . .	18
2.3.1	Trace and Trace-Class Operators . . . . .	19
2.3.2	States and Density Operators . . . . .	20
2.4	Multi-partite Systems . . . . .	22
2.4.1	Tensor Product Spaces . . . . .	22
2.4.2	Separable States and Entanglement . . . . .	24
2.4.3	Purification . . . . .	25
2.4.4	Classical-Quantum Systems . . . . .	25
2.5	Functions on Positive Operators . . . . .	26
2.6	Quantum Channels . . . . .	28
2.6.1	Completely Bounded Maps . . . . .	28
2.6.2	Quantum Channels . . . . .	29
2.6.3	Pinching and Dephasing Channels . . . . .	30
2.6.4	Channel Representations . . . . .	31
2.7	Background and Further Reading . . . . .	32
<b>3</b>	<b>Norms and Metrics</b> . . . . .	33
3.1	Norms for Operators and Quantum States . . . . .	33
3.1.1	Schatten Norms . . . . .	34
3.1.2	Dual Norm for States . . . . .	36
3.2	Trace Distance . . . . .	37



3.3	Fidelity . . . . .	39
3.3.1	Generalized Fidelity . . . . .	41
3.4	Purified Distance . . . . .	43
3.5	Background and Further Reading . . . . .	45
<b>4</b>	<b>Quantum Rényi Divergence . . . . .</b>	<b>47</b>
4.1	Classical Rényi Divergence . . . . .	47
4.1.1	An Axiomatic Approach . . . . .	48
4.1.2	Positive Definiteness and Data-Processing . . . . .	49
4.1.3	Monotonicity in $\alpha$ and Limits . . . . .	51
4.2	Classifying Quantum Rényi Divergences . . . . .	53
4.2.1	Joint Concavity and Data-Processing . . . . .	54
4.2.2	Minimal Quantum Rényi Divergence . . . . .	55
4.2.3	Maximal Quantum Rényi Divergence . . . . .	56
4.2.4	Quantum Max-Divergence . . . . .	56
4.3	Minimal Quantum Rényi Divergence . . . . .	58
4.3.1	Pinching Inequalities . . . . .	59
4.3.2	Limits and Special Cases . . . . .	62
4.3.3	Data-Processing Inequality . . . . .	63
4.4	Petz Quantum Rényi Divergence . . . . .	67
4.4.1	Data-Processing Inequality . . . . .	67
4.4.2	Nussbaum–Szkoła Distributions . . . . .	68
4.5	Background and Further Reading . . . . .	71
<b>5</b>	<b>Conditional Rényi Entropy . . . . .</b>	<b>73</b>
5.1	Conditional Entropy from Divergence . . . . .	73
5.2	Definitions and Properties . . . . .	75
5.2.1	Alternative Expression for $\tilde{H}_\alpha^\uparrow$ . . . . .	77
5.2.2	Conditioning on Classical Information . . . . .	78
5.2.3	Data-Processing Inequalities and Concavity . . . . .	79
5.3	Duality Relations and Their Applications . . . . .	80
5.3.1	Duality Relation for $\tilde{H}_\alpha^\downarrow$ . . . . .	81
5.3.2	Duality Relation for $\tilde{H}_\alpha^\uparrow$ . . . . .	81
5.3.3	Duality Relation for $\tilde{H}_\alpha^\uparrow$ and $\tilde{H}_\alpha^\downarrow$ . . . . .	82
5.3.4	Additivity for Tensor Product States . . . . .	83
5.3.5	Lower and Upper Bounds on Quantum Rényi Entropy . . . . .	84
5.4	Chain Rules . . . . .	86
5.5	Background and Further Reading . . . . .	89
<b>6</b>	<b>Smooth Entropy Calculus . . . . .</b>	<b>91</b>
6.1	Min- and Max-Entropy . . . . .	91
6.1.1	Semi-Definite Programs . . . . .	91
6.1.2	The Min-Entropy . . . . .	92

- 6.1.3 The Max-Entropy . . . . . 94
- 6.1.4 Classical Information and Guessing Probability . . . . . 97
- 6.2 Smooth Entropies . . . . . 98
  - 6.2.1 Definition of the  $\varepsilon$ -Ball . . . . . 98
  - 6.2.2 Definition of Smooth Entropies . . . . . 99
  - 6.2.3 Remarks on Smoothing . . . . . 100
- 6.3 Properties of the Smooth Entropies . . . . . 102
  - 6.3.1 Duality Relation and Beyond . . . . . 102
  - 6.3.2 Chain Rules . . . . . 103
  - 6.3.3 Data-Processing Inequalities . . . . . 105
- 6.4 Fully Quantum Asymptotic Equipartition Property . . . . . 107
  - 6.4.1 Lower Bounds on the Smooth Min-Entropy . . . . . 107
  - 6.4.2 The Asymptotic Equipartition Property . . . . . 110
- 6.5 Background and Further Reading . . . . . 113
  
- 7 Selected Applications . . . . . 115**
  - 7.1 Binary Quantum Hypothesis Testing . . . . . 115
    - 7.1.1 Chernoff Bound . . . . . 116
    - 7.1.2 Stein’s Lemma . . . . . 117
    - 7.1.3 Hoeffding Bound and Strong Converse Exponent . . . . . 118
  - 7.2 Entropic Uncertainty Relations . . . . . 118
    - 7.2.1 Tripartite Uncertainty Relation . . . . . 119
    - 7.2.2 Bipartite Uncertainty Relation . . . . . 120
  - 7.3 Randomness Extraction . . . . . 121
    - 7.3.1 Uniform and Independent Randomness . . . . . 121
    - 7.3.2 Direct Bound: Leftover Hash Lemma . . . . . 123
    - 7.3.3 Converse Bound . . . . . 125
  - 7.4 Background and Further Reading . . . . . 126
  
- Appendix: Some Fundamental Results in Matrix Analysis . . . . . 127**
  
- References . . . . . 131**

# Chapter 1

## Introduction

**Abstract** This chapter motivates the study of finite resource quantum information theory and the mathematical framework that is required to do so. We will present a motivating example and outline the content of the book.

As we further miniaturize information processing devices, the impact of quantum effects will become more and more relevant. Information processing at the microscopic scale poses challenges but also offers various opportunities: How much information can be transmitted through a physical communication channel if we can encode and decode our information using a quantum computer? How can we take advantage of entanglement, a form of correlation stronger than what is allowed by classical physics? What are the implications of Heisenberg's uncertainty principle of quantum mechanics for cryptographic security? These are only a few amongst the many questions studied in the emergent field of quantum information theory.

One of the predominant challenges when engineering future quantum information processors is that large quantum systems are notoriously hard to maintain in a coherent state and difficult to control accurately. Hence, it is prudent to expect that there will be severe limitations on the size of quantum devices for the foreseeable future. It is therefore of immediate practical relevance to investigate quantum information processing with limited physical resources, for example, to ask:

How well can we perform information processing tasks if we only have access to a small quantum device? Can we beat fundamental limits imposed on information processing with non-quantum resources?

This book will introduce the reader to the mathematical framework required to answer such questions, and many others. In quantum cryptography we want to show that a key of *finite* length is secret from an adversary, in quantum metrology we want to infer properties of a *small* quantum system from a *finite* sample, and in quantum thermodynamics we explore the thermodynamic properties of *small* quantum

systems. What all these applications have in common is that they concern properties of small quantum devices and require precise statements that remain valid outside asymptopia—the idealized asymptotic regime where the system size is unbounded.

## 1.1 Finite Resource Information Theory

Through the lens of a physicist it is natural to see Shannon’s information theory [144] as a resource theory. Data sources and communication channels are traditional examples of resources in information theory, and its goal is to investigate how these resources are interrelated and how they can be transformed into each other. For example, we aim to compress a data source that contains redundancy into one that does not, or to transform a noisy channel into a noiseless one. Information theory quantifies how well this can be done and in particular provides us with fundamental limits on the best possible performance of any transformation.

Shannon’s initial work [144] already gives definite answers to the above example questions in the asymptotic regime where resources are unbounded. This means that we can use the input resource as many times as we wish and are interested in the *rate* (the fraction of output to input resource) at which transformations can occur. The resulting statements can be seen as a first approximation to a more realistic setting where resources are necessarily finite, and this approximation is indeed often sufficient for practical purposes.

However, as argued above, specifically when quantum resources are involved we would like to establish more precise statements that remain valid even when the available resources are very limited. This is the goal of *finite resource information theory*. The added difficulty in the finite setting is that we are often not able to produce the output resource perfectly. The best we can hope for is to find a tradeoff between the transformation rate and the error we allow on the output resource. In the most fundamental *one-shot* setting we only consider a single use of the input resource and are interested in the tradeoff between the amount of output resource we can produce and the incurred error. We can then see the finite resource setting as a special case of the one-shot setting where the input resource has additional structure, for example a source that produces a sequence of independent and identically distributed (iid) symbols or a channel that is memoryless or ergodic.

Notably such considerations were part of the development of information theory from the outset. They motivated the study of *error exponents*, for example by Gallager [63]. Roughly speaking, error exponents approximate how fast the error vanishes for a fixed transformation rate as the number of available resources increases. However, these statements are fundamentally asymptotic in nature and make strong assumptions on the structure of the resources. Beyond that, Han and Verdú established the information spectrum method [69, 70] which allows to consider unstructured resources but is asymptotic in nature. More recently finite resource information theory has attracted considerable renewed attention, for example due to the works of Hayashi [77, 78] and Polyanskiy et al. [133]. The approach in these works—based

on Strassen’s techniques [148]—is motivated operationally: in many applications we can admit a small, *fixed error* and our goal is to find the maximal possible transformation rate as a function of the error and the amount of available resource.<sup>1</sup>

In an independent development, approximate or asymptotic statements were also found to be insufficient in the context of cryptography. In particular the advent of quantum cryptography [18, 51] motivated a precise information-theoretic treatment of the security of secret keys of finite length [99, 139]. In the context of quantum cryptography many of the standard assumptions in information theory are no longer valid if one wants to avoid any assumptions on the eavesdropper’s actions. In particular, the common assumption that resources are iid or ergodic is hardly justified. In quantum cryptography we are instead specifically interested in the one-shot setting, where we want to understand how much (almost) secret key can be extracted from a single use of an unstructured resource.

The abstract view of finite resource information theory as a resource theory also reveals why it has found various applications in physical resource theories, most prominently in thermodynamics (see, e.g., [30, 47, 52] and references therein).

### Rényi and Smooth Entropies

The main focus of this book will be on various measures of entropy and information that underly finite resource information theory, in particular Rényi and smooth entropies. The concept of entropy has its origins in physics, in particular in the works of Boltzmann [28] and Gibbs [66] on thermodynamics. Von Neumann [170] generalized these concepts to quantum systems. Later Shannon [144]—well aware of the origins of entropy in physics—interpreted entropy as a measure of uncertainty of the outcome of a random experiment. He found that entropy, or *Shannon entropy* as it is called now in the context of information theory,<sup>2</sup> characterizes the optimal *asymptotic* rate at which information can be compressed. However, we will soon see that it is necessary to consider alternative information measures if we want to move away from asymptotic statements.

Error exponents can often be expressed in terms of *Rényi entropies* [142] or related information measures, which partly explains the central importance of this one-parameter family of entropies in information theory. Rényi entropies share many mathematical properties with the Shannon entropy and are powerful tools in many information-theoretic arguments. A significant part of this book is thus devoted to exploring quantum generalizations of Rényi entropies, for example the ones proposed by Petz [132] and a more recent specimen [122, 175] that has already found many applications.

The particular problems encountered in cryptography led to the development of smooth entropies [141] and their quantum generalizations [139, 140]. Most importantly, the smooth min-entropy captures the amount of uniform randomness that can be extracted from an unstructured source if we allow for a small error. (This

---

<sup>1</sup>The topic has also been reviewed recently by Tan [151].

<sup>2</sup>Notwithstanding the historical development, we follow the established tradition and use *Shannon entropy* to refer to entropy. We use *von Neumann entropy* to refer to its quantum generalization.

example is discussed in detail in Sect. 7.3.) The smooth entropies are variants of Rényi entropies and inherit many of their properties. They have since found various applications ranging from information theory to quantum thermodynamics and will be the topic of the second part of this book.

We will further motivate the study of these information measures with a simple example in the next section.

Besides their operational significance, there are other reasons why the study of information measures is particularly relevant in quantum information theory. Many standard arguments in information theory can be formulated in term of entropies, and often this formulation is most amenable to a generalization to the quantum setting. For example, conditional entropies provide us with a measure of the uncertainty inherent in a quantum state from the perspective of an observer with access to side information. This allows us to circumvent the problem that we do not have a suitable notion of conditional probabilities in quantum mechanics. As another example, arguments based on typicality and the asymptotic equipartition property can be phrased in terms of smooth entropies which often leads to a more concise and intuitive exposition. Finally, the study of quantum generalizations of information measures sometimes also gives new insights into the classical quantities. For example, our definitions and discussions of conditional Rényi entropy also apply to the classical special case where such definitions have not yet been firmly established.

## 1.2 Motivating Example: Source Compression

We are using notation that will be formally introduced in Chap. 2 and concepts that will be expanded on in later chapters (cf. Table 1.1). A data source is described probabilistically as follows. Let  $X$  be a random variable with distribution  $\rho_X(x) = \Pr[X = x]$  that models the distribution of the different symbols that the source emits. The number of bits of memory needed to store one symbol produced by this source so that it can be recovered with certainty is given by  $\lceil H_0(X)_\rho \rceil$ , where  $H_0(X)_\rho$  denotes the *Hartley entropy* [72] of  $X$ , defined as

$$H_0(X)_\rho = \log_2 |\{x : \rho_X(x) > 0\}|. \quad (1.1)$$

The Hartley entropy is a limiting case of a Rényi entropy [142] and simply measures the cardinality of the support of  $X$ . In essence, this means that we can ignore symbols

**Table 1.1** Reference to detailed discussion of the quantities and concepts mentioned in this section

	Concept	To be discussed further in
$H_\alpha$	Rényi entropy	Chapters 4 and 5
$\Delta(\cdot, \cdot)$	Variational distance	Section 3.1, as generalized trace distance
$H_{\max}^\varepsilon$	Smooth Rényi entropy	Chapter 6, as smooth max-entropy <sup>a</sup>
	Entropic AEP	Section 6.4, entropic asymptotic equipartition property

<sup>a</sup>We will use a different metric for the definition of the smooth max-entropy

that never occur but otherwise our knowledge of the distribution of the different symbols does not give us any advantage.

As an example, consider a source that outputs lowercase characters of the English alphabet. If we want to store a single character produced by this source such that it can be recovered with certainty, we clearly need  $\lceil \log_2 26 \rceil = 5$  bits of memory as a resource.

### Analysis with Rényi Entropies

More interestingly, we may ask how much memory we need to store the output of the source if we allow for a small probability of failure,  $\varepsilon \in (0, 1)$ . To answer this we investigate encoders that assign codewords of a fixed length  $\log_2 m$  (in bits) to the symbols the source produces. These codewords are then stored and a decoder is later used to compute an estimate of  $X$  from the codewords. If the probability that this estimate equals the original symbol produced by the source is at least  $1 - \varepsilon$ , then we call such a scheme an  $(\varepsilon, m)$ -code. For a source  $X$  with probability distribution  $\rho_X$ , we are thus interested in finding the tradeoff between code length,  $\log_2 m$ , and the probability of failure,  $\varepsilon$ , for all  $(\varepsilon, m)$ -codes.

Shannon in his seminal work [144] showed that simply disregarding the most unlikely source events (on average) leads to an arbitrarily small failure probability if the code length is chosen sufficiently long. In particular, Gallager's proof [63, 64] implies that  $(\varepsilon, m)$ -codes always exist as long as

$$\log_2 m \geq H_\alpha(X)_\rho + \frac{\alpha}{1-\alpha} \log_2 \frac{1}{\varepsilon} \quad \text{for some } \alpha \in \left[\frac{1}{2}, 1\right). \quad (1.2)$$

Here,  $H_\alpha(X)_\rho$  is the *Rényi entropy of order  $\alpha$* , defined as

$$H_\alpha(X)_\rho = \frac{1}{1-\alpha} \log_2 \left( \sum_x \rho_X(x)^\alpha \right). \quad (1.3)$$

For all  $\alpha \in (0, 1) \cup (1, \infty)$  and as the respective limit for  $\alpha \in \{0, 1, \infty\}$ . The Rényi entropies are monotonically decreasing in  $\alpha$ . Clearly the lower bound in (1.2) thus constitutes a tradeoff: larger values of the order parameter  $\alpha$  lead to a smaller Rényi entropy but will increase the penalty term  $\frac{\alpha}{1-\alpha} \log_2 \frac{1}{\varepsilon}$ . Statements about the existence of codes as in (1.2) are called *achievability bounds* or *direct bounds*.

This analysis can be driven further if we consider sources with structure. In particular, consider a sequence of sources that produce  $n \in \mathbb{N}$  *independent and identically distributed (iid)* symbols  $X^n = (Y_1, Y_2, \dots, Y_n)$ , where each  $Y_i$  is distributed according to the law  $\tau_Y(y)$ . We then consider a sequence of  $(\varepsilon, 2^{nR})$ -codes for these sources,

where the *rate*  $R$  indicates the number of memory bits required per symbol the source produces. For this case (1.2) reads

$$R \geq \frac{1}{n} H_\alpha(X^n)_\rho + \frac{\alpha}{n(1-\alpha)} \log_2 \frac{1}{\varepsilon} = H_\alpha(Y)_\tau + \frac{\alpha}{n(1-\alpha)} \log_2 \frac{1}{\varepsilon} \quad (1.4)$$

where we used additivity of the Rényi entropy to establish the equality. The above inequality implies that such a sequence of  $(\varepsilon, 2^{nR})$ -codes exists for sufficiently large  $n$  if  $R > H_\alpha(X)_\rho$ . And finally, since this holds for all  $\alpha \in [\frac{1}{2}, 1)$ , we may take the limit  $\alpha \rightarrow 1$  in (1.4) to recover Shannon's original result [144], which states that such codes exist if

$$R > H(X)_\rho, \quad \text{where} \quad H(X)_\rho = H_1(X)_\rho = - \sum_x \rho_X(x) \log_2 \rho_X(x) \quad (1.5)$$

is the Shannon entropy of the source. This rate is in fact optimal, meaning that every scheme with  $R < H(X)_\rho$  necessary fails with certainty as  $n \rightarrow \infty$ . This is an example of an asymptotic statement (with infinite resources) and such statements can often be expressed in terms of the Shannon entropy or related information measures.

### Analysis with Smooth Entropies

Another fruitful approach to analyze this problem brings us back to the unstructured, one-shot case. We note that the above analysis can be refined without assuming any structure by “*smoothing*” the entropy. Namely, we construct an  $(\varepsilon, m)$  code for the source  $\rho_X$  using the following recipe:

- Fix  $\delta \in (0, \varepsilon)$  and let  $\tilde{\rho}_X$  be any probability distribution that is  $(\varepsilon - \delta)$ -close to  $\rho_X$  in variational distance. Namely, we require that  $\Delta(\tilde{\rho}_X, \rho_X) \leq \varepsilon - \delta$  where  $\Delta(\cdot, \cdot)$  denotes the variational distance.
- Then, take a  $(\delta, m)$ -code for the source  $\tilde{\rho}_X$ . Instantiating (1.2) with  $\alpha = \frac{1}{2}$ , we find that there exists such a code as long as  $\log_2 m \geq H_{1/2}(X)_{\tilde{\rho}} + \log_2 \frac{1}{\delta}$ .
- Apply this code to a source with the distribution  $\rho_X$  instead, incurring a total error of at most  $\delta + \Delta(\rho_X, \tilde{\rho}_X) \leq \varepsilon$ . (This uses the triangle inequality and the fact that the variational distance contracts when we process information through the encoder and decoder.)

Hence, optimizing this over all such  $\tilde{\rho}_X$ , we find that there exists a  $(\varepsilon, m)$ -code if

$$\log_2 m \geq H_{\max}^{\varepsilon-\delta}(X)_\rho + \log_2 \frac{1}{\delta}, \quad \text{where} \quad H_{\max}^{\varepsilon'}(X)_\rho := \min_{\tilde{\rho}_X: \Delta(\rho_X, \tilde{\rho}_X) \leq \varepsilon'} H_{1/2}(X)_{\tilde{\rho}} \quad (1.6)$$

is the  $\varepsilon'$ -*smooth max-entropy*, which is based on the Rényi entropy of order  $\frac{1}{2}$ .

Furthermore, this bound is approximately optimal in the following sense. It can be shown [138] that all  $(\varepsilon, m)$ -codes must satisfy  $\log_2 m \geq H_{\max}^\varepsilon(X)_\rho$ . Such bounds



that give restrictions valid for all codes are called *converse bounds*. Rewriting this, we see that the minimal value of  $m$  for a given  $\varepsilon$ , denoted  $m_*(\varepsilon)$ , satisfies

$$H_{\max}^\varepsilon(X)_\rho \leq \log_2 m_*(\varepsilon) \leq \inf_{\delta \in (0, \varepsilon)} \left[ H_{\max}^{\varepsilon-\delta}(X)_\rho + \log_2 \frac{1}{\delta} \right]. \quad (1.7)$$

We thus informally say that the memory required for one-shot source compression is *characterized* by the smooth max-Rényi entropy.<sup>3</sup>

Finally, we again consider the case of an iid source, and as before, we expect that in the limit of large  $n$ , the optimal compression rate  $\frac{1}{n}m_*(\varepsilon)$  should be characterized by the Shannon entropy. This is in fact an expression of an entropic version of the *asymptotic equipartition property*, which states that

$$\lim_{n \rightarrow \infty} \frac{1}{n} H_{\max}^{\varepsilon'}(X^n)_\rho = H(Y)_\tau \quad \text{for all } \varepsilon' \in (0, 1). \quad (1.8)$$

### Why Shannon Entropy is Inadequate

To see why the Shannon entropy does not suffice to characterize one-shot source compression, consider a source that produces the symbol ‘ $\sharp$ ’ with probability  $1/2$  and  $k$  other symbols with probability  $1/2k$  each. On the one hand, for any fixed failure probability  $\varepsilon \ll 1$ , the converse bound in (1.7) evaluates to approximately  $\log_2 k$ . This implies that we cannot compress this source much beyond its Hartley entropy. On the other hand, the Shannon entropy of this distribution is  $\frac{1}{2}(\log_2 k + 2)$  and underestimates the required memory by a factor of two.

## 1.3 Outline of the Book

The goal of this book is to explore quantum generalizations of the measures encountered in our example, namely the Rényi entropies and smooth entropies. Our exposition assumes that the reader is familiar with basic probability theory and linear algebra, but not necessarily with quantum mechanics. For the most part we restrict our attention to physical systems whose observable properties are discrete, e.g. spin systems or excitations of particles bound in a potential. This allows us to avoid mathematical subtleties that appear in the study of systems with observable properties that are continuous. We will, however, mention generalizations to continuous systems where applicable and refer the reader to the relevant literature.

The book is organized as follows:

**Chapter 2** introduces the notation used throughout the book and presents the mathematical framework underlying quantum theory for general (potentially continuous) systems. Our notation is summarized in Table 2.1 so that the remainder of

---

<sup>3</sup>The smoothing approach in the classical setting was first formally discussed in [141]. A detailed analysis of one-shot source compression, including quantum side information, can be found in [138].

the chapter can easily be skipped by expert readers. The exposition starts with introducing events as linear operators on a Hilbert space (Sect. 2.2) and then introduces states as functionals on events (Sect. 2.3). Multi-partite systems and entanglement is then discussed using the Hilbert space tensor product (Sect. 2.4) and finally quantum channels are introduced as a means to study the evolution of systems in the Schrödinger and Heisenberg picture (Sect. 2.6). Finally, this chapter assembles the mathematical toolbox required to prove the results in the later chapters, including a discussion of operator monotone, concave and convex functions on positive operators (Sect. 2.5). Most results discussed here are well-known and proofs are omitted. We do not attempt to provide an intuition or physical justification for the mathematical models employed, but instead highlight some connections to classical information theory.

**Chapter 3** treats norms and metrics on quantum states. First we discuss Schatten norms and a variational characterization of the Schatten norms of positive operators that will be very useful in the remainder of the book (Sect. 3.1). We then move on to discuss a natural dual norm for sub-normalized quantum states and the metric it induces, the trace distance (Sect. 3.2). The fidelity is another very prominent measure for the proximity of quantum states, and here we sensibly extend its definition to cover sub-normalized states (Sect. 3.3). Finally, based on this generalized fidelity, we introduce a powerful metric for sub-normalized quantum states, the purified distance (Sect. 3.4). This metric combines the clear operational interpretation of the trace distance with the desirable mathematical properties of the fidelity.

**Chapter 4** discusses quantum generalizations of the Rényi divergence. Divergences (or relative entropies) are measures of distance between quantum states (although they are not metrics) and entropy as well as conditional entropy can conveniently be defined in terms of the divergence. Moreover, the entropies inherit many important properties from corresponding properties of the divergence. In this chapter, we first discuss the classical special case of the Rényi divergence (Sect. 4.1). This allows us to point out several properties that we expect a suitable quantum generalization of the Rényi divergence to satisfy. Most prominently we expect them to satisfy a data-processing inequality which states that the divergence is contractive under application of quantum channels to both states. Based on this, we then explore quantum generalizations of the Rényi divergence and find that there is more than one quantum generalization that satisfies all desired properties (Sect. 4.2).

We will mostly focus on two different quantum Rényi divergences, called the minimal and Petz quantum Rényi divergence (Sects. 4.3 and 4.4). The first quantum generalization is called the minimal quantum Rényi divergence (because it is the smallest quantum Rényi divergence that satisfies a data-processing inequality), and is also known as “sandwiched” Rényi relative entropy in the literature. It has found operational significance in the strong converse regime of asymmetric binary hypothesis testing. The second quantum generalization is Petz’ quantum Rényi relative entropy, which attains operational significance in the quantum

generalization of Chernoff's and Hoeffding's bound on the success probability in binary hypothesis testing (cf. Sect. 7.1).

**Chapter 5** generalizes conditional Rényi entropies (and unconditional entropies as a special case) to the quantum setting. The idea is to define operationally relevant measures of uncertainty about the state of a quantum system from the perspective of an observer with access to some side information stored in another quantum system. As a preparation, we discuss how the conditional Shannon entropy and the conditional von Neumann entropy can be conveniently expressed in terms of relative entropy either directly or using a variational formula (Sect. 5.1). Based on the two families of quantum Rényi divergences, we then define four families of quantum conditional Rényi entropies (Sect. 5.2). We then prove various properties of these entropies, including data-processing inequalities that they directly inherit from the underlying divergence. A genuinely quantum feature of conditional Rényi entropies is the duality relation for pure states (Sect. 5.3). These duality relations also show that the four definitions are not independent, and thereby also reveal a connection between the minimal and the Petz quantum Rényi divergence. Furthermore, even though the chain rule does not hold with equality for our definitions, we present some inequalities that replace the chain rule (Sect. 5.4).

**Chapter 6** deals with smooth conditional entropies in the quantum setting. First, we discuss the min-entropy and the max-entropy, two special cases of Rényi entropies that underly the definition of the smooth entropy (Sect. 6.1). In particular, we show that they can be expressed as semi-definite programs, which means that they can be approximated efficiently (for small quantum systems) using standard numerical solvers. The idea is that these two entropies serve as representatives for the Rényi entropies with large and small  $\alpha$ , respectively. We then define the smooth entropies (Sect. 6.2) as optimizations of the min- and max-entropy over a ball of states close in purified distance. We explore some of their properties, including chain rules and duality relations (Sect. 6.3). Finally, the main application of the smooth entropy calculus is an entropic version of the asymptotic equipartition property for conditional entropies, which states that the (regularized) smooth min- and max-entropies converge to the conditional von Neumann entropy for iid product states (Sect. 6.4).

**Chapter 7** concludes the book with a few selected applications of the mathematical concepts surveyed here. First, we discuss various aspects of binary hypothesis testing, including Stein's lemma, the Chernoff bound and the Hoeffding bound as well as strong converse exponents (Sect. 7.1). This provides an operational interpretation of the Rényi divergences discussed in Chap. 4. Next, we discuss how the duality relations and the chain rule for conditional Rényi entropies can be used to derive entropic uncertainty relations—powerful manifestations of the uncertainty principle of quantum mechanics (Sect. 7.2). Finally, we discuss randomness extraction against quantum side information, a premier application of the smooth entropy formalism that justifies its central importance in quantum cryptography (Sect. 7.3).

### **What This Book Does Not Cover**

It is beyond the scope of this book to provide a comprehensive treatment of the many applications the mathematical framework reviewed here has found. However, in addition to Chap. 7, we will mention a few of the most important applications in the background section of each chapter. Tsallis entropies [162] have found several applications in physics, but they have no solid foundation in information theory and we will not discuss them here. It is worth mentioning, however, that many of the mathematical developments in this book can be applied to quantum Tsallis entropies as well. There are alternative frameworks besides the smooth entropy framework that allow to treat unstructured resources, most prominently the information-spectrum method and its quantum generalization due to Nagaoka and Hayashi [124]. These approaches are not covered here since they are asymptotically equivalent to the smooth entropy approach [45, 157]. Finally, this book does not cover Rényi and smooth versions of mutual information and conditional mutual information. These quantities are a topic of active research.

## Chapter 2

# Modeling Quantum Information

**Abstract** Classical as well as quantum information is stored in physical systems, or “information is inevitably physical” as Rolf Landauer famously said. These physical systems are ultimately governed by the laws of quantum mechanics. In this chapter we quickly review the relevant mathematical foundations of quantum theory and introduce notational conventions that will be used throughout the book.

In particular we will discuss concepts of functional and matrix analysis as well as linear algebra that will be of use later. We consider general separable Hilbert spaces in this chapter, even though in the rest of the book we restrict our attention to the finite-dimensional case. This digression is useful because it motivates the notation we use throughout the book, and it allows us to distinguish between the mathematical structure afforded by quantum theory and the additional structure that is only present in the finite-dimensional case.

Our notation is summarized in Sect. 2.1 and the remainder of this chapter can safely be skipped by expert readers. The presentation here is compressed and we omit proofs. We instead refer to standard textbooks (see Sect. 2.7 for some references) for a more comprehensive treatment.

### 2.1 General Remarks on Notation

The notational conventions for this book are summarized in Table 2.1. The table includes references to the sections where the corresponding concepts are introduced. Throughout this book we are careful to distinguish between linear operators (e.g. events and Kraus operators) and functionals on the linear operators (e.g. states), which are also represented as linear operators (e.g. density operators). This distinction is inspired by the study of infinite-dimensional systems where these objects do not necessarily have the same mathematical structure, but it is also helpful in the finite-dimensional setting.<sup>1</sup>

---

<sup>1</sup>For example, it sheds light on the fact that we use the operator norm for ordinary linear operators and its dual norm, the trace norm, for density operators.

**Table 2.1** Overview of notational conventions

Symbol	Variants	Description	Section
$\mathbb{R}, \mathbb{C}$	$\mathbb{R}_+$	Real and complex fields (and non-negative reals)	
$\mathbb{N}$		Natural numbers	
log, exp	ln, $e$	Logarithm (to unspecified basis), and its inverse, the exponential function (natural logarithm and Euler's constant)	
$\mathcal{H}$	$\mathcal{H}_{AB}, \mathcal{H}_X$	Hilbert spaces (for joint system $AB$ and system $X$ )	2.2.1
$\langle \cdot  ,   \cdot \rangle$		Bra and ket	
$\text{Tr}(\cdot)$	$\text{Tr}_A$	Trace (partial trace)	2.3.1
$\otimes$	$(\cdot)^{\otimes n}$	Tensor product ( $n$ -fold tensor product)	2.4.1
$\oplus$		Direct sum for block diagonal operators	2.2.2
$A \ll B$		$A$ is dominated by $B$ , i.e. kernel of $A$ contains kernel of $B$	
$A \perp B$		$A$ and $B$ are orthogonal, i.e. $AB = BA = 0$	
$\mathcal{L}$	$\mathcal{L}(A, B)$	Bounded linear operators (from $\mathcal{H}_A$ to $\mathcal{H}_B$ )	2.2.1
$\mathcal{L}^\dagger$	$\mathcal{L}^\dagger(B)$	Self-adjoint operators (acting on $\mathcal{H}_B$ )	
$\mathcal{P}$	$\mathcal{P}(CD)$	Positive semi-definite operators (acting on $\mathcal{H}_{CD}$ )	
$\{A \geq B\}$		Projector on subspace where $A - B$ is non-negative	
$\  \cdot \ $		Operator norm	2.2.1
$\mathcal{L}_\bullet$	$\mathcal{L}_\bullet(E)$	Contractions in $\mathcal{L}$ (acting on $\mathcal{H}_E$ )	
$\mathcal{P}_\bullet$	$\mathcal{P}_\bullet(A)$	Contractions in $\mathcal{P}$ (corresponding to events on $A$ )	2.2.2
$I$	$I_Y$	Identity operator (acting on $\mathcal{H}_Y$ )	
$\langle \cdot, \cdot \rangle$		Hilbert-Schmidt inner product	2.3.1
$\mathcal{T}$	$\mathcal{T} \equiv \mathcal{L}^{\ddagger}$	Trace-class operators representing linear functionals	
$\mathcal{S}$	$\mathcal{S} \equiv \mathcal{P}^{\ddagger}$	Operators representing positive functionals	
$\  \cdot \ _*$	$\text{Tr}   \cdot  $	Trace norm on functionals	2.3.1
$\mathcal{S}_\bullet$	$\mathcal{S}_\bullet(A)$	Sub-normalized density operators (on $A$ )	2.3.2
$\mathcal{S}_\circ$	$\mathcal{S}_\circ(B)$	Normalized density operators, or states (on $B$ )	
$\pi$	$\pi_A$	Fully mixed state (on $A$ ), in finite dimensions	2.3.2
$\psi$	$\psi_{AB}$	Maximally entangled state (between $A$ and $B$ ), in finite dimensions	2.4.2
CB	$\text{CB}(A, B)$	Completely bounded maps (from $\mathcal{L}(A)$ to $\mathcal{L}(B)$ )	2.6.1
CP		Completely positive maps	2.6.2
CPTP	CPTNI	Completely positive trace-preserving (trace-non-increasing) map	
$\  \cdot \ _+$	$\  \cdot \ _p$	Positive cone dual norm (Schatten $p$ -norm)	3.1
$\Delta(\cdot, \cdot)$		Generalized trace distance for sub-normalized states	3.2
$F(\cdot, \cdot)$	$F_*(\cdot, \cdot)$	Fidelity (generalized fidelity for sub-normalized states)	3.3
$P(\cdot, \cdot)$		Purified distance for sub-normalized states	3.4

<sup>‡</sup>This equivalence only holds if the underlying Hilbert space is finite-dimensional

We do not specify a particular basis for the logarithm throughout this book, and simply use  $\exp$  to denote the inverse of  $\log$ .<sup>2</sup> The natural logarithm is denoted by  $\ln$ .

We label different physical systems by capital Latin letters  $A, B, C, D$ , and  $E$ , as well as  $X, Y$ , and  $Z$  which are specifically reserved for classical systems. The label thus always determines if a system is quantum or classical. We often use these labels as subscripts to guide the reader by indicating which system a mathematical object belongs to. We drop the subscripts when they are evident in the context of an expression (or if we are not talking about a specific system). We also use the capital Latin letters  $L, K, H, M$ , and  $N$  to denote linear operators, where the last two are reserved for positive semi-definite operators. The identity operator is denoted  $I$ . Density operators, on the other hand, are denoted by lowercase Greek letters  $\rho, \tau, \sigma$ , and  $\omega$ . We reserve  $\pi$  and  $\psi$  for the fully mixed state and the maximally entangled state, respectively. Calligraphic letters are used to denote quantum channels and other maps acting on operators.

## 2.2 Linear Operators and Events

For our purposes, a *physical system* is fully characterized by the set of events that can be observed on it. For classical systems, these events are traditionally modeled as a  $\sigma$ -algebra of subsets of the sample space, usually the power set in the discrete case. For quantum systems the structure of events is necessarily more complex, even in the discrete case. This is due to the non-commutative nature of quantum theory: the union and intersection of events are generally ill-defined since it matters in which order events are observed.

Let us first review the mathematical model used to describe events in quantum mechanics (as positive semi-definite operators on a Hilbert space). Once this is done, we discuss physical systems carrying quantum and classical information.

### 2.2.1 Hilbert Spaces and Linear Operators

For concreteness and to introduce the notation, we consider two physical systems  $A$  and  $B$  as examples in the following. We associate to  $A$  a separable *Hilbert space*  $\mathcal{H}_A$  over the field  $\mathbb{C}$ , equipped with an *inner product*  $\langle \cdot, \cdot \rangle : \mathcal{H}_A \times \mathcal{H}_A \rightarrow \mathbb{C}$ . In the finite-dimensional case, this is simply a complex inner product space, but we will follow a tradition in quantum information theory and call  $\mathcal{H}_A$  a Hilbert space also in this case. Analogously, we associate the Hilbert space  $\mathcal{H}_B$  to the physical system  $B$ .

---

<sup>2</sup>The reader is invited to think of  $\log(x)$  as the binary logarithm of  $x$  and, consequently,  $\exp(x) = 2^x$ , as is customary in quantum information theory.

## Linear Operators

Our main object of study are *linear operators* acting on the system's Hilbert space. We consistently use upper-case Latin letters to denote such linear operators. More precisely, we consider the set of *bounded linear operators* from  $\mathcal{H}_A$  to  $\mathcal{H}_B$ , which we denote by  $\mathcal{L}(A, B)$ . Bounded here refers to the *operator norm* induced by the Hilbert space's inner product.

The **operator norm** on  $\mathcal{L}(A, B)$  is defined as

$$\|\cdot\| : L \mapsto \sup \left\{ \sqrt{\langle Lv, Lv \rangle_B} : v \in \mathcal{H}_A, \langle v, v \rangle_A \leq 1 \right\}. \quad (2.1)$$

For all  $L \in \mathcal{L}(A, B)$ , we have  $\|L\| < \infty$  by definition. A linear operator is continuous if and only if it is bounded.<sup>3</sup> Let us now summarize some important concepts and notation that we will frequently use throughout this book.

- The *identity operator* on  $\mathcal{H}_A$  is denoted  $I_A$ .
- The *adjoint* of a linear operator  $L \in \mathcal{L}(A, B)$  is the unique operator  $L^\dagger \in \mathcal{L}(B, A)$  that satisfies  $\langle w, Lv \rangle_B = \langle L^\dagger w, v \rangle_A$  for all  $v \in \mathcal{H}_A, w \in \mathcal{H}_B$ . Clearly,  $(L^\dagger)^\dagger = L$ .
- For scalars  $\alpha \in \mathbb{C}$ , the adjoint corresponds to the complex conjugate,  $\alpha^\dagger = \bar{\alpha}$ .
- We find  $(LK)^\dagger = K^\dagger L^\dagger$  by applying the definition twice.
- The *kernel* of a linear operator  $L \in \mathcal{L}(A, B)$  is the subspace of  $\mathcal{H}_A$  spanned by vectors  $v \in \mathcal{H}_A$  satisfying  $Lv = 0$ . The *support* of  $L$  is its orthogonal complement in  $\mathcal{H}_A$  and the *rank* is the cardinality of the support. Finally, the image of  $L$  is the subspace of  $\mathcal{H}_B$  spanned by vectors  $w \in \mathcal{H}_B$  such that  $w = Lv$  for some  $v \in \mathcal{H}_A$ .
- For operators  $K, L \in \mathcal{L}(A)$  we say that  $L$  is *dominated* by  $K$  if the kernel of  $K$  is contained in the kernel of  $L$ . Namely, we write  $L \ll K$  if and only if

$$K|v\rangle_A = 0 \implies L|v\rangle_A = 0 \quad \text{for all } v \in \mathcal{H}_A. \quad (2.3)$$

- We say  $K, L \in \mathcal{L}(A)$  are *orthogonal* (denoted  $K \perp L$ ) if  $KL = LK = 0$ .
- We call a linear operator  $U \in \mathcal{L}(A, B)$  an *isometry* if it preserves the inner product, namely if  $\langle Uv, Uw \rangle_B = \langle v, w \rangle_A$  for all  $v, w \in \mathcal{H}_A$ . This holds if  $U^\dagger U = I_A$ .

<sup>3</sup>*Relation to Operator Algebras:* Let us note that  $\mathcal{L}(A, B)$  with the norm  $\|\cdot\|$  is a Banach space over  $\mathbb{C}$ . Furthermore, the operator norm satisfies

$$\|L\|^2 = \|L^\dagger\|^2 = \|L^\dagger L\| \quad \text{and} \quad \|LK\| \leq \|L\| \cdot \|K\|. \quad (2.2)$$

for any  $L \in \mathcal{L}(A, B)$  and  $K \in \mathcal{L}(B, A)$ . The inequality states that the norm is *sub-multiplicative*.

The above properties of the norm imply that the space  $\mathcal{L}(A)$  is (weakly) closed under multiplication and the adjoint operation. In fact,  $\mathcal{L}(A)$  constitutes a (Type I factor) von Neumann algebra or  $C^*$  algebra. Alternatively, we could have started our considerations right here by postulating a Type I von Neumann algebra as the fundamental object describing individual physical systems, and then deriving the Hilbert space structure as a consequence.



- An isometry is an example of a *contraction*, i.e. an operator  $L \in \mathcal{L}(A, B)$  satisfying  $\|L\| \leq 1$ . The set of all such contractions is denoted  $\mathcal{L}_\bullet(A, B)$ . Here the bullet ‘•’ in the subscript of  $\mathcal{L}_\bullet(A, B)$  simply illustrates that we restrict  $\mathcal{L}(A, B)$  to the unit ball for the norm  $\|\cdot\|$ .

For any  $L \in \mathcal{L}(A)$ , we denote by  $L^{-1}$  its Moore-Penrose *generalized inverse* or pseudoinverse [130] (which always exists in finite dimensions). In particular, the generalized inverse satisfies  $LL^{-1}L = L$  and  $L^{-1}LL^{-1} = L^{-1}$ . If  $L = L^\dagger$ , the generalized inverse is just the usual inverse evaluated on the operator’s support.

### Bras, Kets and Orthonormal Bases

We use the *bra-ket notation* throughout this book. For any vector  $v_A \in \mathcal{H}_A$ , we use its *ket*, denoted  $|v\rangle_A$ , to describe the embedding

$$|v\rangle_A: \mathbb{C} \rightarrow \mathcal{H}_A, \quad \alpha \mapsto \alpha v_A. \quad (2.4)$$

Similarly, we use its *bra*, denoted  $\langle v|_A$ , to describe the functional

$$\langle v|_A: \mathcal{H}_A \rightarrow \mathbb{C}, \quad w_A \mapsto \langle v, w \rangle_A. \quad (2.5)$$

It is natural to view kets as linear operators from  $\mathbb{C}$  to  $\mathcal{H}_A$  and bras as linear operators from  $\mathcal{H}_A$  to  $\mathbb{C}$ . The above definitions then imply that

$$|Lv\rangle_A = L|v\rangle_A, \quad \langle Lv|_A = \langle v|_A L^\dagger, \quad \text{and} \quad \langle v|_A = |v\rangle_A^\dagger. \quad (2.6)$$

Moreover, the inner product can equivalently be written as  $\langle w, Lv \rangle_B = \langle w|_B L|v\rangle_A$ . Conjugate symmetry of the inner product then corresponds to the relation

$$\overline{\langle w|_B L|v\rangle_A} = \langle v|_A L^\dagger |w\rangle_B. \quad (2.7)$$

As a further example, we note that  $|v\rangle_A$  is an isometry if and only if  $\langle v|v\rangle_A = 1$ .

In the following we will work exclusively with linear operators (including bras and kets) and we will not use the underlying vectors (the elements of the Hilbert space) or the inner product of the Hilbert space anymore.

We now restrict our attention to the space  $\mathcal{L}(A) := \mathcal{L}(A, A)$  of bounded linear operators acting on  $\mathcal{H}_A$ . An operator  $U \in \mathcal{L}(A)$  is *unitary* if  $U$  and  $U^\dagger$  are isometries. An *orthonormal basis* (ONB) of the system  $A$  (or the Hilbert space  $\mathcal{H}_A$ ) is a set of vectors  $\{e_x\}_x$ , with  $e_x \in \mathcal{H}_A$ , such that

$$\langle e_x | e_y \rangle_A = \delta_{x,y} := \begin{cases} 1 & x = y \\ 0 & x \neq y \end{cases} \quad \text{and} \quad \sum_x |e_x\rangle\langle e_x|_A = I_A. \quad (2.8)$$

We denote the dimension of  $\mathcal{H}_A$  by  $d_A$  if it is finite and note that the index  $x$  ranges over  $d_A$  distinct values. For general separable Hilbert spaces  $x$  ranges over any countable set. (We do not usually specify such index sets explicitly.) Various ONBs

exist and are related by unitary operators: if  $\{e_x\}_x$  is an ONB then  $\{Ue_x\}_x$  is too, and, furthermore, given two ONBs there always exists a unitary operator mapping one basis to the other, and vice versa.

### Positive Semi-Definite Operators

A special role is played by operators that are self-adjoint and positive semi-definite. We call an operator  $H \in \mathcal{L}(A)$  *self-adjoint* if it satisfies  $H = H^\dagger$ , and the set of all self-adjoint operators in  $\mathcal{L}(A)$  is denoted  $\mathcal{L}^\dagger(A)$ . Such self-adjoint operators have a spectral decomposition,

$$H = \sum_x \lambda_x |e_x\rangle\langle e_x| \quad (2.9)$$

where  $\{\lambda_x\}_x \subset \mathbb{R}$  are called *eigenvalues* and  $\{|e_x\rangle\}_x$  is an orthonormal basis with *eigenvectors*  $|e_x\rangle$ . The set  $\{\lambda_x\}_x$  is also called the *spectrum* of  $H$ , and it is unique.

Finally we introduce the set  $\mathcal{P}(A)$  of *positive semi-definite* operators in  $\mathcal{L}(A)$ . An operator  $M \in \mathcal{L}(A)$  is positive semi-definite if and only if  $M = L^\dagger L$  for some  $L \in \mathcal{L}(A)$ , so in particular such operators are self-adjoint and have non-negative eigenvalues. Let us summarize some important concepts and notation concerning self-adjoint and positive semi-definite operators here.

- We call  $P \in \mathcal{P}(A)$  a *projector* if it satisfies  $P^2 = P$ , i.e. if it has only eigenvalues 0 and 1. The identity  $I_A$  is a projector.
- For any  $K, L \in \mathcal{L}^\dagger(A)$ , we write  $K \geq L$  if  $K - L \in \mathcal{P}(A)$ . Thus, the relation ‘ $\geq$ ’ constitutes a partial order on  $\mathcal{L}(A)$ .
- For any  $G, H \in \mathcal{L}^\dagger(A)$ , we use  $\{G \geq H\}$  to denote the projector onto the subspace corresponding to non-negative eigenvalues of  $G - H$ . Analogously,  $\{G < H\} = I - \{G \geq H\}$  denotes the projector onto the subspace corresponding to negative eigenvalues of  $G - H$ .

### Matrix Representation and Transpose

Linear operators in  $\mathcal{L}(A, B)$  can be conveniently represented as matrices in  $\mathbb{C}^{d_A} \times \mathbb{C}^{d_B}$ . Namely for any  $L \in \mathcal{L}(A, B)$ , we can write

$$L = \sum_{x,y} |f_y\rangle\langle f_y|_B L |e_x\rangle\langle e_x|_A = \sum_{x,y} \langle f_y|L|e_x\rangle \cdot |f_y\rangle\langle e_x|, \quad (2.10)$$

where  $\{e_x\}_x$  is an ONB of  $A$  and  $\{f_y\}_y$  an ONB of  $B$ . This decomposes  $L$  into elementary operators  $|f_y\rangle\langle e_x| \in \mathcal{L}_\bullet(A, B)$  and the matrix with entries  $[L]_{yx} = \langle f_y|L|e_x\rangle$ .

Moreover, there always exists a choice of the two bases such that the resulting matrix is diagonal. For such a choice of bases, we find the *singular value decomposition*  $L = \sum_x s_x |f_x\rangle\langle e_x|$ , where  $\{s_x\}_x$  with  $s_x \geq 0$  are called the singular values of  $L$ . In particular, for self-adjoint operators, we can choose  $|f_x\rangle = |e_x\rangle$  and recover the eigenvalue decomposition with  $s_x = |\lambda_x|$ .

The *transpose* of  $L$  with regards to the bases  $\{e_x\}$  and  $\{f_y\}$  is defined as

$$L^T := \sum_{x,y} \langle f_y | L | e_x \rangle \cdot | e_x \rangle \langle f_y |, \quad L^T \in \mathcal{L}(B, A). \quad (2.11)$$

Importantly, in contrast to the adjoint, the transpose is only defined with regards to a particular basis. Also contrast (2.11) with the matrix representation of  $L^\dagger$ ,

$$L^\dagger = \sum_{x,y} (\langle f_y | L | e_x \rangle)^\dagger \cdot | e_x \rangle \langle f_y | = \sum_{x,y} \langle e_x | L^\dagger | f_y \rangle \cdot | e_x \rangle \langle f_y | = \bar{L}^T. \quad (2.12)$$

Here,  $\bar{L}$  denotes the complex conjugate, which is also basis dependent.

### 2.2.2 Events and Measures

We are now ready to attach physical meaning to the concepts introduced in the previous section, and apply them to physical systems carrying quantum information.

Observable **events** on a quantum system  $A$  correspond to operators in the unit ball of  $\mathcal{P}(A)$ , namely the set

$$\mathcal{P}_\bullet(A) := \{M \in \mathcal{L}(A) : 0 \leq M \leq I\}. \quad (2.13)$$

(The bullet ‘ $\bullet$ ’ indicates that we restrict to the unit ball of the norm  $\|\cdot\|$ .)

Two events  $M, N \in \mathcal{P}_\bullet(A)$  are called *exclusive* if  $M + N$  is an event in  $\mathcal{P}_\bullet(A)$  as well. In this case, we call  $M + N$  the *union* of the events  $M$  and  $N$ . A complete set of mutually exclusive events that sum up to the identity is called a *positive operator valued measure* (POVM). More generally, for any measurable space  $(\mathcal{X}, \Sigma)$  with  $\Sigma$  a  $\sigma$ -algebra, a POVM is a function

$$O_A : \Sigma \rightarrow \mathcal{P}_\bullet(A) \quad \text{with} \quad O_A(\mathcal{X}) = I_A \quad (2.14)$$

that is  $\sigma$ -additive, meaning that  $O_A(\bigcup_i \mathcal{X}_i) = \sum_i O_A(\mathcal{X}_i)$  for mutually disjoint subsets  $\mathcal{X}_i \subset \mathcal{X}$ . This definition is too general for our purposes here, and we will restrict our attention to the case where  $\mathcal{X}$  is discrete and  $\Sigma$  the power set of  $\mathcal{X}$ . In that case the POVM is fully determined if we associate mutually exclusive events to each  $x \in \mathcal{X}$ .

A function  $x \mapsto M_A(x)$  with  $M_A(x) \in \mathcal{P}_\bullet(A)$ ,  $\sum_x M_A(x) = I_A$  is called a **positive operator valued measure (POVM)** on  $A$ .

We assume that  $x$  ranges over a countable set for this definition, and we will in fact not discuss measurements with continuous outcomes in this book. We call  $x \mapsto M_A(x)$  a *projective* measure if all  $M_A(x)$  are projectors, and we call it *rank-one* if all  $M_A(x)$  have rank one.

### Structure of Classical Systems

Classical systems have the distinguishing property that all events commute.

To model a classical system  $X$  in our quantum framework, we restrict  $\mathcal{P}_\bullet(X)$  to a set of events that commute. These are diagonalized by a common ONB, which we call the *classical basis* of  $X$ . For simplicity, the classical basis is denoted  $\{|x\rangle_x$  and the corresponding kets are  $|x\rangle_x$ . (To avoid confusion, we will call the index  $y$  or  $z$  instead of  $x$  if the systems  $Y$  and  $Z$  are considered instead.)

Every  $M \in \mathcal{P}_\bullet(X)$  on a classical system can be written as

$$M = \sum_x M(x) |x\rangle_x \langle x|_x = \bigoplus_x M(x), \quad \text{where } 0 \leq M(x) \leq 1. \quad (2.15)$$

Instead of writing down the basis projectors,  $|x\rangle_x \langle x|_x$ , we sometimes employ the direct sum notation to illustrate the block-diagonal structure of such operators. In the following, whenever we introduce a classical event  $M$  on  $X$  we also implicitly introduce the function  $M(x)$ , and vice versa.

This definition of “classical” events still goes beyond the usual classical formalism of discrete probability theory. In the usual formalism,  $M$  represents a subset of the sample space (an element of its  $\sigma$ -algebra), and thus corresponds to a projector in our language, with  $M(x) \in \{0, 1\}$  indicating if  $x$  is in the set. Our formalism, in contrast, allows to model probabilistic events, i.e. the event  $M$  occurs at most with probability  $M(x) \in [0, 1]$  even if the state is deterministically  $x$ .<sup>4</sup>

## 2.3 Functionals and States

States of a physical system are functionals on the set of bounded linear operators that map events to the probability that the respective event occurs.

---

<sup>4</sup>This generalization is quite useful as it, for example, allows us to see the optimal (probabilistic) Neyman-Pearson test as an event.

Continuous linear functionals can be represented as trace-class operators. This then allows us to introduce states for quantum and classical systems.

### 2.3.1 Trace and Trace-Class Operators

The most fundamental linear functional is the *trace*. For any orthonormal basis  $\{e_x\}_x$  of  $A$ , we define the trace over  $A$  as

$$\mathrm{Tr}_A(\cdot) : \mathcal{L}(A) \rightarrow \mathbb{C}, \quad L \mapsto \sum_x \langle e_x | L | e_x \rangle_A. \quad (2.16)$$

Note that  $\mathrm{Tr}(L)$  is finite if  $d_A < \infty$  or more generally if  $L$  is *trace-class*, as we will see below. The trace is cyclic, namely we have

$$\mathrm{Tr}_A(KL) = \mathrm{Tr}_B(LK) \quad (2.17)$$

for any two operators  $L \in \mathcal{L}(A, B)$ ,  $K \in \mathcal{L}(B, A)$  when  $KL$  and  $LK$  are trace-class. Thus, in particular, for any  $L \in \mathcal{L}(A)$ , we have  $\mathrm{Tr}_A(L) = \mathrm{Tr}_B(ULU^\dagger)$  for any *isometry*  $U \in \mathcal{L}(A, B)$ , which shows that the particular choice of basis used for the definition of the trace in (2.16) is irrelevant. Finally, we have  $\mathrm{Tr}(L^\dagger) = \overline{\mathrm{Tr}(L)}$ .

#### Trace-Class Operators

Using the trace, continuous linear functionals can be conveniently represented as elements of the dual Banach space of  $\mathcal{L}(A)$ , namely the space of linear operators on  $\mathcal{H}_A$  with bounded *trace norm*.

The **trace norm** on  $\mathcal{L}(A)$  is defined as

$$\|\cdot\|_* : \xi \mapsto \mathrm{Tr} |\xi| = \mathrm{Tr} \left( \sqrt{\xi^\dagger \xi} \right). \quad (2.18)$$

Operators  $\xi \in \mathcal{L}(A)$  with  $\|\xi\|_* < \infty$  are called **trace-class operators**.

We denote the subspace of  $\mathcal{L}(A)$  consisting of trace-class operators by  $\mathcal{T}(A)$  and we use lower-case Greek letters to denote elements of  $\mathcal{T}(A)$ . In infinite dimensions  $\mathcal{T}(A)$  is a proper subspace of  $\mathcal{L}(A)$ . In finite dimensions  $\mathcal{L}(A)$  and  $\mathcal{T}(A)$  coincide, but we will use this convention to distinguish between linear operators and linear operators representing functionals nonetheless.

For every trace-class operator  $\xi \in \mathcal{T}(A)$ , we define the functional  $F_\xi(L) := \langle \xi, L \rangle$  using the sesquilinear form

$$\langle \cdot, \cdot \rangle : \mathcal{T}(A) \times \mathcal{L}(A) \rightarrow \mathbb{C}, \quad (\xi, L) \mapsto \text{Tr}(\xi^\dagger L). \quad (2.19)$$

This form is continuous in both  $\mathcal{L}(A)$  and  $\mathcal{T}(A)$  with regards to the respective norms on these spaces, which is a direct consequence of Hölder's inequality  $|\text{Tr}(\xi^\dagger L)| \leq \|\xi\|_* \cdot \|L\|$ .<sup>5</sup> In finite dimensions it is also tempting to view  $\mathcal{L}(A) = \mathcal{T}(A)$  as a Hilbert space with  $\langle \cdot, \cdot \rangle$  as its inner product, the *Hilbert-Schmidt inner product*. Finally, *positive functionals* map  $\mathcal{P}(A)$  onto the positive reals. Since  $\text{Tr}(\omega M) \geq 0$  for all  $M \geq 0$  if and only if  $\omega \geq 0$ , we find that positive functionals correspond to positive semi-definite operators in  $\mathcal{T}(A)$ , and we denote these by  $\mathcal{S}(A)$ .

### 2.3.2 States and Density Operators

A *state* of a physical system  $A$  is a functional that maps events  $M \in \mathcal{P}_\bullet(A)$  to the respective probability that  $M$  is observed. We want the probability of the union of two mutually exclusive events to be additive, and thus such functionals must be linear. Furthermore, we require them to be continuous with regards to small perturbations of the events. Finally, they ought to map events into the interval  $[0, 1]$ , hence they must also be positive and normalized.

Based on the discussion in the previous section, we can conveniently parametrize all functionals corresponding to states as follows. We define the set of *sub-normalized density operators* as trace-class operators in the unit ball,

$$\mathcal{S}_\bullet(A) := \{\rho_A \in \mathcal{T}(A) : \rho_A \geq 0 \wedge \text{Tr}(\rho_A) \leq 1\}. \quad (2.21)$$

Here the bullet '•' refers to the unit ball in the norm  $\|\cdot\|_*$ . (This norm simply corresponds to the trace for positive semi-definite operators.)

For any operator  $\rho_A \in \mathcal{S}_\bullet(A)$ , we define the functional

$$\Pr_\rho(\cdot) : \mathcal{P}_\bullet(A) \rightarrow [0, 1], \quad M \mapsto \langle \rho_A, M \rangle = \text{Tr}(\rho_A M), \quad (2.22)$$

which maps events to the probability that the event occurs.

<sup>5</sup>Note also that the norms  $\|\cdot\|$  and  $\|\cdot\|_*$  are dual with regards to this form, namely we have

$$\|\xi\|_* = \sup \{ |\langle \xi, L \rangle| : L \in \mathcal{L}_\bullet(A) \}. \quad (2.20)$$

The trace norm is thus sometimes also called the *dual norm*.

This is an expression of Born's rule, and often taken as an axiom of quantum mechanics. Here it is just a natural way to map events to probabilities. We call such operators  $\rho_A$  density operators.

It is often prudent to further require that the union of all events in a POVM, namely the event  $I$ , has probability 1. This leads us to normalized density operators:

Quantum states are represented as **normalized density operators** in

$$\mathcal{S}_\circ(A) := \{\rho_A \in \mathcal{T}(A) : \rho_A \geq 0 \wedge \text{Tr}(\rho_A) = 1\}, \quad (2.23)$$

(The circle 'o' indicates that we restrict to the unit sphere of the norm  $\|\cdot\|_*$ .)

In the following we will use the expressions state and density operator interchangeably. We also use the set  $\mathcal{S}$  which contains all positive semi-definite operators, if there is no need for normalization.

States form a convex set, and a state is called *mixed* if it lies in the interior of this set. The fully mixed state (in finite dimensions) is denoted  $\pi_A := I_A/d_A$ . On the other hand, states on the boundary are called *pure*. Pure states are represented by density operators with rank one, and can be written as  $\phi_A = |\phi\rangle\langle\phi|_A$  for some  $\phi \in \mathcal{H}_A$ . With a slight abuse of nomenclature, we often call the corresponding ket,  $|\phi\rangle_A$ , a state.

### Probability Mass Functions

The structure of density operators simplifies considerably for classical systems. We are interested in evaluating the probabilities for events of the form (2.15). Hence, for any  $\rho_X \in \mathcal{S}_\circ(X)$ , we find

$$\Pr_\rho(M) = \text{Tr}(\rho_X M) = \sum_x M(x) \langle x | \rho_X | x \rangle_X = \sum_x M(x) \rho(x), \quad (2.24)$$

where we defined  $\rho_X(x) = \langle x | \rho_X | x \rangle_X$ . We thus see that it suffices to consider states of the following form:

States  $\rho_X \in \mathcal{S}_\circ(X)$  on a classical system  $X$  have the form

$$\rho_X = \sum_x \rho(x) |x\rangle\langle x|_X, \quad \text{where } \rho(x) \geq 0, \quad \sum_x \rho(x) = 1. \quad (2.25)$$

where  $\rho(x)$  is called a **probability mass function**.

Moreover, if  $\rho_X \in \mathcal{S}_\bullet(X)$  is a sub-normalized density operator, we require that  $\sum_x \rho(x) \leq 1$  instead of the equality. Again, whenever we introduce a density operator  $\rho_X$  on  $X$ , we implicitly also introduce the function  $\rho(x)$ , and vice versa.

## 2.4 Multi-partite Systems

A joint system  $AB$  is modeled using bounded linear operators on a tensor product of Hilbert spaces,  $\mathcal{H}_{AB} := \mathcal{H}_A \otimes \mathcal{H}_B$ . The respective set of bounded linear operators is denoted  $\mathcal{L}(AB)$  and the events on the joint systems are thus the elements of  $\mathcal{P}_\bullet(AB)$ . Analogously, all the other sets of operators defined in the previous sections are defined analogously for the joint system.

### 2.4.1 Tensor Product Spaces

For every  $v \in \mathcal{H}_{AB}$  on the joint system  $AB$ , there exist two ONBs,  $\{e_x\}_x$  on  $A$  and  $\{f_y\}_y$  on  $B$ , as well as a unique set of positive reals,  $\{\lambda_x\}_x$ , such that we can write

$$|v\rangle_{AB} = \sum_x \sqrt{\lambda_x} |e_x\rangle_A \otimes |f_x\rangle_B. \quad (2.26)$$

This is called the *Schmidt decomposition* of  $v$ . The convention to use a square root is motivated by the fact that the sequence  $\{\sqrt{\lambda_x}\}_x$  is square summable, i.e.  $\sum_x \lambda_x < \infty$ . Note also that  $\{e_x \otimes f_y\}_{x,y}$  can be extended to an ONB on the joint system  $AB$ .

#### Embedding Linear Operators

We embed the bounded linear operators  $\mathcal{L}(A)$  into  $\mathcal{L}(AB)$  by taking a tensor product with the identity on  $B$ . We often omit to write this identity explicitly and instead use subscripts to indicate on which system an operator acts. For example, for any  $L_A \in \mathcal{L}(A)$  and  $|v\rangle_{AB} \in \mathcal{H}_{AB}$  as in (2.26), we write

$$L_A |v\rangle_{AB} = L_A \otimes I_B |v\rangle_{AB} = \sum_x \lambda_x L_A |e_x\rangle_A \otimes |f_x\rangle_B \quad (2.27)$$

Clearly,  $\|L_A \otimes I_B\| = \|L_A\|$ , and in fact, more generally for all  $L_A \in \mathcal{L}(A)$  and  $L_B \in \mathcal{L}(B)$ , we have

$$\|L_A \otimes L_B\| = \|L_A\| \cdot \|L_B\|. \quad (2.28)$$

We say that two operators  $K, L \in \mathcal{L}(A)$  *commute* if  $[K, L] := KL - LK = 0$ . Clearly, elements of  $\mathcal{L}(A)$  and  $\mathcal{L}(B)$  mutually commute as operators in  $\mathcal{L}(AB)$ , i.e. for all  $L_A \in \mathcal{L}(A)$ ,  $K_B \in \mathcal{L}(B)$ , we have  $[L_A \otimes I_B, I_A \otimes K_B] = 0$ .



Finally, every linear operator  $L_{AB} \in \mathcal{L}(AB)$  has a decomposition

$$L_{AB} = \sum_k L_A^k \otimes L_B^k, \quad \text{where } L_A^k \in \mathcal{L}(A), L_B^k \in \mathcal{L}(B) \quad (2.29)$$

Similarly, every self-adjoint operator  $L_{AB} \in \mathcal{L}^\dagger(AB)$  decomposes in the same way but now  $L_A^k \in \mathcal{L}^\dagger(A)$  and  $L_B^k \in \mathcal{L}^\dagger(B)$  can be chosen self-adjoint as well. However, crucially, it is not always possible to decompose a positive semi-definite operator into products of positive semi-definite operators in this way.

### Representing Traces of Matrix Products Using Tensor Spaces

Let us next consider trace terms of the form  $\text{Tr}_A(K_A L_A)$  where  $K_A, L_A \in \mathcal{L}(A)$  are general linear operators and  $\mathcal{H}_A$  is finite-dimensional. It is often convenient to represent such traces as follows.

First, we introduce an auxiliary system  $A'$  such that  $\mathcal{H}_A$  and  $\mathcal{H}_{A'}$  are isomorphic (i.e. they have the same dimension). Furthermore, we fix a pair of bases  $\{|e_x\rangle_A\}_x$  of  $A$  and  $\{|e_x\rangle_{A'}\}_x$  of  $A'$ . (We can use the same index set here since these spaces are isomorphic.) Clearly every linear operator on  $A$  has a natural embedding into  $A'$  given by this isomorphism. Using these bases, we further define a rank one operator  $\Psi \in \mathcal{L}(AA')$  in its Schmidt decomposition as

$$|\Psi\rangle_{AA'} = \sum_x |x\rangle_A \otimes |x\rangle_{A'}. \quad (2.30)$$

(Note that this state has norm  $\|\Psi\|_* = d_A$ , which is why this discussion is restricted to finite dimensions.) Using the matrix representation of the transpose in (2.11), we now observe that  $L_A \otimes I_{A'} |\Psi\rangle_{AA'} = I_A \otimes L_{A'}^T |\Psi\rangle_{AA'}$  and, therefore,

$$\text{Tr}(K_A L_A) = \langle \Psi | K_A L_A | \Psi \rangle = \langle \Psi |_{AA'} K_A \otimes L_{A'}^T | \Psi \rangle_{AA'}. \quad (2.31)$$

We will encounter this representation many times and keep  $\Psi$  thus reserved for this purpose, without going through the construction explicitly every time.<sup>6</sup>

### Marginals of Functionals

Given a bipartite system  $AB$  that consists of two sets of operators  $\mathcal{L}(A)$  and  $\mathcal{L}(B)$ , we now want to specify how a trace-class operator  $\xi_{AB} \in \mathcal{T}(AB)$  acts on  $\mathcal{L}(A)$ . For any  $L_A \in \mathcal{L}(A)$ , we have

$$F_{\xi_{AB}}(L_A) = \langle \xi_{AB}, L_A \otimes I_B \rangle = \text{Tr}(\xi_{AB}^\dagger L_A \otimes I_B) = \text{Tr}_A(\text{Tr}_B(\xi_{AB}^\dagger) L_A), \quad (2.32)$$

where we simply used that  $\text{Tr}_{AB}(\cdot) = \text{Tr}_A(\text{Tr}_B(\cdot))$  where  $\text{Tr}_B$  as defined in (2.16) naturally embeds as a map from  $\mathcal{T}(AB)$  into  $\mathcal{T}(A)$ , i.e.

---

<sup>6</sup>Note that  $\Psi$  is an (unnormalized) maximally entangled state, usually denoted  $\psi$ .

$$\mathrm{Tr}_B (\xi_{AB}^\dagger) = \sum_x (\langle e_x |_A \otimes I_B) \xi_{AB}^\dagger (|e_x\rangle_A \otimes I_B) = \mathrm{Tr}_B (\xi_{AB})^\dagger. \quad (2.33)$$

This is also called the *partial trace* and will be discussed further in the context of completely bounded maps in Sect. 2.6.2.

The above discussion allows us to define the *marginal* on  $A$  of the trace-class operator  $\xi_{AB} \in \mathcal{T}(A)$  as follows:

$$\xi_A := \mathrm{Tr}_B (\xi_{AB}) \quad \text{such that} \quad F_{\xi_{AB}}(L_A) = F_{\xi_A}(L_A) = \langle \xi_A, L_A \rangle. \quad (2.34)$$

We usually do not introduce marginals explicitly. For example, if we introduce a trace-class operator  $\xi_{AB}$  then its marginals  $\xi_A$  and  $\xi_B$  are implicitly defined as well.

## 2.4.2 Separable States and Entanglement

The occurrence of entangled states on two or more quantum systems is one of the most intriguing features of the formalism of quantum mechanics.

We call a positive operator  $M_{AB} \in \mathcal{P}(AB)$  of a joint quantum system  $AB$  **separable** if it can be written in the form

$$M_{AB} = \sum_{k \in \mathcal{K}} L_A(k) \otimes K_B(k), \quad \text{where} \quad L_A(k) \in \mathcal{P}(A), \quad K_B(k) \in \mathcal{P}(B), \quad (2.35)$$

for some index set  $\mathcal{K}$ . Otherwise, it is called **entangled**.

The prime example of an entangled state is the *maximally entangled* state. For two quantum systems  $A$  and  $B$  of finite dimension, a maximally entangled state is a state of the form

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_x |e_x\rangle_A \otimes |f_x\rangle_B, \quad d = \min\{d_A, d_B\} \quad (2.36)$$

where  $\{e_x\}_x$  is an ONB of  $A$  and  $\{f_x\}_x$  is an ONB of  $B$ .

This state cannot be written in the form (2.35) as the following argument, due to Peres [131] and Horodecki [89], shows. Consider the operation  $(\cdot)^{T_B}$  of taking a

*partial transpose* on the system  $B$  with regards to  $\{f_x\}_x$  on  $B$ . Applied to separable states of the form (2.35), this always results in a state, i.e.

$$\rho_{AB}^{T_B} = \sum_k \sigma_A(k) \otimes (\tau_B(k))^{T_B} \geq 0. \quad (2.37)$$

Is positive semi-definite. Applied to  $\psi_{AB}$ , however, we get

$$\psi_{AB}^{T_B} = \frac{1}{d} \sum_{x,x'} |e_x\rangle\langle e_{x'}| \otimes (|f_x\rangle\langle f_{x'}|)^{T_B} = \frac{1}{d} \sum_{x,x'} |e_x\rangle\langle e_{x'}| \otimes |f_{x'}\rangle\langle f_x|. \quad (2.38)$$

This operator is not positive semi-definite. For example, we have

$$\langle \phi | \psi_{AB}^{T_B} | \phi \rangle = -\frac{2}{d}, \quad \text{where } |\phi\rangle = |e_1\rangle \otimes |e_2\rangle - |e_2\rangle \otimes |e_1\rangle. \quad (2.39)$$

Generally, we have seen that a bipartite state is separable only if it remains positive semi-definite under the partial transpose. The converse is not true in general.

### 2.4.3 Purification

Consider any state  $\rho_{AB} \in \mathcal{S}(AB)$ , and its marginals  $\rho_A$  and  $\rho_B$ . Then we say that  $\rho_{AB}$  is an *extension* of  $\rho_A$  and  $\rho_B$ . Moreover, if  $\rho_{AB}$  is pure, we call it a *purification* of  $\rho_A$  and  $\rho_B$ . Moreover, we can always construct a purification of a given state  $\rho_A \in \mathcal{S}(A)$ . Let us say that  $\rho_A$  has eigenvalue decomposition

$$\rho_A = \sum_x \lambda_x |e_x\rangle\langle e_x|_A, \quad \text{then the state } |\rho\rangle_{AA'} = \sum_x \sqrt{\lambda_x} |e_x\rangle_A \otimes |e_x\rangle_{A'} \quad (2.40)$$

is a *purification* of  $\rho_A$ . Here,  $A'$  is an auxiliary system of the same dimension as  $A$  and  $\{|e_x\rangle_{A'}\}_x$  is any ONB of  $A'$ . Clearly,  $\text{Tr}_{A'}(\rho_{AA'}) = \rho_A$ .

### 2.4.4 Classical-Quantum Systems

An important special case are joint systems where one part consists of a classical system. Events  $M \in \mathcal{P}_\bullet(XA)$  on such joint systems can be decomposed as

$$M_{XA} = \sum_x |x\rangle\langle x|_X \otimes M_A(x) = \bigoplus_x M_A(x), \quad \text{where } M_A(x) \in \mathcal{P}_\bullet(A). \quad (2.41)$$

Moreover, we call states of such systems *classical-quantum* states. For example, consistent with our notation for classical systems in (2.25), a state  $\rho_{XA} \in \mathcal{S}_\bullet(XA)$  can be decomposed as

$$\rho_{XA} = \sum_x |x\rangle\langle x|_X \otimes \rho_A(x), \quad \text{where } \rho_A(x) \geq 0, \quad \sum_x \text{Tr}(\rho_A(x)) \leq 1. \quad (2.42)$$

Clearly,  $\rho_A(x) \in \mathcal{S}_\bullet(A)$  is a sub-normalized density operator on  $A$ . Furthermore, comparing with (2.35), it is evident that such states are always separable.

If  $\rho_{XA} \in \mathcal{S}_\circ(XA)$ , it is sometimes more convenient to instead further decompose

$$\rho_A(x) = \rho(x) \hat{\rho}_A(x), \quad (2.43)$$

where  $\rho(x)$  is a probability mass function and  $\hat{\rho}_A(x) \in \mathcal{S}_\circ(A)$  normalized as well.

## 2.5 Functions on Positive Operators

Besides the inverse, we often need to lift other continuous real-valued functions to positive semi-definite operators. For any continuous function  $f : \mathbb{R}_+ \setminus \{0\} \rightarrow \mathbb{R}$  and  $M \in \mathcal{P}(A)$ , we use the convention

$$f(M) = \sum_{x:\lambda_x \neq 0} f(\lambda_x) |e_x\rangle\langle e_x|. \quad (2.44)$$

If the resulting operator is bounded (e.g. if the spectrum of  $M$  is compact). That is, as for the generalized inverse, we simply ignore the kernel of  $M$ .<sup>7</sup> By definition, we thus have  $f(UMU^\dagger) = Uf(M)U^\dagger$  for any unitary  $U$ . Moreover, we have

$$Lf(L^\dagger L) = f(LL^\dagger)L, \quad (2.45)$$

which can be verified using the *polar decomposition*, stating that we can always write  $L = U|L|$  for some unitary operator  $U$ . An important example is the *logarithm*, defined as  $\log M = \sum_{x:\lambda_x \neq 0} \log \lambda_x |e_x\rangle\langle e_x|$ .

Let us in the following restrict our attention to the finite-dimensional case. Notably, trace functionals of the form  $M \mapsto \text{Tr}(f(M))$  inherit continuity, monotonicity, concavity and convexity from  $f$  (see, e.g., [34]). For example, for any monotonically increasing continuous function  $f$ , we have

$$\text{Tr}(f(M)) \leq \text{Tr}(f(N)) \quad \text{for all } M, N \in \mathcal{P}(A) \text{ with } M \leq N. \quad (2.46)$$

<sup>7</sup>This convention is very useful to keep the presentation in the following chapters concise, but some care is required. If  $\lim_{\varepsilon \rightarrow 0} f(\varepsilon) \neq 0$ , then  $M \mapsto f(M)$  is not necessarily continuous even if  $f$  is continuous on its support.

**Table 2.2** Examples of operator monotone, concave and convex functions

Function	Range	Op. monotone	Op. anti-monotone	Op. convex	Op. concave
$\sqrt{t}$	$[0, \infty)$	Yes	No	No	Yes
$t^2$	$[0, \infty)$	No	No	Yes	No
$\frac{1}{t}$	$(0, \infty)$	No	Yes	Yes	No
$t^\alpha$		$\alpha \in [0, 1]$	$\alpha \in [-1, 0)$	$\alpha \in [-1, 0) \cup [1, 2]$	$\alpha \in (0, 1]$
$\log t$	$(0, \infty)$	Yes	No	No	Yes
$t \log t$	$[0, \infty)$	No	No	Yes	No

Note in particular that  $t^\alpha$  is neither operator monotone, convex nor concave for  $\alpha < -1$  and  $\alpha > 2$

### Operator Monotone and Concave Functions

Here we discuss classes of functions that, when lifted to positive semi-definite operators, retain their defining properties. A function  $f : \mathbb{R}_+ \rightarrow \mathbb{R}$  is called *operator monotone* if

$$M \leq N \implies f(M) \leq f(N) \quad \text{for all } M, N \geq 0. \quad (2.47)$$

If  $f$  is operator monotone then  $-f$  is *operator anti-monotone*. Furthermore,  $f$  is called *operator convex* if

$$\lambda f(M) + (1 - \lambda)f(N) \geq f(\lambda M + (1 - \lambda)N) \quad \text{for all } M, N \geq 0 \quad (2.48)$$

and  $\lambda \in [0, 1]$ . If this holds with the inequality reversed, then the function is called *operator concave*. These definitions naturally extend to functions  $f : (0, \infty) \rightarrow \mathbb{R}$ , where we consequently choose  $M, N > 0$ .

There exists a rich theory concerning such functions and their properties (see, for example, Bhatia's book [26]), but we will only mention a few prominent examples in Table 2.2 that will be of use later.

We say that a two-parameter function is *jointly concave* (*jointly convex*) if it is concave (convex) when we take convex combinations of input tuples. Lieb [106] and Ando [4] established the following extremely powerful result. The map

$$\mathcal{P}(A) \times \mathcal{P}(B) \rightarrow \mathcal{P}(AB), \quad (M_A, N_B) \mapsto f(M_A \otimes N_B^{-1})M_A \otimes I_B \quad (2.49)$$

is jointly convex on strictly positive operators if  $f : (0, \infty) \rightarrow \mathbb{R}$  is operator monotone. This is *Ando's convexity theorem* [4]. In particular, we find that the functional

$$(M_A, N_B) \mapsto \langle \Psi | K \cdot (M_A \otimes N_B^{-T})^{\alpha-1} M_A \cdot K^\dagger | \Psi \rangle_{BB'} = \text{Tr}_A(M_A^\alpha K^\dagger N_B^{1-\alpha} K) \quad (2.50)$$

for any  $K \in \mathcal{L}(A, B)$  is jointly concave for  $\alpha \in (0, 1)$  and jointly convex for  $\alpha \in (1, 2)$ . The former is known as Lieb's concavity theorem. Since this will be used extensively, we include a derivation of this particular result in Appendix.

## 2.6 Quantum Channels

Quantum channels are used to model the time evolution of physical systems. There are two equivalent ways to model a quantum channel, and we will see that they are intimately related. In the Schrödinger picture, the events are fixed and the state of a system is time dependent. Consequently, we model evolutions as quantum channels acting on the space of density operators. In the Heisenberg picture, the observable events are time dependent and the state of a system is fixed, and we thus model evolutions as adjoint quantum channels acting on events.

### 2.6.1 Completely Bounded Maps

Here, we introduce linear maps between bounded linear operators on different systems, and their adjoints, which map between functionals on different systems. For later convenience, we use calligraphic letters to denote the latter maps, for example  $\mathcal{E}$  and  $\mathcal{F}$  and use the adjoint notation for maps between bounded linear operators. The action of a linear map on an operator in a tensor space is well-defined by linearity via the decomposition in (2.29), and as for linear operators, we usually omit to make this embedding explicit.

The set of *completely bounded* (CB) linear maps from  $\mathcal{L}(A)$  to  $\mathcal{L}(B)$  is denoted by  $\text{CB}(A, B)$ . Completely bounded maps  $\mathcal{E}^\dagger \in \text{CB}(A, B)$  have the defining property that for any operator  $L_{AC} \in \mathcal{L}(AC)$  and any auxiliary system  $C$ , we have  $\|\mathcal{E}^\dagger(L_{AC})\| < \infty$ .<sup>8</sup> We then define the linear map  $\mathcal{E}$  from  $\mathcal{T}(A)$  to  $\mathcal{T}(B)$  as the *adjoint map* for some  $\mathcal{E}^\dagger \in \text{CB}(B, A)$  via the sesquilinear form. Namely,  $\mathcal{E}$  is defined as the unique linear map satisfying

$$\langle \mathcal{E}(\xi), L \rangle = \langle \xi, \mathcal{E}^\dagger(L) \rangle \quad \text{for all } \xi \in \mathcal{T}(A), L \in \mathcal{L}(B). \quad (2.51)$$

Clearly,  $\mathcal{E}$  maps  $\mathcal{T}(A)$  into  $\mathcal{T}(B)$ . Moreover, for any  $\xi_{AC}$  in  $\mathcal{T}(AC)$ , we have

$$\|\mathcal{E}(\xi_{AC})\|_* = \sup \left\{ \left| \langle \xi_{AC}, \mathcal{E}^\dagger(L_{BC}) \rangle \right| : L_{BC} \in \mathcal{L}_\bullet(BC) \right\} < \infty. \quad (2.52)$$

So these maps are in fact completely bounded in the trace norm and we collect them in the set  $\text{CB}_*(A, B)$ . Again, in finite dimensions  $\text{CB}(A, B)$  and  $\text{CB}_*(A, B)$  coincide.

---

<sup>8</sup>It is noteworthy that the weaker condition that the map be bounded, i.e.  $\|\mathcal{E}^\dagger(L_A)\| < \infty$ , is not sufficient here and in particular does not imply that the map is completely bounded. In contrast, bounded linear operators in  $\mathcal{L}(A)$  are in fact also completely bounded in the above sense.

### 2.6.2 Quantum Channels

Physical channels necessarily map positive functionals onto positive functionals. A map  $\mathcal{E} \in \text{CB}_*(A, B)$  is called *completely positive* (CP) if it maps  $\mathcal{S}(AC)$  to  $\mathcal{S}(BC)$  for any auxiliary system  $C$ , namely if

$$\langle \mathcal{E}(\omega_{AC}), M_{BC} \rangle \geq 0 \quad \text{for all } \omega \in \mathcal{S}(AC), M \in \mathcal{P}(BC). \quad (2.53)$$

A map  $\mathcal{E}$  is CP if and only if  $\mathcal{E}^\dagger$  is CP, in the respective sense. The set of all CP maps from  $\mathcal{T}(A)$  to  $\mathcal{T}(B)$  is denoted  $\text{CP}(A, B)$ .

Physical channels in the Schrödinger picture are modeled by completely positive trace-preserving maps, or quantum channels.

A **quantum channel** is a map  $\mathcal{E} \in \text{CP}(A, B)$  that is **trace-preserving**, namely a map that satisfies

$$\text{Tr}(\mathcal{E}(\xi)) = \text{Tr}(\xi) \quad \text{for all } \xi \in \mathcal{T}(A). \quad (2.54)$$

Naturally, such maps take states to states, more precisely, they map  $\mathcal{S}_\circ(A)$  to  $\mathcal{S}_\circ(B)$  and  $\mathcal{S}_\bullet(A)$  to  $\mathcal{S}_\bullet(B)$ . The corresponding adjoint quantum channel  $\mathcal{E}^\dagger$  from  $\mathcal{L}(B)$  to  $\mathcal{L}(A)$  in the Heisenberg picture is a completely positive and *unital* map, namely it satisfies  $\mathcal{E}^\dagger(I_B) = I_A$ . In fact, a map  $\mathcal{E}$  is trace-preserving if and only if  $\mathcal{E}^\dagger$  is unital. Unital maps take  $\mathcal{P}_\bullet(B)$  to  $\mathcal{P}_\bullet(A)$  and thus map events to events. Clearly,

$$\Pr_{\mathcal{E}(\rho)}(M) = \langle \mathcal{E}(\rho), M \rangle = \left\langle \rho, \mathcal{E}^\dagger(M) \right\rangle = \Pr_\rho(\mathcal{E}^\dagger(M)). \quad (2.55)$$

Let us summarize some further notation:

- We denote the set of all completely positive trace-preserving (CPTP) maps from  $\mathcal{T}(A)$  to  $\mathcal{T}(B)$  by  $\text{CPTP}(A, B)$ .
- The set of all CP unital maps from  $\mathcal{L}(A)$  to  $\mathcal{L}(B)$  is denoted  $\text{CPU}(A, B)$ .
- Finally, a map  $\mathcal{E} \in \text{CP}(A, B)$  is called *trace-non-increasing* if  $\text{Tr}(\mathcal{E}(\omega)) \leq \text{Tr}(\omega)$  for all  $\omega \in \mathcal{S}(A)$ . A CP map is trace-non-increasing if and only if its adjoint is *sub-unital*, i.e. it satisfies  $\mathcal{E}^\dagger(I_B) \leq I_A$ .

#### Some Examples of Channels

The simplest example of such a CP map is the *conjugation* with an operator  $L \in \mathcal{L}(A, B)$ , that is the map  $\mathcal{L} : \xi \mapsto L\xi L^\dagger$ . We will often use the following basic property of completely positive maps. Let  $\mathcal{E} \in \text{CP}(A, B)$ , then

$$\xi \geq \zeta \implies \mathcal{E}(\xi) \geq \mathcal{E}(\zeta) \quad \text{for all } \xi, \zeta \in \mathcal{T}(A). \quad (2.56)$$

As a consequence, we take note of the following property of positive semi-definite operators. For any  $M \in \mathcal{P}(A)$ ,  $\xi \in \mathcal{S}(A)$ , we have

$$\mathrm{Tr}(\xi M) = \mathrm{Tr}(\sqrt{M}\xi\sqrt{M}) \geq 0, \quad (2.57)$$

where the last inequality follows from the fact that the conjugation with  $\sqrt{M}$  is a completely positive map. In particular, if  $L, K \in \mathcal{L}(A)$  satisfy  $L \geq K$ , we find  $\mathrm{Tr}(\xi L) \geq \mathrm{Tr}(\xi K)$ .

An instructive example is the embedding map  $L_A \mapsto L_A \otimes I_B$ , which is completely bounded, CP and unital. Its adjoint map is the CPTP map  $\mathrm{Tr}_B$ , the partial trace, as we have seen in Sect. 2.4.1. Finally, for a POVM  $x \mapsto M_A(x)$ , we consider the measurement map  $\mathcal{M} \in \mathrm{CPTP}(A, X)$  given by

$$\mathcal{M} : \rho_A \mapsto \sum_x |x\rangle\langle x| \mathrm{Tr}(\rho_A M_A(x)). \quad (2.58)$$

This maps a quantum system into a classical system with a state corresponding to the probability mass function  $\rho(x) = \mathrm{Tr}(\rho_A M_A(x))$  that arises from Born's rule. If the events  $\{M_A(x)\}_x$  are rank-one projectors, then this map is also unital.

### 2.6.3 Pinching and Dephasing Channels

Pinching maps (or channels) constitute a particularly important class of quantum channels that we will use extensively in our technical derivations. A *pinching map* is a channel of the form  $\mathcal{P} : L \mapsto \sum_x P_x L P_x$  where  $\{P_x\}_x$ ,  $x \in [m]$  are orthogonal projectors that sum up to the identity. Such maps are CPTP, unital and equal to their own adjoints. Alternatively, we can see them as *dephasing* operations that remove off-diagonal blocks of a matrix. They have two equivalent representations:

$$\mathcal{P}(L) = \sum_{x \in [m]} P_x L P_x = \frac{1}{m} \sum_{y \in [m]} U_y L U_y^\dagger, \quad \text{where } U_y = \sum_{x \in [m]} e^{\frac{2\pi i y x}{m}} P_x \quad (2.59)$$

are unitary operators. Note also that  $U_m = I$ .

For any self-adjoint operator  $H \in \mathcal{L}^\dagger(A)$  with eigenvalue decomposition  $H = \sum_x \lambda_x |e_x\rangle\langle e_x|$ , we define the set  $\mathrm{spec}(H) = \{\lambda_x\}_x$  and its cardinality,  $|\mathrm{spec}(H)|$ , is the number of distinct eigenvalues of  $H$ . For each  $\lambda \in \mathrm{spec}(H)$ , we also define  $P_\lambda = \sum_{x:\lambda_x=\lambda} |e_x\rangle\langle e_x|$  such that  $H = \sum_\lambda \lambda P_\lambda$  is its *spectral decomposition*. Then, the *pinching map* for this spectral decomposition is denoted

$$\mathcal{P}_H : L \mapsto \sum_{\lambda \in \mathrm{spec}(H)} P_\lambda L P_\lambda. \quad (2.60)$$



Clearly,  $\mathcal{P}_H(H) = H$ ,  $\mathcal{P}_H(L)$  commutes with  $H$ , and  $\text{Tr}(\mathcal{P}_H(L)H) = \text{Tr}(LH)$ .

For any  $M \in \mathcal{P}(A)$ , using the second expression in (2.59) and the fact that  $U_x M U_x^\dagger \geq 0$ , we immediately arrive at

$$\mathcal{P}_H(M) = \frac{1}{|\text{spec}(H)|} \sum_{y \in [m]} U_y M U_y^\dagger \geq \frac{1}{|\text{spec}(H)|} M. \quad (2.61)$$

This is Hayashi's *pinching inequality* [74].

Finally, if  $f$  is operator concave, then for every pinching  $\mathcal{P}$ , we have

$$f(\mathcal{P}(M)) = f\left(\frac{1}{m} \sum_{x \in [m]} U_x M U_x^\dagger\right) \geq \frac{1}{m} \sum_{x \in [m]} f(U_x M U_x^\dagger) \quad (2.62)$$

$$= \frac{1}{m} \sum_{x \in [m]} U_x f(M) U_x^\dagger = \mathcal{P}(f(M)). \quad (2.63)$$

This is a special case of the *operator Jensen inequality* established by Hansen and Pedersen [71]. For all  $H \in \mathcal{L}^\dagger(A)$ , every operator concave function  $f$  defined on the spectrum of  $H$ , and all unital maps  $\mathcal{E} \in \text{CPU}(A, B)$ , we have

$$f(\mathcal{E}(H)) \geq \mathcal{E}(f(H)). \quad (2.64)$$

## 2.6.4 Channel Representations

The following representations for trace non-increasing and trace preserving CP maps are of crucial importance in quantum information theory.

### Kraus Operators

Every CP map can be represented as a sum of conjugations of the input [82, 83]. More precisely,  $\mathcal{E} \in \text{CP}(A, B)$  if and only if there exists a set of linear operators  $\{E_k\}_k$ ,  $E_k \in \mathcal{L}(A, B)$  such that

$$\mathcal{E}(\xi) = \sum_k E_k \xi E_k^\dagger \quad \text{for all } \xi \in \mathcal{T}(A). \quad (2.65)$$

Furthermore, such a channel is trace-preserving if and only if  $\sum_k E_k^\dagger E_k = I$ , and trace-non-increasing if and only if  $\sum_k E_k^\dagger E_k \leq I$ . The operators  $\{E_k\}$  are called *Kraus operators*. Moreover, the adjoint  $\mathcal{E}^\dagger$  of  $\mathcal{E}$  is completely positive and has Kraus operators  $\{E_k^\dagger\}$  since

$$\text{Tr}(\xi \mathcal{E}^\dagger(L)) = \text{Tr}(\mathcal{E}(\xi)L) = \text{Tr}\left(\xi \sum_k E_k^\dagger L E_k\right). \quad (2.66)$$

### Stinespring Dilation

Moreover, every CP map can be decomposed into its *Stinespring dilation* [147]. That is,  $\mathcal{E} \in \text{CP}(A, B)$  if and only if there exists a system  $C$  and an operator  $L \in \mathcal{L}(A, BC)$  such that

$$\mathcal{E}(\xi) = \text{Tr}_C(L\xi L^\dagger) \quad \text{for all } \xi \in \mathcal{T}(A). \quad (2.67)$$

Moreover, if  $\mathcal{E}$  is trace-preserving then  $L = U$ , where  $U \in \mathcal{L}_\bullet(A, BC)$  is an isometry. If  $\mathcal{E}$  is trace-non-increasing, then  $L = PU$  is an isometry followed by a projection  $P \in \mathcal{P}_\bullet(C)$ .

### Choi-Jamiolkowski Isomorphism

For finite-dimensional Hilbert spaces, the *Choi-Jamiolkowski isomorphism* [96] between bounded linear maps from  $A$  to  $B$  and linear functionals on  $A'B$  is given by

$$\Gamma : \mathcal{T}(\mathcal{T}(A), \mathcal{T}(B)) \rightarrow \mathcal{T}(A'B), \quad \mathcal{E} \mapsto \gamma_{A'B}^\mathcal{E} = \mathcal{E}(|\Psi\rangle\langle\Psi|_{A'A}), \quad (2.68)$$

where the state  $\gamma_{A'B}^\mathcal{E}$  is called the Choi-Jamiolkowski state of  $\mathcal{E}$ . The inverse operation,  $\Gamma^{-1}$ , maps linear functionals to bounded linear maps

$$\Gamma^{-1} : \gamma_{A'B} \mapsto \left\{ \mathcal{E}^\gamma : \rho_A \mapsto \text{Tr}_{A'}(\gamma_{A'B}(I_B \otimes \rho_{A'}^T)) \right\}, \quad (2.69)$$

where the transpose is taken with regards to the Schmidt basis of  $\Psi$ .

There are various relations between properties of bounded linear maps and properties of the corresponding Choi-Jamiolkowski functionals, for example:

$$\mathcal{E} \text{ is completely positive} \Leftrightarrow \gamma_{A'B}^\mathcal{E} \geq 0 \quad (2.70)$$

$$\mathcal{E} \text{ is trace-preserving} \Leftrightarrow \text{Tr}_B(\gamma_{A'B}^\mathcal{E}) = I_{A'} \quad (2.71)$$

$$\mathcal{E} \text{ is unital} \Leftrightarrow \text{Tr}_{A'}(\gamma_{A'B}^\mathcal{E}) = I_B. \quad (2.72)$$

## 2.7 Background and Further Reading

Nielsen and Chuang's book [125] offers a good introduction to the quantum formalism. Hayashi's [75] and Wilde's [174] books both also carefully treat the concepts relevant for quantum information theory in finite dimensions. Finally, Holevo's recent book [88] offers a comprehensive mathematical introduction to quantum information processing in finite and infinite dimensions.

Operator monotone functions and other aspects of matrix analysis are covered in Bhatia's books [26, 27], and Hiai and Petz' book [87].

# Chapter 3

## Norms and Metrics

**Abstract** In this chapter we equip the space of quantum states with some additional structure by discussing various norms and metrics for quantum states. We discuss Schatten norms and an important variational characterization of these norms, amongst other properties. We go on to discuss the trace norm on positive semi-definite operators and the trace distance associated with it. Uhlmann's fidelity for quantum states is treated next, as well as the purified distance, a useful metric based on the fidelity.

Particular emphasis is given to sub-normalized quantum states, and the above quantities are generalized to meaningfully include them. This will be essential for the definition of the smooth entropies in Chap. 6.

### 3.1 Norms for Operators and Quantum States

We restrict ourselves to finite-dimensional Hilbert spaces hereafter. We start by giving a formal definition for unitarily invariant norms on linear operators. An example of such a norm is the operator norm  $\|\cdot\|$  of the previous chapter.

**Definition 3.1** A **norm** for linear operators is a map  $\|\cdot\| : \mathcal{L}(A) \rightarrow [0, \infty)$  which satisfies the following properties, for any  $L, K \in \mathcal{L}(A)$ .

Positive-definiteness:  $\|L\| \geq 0$  with equality if and only if  $L = 0$ .

Absolute scalability:  $\|aL\| = |a| \cdot \|L\|$  for all  $a \in \mathbb{C}$ .

Subadditivity:  $\|L + K\| \leq \|L\| + \|K\|$ .

A norm  $\|\cdot\|$  is called a **unitarily invariant norm** if it further satisfies

Unitary invariance:  $\|UV^\dagger L\| = \|L\|$  for any isometries  $U, V \in \mathcal{L}(A, B)$ .

We reserve the notation  $\|\cdot\|$  for unitarily invariant norms. Combining subadditivity and scalability, we note that norms are convex:

$$\|\lambda L + (1 - \lambda)K\| \leq \lambda \|L\| + (1 - \lambda) \|K\| \quad \text{for all } \lambda \in [0, 1]. \quad (3.1)$$

### 3.1.1 Schatten Norms

The *singular values* of a general linear operator  $L \in \mathcal{L}(A)$  are the eigenvalues of its *modulus*, the positive semi-definite operator  $|L| := \sqrt{L^\dagger L}$ . The Schatten  $p$ -norm of  $L$  is then simply defined as the  $p$ -norm of its singular values.

**Definition 3.2** For any  $L \in \mathcal{L}(A)$ , we define the **Schatten  $p$ -norm** of  $L$  as

$$\|L\|_p := \left( \text{Tr} (|L|^p) \right)^{\frac{1}{p}} \quad \text{for } p \geq 1. \quad (3.2)$$

We extend this definition to all  $p > 0$ , but note that in this case  $\|L\|_p$  is not a norm. In particular,  $|L|_p$  for  $p \in [0, 1)$  does not satisfy the subadditivity inequality in Definition 3.1. The operator norm is recovered in the limit  $p \rightarrow \infty$ . We have

$$\|L\|_\infty = \|L\|, \quad \|L\|_2 = \sqrt{\text{Tr}(L^\dagger L)}, \quad \|L\|_1 = \text{Tr} |L| = \|L\|_*. \quad (3.3)$$

The latter two norms are the *Frobenius* or *Hilbert-Schmidt* norm and the *trace norm*.

The Schatten norms are unitarily invariant and subadditive. Using this and the representation of pinching channels in (2.59), we find

$$\|\mathcal{P}(L)\| = \left\| \sum_{x \in [m]} \frac{1}{m} U_x L U_x^\dagger \right\| \leq \sum_{x \in [m]} \frac{1}{m} \|U_x L U_x^\dagger\| = \|L\|. \quad (3.4)$$

This is called the *pinching inequality* for (unitarily invariant) norms.

### Hölder Inequalities and Variational Characterization of Norms

Next we introduce the following powerful generalization of the *Hölder and reverse Hölder inequalities* to the trace of linear operators:

**Lemma 3.1** *Let  $L, K \in \mathcal{L}(A)$ ,  $M, N \in \mathcal{P}(A)$  and  $p, q \in \mathbb{R}$  such that  $p > 0$  and  $\frac{1}{p} + \frac{1}{q} = 1$ . Then, we have*

$$|\operatorname{Tr}(LK)| \leq \operatorname{Tr} |LK| \leq \|L\|_p \cdot \|K\|_q \quad \text{if } p > 1 \quad (3.5)$$

$$\operatorname{Tr}(MN) \geq \|M\|_p \cdot \|N^{-1}\|_{-q}^{-1} \quad \text{if } p \in (0, 1) \text{ and } M \ll N. \quad (3.6)$$

*Moreover, for every  $L$  there exists a  $K$  such that equality is achieved in (3.5). In particular, for  $M, N \in \mathcal{P}(A)$ , equality is achieved in all inequalities if  $M^p = aN^q$  for some constant  $a \geq 0$ .*

*Proof* We omit the proof of the first statement (see, e.g., Bhatia [26, Corollary IV.2.6]).

For  $p \in (0, 1)$ , let us first consider the case where  $M$  and  $N$  commute. Then, (3.5) yields

$$\|M\|_p^p = \operatorname{Tr}(M^p) = \operatorname{Tr}(M^p N^p N^{-p}) \leq \|M^p N^p\|_{\frac{1}{p}} \cdot \|N^{-p}\|_{\frac{1}{1-p}} \quad (3.7)$$

$$= (\operatorname{Tr}(MN))^p \cdot \left( \operatorname{Tr} \left( |N|^{-\frac{p}{1-p}} \right) \right)^{1-p}, \quad (3.8)$$

which establishes the desired statement. To generalize (3.6) to non-commuting operators, note that the commutative inequality yields

$$\operatorname{Tr}(MN) = \operatorname{Tr}(\mathcal{P}_N(M)N) \geq \|\mathcal{P}_N(M)\|_p \cdot \| |N|^{-1} \|_{-q}^{-1}. \quad (3.9)$$

Moreover, since  $t \mapsto t^p$  is operator concave, the operator Jensen inequality (2.64) establishes that

$$\|\mathcal{P}_N(M)\|_p^p = \operatorname{Tr}((\mathcal{P}_N(M))^p) \geq \operatorname{Tr}(\mathcal{P}_N(M^p)) = \operatorname{Tr}(M^p). \quad (3.10)$$

Substituting this into (3.9) yields the desired statement for general  $M$  and  $N$ .  $\square$

These Hölder inequalities are extremely useful, for example they allow us to derive various variational characterizations of Schatten norms and trace terms. For  $p > 1$ , the Hölder inequality implies norm duality, namely [26, Sect. IV.2]

$$\|L\|_p = \max_{\substack{K \in \mathcal{L}(A) \\ \|K\|_q \leq 1}} \left| \operatorname{Tr}(L^\dagger K) \right| \quad \text{for } \frac{1}{p} + \frac{1}{q} = 1, \quad p, q > 1. \quad (3.11)$$

This is a quite useful variational characterization of the Schatten norm, which we extend to  $p \in (0, 1)$  using the reverse Hölder inequality. Here we state the resulting variational formula for positive operators.

**Lemma 3.2** *Let  $M \in \mathcal{P}(A)$  and  $p > 0$ . Then, for  $r = 1 - \frac{1}{p}$ , we find*

$$\|M\|_p = \max \left\{ \text{Tr}(MN^r) : N \in \mathcal{S}_o(A) \right\} \quad \text{if } p \geq 1 \quad (3.12)$$

$$\|M\|_p = \min \left\{ \text{Tr}(MN^r) : N \in \mathcal{S}_o(A) \wedge M \ll N \right\} \quad \text{if } p \in (0, 1]. \quad (3.13)$$

Furthermore, as a consequence of the Hölder inequality for  $p > 1$  we find

$$\log \text{Tr}(MN) \leq \frac{1}{p} \log \text{Tr}(M^p) + \frac{1}{q} \log \text{Tr}(N^q) \quad (3.14)$$

$$\leq \log \left( \frac{1}{p} \text{Tr}(M^p) + \frac{1}{q} \text{Tr}(N^q) \right), \quad (3.15)$$

where the last inequality follows by the concavity of the logarithm. Hence, we have

$$\text{Tr}(MN) \leq \frac{1}{p} \text{Tr}(M^p) + \frac{1}{q} \text{Tr}(N^q) \quad \text{with equality iff } M^p = N^q, \quad (3.16)$$

which is a matrix trace version of Young's inequality. Similarly, the reverse Hölder inequality for  $p \in (0, 1)$  and  $M \ll N$  yields again (3.16) with the inequality reversed.

### 3.1.2 Dual Norm for States

We have already encountered the norm  $\|\cdot\|_*$ , which is the dual norm of the operator norm on linear operators. Given the operational relation between density operators (positive functionals) and events (positive semi-definite operators), it is natural to consider the following dual norm on positive functionals:

**Definition 3.3** We define the **positive cone dual norm** as

$$\|\cdot\|_+ : \mathcal{T}(A) \rightarrow \mathbb{R}_+, \quad \omega \mapsto \max_{M \in \mathcal{P}_\bullet(A)} |\text{Tr}(\omega M)|. \quad (3.17)$$

Here we emphasize that the maximization in the definition of the dual norm is only over events in  $\mathcal{P}_\bullet(A)$ . In fact, optimizing over operators in  $\mathcal{L}_\bullet(A)$  in the above expression yields the Schatten-1 norm as we have seen in (3.11). Thus, we clearly have  $\|\xi\|_+ \leq \|\xi\|_1$ .

Let us verify that this is indeed a norm according to Definition 3.1. (However, it is not unitarily invariant.)

*Proof* From the definition it is evident that  $\|\alpha\xi\|_+ = |\alpha| \cdot \|\xi\|$  for every scalar  $\alpha \in \mathbb{C}$ . Furthermore, the triangle inequality is a consequence of the fact that

$$\begin{aligned} \|\xi + \zeta\|_+ &= \max_{M \in \mathcal{P}_\bullet(A)} |\text{Tr}((\xi + \zeta)M)| \leq \max_{M \in \mathcal{P}_\bullet(A)} |\text{Tr}(\xi M)| + \max_{M \in \mathcal{P}_\bullet(A)} |\text{Tr}(\zeta M)| \\ &= \|\xi\|_+ + \|\zeta\|_+ \end{aligned} \quad (3.18)$$

for every  $\xi, \zeta \in \mathcal{L}$ . It remains to show that  $\|\xi\|_+ \geq 0$  with equality if and only if  $\xi = 0$ . This follows from the following lower bound on the dual norm:

$$\|\xi\|_+ \geq \max_{|v\rangle: \langle v|v\rangle=1} |\langle v|\xi|v\rangle| = w(\xi) \geq 0 \quad \text{with equality only if } \xi = 0. \quad (3.19)$$

To arrive at (3.19), we chose  $M = |v\rangle\langle v|$  and let  $w(\cdot)$  denote the numerical radius (see, e.g., Bhatia [26, Sect. I.1]). The equality condition is thus inherited from the numerical radius.  $\square$

For functionals represented by self-adjoint operators  $\xi \in \mathcal{T}(A)$ , we can explicitly find the operator that achieves the maximum in (3.17) using the spectral decomposition of  $\xi$ . Specifically, we find that the expression is always maximized by the projector  $\{\xi \geq 0\}$  or its complement  $\{\xi < 0\}$ , namely we want to either sum up all positive or all negative eigenvalues to maximize the absolute value. The dual norm thus evaluates to

$$\|\xi\|_+ = \max \left\{ \text{Tr}(\{\xi \geq 0\}\xi), -\text{Tr}(\{\xi < 0\}\xi) \right\}. \quad (3.20)$$

This can be further simplified using  $\max\{a, b\} = \frac{1}{2}(a + b + |a - b|)$ , which yields

$$\|\xi\|_+ = \frac{1}{2} \text{Tr}(\{(\xi \geq 0) - (\xi < 0)\}\xi) + \frac{1}{2} \left| \text{Tr}(\{(\xi \geq 0) + (\xi < 0)\}\xi) \right| \quad (3.21)$$

$$= \frac{1}{2} \text{Tr}|\xi| + \frac{1}{2} |\text{Tr}(\xi)| = \frac{1}{2} \|\xi\|_1 + \frac{1}{2} |\text{Tr}(\xi)|. \quad (3.22)$$

Finally, for positive functionals this further simplifies to  $\|\omega\|_+ = \|\omega\|_1 = \text{Tr}(\omega)$ .

## 3.2 Trace Distance

We start by introducing a straightforward generalization of the trace distance to general (not necessarily normalized) states. The definition also makes sense for general trace-class operators, so we will state the results in their most general form.

**Definition 3.4** For  $\xi, \zeta \in \mathcal{T}(A)$ , we define the **generalized trace distance** between  $\xi$  and  $\zeta$  as  $\Delta(\xi, \zeta) := \|\xi - \zeta\|_+$ .

This distance is also often called *total variation distance* in the classical literature. It is a *metric* on  $\mathcal{T}(A)$ , an immediate consequence of the fact that  $\|\cdot\|_+$  is a norm.

**Definition 3.5** A **metric** is a functional  $\mathcal{T}(A) \times \mathcal{T}(A) \rightarrow \mathbb{R}_+$  with the following properties. For any  $\xi, \zeta, \kappa \in \mathcal{T}(A)$ , it satisfies

- Positive-definiteness:  $\Delta(\xi, \zeta) \geq 0$  with equality if and only if  $\xi = \zeta$ .  
 Symmetry:  $\Delta(\xi, \zeta) = \Delta(\zeta, \xi)$ .  
 Triangle inequality:  $\Delta(\xi, \zeta) \leq \Delta(\xi, \kappa) + \Delta(\kappa, \zeta)$ .

When used with states, the generalized trace distance can be expressed in terms of the trace norm and the absolute value of the trace using (3.22). This yields

$$\Delta(\rho, \tau) = \frac{1}{2} \|\rho - \tau\|_1 + \frac{1}{2} |\text{Tr}(\rho - \tau)|. \quad (3.23)$$

Hence the definition reduces the usual trace distance  $\Delta(\rho, \tau) = \frac{1}{2} \|\rho - \tau\|_1$  in case both density operators have the same trace, for example if  $\rho, \tau \in \mathcal{S}_o(A)$ . More generally, for sub-normalized states in  $\mathcal{S}_\bullet(A)$ , we can express the generalized trace distance as

$$\Delta(\rho, \tau) = \frac{1}{2} \|\hat{\rho} - \hat{\tau}\|_1 = \Delta(\hat{\rho}, \hat{\tau}), \quad (3.24)$$

where  $\hat{\rho} = \rho \oplus (1 - \text{Tr}(\rho))$  and  $\hat{\tau} = \tau \oplus (1 - \text{Tr}(\tau))$  are block-diagonal. We will use the hat notation to refer to this construction in the following.

For normalized states  $\rho, \tau \in \mathcal{S}_o(A)$ , this definition expresses the *distinguishing advantage* in binary hypothesis testing. Let us consider the task of distinguishing between two hypotheses,  $\rho$  and  $\tau$ , with uniform prior using a single observation. For every event  $M \in \mathcal{P}_\bullet(A)$ , we consider the following strategy: we perform the POVM  $\{M, I - M\}$  and select  $\rho$  in case we measure  $M$  and  $\tau$  otherwise. Optimizing over all strategies, the probability of selecting the correct state can be expressed in terms of the distinguishing advantage,  $\Delta(\rho, \tau)$ , as follows:

$$p_{\text{corr}}(\rho, \tau) := \max_{M \in \mathcal{P}_\bullet(A)} \left( \frac{1}{2} \text{Tr}(\rho M) + \frac{1}{2} \text{Tr}(\tau(I - M)) \right) = \frac{1}{2} (1 + \Delta(\rho, \tau)). \quad (3.25)$$

Like any metric based on a norm, the generalized trace distance is also jointly convex. For all  $\lambda \in [0, 1]$ , we have

$$\Delta(\lambda\rho_1 + (1 - \lambda)\rho_2, \lambda\tau_1 + (1 - \lambda)\tau_2) \leq \lambda\Delta(\rho_1, \tau_1) + (1 - \lambda)\Delta(\rho_2, \tau_2). \quad (3.26)$$

Moreover, the generalized trace distance contracts when we apply a quantum channel (or any trace-non-increasing completely positive map) on both states.



**Proposition 3.1** *Let  $\xi, \zeta \in \mathcal{T}(A)$ , and let  $\mathcal{F} \in \text{CPTNI}(A, B)$  be a trace-non-increasing CP map. Then,  $\Delta(\mathcal{F}(\xi), \mathcal{F}(\zeta)) \leq \Delta(\xi, \zeta)$ .*

*Proof* Note that if  $\mathcal{F} \in \text{CP}(A, B)$  is trace non-increasing, then  $\mathcal{F}^\dagger \in \text{CP}(B, A)$  is sub-unital. In particular,  $\mathcal{F}^\dagger$  maps  $\mathcal{P}_\bullet(B)$  into  $\mathcal{P}_\bullet(A)$ . Then,

$$\Delta(\mathcal{F}(\xi), \mathcal{F}(\zeta)) = \max_{M \in \mathcal{P}_\bullet(B)} \left| \text{Tr}(M\mathcal{F}(\xi - \zeta)) \right| = \max_{M \in \mathcal{P}_\bullet(B)} \left| \text{Tr}(\mathcal{F}^\dagger(M)(\xi - \zeta)) \right| \quad (3.27)$$

$$\leq \max_{M \in \mathcal{P}_\bullet(A)} |\text{Tr}(M(\xi - \zeta))| = \Delta(\xi, \zeta). \quad (3.28)$$

where we used the definition of the norm in (3.17) twice.  $\square$

As a special case when we take the map to be a partial trace, this relation yields

$$\Delta(\rho_A, \tau_A) \leq \min_{\rho_{AB}, \tau_{AB}} \Delta(\rho_{AB}, \tau_{AB}) \quad (3.29)$$

where  $\rho_{AB}$  and  $\tau_{AB}$  are extensions (e.g. purifications) of  $\rho_A$  and  $\tau_A$ , respectively.

Can we always find two purifications such that (3.29) becomes an equality? To see that this is in fact not true, consider the following example. If  $\rho$  is fully mixed on a qubit and  $\tau$  is pure, then,  $\Delta(\rho, \tau) = \frac{1}{2}$ , but  $\Delta(\psi, \vartheta) \geq \frac{1}{\sqrt{2}}$  for all maximally entangled states  $\psi$  that purify  $\rho$  and product states  $\vartheta$  that purify  $\tau$ .

### 3.3 Fidelity

The last observation motivates us to look at other measures of distance between states. Uhlmann's fidelity [165] is ubiquitous in quantum information theory and we define it here for general states.

**Definition 3.6** For any  $\rho, \sigma \in \mathcal{S}(A)$ , we define the **fidelity** of  $\rho$  and  $\tau$  as

$$F(\rho, \tau) := \left( \text{Tr} \left| \sqrt{\rho} \sqrt{\tau} \right| \right)^2. \quad (3.30)$$

Next we will discuss a few basic properties of the fidelity, and we will provide further details when we discuss the minimal quantum Rényi divergence in Sect. 4.3. In fact, the analysis in Sect. 4.3 will reveal that  $(\rho, \tau) \mapsto \sqrt{F(\rho, \tau)}$  is jointly concave

and non-decreasing when we apply a CPTP map to both states. The latter property thus also holds for the fidelity itself.

Beyond that, Uhlmann's theorem [165] states that there always exist purifications with the same fidelity as their marginals.

**Theorem 3.1** *For any states  $\rho_A, \tau_A \in \mathcal{S}(A)$  and any purification  $\rho_{AB} \in \mathcal{S}(AB)$  of  $\rho_A$  with  $d_B \geq d_A$ , there exists a purification  $\tau_{AB} \in \mathcal{S}(AB)$  of  $\tau_A$  such that  $F(\rho_A, \tau_A) = F(\rho_{AB}, \tau_{AB})$ .*

In particular, combining this with the fact that the fidelity cannot decrease when we take a partial trace, we can write

$$F(\rho_A, \tau_A) = \max_{\tau_{AB} \in \mathcal{S}(AB)} F(\rho_{AB}, \tau_{AB}) = \max_{\phi_{AB}, \vartheta_{AB} \in \mathcal{S}(AB)} |\langle \phi_{AB} | \vartheta_{AB} \rangle|^2, \quad (3.31)$$

where  $\tau_{AB}$  is any extension of  $\tau_A$ . The latter optimization is over all purifications  $|\phi_{AB}\rangle$  of  $\rho_A$  and  $|\vartheta_{AB}\rangle$  of  $\tau_A$ , respectively, and assumes that  $d_B \geq d_A$ .

Uhlmann's theorem has many immediate consequences. For example, for any linear operator  $L \in \mathcal{L}(A)$ , we see that

$$F(L\rho L^\dagger, \tau) = F(\rho, L^\dagger \tau L) \quad (3.32)$$

by using the latter expression in (3.31). This can be generalized further as follows.

**Lemma 3.3** *For  $\rho, \tau \in \mathcal{S}(A)$  and a pinching  $\mathcal{P}$ , we have  $F(\mathcal{P}(\rho), \tau) = F(\rho, \mathcal{P}(\tau))$ .*

*Proof* By symmetry, it is sufficient to show an inequality in one direction. Let  $\sigma_A = \mathcal{P}(\rho_A) = \sum_x P^x \rho_A P^x$  and  $\{\sigma_A^x\}_x$  with  $\sigma_A^x = P^x \rho_A P^x$  be a set of orthogonal states. Then, introducing an auxiliary Hilbert space  $A'$  with  $d_{A'} = d_A$ , we define the projector  $\Pi = \sum_x P_A^x \otimes P_{A'}^x$ . The state  $\sigma_A$  entertains a purification in the support of  $\Pi$ , namely we can write

$$|\sigma\rangle_{AA'} = \Pi |\rho\rangle_{AA'} = \sum_x |\sigma^x\rangle_{AA'}, \quad \text{where } \sigma_{A'}^x = \text{Tr}_A(\sigma_{AA'}^x) \quad (3.33)$$

are again mutually orthogonal. Hence, by Uhlmann's theorem

$$F(\mathcal{P}(\rho_A), \tau_A) = \max_{\tau_{AA'}} \text{Tr}(\sigma_{AA'} \tau_{AA'}) = \max_{\tau_{AA'}} \text{Tr}(\rho_{AA'} \Pi \tau_{AA'} \Pi) \quad (3.34)$$

$$\leq \max_{\tau_{AA'}} F(\rho_A, \text{Tr}_{A'}(\Pi \tau_{AA'} \Pi)), \quad (3.35)$$

where the maximization is over purifications of  $\tau_A$ . Finally, by choosing a basis  $\{|z\rangle_{A'}\}_z$  that commutes with all projectors  $P_{A'}^x$ , we find that

$$\mathrm{Tr}_{A'}(\Pi \tau_{AA'} \Pi) = \sum_{x,y,z} \langle z|_{A'} P_A^x \otimes P_{A'}^x \tau_{AA'} P_A^y \otimes P_{A'}^y |z\rangle_{A'} \quad (3.36)$$

$$= \sum_{x,z} P_A^x \langle z|_{A'} \tau_{AA'} |z\rangle_{A'} P_A^x = \sum_x P_A^x \tau_A P_A^x = \mathcal{P}(\tau_A), \quad (3.37)$$

which concludes the proof.  $\square$

Finally, we find that the fidelity is concave in each of its arguments.

**Lemma 3.4** *The functionals  $\rho \mapsto F(\rho, \tau)$  and  $\tau \mapsto F(\rho, \tau)$  are concave.*

*Proof* By symmetry it suffices to show concavity of  $\rho \mapsto F(\rho, \tau)$ . Let  $\rho_A^1, \rho_A^2 \in \mathcal{S}_\circ(A)$  and  $\lambda \in (0, 1)$  such that  $\lambda \rho_A^1 + (1 - \lambda) \rho_A^2 = \rho_A$ . Moreover, let  $\tau_{AA'} \in \mathcal{S}_\circ(AA')$  be a fixed purification of  $\tau_A$ .

Then, due to Uhlmann's theorem there exist purifications  $\rho_{AA'}^1$  and  $\rho_{AA'}^2$  of  $\rho_A^1$  and  $\rho_A^2$ , respectively, such that the following chain of inequalities holds:

$$\lambda F(\rho_A^1, \sigma_A) + (1 - \lambda) F(\rho_A^2, \sigma_A) = \lambda |\langle \tau_{AA'} | \rho_{AA'}^1 \rangle|^2 + (1 - \lambda) |\langle \tau_{AA'} | \rho_{AA'}^2 \rangle|^2 \quad (3.38)$$

$$= \langle \tau_{AA'} | (\lambda |\rho_{AA'}^1\rangle\langle \rho_{AA'}^1| + (1 - \lambda) |\rho_{AA'}^2\rangle\langle \rho_{AA'}^2|) | \tau_{AA'} \rangle \quad (3.39)$$

$$= F(\tau_{AA'}, \lambda |\rho_{AA'}^1\rangle\langle \rho_{AA'}^1| + (1 - \lambda) |\rho_{AA'}^2\rangle\langle \rho_{AA'}^2|) \quad (3.40)$$

$$\leq F(\tau_A, \lambda \rho_A^1 + (1 - \lambda) \rho_A^2). \quad (3.41)$$

The final inequality follows since the fidelity is non-decreasing when we apply a partial trace.  $\square$

### 3.3.1 Generalized Fidelity

Before we commence, we define a very useful generalization of the fidelity to sub-normalized density operators, which we call the generalized fidelity.

**Definition 3.7** For  $\rho, \tau \in \mathcal{S}_\bullet(A)$ , we define the **generalized fidelity** between  $\rho$  and  $\tau$  as

$$F_*(\rho, \tau) := \left( \mathrm{Tr} |\sqrt{\rho} \sqrt{\tau}| + \sqrt{(1 - \mathrm{Tr} \rho)(1 - \mathrm{Tr} \tau)} \right)^2. \quad (3.42)$$

Uhlmann's theorem (Theorem 3.1) adapted to the generalized fidelity states that

$$F_*(\rho, \tau) = \max_{\varphi, \vartheta} F_*(\varphi, \vartheta) = \max_{\vartheta} F_*(\phi, \vartheta), \quad \text{where} \quad (3.43)$$

$$\sqrt{F_*(\varphi, \vartheta)} = |\langle \varphi | \vartheta \rangle| + \sqrt{(1 - \text{Tr } \varphi)(1 - \text{Tr } \vartheta)}, \quad (3.44)$$

and  $\varphi$  and  $\vartheta$  range over all purifications of  $\rho$  and  $\tau$ , respectively, and  $\phi$  is a fixed purification of  $\rho$ . Moreover, using the operators  $\hat{\rho}$  and  $\hat{\tau}$  defined in the preceding section, we can write

$$F_*(\rho, \tau) = F_*(\hat{\rho}, \hat{\tau}) = \left( \text{Tr} \left| \sqrt{\hat{\rho}} \sqrt{\hat{\tau}} \right| \right)^2. \quad (3.45)$$

From this representation also follows that the square root of the generalized fidelity is jointly concave on  $\mathcal{S}_\bullet(A) \times \mathcal{S}_\bullet(A)$ , inheriting this property from the fidelity. Moreover, the generalized fidelity itself is concave in each of its arguments separately due to Lemma 3.4.

The extension to sub-normalized states in Definition 3.7 is chosen diligently so that the generalized fidelity is non-decreasing when we apply a quantum channel, or more generally a trace non-increasing CP map.

**Proposition 3.2** *Let  $\rho, \tau \in \mathcal{S}_\bullet(A)$ , and let  $\mathcal{E}$  be a trace non-increasing CP map. Then,  $F_*(\mathcal{E}(\rho), \mathcal{E}(\tau)) \geq F_*(\rho, \tau)$ .*

*Proof* Recall that a trace non-increasing map  $\mathcal{F} \in \text{CP}(A, B)$  can be decomposed into an isometry  $\mathcal{U} \in \text{CP}(A, BC)$  followed by a projection  $\Pi \in \mathcal{P}(BC)$  and a partial trace over  $C$  according to the Stinespring dilation representation.

Let us first restrict our attention to CPTP maps  $\mathcal{E}$  where  $\Pi = I$ . We write  $\rho'_B = \mathcal{E}[\rho_A]$  and  $\tau'_B = \mathcal{E}[\tau_A]$ . From the representation of the fidelity in (3.44) we can immediately deduce that

$$F_*(\rho_A, \tau_A) = \max_{\varphi_{AD}, \vartheta_{AD}} F_*(\varphi_{AD}, \vartheta_{AD}) = \max_{\varphi_{AD}, \vartheta_{AD}} F_*(\mathcal{U}(\varphi_{AD}), \mathcal{U}(\vartheta_{AD})) \quad (3.46)$$

$$\leq \max_{\varphi'_{BCD}, \vartheta'_{BCD}} F_*(\varphi'_{BCD}, \vartheta'_{BCD}) = F_*(\rho'_B, \tau'_B). \quad (3.47)$$

The maximizations above are restricted to purifications of  $\rho_A$  and  $\tau_A$ , respectively. The sole inequality follows since  $\mathcal{U}(\varphi_{AD})$  and  $\mathcal{U}(\vartheta_{AD})$  are particular purifications of  $\rho'_B$  and  $\tau'_B$  in  $\mathcal{S}_\bullet(BCD)$ .

Next, consider a projection  $\Pi \in \mathcal{P}(BC)$  and the CPTP map  $\mathcal{E} : \rho \mapsto \begin{pmatrix} \Pi \rho \Pi & 0 \\ 0 & \text{Tr}(\Pi^\perp \rho) \end{pmatrix}$  with  $\Pi^\perp = I - \Pi$ . Applying the inequality for CPTP maps to  $\mathcal{E}$ , we find

$$\begin{aligned} \sqrt{F_*(\rho, \tau)} &\leq \left\| \sqrt{\Pi\rho\Pi}\sqrt{\Pi\tau\Pi} \right\|_1 + \sqrt{\text{Tr}(\Pi^\perp\rho)\text{Tr}(\Pi^\perp\tau)} \\ &\leq \sqrt{F_*(\Pi\rho\Pi, \Pi\tau\Pi)} \end{aligned} \quad (3.48)$$

where we used that  $\text{Tr } \rho \leq 1$  and  $\text{Tr } \tau \leq 1$  in the last step.  $\square$

The main strength of the generalized fidelity compared to the trace distance lies in the following property, which tells us that the inequality in Proposition 3.2 is tight if the map is a partial trace. Given two marginal states and an extension of one of these states, we can always find an extension of the other state such that the generalized fidelity is preserved by the partial trace. This is a simple corollary of Uhlmann's theorem.

**Corollary 3.1** *Let  $\rho_{AB} \in \mathcal{S}_\bullet(AB)$  and  $\tau_A \in \mathcal{S}_\bullet(A)$ . Then, there exists an extension  $\tau_{AB}$  such that  $F_*(\rho_{AB}, \tau_{AB}) = F_*(\rho_A, \tau_A)$ . Moreover, if  $\rho_{AB}$  is pure and  $d_B \geq d_A$ , then  $\tau_{AB}$  can be chosen pure as well.*

*Proof* Clearly  $F_*(\rho_A, \tau_A) \geq F_*(\rho_{AB}, \tau_{AB})$  by Proposition 3.2 for any choice of  $\tau_{AB}$ . Let us first treat the case where  $\rho_{AB}$  is pure. Using Uhlmann's theorem in (3.44), we can write

$$F_*(\rho_A, \tau_A) = \max_{\vartheta_{AB}} F_*(\phi_{AB}, \vartheta_{AB}), \quad \text{where } \phi_{AB} = \rho_{AB}. \quad (3.49)$$

We then take  $\tau_{AB}$  to be any maximizer. For the general case, consider a purification  $\rho_{ABC}$  of  $\rho_{AB}$ . Then, by the above argument there exists a state  $\tau_{ABC}$  with  $F_*(\rho_{ABC}, \tau_{ABC}) = F_*(\rho_A, \tau_A)$ . Moreover, by Proposition 3.2, we have  $F_*(\rho_{ABC}, \tau_{ABC}) \leq F_*(\rho_{AB}, \tau_{AB}) \leq F_*(\rho_A, \tau_A)$ . Hence, all inequalities must be equalities, which concludes the proof.  $\square$

### 3.4 Purified Distance

The fidelity is not a metric itself, but for example the *angular distance* [125] and the *Bures metric* [31] are metrics. They are respectively defined as

$$A(\rho, \tau) := \arccos \sqrt{F(\rho, \tau)} \quad \text{and} \quad B(\rho, \tau) := \sqrt{2 \left( 1 - \sqrt{F(\rho, \tau)} \right)}. \quad (3.50)$$

We will now discuss another metric, which we find particularly convenient since it is related to the minimal trace distance of purifications [67, 134, 156].

**Definition 3.8** For  $\rho, \tau \in \mathcal{S}_\bullet(A)$ , we define the **purified distance** between  $\rho$  and  $\tau$  as  $P(\rho, \tau) := \sqrt{1 - F_*(\rho, \tau)}$ .

Then, for quantum states  $\rho, \tau \in \mathcal{S}_\circ(A)$ , using Uhlmann's theorem we find

$$P(\rho, \tau) = \sqrt{1 - F_*(\rho, \tau)} = \sqrt{1 - \max_{\varphi, \vartheta} |\langle \varphi | \vartheta \rangle|^2} = \min_{\varphi, \vartheta} \Delta(\varphi, \vartheta). \quad (3.51)$$

Here,  $|\varphi\rangle$  and  $|\vartheta\rangle$  are purifications of  $\rho$  and  $\tau$ , respectively.

As it is defined in terms of the generalized fidelity, the purified distance inherits many of its properties. For example, for trace non-increasing CP maps  $\mathcal{F}$ , we find

$$P(\mathcal{F}(\rho), \mathcal{F}(\tau)) \leq P(\rho, \tau). \quad (3.52)$$

Moreover, the purified distance is a metric on the set of sub-normalized states.

**Proposition 3.3** *The purified distance is a metric on  $\mathcal{S}_\bullet(A)$ .*

*Proof* Let  $\rho, \tau, \sigma \in \mathcal{S}_\bullet(A)$ . The condition  $P(\rho, \tau) = 0$  if and only if  $\rho = \tau$  can be verified by inspection, and symmetry  $P(\rho, \tau) = P(\tau, \rho)$  follows from the symmetry of the fidelity.

It remains to show the triangle inequality,  $P(\rho, \tau) \leq P(\rho, \sigma) + P(\sigma, \tau)$ . Using (3.45), the generalized fidelities between  $\rho, \tau$  and  $\sigma$  can be expressed as fidelities between the corresponding extensions  $\hat{\rho}, \hat{\tau}$  and  $\hat{\sigma}$ . We employ the triangle inequality of the angular distance, which can be expressed in terms of the purified distance as  $A(\hat{\rho}, \hat{\tau}) = \arccos \sqrt{F_*(\rho, \tau)} = \arcsin P(\rho, \tau)$ . We find

$$P(\rho, \tau) = \sin A(\hat{\rho}, \hat{\tau}) \quad (3.53)$$

$$\leq \sin (A(\hat{\rho}, \hat{\sigma}) + A(\hat{\sigma}, \hat{\tau})) \quad (3.54)$$

$$= \sin A(\hat{\rho}, \hat{\sigma}) \cos A(\hat{\sigma}, \hat{\tau}) + \sin A(\hat{\sigma}, \hat{\tau}) \cos A(\hat{\rho}, \hat{\sigma}) \quad (3.55)$$

$$= P(\rho, \sigma) \sqrt{F_*(\sigma, \tau)} + P(\sigma, \tau) \sqrt{F_*(\rho, \sigma)} \quad (3.56)$$

$$\leq P(\rho, \sigma) + P(\sigma, \tau), \quad (3.57)$$

where we employed the trigonometric addition formula to arrive at (3.55).  $\square$

Note that the purified distance is not an intrinsic metric. Given two states  $\rho, \tau$  with  $P(\rho, \tau) \leq \varepsilon$  it is in general not possible to find intermediate states  $\sigma^\lambda$  with  $P(\rho, \sigma^\lambda) = \lambda\varepsilon$  and  $P(\sigma^\lambda, \tau) = (1 - \lambda)\varepsilon$ . In this sense, the above triangle inequality

is not tight. It is thus sometimes useful to employ the upper bound in (3.56) instead. For example, we find that  $P(\rho, \sigma) \leq \sin(\varphi)$  and  $P(\sigma, \tau) \leq \sin(\vartheta)$  implies

$$P(\rho, \tau) \leq \sin(\varphi + \vartheta) < \sin(\varphi) + \sin(\vartheta) \quad (3.58)$$

if  $\varphi, \vartheta > 0$  and  $\varphi + \vartheta \leq \frac{\pi}{2}$ .

The purified distance is jointly quasi-convex since it is an anti-monotone function of the square root of the generalized fidelity, which is jointly concave. Formally, for any  $\rho_1, \rho_2, \tau_1, \tau_2 \in \mathcal{S}_\bullet(A)$  and  $\lambda \in [0, 1]$ , we have

$$P(\lambda\rho_1 + (1-\lambda)\rho_2, \lambda\tau_1 + (1-\lambda)\tau_2) \leq \max_{i \in \{1,2\}} P(\rho_i, \tau_i). \quad (3.59)$$

The purified distance has simple upper and lower bounds in terms of the generalized trace distance. This results from a simple reformulation of the Fuchs–van de Graaf inequalities [59] between the trace distance and the fidelity.

**Lemma 3.5** *Let  $\rho, \tau \in \mathcal{S}_\bullet(A)$ . Then, the following inequalities hold:*

$$\Delta(\rho, \tau) \leq P(\rho, \tau) \leq \sqrt{2\Delta(\rho, \tau) - \Delta(\rho, \tau)^2} \leq \sqrt{2\Delta(\rho, \tau)}. \quad (3.60)$$

*Proof* We first express the quantities using the normalized density operators  $\hat{\rho}$  and  $\hat{\tau}$ , i.e.  $P(\rho, \tau) = P(\hat{\rho}, \hat{\tau})$  and  $\Delta(\rho, \tau) = \Delta(\hat{\rho}, \hat{\tau})$ . Then, the result follows from the inequalities

$$1 - \sqrt{F(\hat{\rho}, \hat{\tau})} \leq D(\hat{\rho}, \hat{\tau}) \leq \sqrt{1 - F(\hat{\rho}, \hat{\tau})} \quad (3.61)$$

between the trace distance and fidelity, which were first shown by Fuchs and van de Graaf [59].  $\square$

### 3.5 Background and Further Reading

We defer to Bhatia’s book [26, Chap. IV] for a comprehensive introduction to matrix norms. Fuchs’ thesis [58] gives a useful overview over distance measures in quantum information. The fidelity was first investigated by Uhlmann [165] and popularized in quantum information theory by Jozsa [97] who also gave it its name. Some recent literature (most prominently Nielsen and Chuang’s standard textbook [125]) defines the fidelity as  $\sqrt{F(\cdot, \cdot)}$ , also called the square root fidelity. Here we adopted the historical definition.

The discussion on generalized fidelity and purified distance is based on [152] and [156]. The purified distance was independently proposed by Gilchrist et al. [67] and Rastegin [134, 135], where it is sometimes called ‘sine distance’. However, in these papers the discussion is restricted to normalized states. The name ‘purified distance’ was coined in [156], where the generalization to sub-normalized states was first investigated.

# Chapter 4

## Quantum Rényi Divergence

**Abstract** Shannon entropy as well as conditional entropy and mutual information can be compactly expressed in terms of the relative entropy, or Kullback–Leibler divergence. In this sense, the divergence can be seen as a parent quantity to entropy, conditional entropy and mutual information, and many properties of the latter quantities can be derived from properties of the divergence. Similarly, we will define Rényi entropy, conditional entropy and mutual information in terms of a parent quantity, the Rényi divergence. We will see in the following chapters that this approach is very natural and leads to operationally significant measures that have powerful mathematical properties. This observation allows us to first focus our attention on quantum generalizations of the Kullback–Leibler and Rényi divergence and explore their properties, which is the topic of this chapter.

There exist various quantum generalizations of the classical Rényi divergence due to the non-commutative nature of quantum physics.<sup>1</sup> Thus, it is prudent to restrict our attention to quantum generalizations that attain operational significance in quantum information theory. A natural application of classical Rényi divergence is in hypothesis testing, where error and strong converse exponents are naturally expressed in terms of the Rényi divergence. In this chapter we focus on two variants of the quantum Rényi divergence that both attain operational significance in quantum hypothesis testing. Here we explore their mathematical properties, whereas their application to hypothesis testing will be reviewed in Chap. 7.

### 4.1 Classical Rényi Divergence

Before we tackle quantum Rényi divergences, let us first recapitulate some properties of the classical Rényi divergence they are supposed to generalize. We formulate these properties in the quantum language, and we will later see that most of them are also satisfied by some quantum Rényi divergences.

---

<sup>1</sup>In fact, uncountably infinite quantum generalizations with interesting mathematical properties can easily be constructed (see, e.g. [9]).



### 4.1.1 An Axiomatic Approach

Alfréd Rényi, in his seminal 1961 paper [142] investigated an axiomatic approach to derive the Shannon entropy [144]. He found that five natural requirements for functionals on a probability space single out the Shannon entropy, and by relaxing one of these requirements, he found a family of entropies now named after him.

The requirements can be readily translated to the quantum language. Here we consider general functionals  $\mathbb{D}(\cdot\|\cdot)$  that map a pair of operators  $\rho, \sigma \in \mathcal{S}(A)$  with  $\rho \neq 0, \sigma \gg \rho$  onto the real line. Rényi's six axioms naturally translate as follows:

- (I) **Continuity:**  $\mathbb{D}(\rho\|\sigma)$  is continuous in  $\rho, \sigma \in \mathcal{S}(A)$ , wherever  $\rho \neq 0$  and  $\sigma \gg \rho$ .
- (II) **Unitary invariance:**  $\mathbb{D}(\rho\|\sigma) = \mathbb{D}(U\rho U^\dagger\|U\sigma U^\dagger)$  for any unitary  $U$ .
- (III) **Normalization:**  $\mathbb{D}(1\|\frac{1}{2}) = \log(2)$ .
- (IV) **Order:** If  $\rho \geq \sigma$ , then  $\mathbb{D}(\rho\|\sigma) \geq 0$ . And, if  $\rho \leq \sigma$ , then  $\mathbb{D}(\rho\|\sigma) \leq 0$ .
- (V) **Additivity:**  $\mathbb{D}(\rho \otimes \tau\|\sigma \otimes \omega) = \mathbb{D}(\rho\|\sigma) + \mathbb{D}(\tau\|\omega)$  for all  $\rho, \sigma \in \mathcal{S}(A)$ ,  $\tau, \omega \in \mathcal{S}(B)$  with  $\rho \neq 0, \tau \neq 0$ .
- (VI) **General mean:** There exists a continuous and strictly monotonic function  $g$  such that  $\mathbb{Q}(\cdot\|\cdot) := g(\mathbb{D}(\cdot\|\cdot))$  satisfies the following. For  $\rho, \sigma \in \mathcal{S}(A)$ ,  $\tau, \omega \in \mathcal{S}(B)$ ,

$$\mathbb{Q}(\rho \oplus \tau\|\sigma \oplus \omega) = \frac{\text{Tr}(\rho)}{\text{Tr}(\rho + \tau)} \cdot \mathbb{Q}(\rho\|\sigma) + \frac{\text{Tr}(\tau)}{\text{Tr}(\rho + \tau)} \cdot \mathbb{Q}(\tau\|\omega). \quad (4.1)$$

Rényi [142] first shows that (I)–(V) imply  $\mathbb{D}(\lambda\|\mu) = \log \lambda - \log \mu$  for two scalars  $\lambda, \mu > 0$ , a quantity that is often referred to as the *log-likelihood ratio*. In fact, the axioms imply the following constraint, which will be useful later since it allows us to restrict our attention to normalized states.

- (III+) **Normalization:**  $\mathbb{D}(a\rho\|b\sigma) = \mathbb{D}(\rho\|\sigma) + \log a - \log b$  for  $a, b > 0$ .

We also remark that invariance under unitaries (II) is implied by a slightly stronger property, invariance under isometries.

- (II+) **Isometric Invariance:**  $\mathbb{D}(\rho\|\sigma) = \mathbb{D}(V\rho V^\dagger\|V\sigma V^\dagger)$  for  $\rho, \sigma \in \mathcal{S}(A)$  and any isometry  $V$  from  $A$  to  $B$ .

Rényi then considers general continuous and strictly monotonic functions to define a mean in (VI), such that the resulting quantity is still compatible with (I)–(V). Under the assumption that the states  $\rho_X$  and  $\sigma_X$  are classical, he then establishes that Properties (I)–(VI) are satisfied only by the *Kullback–Leibler divergence* [103] and the *Rényi divergence* for  $\alpha \in (0, 1) \cup (1, \infty)$ , which are respectively given as

$$D(\rho_X\|\sigma_X) = \frac{\sum_x \rho(x)(\log \rho(x) - \log \sigma(x))}{\sum_x \rho(x)} \quad \text{with } g : t \mapsto t, \quad (4.2)$$

$$D_\alpha(\rho_X \parallel \sigma_X) = \frac{1}{\alpha - 1} \log \frac{\sum_x \rho(x)^\alpha \sigma(x)^{1-\alpha}}{\sum_x \rho(x)} \quad \text{with } g_\alpha : t \mapsto \exp((\alpha - 1)t). \quad (4.3)$$

These quantities are well-defined if  $\rho_X$  and  $\sigma_X$  have full support and otherwise we use the convention that  $0 \log 0 = 0$  and  $\frac{0}{0} = 1$ , which ensures that the divergences are indeed continuous whenever  $\rho_X \neq 0$  and  $\sigma_X \gg \rho_X$ . Finally, note that both quantities diverge to  $+\infty$  if the latter condition is not satisfied and  $\alpha > 1$ .

### 4.1.2 Positive Definiteness and Data-Processing

Unlike in the classical case, the above axioms do not uniquely determine a quantum generalization of these divergences. Hence, we first list some additional properties we would like a quantum generalization of the Rényi divergence to have. These are operationally significant, but mathematically more involved than the axioms used by Rényi. The classical Rényi divergences satisfy all these properties.

The two most significant properties from an operational point of view are positive definiteness and the data-processing inequality. First, *positive definiteness* ensures that the divergence is positive for normalized states and vanishes only if both arguments are equal. This allows us to use the divergence as a measure of distinguishability in place of a metric in some cases, even though it is not symmetric and does not satisfy a triangle inequality.

(VII) **Positive definiteness:** If  $\rho, \sigma \in \mathcal{S}_o(A)$ , then  $\mathbb{D}(\rho \parallel \sigma) \geq 0$  with equality iff  $\rho = \sigma$ .

The *data-processing inequality* (DPI) ensures the divergence never increases when we apply a quantum channel to both states. This strengthens the interpretation of the divergence as a measure of distinguishability—the outputs of a channel are at least as hard to distinguish as the inputs.

(VIII) **Data-processing inequality:** For any  $\mathcal{E} \in \text{CPTP}(A, B)$  and  $\rho, \sigma \in \mathcal{S}(A)$ , we have

$$\mathbb{D}(\rho \parallel \sigma) \geq \mathbb{D}(\mathcal{E}(\rho) \parallel \mathcal{E}(\sigma)). \quad (4.4)$$

Finally, the following mathematical properties will prove extremely useful. (Note that we expect that either (IXa) or (IXb) holds, but not both.)

(IXa) **Joint convexity** (applies only to Rényi divergence with  $\alpha > 1$ ): For sets of normalized states  $\{\rho_i\}_i, \{\sigma_i\}_i \subset \mathcal{S}_o(A)$  and a probability mass function  $\{\lambda_i\}_i$  such that  $\lambda_i \geq 0$  and  $\sum_i \lambda_i = 1$ , we have

$$\sum_i \lambda_i \mathbb{Q}(\rho_i \parallel \sigma_i) \geq \mathbb{Q}\left(\sum_i \lambda_i \rho_i \parallel \sum_i \lambda_i \sigma_i\right). \quad (4.5)$$

Consequently,  $(\rho, \sigma) \mapsto \mathbb{D}(\rho\|\sigma)$  is jointly quasi-convex, namely

$$\mathbb{D}\left(\sum_i \lambda_i \rho_i \left\| \sum_i \lambda_i \sigma_i\right.\right) \leq \max_i \mathbb{D}(\rho_i\|\sigma_i). \quad (4.6)$$

(IXb) **Joint concavity** (applies only to Rényi divergence with  $\alpha \leq 1$ ): The inequality (4.5) holds in the opposite direction, i.e.  $(\rho, \sigma) \mapsto \mathbb{Q}(\rho\|\sigma)$  is jointly concave. Moreover,  $(\rho, \sigma) \mapsto \mathbb{D}(\rho\|\sigma)$  is jointly convex.

These properties are interrelated. For example, we clearly have  $\mathbb{D}(\rho\|\sigma) \geq 0$  in (VII) if data-processing holds, since  $\mathbb{D}(\rho\|\sigma) \geq \mathbb{D}(\text{Tr}(\rho)\|\text{Tr}(\sigma)) = \mathbb{D}(1\|1) = 0$ . Furthermore,  $\mathbb{D}(\rho\|\rho) = 0$  follows from (IV). To establish positive definiteness (VII) it in fact suffices to show

(VII-) **Definiteness:** For  $\rho, \sigma \in \mathcal{S}_o$ , we have  $\mathbb{D}(\rho\|\sigma) = 0 \implies \rho = \sigma$ .

when (IV) and (VIII) hold. The most important connection is drawn in Proposition 4.2 in Sect. 4.2, and establishes that data-processing holds if and only if joint convexity resp. concavity holds (depending on the value of  $\alpha$ ) for all quantum Rényi divergences. The last property generalizes the order property (IV) as follows.

(X) **Dominance:** For states  $\rho, \sigma, \sigma' \in \mathcal{S}(A)$  with  $\sigma \leq \sigma'$ , we have  $\mathbb{D}(\rho\|\sigma) \geq \mathbb{D}(\rho\|\sigma')$ .

Clearly, dominance (X) and positive definiteness (VII) imply order (IV).

In the following we will show that these properties hold for the classical Rényi divergence, i.e. for the case when the states  $\rho$  and  $\sigma$  commute. As we have argued above (and will show in Proposition 4.2), to establish data-processing, it suffices to prove that the KL divergence in (4.2) and the classical Rényi divergences (4.3) satisfy joint convexity resp. concavity as in (IXa) and (IXb). For this purpose we will need the following elementary lemma:

**Lemma 4.1** *If  $f$  is convex on positive reals, then  $F : (p, q) \mapsto qf\left(\frac{p}{q}\right)$  is jointly convex. Moreover, if  $f$  is strictly convex, then  $F$  is strictly convex in  $p$  and in  $q$ .*

*Proof* Let  $\{\lambda_i\}_i, \{p_i\}_i, \{q_i\}_i$  be positive reals such that  $\sum_i \lambda_i p_i = p$  and  $\sum_i \lambda_i q_i = q$ . Then, employing Jensen's inequality, we find

$$\sum_i \lambda_i q_i f\left(\frac{p_i}{q_i}\right) = q \sum_i \frac{\lambda_i q_i}{q} f\left(\frac{p_i}{q_i}\right) \geq qf\left(\sum_i \frac{\lambda_i q_i}{q} \frac{p_i}{q_i}\right) = qf\left(\frac{p}{q}\right). \quad (4.7)$$

The second statement is evident if we fix either  $p_i = p$  or  $q_i = q$ . □

This lemma is a generalization of the famous *log sum inequality*, which we recover using the convex function  $f : t \mapsto t \log t$ .

Let us then recall that for normalized  $\rho_X, \sigma_X \in \mathcal{S}_\circ(X)$ , we have

$$Q_\alpha(\rho_X \parallel \sigma_X) := g_\alpha(D_\alpha(\rho_X \parallel \sigma_X)) = \sum_x \sigma(x) \left( \frac{\rho(x)}{\sigma(x)} \right)^\alpha. \quad (4.8)$$

First, note that  $Q_\alpha$  has the form of a Csiszár-Morimoto  $f$ -divergence [39, 117], where  $f_\alpha : t \mapsto t^\alpha$  is concave for  $\alpha \in (0, 1)$  and convex for  $\alpha > 1$ . Joint convexity resp. concavity of  $Q_\alpha$  is then a direct consequence of Lemma 4.1, which we apply for each summand of the sum over  $x$  individually. By the same argument applied for  $f : t \mapsto t \log t$  (i.e. the log sum inequality), we also find that

$$D(\rho_X \parallel \sigma_X) = \sum_x \sigma(x) f \left( \frac{\rho(x)}{\sigma(x)} \right) \quad (4.9)$$

is jointly convex.

The Rényi divergences satisfy the data-processing inequality (VIII), i.e.  $D_\alpha$  is contractive under application of classical channels to both arguments. This can be shown directly, but since we have established joint convexity resp. concavity, it also follows from (a classical adaptation of) Proposition 4.2 below and we thus omit the proof here.

Dominance (X) is evident from the definition. It remains to show definiteness (VII-) and thus (VII). This is a consequence of the fact that  $Q$  and  $Q_\alpha$  are strictly convex resp. concave in the second argument due to Lemma 4.1. Namely, let us assume for the sake of contradiction that  $D(\rho_X \parallel \rho_X) = D(\rho_X \parallel \sigma_X) = 0$ . Then we get that  $D(\rho_X \parallel \frac{1}{2}\rho_X + \frac{1}{2}\sigma_X) < 0$  if  $\rho_X \neq \sigma_X$ , which contradicts positivity. A similar argument applies to  $Q_\alpha$ , and we are done.

The Kullback–Leibler divergence and the classical Rényi divergence as defined in (4.2) and (4.3) satisfy Properties (I)–(X).

### 4.1.3 Monotonicity in $\alpha$ and Limits

Due to the parametrization in terms of the parameter  $\alpha$ , we also find the following relation between different Rényi divergences.

**Proposition 4.1** *The function  $(0, 1) \cup (1, \infty) \ni \alpha \mapsto \log Q_\alpha(\rho_X \parallel \sigma_X)$  is convex for all  $\rho_X, \sigma_X \in \mathcal{S}(X)$  with  $\rho_X \neq 0$  and  $\sigma_X \gg \rho_X$ . Moreover, it is strictly convex unless  $\rho_X = a\sigma_X$  for some  $a > 0$ .*

*Proof* It is sufficient to show this property for  $\rho_X, \sigma_X \in \mathcal{S}_\circ(X)$  due to (III+). We simply evaluate the second derivative of this function, which is

$$F'' = \frac{Q''_{\alpha}(\rho_X \|\sigma_X) Q_{\alpha}(\rho_X \|\sigma_X) - Q'_{\alpha}(\rho_X \|\sigma_X)^2}{Q_{\alpha}(\rho_X \|\sigma_X)^2} \quad (4.10)$$

where

$$Q'_{\alpha}(\rho_X \|\sigma_X) = \sum_x \rho(x)^{\alpha} \sigma(x)^{1-\alpha} (\ln \rho(x) - \ln \sigma(x)), \quad (4.11)$$

$$Q''_{\alpha}(\rho_X \|\sigma_X) = \sum_x \rho(x)^{\alpha} \sigma(x)^{1-\alpha} (\ln \rho(x) - \ln \sigma(x))^2. \quad (4.12)$$

Note that  $P(x) = \rho(x)^{\alpha} \sigma(x)^{1-\alpha} / Q_{\alpha}(\rho_X \|\sigma_X)$  is a probability mass function. Using this, the above expression can be simplified to

$$F'' = \sum_x P(x) (\ln \rho(x) - \ln \sigma(x))^2 - \left( \sum_x P(x) (\ln \rho(x) - \ln \sigma(x)) \right)^2. \quad (4.13)$$

Hence,  $F'' \geq 0$  by Jensen's inequality and the strict convexity of the function  $t \mapsto t^2$ , with equality if and only if  $\rho(x) = a\sigma(x)$  for all  $x$ .  $\square$

As a corollary, we find that the Rényi divergences are monotone functions of  $\alpha$ .

**Corollary 4.1** *The function  $\alpha \mapsto D_{\alpha}(\rho_X \|\sigma_X)$  is monotonically increasing. Moreover, it is strictly increasing unless  $\rho_X = a\sigma_X$  for some  $a > 0$ .*

*Proof* We set  $Q_{\alpha} \equiv Q_{\alpha}(\rho_X \|\sigma_X)$  to simplify notation and note that  $\log Q_1 = 0$ . Let us assume that  $\alpha > \beta > 1$  and set  $\lambda = \frac{\beta-1}{\alpha-1} \in (0, 1)$ . Then, by convexity of  $\alpha \rightarrow \log Q_{\alpha}$ , we have

$$\log Q_{\beta} = \log Q_{\lambda\alpha+(1-\lambda)} \leq \lambda \log Q_{\alpha} + (1-\lambda) \log Q_1 = \frac{\beta-1}{\alpha-1} \log Q_{\alpha}. \quad (4.14)$$

This establishes that  $D_{\alpha}(\rho_X \|\sigma_X) \geq D_{\beta}(\rho_X \|\sigma_X)$ , as desired. The inequality is strict unless  $\rho_X = \sigma_X$ , as we have seen in Proposition 4.1.

For  $1 > \alpha \geq \beta$ , an analogous argument with  $\lambda = \frac{1-\alpha}{1-\beta}$  establishes that  $\log Q_{\alpha} \leq \frac{1-\alpha}{1-\beta} \log Q_{\beta}$ , which again yields  $D_{\alpha}(\rho_X \|\sigma_X) \geq D_{\beta}(\rho_X \|\sigma_X)$  taking into account the sign of the prefactor.  $\square$

Since we have now established that  $D_{\alpha}$  is continuous in  $\alpha$  for  $\alpha \in (0, 1) \cup (1, \infty)$ , it will be interesting to take a look at the limits as  $\alpha$  approaches 0, 1 and  $\infty$ . First, a direct application of l'Hôpital's rule yields

$$\lim_{\alpha \searrow 1} D_{\alpha}(\rho_X \|\sigma_X) = \lim_{\alpha \nearrow 1} D_{\alpha}(\rho_X \|\sigma_X) = D(\rho_X \|\sigma_X). \quad (4.15)$$

So in fact the KL divergence is a limiting case of the Rényi divergences and we consequently define  $D_1(\rho_X \|\sigma_X) := D(\rho_X \|\sigma_X)$ . In the limit  $\alpha \rightarrow \infty$ , we find

$$D_\infty(\rho_X \|\sigma_X) := \lim_{\alpha \rightarrow \infty} D_\alpha(\rho_X \|\sigma_X) = \max_x \log \frac{\rho(x)}{\sigma(x)}, \quad (4.16)$$

which is the maximum log-likelihood ratio. We call this the *max-divergence*, and note that it satisfies all the properties except the general mean property (VI). However, the max-divergence instead satisfies

$$\mathbb{D}(\rho \oplus \tau \|\sigma \oplus \omega) = \max \{ \mathbb{D}(\rho \|\sigma), \mathbb{D}(\tau \|\omega) \}. \quad (4.17)$$

The limit  $\alpha \rightarrow 0$  is less interesting because it leads to the expression

$$D_0(\rho_X \|\sigma_X) := \lim_{\alpha \rightarrow 0} D_\alpha(\rho_X \|\sigma_X) = -\log \sum_{x:\rho(x)>0} \sigma(x), \quad (4.18)$$

which is discontinuous in  $\rho_X$  and thus does not satisfy (I). Hence, we hereafter consider  $D_\alpha$  with  $\alpha > 0$  as a single continuous one-parameter family of divergences.

Monotonicity of  $D_\alpha$  is not the only byproduct of the convexity of  $\log Q_\alpha$ . For example, we also find that

$$\lambda D_{1+\lambda}(\rho \|\sigma) + (1-\lambda) D_\infty(\rho \|\sigma) \geq D_2(\rho \|\sigma). \quad (4.19)$$

for  $\lambda \in [0, 1]$  and various similar relations.

## 4.2 Classifying Quantum Rényi Divergences

Clearly, we expect suitable quantum Rényi divergences to have the properties discussed in the previous section.

**Definition 4.1** A **quantum Rényi divergence** is a quantity  $\mathbb{D}(\cdot \|\cdot)$  that satisfies Properties (I)–(X) in Sect. 4.1.1. (It either satisfies IXa or IXb.)

A **family of quantum Rényi divergences** is a one-parameter family  $\alpha \mapsto \mathbb{D}_\alpha(\cdot \|\cdot)$  of quantum Rényi divergences such that Corollary 4.1 in Sect. 4.1.3 holds on some open interval containing 1.

Before we discuss two specific families of Rényi divergences in Sects. 4.3 and 4.4, let us first make a few observations that apply more generally to all quantum Rényi divergences.

### 4.2.1 Joint Concavity and Data-Processing

First, the following observation relates joint convexity resp. concavity and data-processing for all quantum Rényi divergences. It establishes that for functionals satisfying (I)–(VI), these properties are equivalent.

**Proposition 4.2** *Let  $\mathbb{D}$  be a functional satisfying (I)–(VI) and let  $g$  and  $\mathbb{Q}$  be defined as in (VI). Then, the following two statements are equivalent.*

- (1)  $\mathbb{Q}$  is jointly convex (IXa) if  $g$  is monotonically increasing, or jointly concave (IXb) if  $g$  is monotonically decreasing.
- (2)  $\mathbb{D}$  satisfies the data-processing inequality (VIII).

*Proof* First, we show (1)  $\implies$  (2). Note that the axioms enforce that  $\mathbb{Q}$  is invariant under isometries and consulting the Stinespring dilation, it thus remains to show that the data-processing inequality is satisfied for the partial trace operation. For the case where  $\mathbb{Q}$  is jointly convex, we thus need to show that  $\mathbb{Q}(\rho_{AB} \|\sigma_{AB}) \geq \mathbb{Q}(\rho_A \|\sigma_A)$  for  $\rho_{AB}, \sigma_{AB} \in \mathcal{S}_\circ(AB)$  and  $A$  and  $B$  are arbitrary quantum systems.

To show this, consider a unitary basis of  $\mathcal{L}(B)$ , for example the generalized Pauli operators  $\{X_B^l Z_B^m\}_{l,m}$ , where  $l, m \in [d_B]$ . These act on the computational basis as

$$X_B |k\rangle = |k + 1 \bmod d_B\rangle \quad \text{and} \quad Z_B |k\rangle = e^{\frac{2\pi i k}{d_B}} |k\rangle. \quad (4.20)$$

(If we only consider classical distributions, we can set  $Z_B = I_B$ .) Then, after collecting these operators in a set  $\{U_i = X_B^l Z_B^m\}_i$  with a single index  $i = (l, m)$ , a short calculation reveals that

$$\sum_i \frac{1}{d_B^2} (I_A \otimes U_i) \xi_{AB} (I_A \otimes U_i)^\dagger = \xi_A \otimes \pi_B \quad (4.21)$$

for any  $\xi_{AB} \in \mathcal{T}(AB)$ . Consequently, unitary invariance and joint convexity yield

$$\mathbb{Q}(\rho_{AB} \|\sigma_{AB}) = \sum_i \frac{1}{d_B^2} \mathbb{Q}(U_i \rho_{AB} U_i^\dagger \|\| U_i \sigma_{AB} U_i^\dagger) \quad (4.22)$$

$$\begin{aligned} &\geq \mathbb{Q}\left(\sum_i \frac{1}{d_B^2} U_i \rho_{AB} U_i^\dagger \|\| \sum_i \frac{1}{d_B^2} U_i \sigma_{AB} U_i^\dagger\right) \\ &= \mathbb{Q}(\rho_A \otimes \pi_B \|\| \sigma_A \otimes \pi_B). \end{aligned} \quad (4.23)$$

Finally,  $\mathbb{Q}(\rho_A \otimes \pi_B \|\| \sigma_A \otimes \pi_B) = \mathbb{Q}(\rho_A \|\| \sigma_A)$  by Properties (IV) and (V). Analogously, joint concavity of  $\mathbb{Q}$  implies data-processing for  $-\mathbb{Q}$ , and thus  $\mathbb{D}$ .

Next, we show that (2)  $\implies$  (1). Consider  $\rho, \sigma, \tau, \omega \in \mathcal{S}_\circ$  and  $\lambda \in (0, 1)$ . Then, the data-processing inequality implies that

$$\mathbb{D}(\lambda\rho + (1-\lambda)\tau \parallel \lambda\sigma + (1-\lambda)\omega) \leq \mathbb{D}(\lambda\rho \oplus (1-\lambda)\tau \parallel \lambda\sigma \oplus (1-\lambda)\omega). \quad (4.24)$$

If  $g$  is monotonically increasing, we find that

$$g(\mathbb{D}(\lambda\rho + (1-\lambda)\tau \parallel \lambda\sigma + (1-\lambda)\omega)) \quad (4.25)$$

$$\leq g(\mathbb{D}(\lambda\rho \oplus (1-\lambda)\tau \parallel \lambda\sigma \oplus (1-\lambda)\omega)) \quad (4.26)$$

$$= \lambda g(\mathbb{D}(\lambda\rho \parallel \lambda\sigma)) + (1-\lambda)g(\mathbb{D}((1-\lambda)\tau \parallel (1-\lambda)\omega)) \quad (4.27)$$

$$= \lambda g(\mathbb{D}(\rho \parallel \sigma)) + (1-\lambda)g(\mathbb{D}(\tau \parallel \omega)), \quad (4.28)$$

where we used property (VI) for the first equality and (V) and (IV) for the last. It follows that  $\mathbb{Q}(\cdot \parallel \cdot)$  is jointly convex. An analogous argument yields joint concavity if  $g$  is decreasing.

## 4.2.2 Minimal Quantum Rényi Divergence

Let us assume a quantum Rényi divergence  $\mathbb{D}_\alpha$  satisfies additivity (V) and the data-processing inequality (VIII). Then, for any pair of states  $\rho$  and  $\sigma$  and their  $n$ -fold products,  $\rho^{\otimes n}$  and  $\sigma^{\otimes n}$ , we have

$$\mathbb{D}_\alpha(\rho \parallel \sigma) = \frac{1}{n} \mathbb{D}_\alpha(\rho^{\otimes n} \parallel \sigma^{\otimes n}) \geq \frac{1}{n} \mathbb{D}_\alpha(\mathcal{P}_{\sigma^{\otimes n}}(\rho^{\otimes n}) \parallel \sigma^{\otimes n}), \quad (4.29)$$

where  $\mathcal{P}_\sigma(\cdot)$  is the pinching channel discussed in Sect. 2.6.3 and the quantity on the right-hand side is evaluated for two commuting and hence classical states.

So, in particular, a quantum Rényi divergence  $\mathbb{D}_\alpha$  with property (V) and (VIII) that generalizes  $D_\alpha$  must satisfy

$$\mathbb{D}_\alpha(\rho \parallel \sigma) \geq \lim_{n \rightarrow \infty} \frac{1}{n} D_\alpha(\mathcal{P}_{\sigma^{\otimes n}}(\rho^{\otimes n}) \parallel \sigma^{\otimes n}) \quad (4.30)$$

$$= \frac{1}{\alpha - 1} \log \text{Tr} \left( \left( \sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}} \right)^\alpha \right). \quad (4.31)$$

The proof of the last equality is non-trivial and will be the topic of Sect. 4.3.1. Conversely, this inequality is a necessary but not a sufficient condition for additivity and data-processing. Potentially tighter lower bounds are possible, for example by maximizing over all possible measurement maps on  $n$  systems on the right-hand side. However, we will see in the next section that the *minimal quantum Rényi divergence* (also known as *sandwiched Rényi divergence*), defined as the expression in (4.31), has all the desired properties of a quantum Rényi divergence for a large range of  $\alpha$ .



### 4.2.3 Maximal Quantum Rényi Divergence

A general upper bound can be found by considering a preparation map, using Matsumoto's elegant construction [113]. For two fixed states  $\rho$  and  $\sigma$ , consider the operator  $\Delta = \sigma^{-1/2} \rho \sigma^{-1/2}$  with spectral decomposition

$$\Delta = \sum_x \lambda_x \Pi_x, \quad \text{as well as} \quad q(x) = \text{Tr}(\sigma \Pi_x), \quad p(x) = \lambda_x q(x). \quad (4.32)$$

Then, the CPTP map  $\Lambda(\cdot) = \sum_x \langle x | \cdot | x \rangle \frac{1}{q(x)} \sqrt{\sigma} \Pi_x \sqrt{\sigma}$  satisfies

$$\Lambda(p) = \sum_x \frac{p(x)}{q(x)} \sqrt{\sigma} \Pi_x \sqrt{\sigma} = \rho, \quad \Lambda(q) = \sum_x \frac{q(x)}{q(x)} \sqrt{\sigma} \Pi_x \sqrt{\sigma} = \sigma. \quad (4.33)$$

Hence, any quantum generalization of the Rényi divergence  $\mathbb{D}_\alpha$  with data-processing (VIII) must satisfy

$$\mathbb{D}_\alpha(\rho \| \sigma) \leq D_\alpha(p \| q) = \frac{1}{\alpha - 1} \log \text{Tr} \left( \sigma^{\frac{1}{2}} (\sigma^{-\frac{1}{2}} \rho \sigma^{-\frac{1}{2}})^\alpha \sigma^{\frac{1}{2}} \right). \quad (4.34)$$

We call the quantity on the right-hand side of (4.34) the *maximal quantum Rényi divergence*. For  $\alpha \in (0, 1)$ , the term in the trace evaluates to a mean [102]. Specifically, for  $\alpha = \frac{1}{2}$  the right-hand side of (4.34) evaluates to  $-2 \log \text{Tr}(\rho \# \sigma)$ , where ‘#’ denotes the *geometric mean*. These means are jointly concave and thus we also satisfy a data-processing inequality. Furthermore,  $D_2(p \| q) = \log \text{Tr}(\rho^2 \sigma^{-1})$  is an upper bound on  $\mathbb{D}_2(\rho \| \sigma)$ . and in the limit  $\alpha \rightarrow 1$  we find that

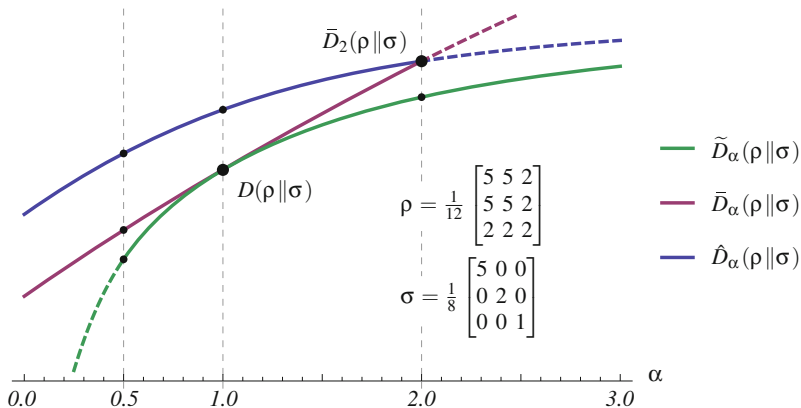
$$\mathbb{D}_1(\rho \| \sigma) \leq \text{Tr} \left( \sigma^{\frac{1}{2}} \rho \sigma^{-\frac{1}{2}} \log \left( \sigma^{-\frac{1}{2}} \rho \sigma^{-\frac{1}{2}} \right) \right) = \text{Tr} \left( \rho \log \left( \rho^{\frac{1}{2}} \sigma^{-1} \rho^{\frac{1}{2}} \right) \right). \quad (4.35)$$

The last equality follows from (2.45) and the expression on the right is the Belavkin-Staszewski relative entropy [17]. In spite of its appealing form, the maximal quantum Rényi divergence has not found many applications yet, and we will not consider it further in this text.

The minimal and maximal Rényi divergences are compared in Fig. 4.1.

### 4.2.4 Quantum Max-Divergence

The bounds in the previous subsection are not sufficient to single out a unique quantum generalization of the Rényi divergence for general  $\alpha$  (and neither are the other desirable properties discussed above), except in the limit  $\alpha \rightarrow \infty$ , where the lower bound in (4.31) and upper bound in (4.34) converge. Hence, the max-divergence has a unique quantum generalization.



**Fig. 4.1** Minimal, Petz and maximal quantum Rényi entropy (for small  $\alpha$ ). These divergences are discussed in Sects. 4.3, 4.4, and 4.2.3, respectively. *Solid lines* are used to indicate that the quantity satisfies the data-processing inequality in this range of  $\alpha$

Let us verify this now. First note that for  $\alpha \rightarrow \infty$  Eq. (4.34) yields

$$\mathbb{D}_\infty(\rho\|\sigma) \leq D_\infty(\rho\|q) = \max_x \log \lambda_x = \log \|\Delta\|_\infty = \inf\{\lambda : \rho \leq \exp(\lambda)\sigma\}. \quad (4.36)$$

So let us thus define the *quantum max-divergence* as follows [41, 139]:

**Definition 4.2** For any  $\rho, \sigma \in \mathcal{P}(A)$  with  $\rho \neq 0$ , we define the **quantum max-divergence** as

$$D_\infty(\rho\|\sigma) := \inf\{\lambda : \rho \leq \exp(\lambda)\sigma\}, \quad (4.37)$$

where we follow the usual convention that  $\inf \emptyset = \infty$ .

Using the pinching inequality (2.61), we find that

$$\rho \leq \exp(\lambda)\sigma \implies \mathcal{P}_\sigma(\rho) \leq \exp(\lambda)\sigma, \quad (4.38)$$

$$\mathcal{P}_\sigma(\rho) \leq \exp(\lambda)\sigma \implies \rho \leq |\text{spec}(\sigma)| \exp(\lambda)\sigma, \quad (4.39)$$

and, thus, the quantum max-divergence satisfies

$$D_\infty(\mathcal{P}_\sigma(\rho)\|\sigma) \leq D_\infty(\rho\|\sigma) \leq D_\infty(\mathcal{P}_\sigma(\rho)\|\sigma) + \log |\text{spec}(\sigma)|. \quad (4.40)$$

We now apply this to  $n$ -fold product states  $\rho^{\otimes n}$  and  $\sigma^{\otimes n}$  and use the fact that  $|\text{spec}(\sigma^{\otimes n})| \leq (n+1)^{d_A-1}$  grows at most polynomially in  $n$ , such that

$$0 \leq \lim_{n \rightarrow \infty} \frac{1}{n} \log |\text{spec}(\sigma)| \leq \lim_{n \rightarrow \infty} \frac{d_A - 1}{n} \log(n + 1) = 0. \quad (4.41)$$

The term thus vanishes asymptotically as  $n \rightarrow \infty$ , which means that

$$\frac{1}{n} D_\infty(\rho^{\otimes n} \parallel \sigma^{\otimes n}) \quad \text{and} \quad \frac{1}{n} D_\infty(\mathcal{P}_{\sigma^{\otimes n}}(\rho^{\otimes n}) \parallel \sigma^{\otimes n}) \quad (4.42)$$

are asymptotically equivalent. Further using that  $D_\infty$  is additive, we establish that

$$D_\infty(\rho \parallel \sigma) = \lim_{n \rightarrow \infty} \frac{1}{n} D_\infty(\rho^{\otimes n} \parallel \sigma^{\otimes n}) = \lim_{n \rightarrow \infty} \frac{1}{n} D_\infty(\mathcal{P}_{\sigma^{\otimes n}}(\rho^{\otimes n}) \parallel \sigma^{\otimes n}). \quad (4.43)$$

This argument is in fact a special case of the discussion that we will follow in Sect. 4.3.1 for general Rényi divergences.

Hence, Eq. (4.31) yields that  $\mathbb{D}_\infty(\rho \parallel \sigma) \geq D_\infty(\rho \parallel \sigma)$  for any quantum generalization of the max-divergence satisfying data-processing and additivity. We summarize these findings as follows:

**Proposition 4.3**  *$D_\infty$  is the unique quantum generalization of the max-divergence that satisfies additivity (V) and data-processing (VIII).*

We leave it as an exercise for the reader to verify that that the quantum max-divergence also satisfies Properties (I)–(X).

### 4.3 Minimal Quantum Rényi Divergence

In this section we further discuss the minimal quantum Rényi divergence mentioned in Sect. 4.2.2. In particular, we will see that the following closed formula for the minimal quantum Rényi divergence corresponds to the limit in (4.30) for all  $\alpha$ .

**Definition 4.3** Let  $\alpha \in (0, 1) \cup (1, \infty)$ , and  $\rho, \sigma \in \mathcal{S}(A)$  with  $\rho \neq 0$ . Then we define the **minimal quantum Rényi divergence** of  $\sigma$  with  $\rho$  as

$$\tilde{D}_\alpha(\rho \parallel \sigma) := \begin{cases} \frac{1}{\alpha-1} \log \frac{\|\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}}\|_\alpha^\alpha}{\text{Tr}(\rho)} & \text{if } (\alpha < 1 \wedge \rho \not\ll \sigma) \vee \rho \ll \sigma. \\ +\infty & \text{else} \end{cases} \quad (4.44)$$

Moreover,  $\tilde{D}_0$ ,  $\tilde{D}_1$  and  $\tilde{D}_\infty$  are defined as limits of  $\tilde{D}_\alpha$  for  $\alpha \rightarrow \{0, 1, \infty\}$ .

In Sect. 4.3.2 we will see that  $\tilde{D}_\infty(\rho \parallel \sigma) = D_\infty(\rho \parallel \sigma)$  (cf. Definition 4.2). The minimal quantum Rényi divergence is also called ‘quantum Rényi divergence’ [122] and ‘sandwiched quantum Rényi relative entropy’ [175] in the literature, but we

propose here to call it *minimal* quantum Rényi divergence since it is the smallest quantum Rényi divergence that still satisfies the crucial data-processing inequality as seen in (4.31). Thus, it is the minimal quantum Rényi divergence for which we can expect operational significance.

By inspection, it is evident that this quantity satisfies isometric invariance (II+), normalization (III+), additivity (V), and general mean (VI). Continuity (I) also holds, but one has to be a bit more careful since we are employing the generalized inverse in the definition. (See [122] for a proof of continuity when the rank of  $\rho$  or  $\sigma$  changes.)

### 4.3.1 Pinching Inequalities

The goal of this section is to establish that  $\tilde{D}_\alpha$  is contractive under pinching maps and can be asymptotically achieved by the respective pinched quantity. For this purpose, let us investigate some properties of

$$\tilde{Q}_\alpha(\rho\|\sigma) := \left\| \sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}} \right\|_\alpha^\alpha = \text{Tr} \left( \left( \sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}} \right)^\alpha \right) \quad (4.45)$$

$$= \text{Tr} \left( \left( \rho^{\frac{1}{2}} \sigma^{\frac{1-\alpha}{\alpha}} \rho^{\frac{1}{2}} \right)^\alpha \right). \quad (4.46)$$

for  $\rho, \sigma \in \mathcal{S}_\circ(A)$  with  $\rho \ll \sigma$ . First, we find that it is monotone under the pinching channel [122].

**Lemma 4.2** *For  $\alpha > 1$ , we have*

$$\tilde{Q}_\alpha(\rho\|\sigma) \geq \tilde{Q}_\alpha(\mathcal{P}_\sigma(\rho)\|\sigma) \quad (4.47)$$

and the opposite inequality holds for  $\alpha \in (0, 1)$ .

*Proof* We have  $\sigma^{\frac{1-\alpha}{2\alpha}} \mathcal{P}_\sigma(\rho) \sigma^{\frac{1-\alpha}{2\alpha}} = \mathcal{P}_\sigma(\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}})$  since the pinching projectors commute with  $\sigma$ . For  $\alpha > 1$ , we find

$$\tilde{Q}_\alpha(\mathcal{P}_\sigma(\rho)\|\sigma) = \left\| \mathcal{P}_\sigma(\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}}) \right\|_\alpha \leq \left\| \sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}} \right\|_\alpha = \tilde{Q}_\alpha(\rho\|\sigma), \quad (4.48)$$

where the inequality follows from the pinching inequality for norms (3.4). For  $\alpha < 1$ , the operator Jensen inequality (2.64) establishes that  $(\mathcal{P}_\sigma(\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}}))^\alpha \geq \mathcal{P}_\sigma((\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}})^\alpha)$ . Thus,

$$\tilde{Q}_\alpha(\mathcal{P}_\sigma(\rho)\|\sigma) \geq \text{Tr} \left( \mathcal{P}_\sigma \left( (\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}})^\alpha \right) \right) = \tilde{Q}_\alpha(\rho\|\sigma). \quad (4.49)$$

The following general purpose inequalities will turn out to be very useful:

**Lemma 4.3** *For any  $\rho \leq \rho'$ , we have  $\tilde{Q}_\alpha(\rho\|\sigma) \leq \tilde{Q}_\alpha(\rho'\|\sigma)$ . Furthermore, if  $\sigma \leq \sigma'$  and  $\alpha > 1$ , we have*

$$\tilde{Q}_\alpha(\rho\|\sigma) \geq \tilde{Q}_\alpha(\rho\|\sigma') \quad (4.50)$$

and the opposite inequality holds for  $\alpha \in [\frac{1}{2}, 1)$ .

*Proof* Set  $c = \frac{1-\alpha}{\alpha}$ . If  $\rho \leq \rho'$ , then  $\sigma^{\frac{c}{2}}\rho\sigma^{\frac{c}{2}} \leq \sigma^{\frac{c}{2}}\rho'\sigma^{\frac{c}{2}}$  and the first statement follows from the monotonicity of the trace of monotone functions (2.46).

To prove the second statement for  $\alpha \in [\frac{1}{2}, 1)$ , we note that  $t \mapsto t^c$  is operator monotone. Hence,

$$\rho^{\frac{1}{2}}\sigma^{\frac{1-\alpha}{\alpha}}\rho^{\frac{1}{2}} \leq \rho^{\frac{1}{2}}\sigma'^{\frac{1-\alpha}{\alpha}}\rho^{\frac{1}{2}} \quad (4.51)$$

and the statement again follows by (2.46). Analogously, for  $\alpha > 1$  we find that  $t \mapsto t^{-c}$  is operator monotone and the inequality goes in the opposite direction.  $\square$

In particular, the second statement establishes the dominance property (X). On the other hand, we can employ the first inequality to get a very general pinching inequality. For any CP maps  $\mathcal{E}$  and  $\mathcal{F}$ , and any  $\alpha > 0$ , we have

$$\tilde{Q}_\alpha(\mathcal{E}(\rho)\|\mathcal{F}(\sigma)) \leq |\text{spec}(\sigma)|^\alpha \tilde{Q}_\alpha(\mathcal{E}(\mathcal{P}_\sigma(\rho))\|\mathcal{F}(\sigma)). \quad (4.52)$$

A more delicate analysis is possible for the pinching case when  $\alpha \in (0, 2]$ . We establish the following stronger bounds [80]:

**Lemma 4.4** *For  $\alpha \in [1, 2]$ , we have*

$$\tilde{Q}_\alpha(\rho\|\sigma) \leq |\text{spec}(\sigma)|^{\alpha-1} \tilde{Q}_\alpha(\mathcal{P}_\sigma(\rho)\|\sigma) \quad (4.53)$$

and the opposite inequality holds for  $\alpha \in (0, 1]$ .

*Proof* By the pinching inequality, we have  $\rho \leq |\text{spec}(\sigma)| \mathcal{P}_\sigma(\rho)$ . Then, we write

$$\tilde{Q}_\alpha(\rho\|\sigma) = \text{Tr} \left( \left( \sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}} \right)^{\alpha-1} \sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}} \right) \quad (4.54)$$

Then, for  $\alpha \in (1, 2]$ , we use the fact that  $t \mapsto t^{\alpha-1}$  is operator monotone, such that the pinching inequality yields the following bound:

$$\tilde{Q}_\alpha(\rho\|\sigma) \leq |\text{spec}(\sigma)|^{\alpha-1} \text{Tr} \left( \left( \sigma^{\frac{1-\alpha}{2\alpha}} \mathcal{P}_\sigma(\rho) \sigma^{\frac{1-\alpha}{2\alpha}} \right)^{\alpha-1} \sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}} \right). \quad (4.55)$$

Now, note that the pinching projectors commute with all operators except for the single  $\rho$  in the term that we pulled out initially, and hence we can pinch this operator “for free”. This yields

$$\mathrm{Tr} \left( \left( \sigma^{\frac{1-\alpha}{2\alpha}} \mathcal{P}_\sigma(\rho) \sigma^{\frac{1-\alpha}{2\alpha}} \right)^{\alpha-1} \sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}} \right) = \tilde{Q}_\alpha(\mathcal{P}_\sigma(\rho) \parallel \sigma) \quad (4.56)$$

and we have established Eq. (4.53). Similarly, we proceed for  $\alpha \in (0, 1)$ , where the pinching inequality again yields  $\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}} \leq |\mathrm{spec}(\sigma)| \sigma^{\frac{1-\alpha}{2\alpha}} \mathcal{P}_\sigma(\rho) \sigma^{\frac{1-\alpha}{2\alpha}}$ , and thus we have

$$\left( \sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}} \right)^{\alpha-1} \geq |\mathrm{spec}(\sigma)|^{\alpha-1} \left( \sigma^{\frac{1-\alpha}{2\alpha}} \mathcal{P}_\sigma(\rho) \sigma^{\frac{1-\alpha}{2\alpha}} \right)^{\alpha-1} \quad (4.57)$$

on the support of  $\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}}$ . Combining this with the development leading to (4.53) yields the desired bound.  $\square$

A combination of the above Lemmas yields an alternative characterization of the minimal quantum Rényi divergence in terms of an asymptotic limit of classical Rényi divergences, as desired.

**Proposition 4.4** For  $\rho, \sigma \in \mathcal{S}(A)$  with  $\rho \neq 0$ ,  $\rho \ll \sigma$ , and  $\alpha \geq 0$ , we have

$$\tilde{D}_\alpha(\rho \parallel \sigma) = \lim_{n \rightarrow \infty} \frac{1}{n} D_\alpha(\mathcal{P}_{\sigma^{\otimes n}}(\rho^{\otimes n}) \parallel \sigma^{\otimes n}).$$

*Proof* It suffices to show the statement for  $\rho, \sigma \in \mathcal{S}_\circ(A)$ . Summarizing Lemmas 4.2–4.4 yields

$$\tilde{D}_\alpha(\mathcal{P}_\sigma(\rho) \parallel \sigma) \geq \tilde{D}_\alpha(\rho \parallel \sigma) \quad (4.58)$$

$$\geq \tilde{D}_\alpha(\mathcal{P}_\sigma(\rho) \parallel \sigma) - \begin{cases} \log |\mathrm{spec}(\sigma)| & \text{for } \alpha \in (0, 1) \cup (1, 2] \\ \frac{\alpha}{\alpha-1} \log |\mathrm{spec}(\sigma)| & \text{for } \alpha > 2 \end{cases}. \quad (4.59)$$

Since  $\frac{\alpha}{\alpha-1} < 2$  for  $\alpha > 2$ , we can replace the correction term on the right-hand side by  $2 \log |\mathrm{spec}(\sigma)|$ , which has the nice feature that it is independent of  $\alpha$ . Hence, for  $n$ -fold product states, we have

$$\left| \frac{1}{n} \tilde{D}_\alpha(\mathcal{P}_{\sigma^{\otimes n}}(\rho^{\otimes n}) \parallel \sigma^{\otimes n}) - \tilde{D}_\alpha(\rho \parallel \sigma) \right| \leq \frac{2}{n} \log |\mathrm{spec}(\sigma^{\otimes n})|. \quad (4.60)$$

The result then follows by employing (4.41) in the limit  $n \rightarrow \infty$ .

Finally, we note that the convergence is uniform in  $\alpha$  (as well as  $\rho$  and  $\sigma$ ), and thus the equality also holds for the limiting cases  $\tilde{D}_0$ ,  $\tilde{D}_1$  and  $\tilde{D}_\infty$ .  $\square$

The strength of this result lies in the fact that we immediately inherit some properties of the classical Rényi divergence. More precisely,  $\alpha \mapsto \log \tilde{Q}_\alpha(\rho \parallel \sigma)$  is the point-wise limit of a sequence of convex functions, and thus also convex.

**Corollary 4.2** *The function  $\alpha \mapsto \log \tilde{Q}_\alpha(\rho\|\sigma)$  is convex, and  $\alpha \mapsto \tilde{D}_\alpha(\rho\|\sigma)$  is monotonically increasing.*

### 4.3.2 Limits and Special Cases

Instead of evaluating the limits for  $\alpha \rightarrow \infty$  explicitly as in [122], we can take advantage of the fact that Proposition 4.4 already gives an alternative characterization of the limiting quantity in terms of the pinched divergence. Hence, as Eq. (4.43) reveals, the limit is the quantum max-divergence of Definition 4.2 as claimed earlier.

In the limit  $\alpha \rightarrow 1$ , we expect to find the ‘ordinary’ quantum relative entropy or quantum divergence, first studied by Umegaki [166].

**Definition 4.4** For any state  $\rho \in \mathcal{S}(A)$  with  $\rho \neq 0$  and any  $\sigma \in \mathcal{S}(A)$ , we define the **quantum divergence** of  $\sigma$  with  $\rho$  as

$$D(\rho\|\sigma) := \begin{cases} \frac{\text{Tr}(\rho(\log \rho - \log \sigma))}{\text{Tr}(\rho)} & \text{if } \rho \ll \sigma \\ +\infty & \text{else} \end{cases}. \quad (4.61)$$

This reduces to the Kullback–Leibler (KL) divergence [103] if  $\rho$  and  $\sigma$  are classical (commuting) operators. We now prove that  $\tilde{D}_1(\rho\|\sigma) = D(\rho\|\sigma)$ .

**Proposition 4.5** *For  $\rho, \sigma \in \mathcal{P}(A)$  with  $\rho \neq 0$ , we find that  $\tilde{D}_1(\rho\|\sigma)$  equals*

$$\lim_{\alpha \searrow 1} \tilde{D}_\alpha(\rho\|\sigma) = \lim_{\alpha \nearrow 1} \tilde{D}_\alpha(\rho\|\sigma) = D(\rho\|\sigma). \quad (4.62)$$

The proof proceeds by finding an explicit expression for the limiting divergence [122, 175]. (Alternatively one could show that the quantum relative entropy is achieved by pinching, as is done in [73].) We follow [175] here:

*Proof* Since the proposed limit satisfies the normalization property (III+), it is sufficient to evaluate the limit for  $\rho, \sigma \in \mathcal{S}_\circ(A)$ . Furthermore, we restrict our attention to the case  $\rho \ll \sigma$ . By l’Hôpital’s rule and the fact that  $\tilde{Q}_1(\rho\|\sigma) = 1$ , we have

$$\lim_{\alpha \searrow 1} \tilde{D}_\alpha(\rho\|\sigma) = \lim_{\alpha \nearrow 1} \tilde{D}_\alpha(\rho\|\sigma) = \log(e) \cdot \left. \frac{d}{d\alpha} Q_\alpha(\rho\|\sigma) \right|_{\alpha=1}. \quad (4.63)$$

To evaluate this derivative, it is convenient to introduce a continuously differentiable two-parameter function (for fixed  $\rho$  and  $\sigma$ ) as follows:

$$q(r, z) = \text{Tr} \left( (\sigma^{\frac{r}{2}} \rho \sigma^{\frac{r}{2}})^z \right) \quad \text{with} \quad r(\alpha) = \frac{1-\alpha}{\alpha} \quad \text{and} \quad z(\alpha) = \alpha \quad (4.64)$$

such that  $\frac{\partial r}{\partial \alpha} = -\frac{1}{\alpha^2}$  and  $\frac{\partial z}{\partial \alpha} = 1$  and therefore

$$\frac{d}{d\alpha} Q_\alpha(\rho \parallel \sigma) \Big|_{\alpha=1} = -\frac{1}{\alpha^2} \frac{\partial}{\partial r} q(r, z) \Big|_{\alpha=1} + \frac{\partial}{\partial z} q(r, z) \Big|_{\alpha=1} \quad (4.65)$$

$$= -\frac{\partial}{\partial r} \text{Tr}(\sigma^r \rho) \Big|_{r=0} + \frac{\partial}{\partial z} \text{Tr}(\rho^z) \Big|_{z=1} = \text{Tr}(\rho(\ln \rho - \ln \sigma)). \quad (4.66)$$

In the penultimate step we exchanged the limits with the differentiation and in the last step we simply used the fact that the derivate commutes with the trace and that  $\frac{d}{dz} \rho^z = \ln(\rho) \rho^z$ .  $\square$

Let us have a look at two other special cases that are important for applications. First, at  $\alpha = \{\frac{1}{2}, 2\}$ , we find the negative logarithm of the quantum fidelity and the *collision relative entropy* [139], respectively. For  $\rho, \sigma \in \mathcal{S}(A)$ , we have

$$\tilde{D}_{1/2}(\rho \parallel \sigma) = -\log F(\rho, \sigma), \quad \tilde{D}_2(\rho \parallel \sigma) = \log \text{Tr}(\rho \sigma^{-\frac{1}{2}} \rho \sigma^{-\frac{1}{2}}). \quad (4.67)$$

### 4.3.3 Data-Processing Inequality

Here we show that  $\tilde{D}_\alpha$  satisfies the data-processing inequality for  $\alpha \geq \frac{1}{2}$ . First, we show that our pinching inequalities in fact already imply the data-processing inequality for  $\alpha > 1$ , following an instructive argument due to Mosonyi and Ogawa in [119]. (For  $\alpha \in [\frac{1}{2}, 1)$  we will need a completely different argument.)

#### From Pinching to Measuring and Data-Processing

First, we restrict our attention to  $\alpha > 1$ . According to (4.52), for any measurement map  $\mathcal{M} \in \text{CPTP}(A, X)$  with POVM elements  $\{M_x\}_x$ , we find

$$\frac{\tilde{Q}_\alpha(\mathcal{M}(\rho) \parallel \mathcal{M}(\sigma))}{|\text{spec}(\sigma)|^\alpha} \leq \tilde{Q}_\alpha(\mathcal{M}(\mathcal{P}_\sigma(\rho)) \parallel \mathcal{M}(\sigma)) \quad (4.68)$$

$$= \sum_x \left( \text{Tr}(M_x \mathcal{P}_\sigma(\rho)) \right)^\alpha \left( \text{Tr}(M_x \sigma) \right)^{1-\alpha} \quad (4.69)$$

$$= \sum_x \left( \text{Tr}(\mathcal{P}_\sigma(M_x) \mathcal{P}_\sigma(\rho)) \right)^\alpha \left( \text{Tr}(\mathcal{P}_\sigma(M_x) \sigma) \right)^{1-\alpha}. \quad (4.70)$$



Now, note that  $W(x|a) = \langle a | \mathcal{P}_\sigma(M_x) | a \rangle$  is a classical channel for states that are diagonal in the eigenbasis  $\{|a\rangle\}_a$  of  $\sigma$ . Hence the classical data-processing inequality together with Lemma 4.2 yields

$$|\text{spec}(\sigma)|^{-\alpha} \tilde{Q}_\alpha(\mathcal{M}(\rho) \parallel \mathcal{M}(\sigma)) \leq \tilde{Q}_\alpha(\mathcal{P}_\sigma(\rho) \parallel \sigma) \leq \tilde{Q}_\alpha(\rho \parallel \sigma). \quad (4.71)$$

Using a by now standard argument, we consider  $n$ -fold product states  $\rho^{\otimes n}$  and  $\sigma^{\otimes n}$  and a product measurement  $\mathcal{M}^{\otimes n}$  in order to get rid of the spectral term in the limit as  $n \rightarrow \infty$ . This yields

$$\tilde{D}_\alpha(\rho \parallel \sigma) \geq \tilde{D}_\alpha(\mathcal{M}(\rho) \parallel \mathcal{M}(\sigma)) \quad (4.72)$$

for all measurement maps  $\mathcal{M}$ .

Combining this with Proposition 4.4 and interpreting the pinching map as a measurement in the eigenbasis of  $\sigma$ , we have established that, for  $\alpha > 1$ , the minimal quantum Rényi divergence is *asymptotically achievable by a measurement*:

$$\tilde{D}_\alpha(\rho \parallel \sigma) = \lim_{n \rightarrow \infty} \frac{1}{n} \max \left\{ D_\alpha(\mathcal{M}_n(\rho^{\otimes n}) \parallel \mathcal{M}_n(\sigma^{\otimes n})) : \mathcal{M}_n \in \text{CPTP}(A^n, X) \right\}. \quad (4.73)$$

We will discuss this further below. Using the representation in (4.73) we can derive the data-processing inequality using a very general argument.

**Proposition 4.6** *Let  $\mathbb{D}_\alpha$  be a quantum Rényi divergence satisfying (4.73). Then, it also satisfies data-processing (VIII).*

*Proof* We show that  $\mathbb{D}_\alpha(\rho \parallel \sigma) \geq \mathbb{D}_\alpha(\mathcal{E}(\rho) \parallel \mathcal{E}(\sigma))$  for all  $\mathcal{E} \in \text{CPTP}(A, B)$  and  $\rho, \sigma \in \mathcal{S}(A)$ .

First note that since  $\mathcal{E}$  is trace-preserving,  $\mathcal{E}^\dagger$  is unital. For every measurement map  $\mathcal{M} \in \text{CPTP}(B, X)$  consisting of POVM elements  $\{M_x\}_x$ , we define the measurement map  $\mathcal{M}^\mathcal{E} \in \text{CPTP}(A, X)$  that consists of the POVM elements  $\{\mathcal{E}^\dagger(M_x)\}_x$ . Then, using (4.73) twice, we find

$$\begin{aligned} & \mathbb{D}_\alpha(\mathcal{E}(\rho) \parallel \mathcal{E}(\sigma)) \\ &= \lim_{n \rightarrow \infty} \frac{1}{n} \sup \left\{ D_\alpha(\mathcal{M}_n(\mathcal{E}(\rho)^{\otimes n}) \parallel \mathcal{M}_n(\mathcal{E}(\sigma)^{\otimes n})) : \mathcal{M}_n \in \text{CPTP}(B^n, X) \right\} \end{aligned} \quad (4.74)$$

$$= \lim_{n \rightarrow \infty} \frac{1}{n} \sup \left\{ D_\alpha(\mathcal{M}_n^{\mathcal{E}^{\otimes n}}(\rho^{\otimes n}) \parallel \mathcal{M}_n^{\mathcal{E}^{\otimes n}}(\sigma^{\otimes n})) : \mathcal{M}_n \in \text{CPTP}(B^n, X) \right\} \quad (4.75)$$

$$\leq \lim_{n \rightarrow \infty} \frac{1}{n} \sup \left\{ D_\alpha(\mathcal{M}_n(\rho^{\otimes n}) \parallel \mathcal{M}_n(\sigma^{\otimes n})) : \mathcal{M}_n \in \text{CPTP}(A^n, X) \right\} \quad (4.76)$$

$$= \mathbb{D}_\alpha(\rho \parallel \sigma). \quad (4.77)$$

This concludes the proof.  $\square$

### Data-Processing via Joint Concavity

Unfortunately, the first part of the above argument leading to (4.73) only goes through for  $\alpha > 1$  (and consequently in the limits  $\alpha \rightarrow 1$  and  $\alpha \rightarrow \infty$ ). However, the data-processing inequality holds more generally for all  $\alpha \geq \frac{1}{2}$ , as was shown by Frank and Lieb [57].

It thus remains to show data-processing for  $\alpha \in [\frac{1}{2}, 1)$ . Here we show the following equivalent statement (cf. Proposition 4.2):

**Proposition 4.7** *The map  $(\rho, \sigma) \mapsto \tilde{Q}_\alpha(\rho\|\sigma)$  is jointly concave for  $\alpha \in [\frac{1}{2}, 1)$ .*

*Proof* First, we express  $\tilde{Q}_\alpha$  as a minimization problem. To do this, we use (3.16) and set  $c = \frac{1-\alpha}{\alpha} \in (0, 1]$ ,  $M = \sigma^{\frac{c}{2}} \rho \sigma^{\frac{c}{2}}$ , and  $N = \sigma^{-\frac{c}{2}} H \sigma^{-\frac{c}{2}}$  to find

$$\tilde{Q}_\alpha(\rho\|\sigma) = \text{Tr} \left( (\sigma^{\frac{c}{2}} \rho \sigma^{\frac{c}{2}})^\alpha \right) \leq \alpha \text{Tr}(H\rho) + (1-\alpha) \text{Tr} \left( (\sigma^{-\frac{c}{2}} H \sigma^{-\frac{c}{2}})^{-\frac{1}{c}} \right). \quad (4.78)$$

for all  $H \geq 0$  with  $H \gg \rho$  and equality can be achieved. Thus, we can write

$$\tilde{Q}_\alpha(\rho\|\sigma) = \min \left\{ \alpha \text{Tr}(H\rho) + (1-\alpha) \text{Tr} \left( (H^{-\frac{1}{2}} \sigma^c H^{-\frac{1}{2}})^{\frac{1}{c}} \right) : H \geq 0, H \gg \rho \right\}. \quad (4.79)$$

This nicely splits the contributions of  $\rho$  and  $\sigma$  and we can deal with them separately. The term  $\text{Tr}(H\rho)$  is linear and thus concave in  $\rho$ . Next, we want to show that the second term is concave in  $\sigma$ . To do this, we further decompose it as follows, using essentially the same ideas that we used above. First, using (3.16), we find

$$\text{Tr} \left( H^{-\frac{1}{2}} \sigma^c H^{-\frac{1}{2}} X^{1-c} \right) \leq c \text{Tr} \left( (H^{-\frac{1}{2}} \sigma^c H^{-\frac{1}{2}})^{\frac{1}{c}} \right) + (1-c) \text{Tr}(X), \quad (4.80)$$

which allows us to write

$$\text{Tr} \left( (H^{-\frac{1}{2}} \sigma^c H^{-\frac{1}{2}})^{\frac{1}{c}} \right) = \max \left\{ \frac{1}{c} \text{Tr} \left( H^{-\frac{1}{2}} \sigma^c H^{-\frac{1}{2}} X^{1-c} \right) - \frac{1-c}{c} \text{Tr}(X) : X \geq 0 \right\}. \quad (4.81)$$

Since  $c \in (0, 1)$ , Lieb's concavity theorem (2.50) reveals that the function we maximize over is jointly concave in  $\sigma$  and  $X$ . Note that generally the maximum of concave functions is not necessarily concave, but joint concavity in  $\sigma$  and  $X$  is sufficient to ensure that the maximum is concave in  $\sigma$ . Hence,  $\tilde{Q}_\alpha(\rho\|\sigma)$  is the minimum of a jointly concave function, and thus jointly concave.  $\square$

The same proof strategy can be used to show that  $\tilde{Q}_\alpha(\rho\|\sigma)$  is jointly convex for  $\alpha > 1$ , but we already know that this holds due to our previous argument in Sect. 4.3.3 that established the data-processing inequality directly.

## Summary and Remarks

Let us now summarize the results of this subsection in the following theorem.

**Theorem 4.1** *Let  $\alpha \geq \frac{1}{2}$  and  $\rho, \sigma \in \mathcal{S}(A)$  with  $\rho \neq 0$ . The minimal quantum Rényi divergence has the following properties:*

- *The functional  $(\rho, \sigma) \mapsto \tilde{Q}_\alpha(\rho\|\sigma)$  is jointly concave for  $\alpha \in (\frac{1}{2}, 1)$  and jointly convex for  $\alpha \in (0, \infty)$ .*
- *The functional  $(\rho, \sigma) \mapsto \tilde{D}_\alpha(\rho\|\sigma)$  is jointly convex for  $\alpha \in (\frac{1}{2}, 1]$ .*
- *For every  $\mathcal{E} \in \text{CPTP}(A, B)$ , the data-processing inequality holds, i.e.*

$$\tilde{D}_\alpha(\rho\|\sigma) \geq \tilde{D}_\alpha(\mathcal{E}(\rho)\|\mathcal{E}(\sigma)). \quad (4.82)$$

- *It is asymptotically achievable by a measurement, i.e.*

$$\tilde{D}_\alpha(\rho\|\sigma) = \lim_{n \rightarrow \infty} \frac{1}{n} \max \left\{ D_\alpha(\mathcal{M}_n(\rho^{\otimes n})\|\mathcal{M}_n(\sigma^{\otimes n})) : \mathcal{M}_n \in \text{CPTP}(A^n, X) \right\}. \quad (4.83)$$

A few remarks are in order here. First, note that one could potentially hope that the limit  $n \rightarrow \infty$  in (4.83) is not necessary. However, except for the two boundary points  $\alpha = \frac{1}{2}$  and  $\alpha = \infty$ , it is generally not sufficient to just consider measurements on a single system. (This effect is also called “information locking”.)

For  $\alpha \in \{\frac{1}{2}, \infty\}$ , we have in fact (without proof)

$$\tilde{D}_\alpha(\rho\|\sigma) = \max \left\{ \tilde{D}_\alpha(\mathcal{M}(\rho)\|\mathcal{M}(\sigma)) : \mathcal{M} \in \text{CPTP}(A, X) \right\}, \quad (4.84)$$

which has an interesting consequence. Namely, if we go through the proof of Proposition 4.6 we realize that we never use the fact that  $\mathcal{E}$  is completely positive, and in fact the data-processing inequality holds for all positive trace-preserving maps. Generally, for all  $\alpha$ , the data-processing inequality holds if  $\mathcal{E}^{\otimes n}$  is positive for all  $n$ , which is also strictly weaker than complete positivity.

The data-processing inequality together with definiteness of the classical Rényi divergence also establishes definiteness (VII-) of the minimal quantum Rényi divergence for  $\alpha \geq \frac{1}{2}$ , and thus of all quantum Rényi divergences. Namely, if  $\rho \neq \sigma$ , then there exists a measurements (for example an informationally complete measurement)  $\mathcal{M}$  such that  $\mathcal{M}(\rho) \neq \mathcal{M}(\sigma)$ , and thus

$$\tilde{D}_\alpha(\rho\|\sigma) \geq D_\alpha(\mathcal{M}(\rho)\|\mathcal{M}(\sigma)) > 0. \quad (4.85)$$

This completes the discussion of the minimal quantum Rényi divergence.

The minimal quantum Rényi divergences satisfy Properties (I)–(X) for  $\alpha \geq \frac{1}{2}$ , and thus constitute a family of Rényi divergences according to Definition 4.1.

## 4.4 Petz Quantum Rényi Divergence

A straight-forward generalization of the classical expression to quantum states is given by the following expression, which was originally investigated by Petz [132].

**Definition 4.5** Let  $\alpha \in (0, 1) \cup (1, \infty)$ , and  $\rho, \sigma \in \mathcal{S}(A)$  with  $\rho \neq 0$ . Then we define the **Petz quantum Rényi divergence** of  $\sigma$  with  $\rho$  as

$$\bar{D}_\alpha(\rho\|\sigma) := \begin{cases} \frac{1}{\alpha-1} \log \frac{\text{Tr}(\rho^\alpha \sigma^{1-\alpha})}{\text{Tr}(\rho)} & \text{if } (\alpha < 1 \wedge \rho \not\ll \sigma) \vee \rho \ll \sigma \\ +\infty & \text{else} \end{cases}. \quad (4.86)$$

Moreover,  $\bar{D}_0$  and  $\bar{D}_1$  are defined as the respective limits of  $\bar{D}_\alpha$  for  $\alpha \rightarrow \{0, 1\}$ .

This quantity turns out to have a clear operational interpretation in binary hypothesis testing, where it appears in the quantum generalization of the Chernoff and Hoeffding bounds. More surprisingly, it is also connected to the minimal quantum Rényi divergence via duality relations for conditional entropies, as we will see in the next chapter.

We could as well have restricted the definition to  $\alpha \in [0, 2]$  since the quantity appears not to be useful outside this range. For  $\alpha = 2$  it matches the maximal quantum Rényi divergence (cf. Fig. 4.1) and it is also evident that

$$\bar{Q}_\alpha(\rho\|\sigma) := \text{Tr}(\rho^\alpha \sigma^{1-\alpha}) \quad (4.87)$$

is not convex in  $\rho$  (for general  $\sigma$ ) since  $\rho^\alpha$  is not operator convex for  $\alpha > 2$ .

### 4.4.1 Data-Processing Inequality

As a direct consequence of the Lieb concavity theorem and the Ando convexity theorem in (2.50), we find the following.

**Proposition 4.8** *The functional  $\bar{Q}_\alpha(\rho\|\sigma)$  is jointly concave for  $\alpha \in (0, 1)$  and jointly convex for  $\alpha \in (1, 2]$ .*

In particular, the Petz quantum Rényi divergence  $\bar{D}_\alpha$  thus satisfies the data-processing inequality. As such, we must also have

$$\bar{D}_\alpha(\rho\|\sigma) \geq \tilde{D}_\alpha(\rho\|\sigma) \quad (4.88)$$

since the latter quantity is the smallest quantity that satisfies data-processing. This inequality is in fact also a direct consequence of the Araki–Lieb–Thirring trace inequalities [5, 108], which we will not discuss further here.

Alternatively, the function  $\bar{Q}_\alpha$  can be seen as a Petz quasi-entropy [132] (see also [85]). For this purpose, using the notation of Sect. 2.4.1, let us write

$$\bar{Q}_\alpha(\rho\|\sigma) = \text{Tr}(\rho^\alpha \sigma^{1-\alpha}) = \langle \Psi | \sigma^{\frac{1}{2}} f_\alpha(\sigma^{-1} \otimes \rho^T) \sigma^{\frac{1}{2}} | \Psi \rangle \quad (4.89)$$

where  $f_\alpha : t \mapsto t^\alpha$  is operator concave or convex for  $\alpha \in (0, 1)$  and  $\alpha \in (1, 2]$ . Petz used a variation of this representation to show the data-processing inequality.

We leave it as an exercise to verify the remaining properties mentioned in Sects. 4.1.1 and 4.1.2 for the Petz Rényi divergence.

The Petz quantum Rényi divergences satisfy Properties (I)–(X) for  $\alpha \in (0, 2]$ .

#### 4.4.2 Nussbaum–Szkoła Distributions

The following representation due to Nussbaum and Szkoła [127] turns out to be quite useful in applications, and also allows us to further investigate the divergence. Let us fix  $\rho, \sigma \in \mathcal{S}_o(A)$  and write their eigenvalue decomposition as

$$\rho = \sum_x \lambda_x |e_x\rangle \langle e_x|_A \quad \text{and} \quad \sigma = \sum_y \mu_y |f_y\rangle \langle f_y|. \quad (4.90)$$

Then, the two probability mass functions

$$P_{XY}^{[\rho, \sigma]}(x, y) = \lambda_x | \langle e_x | f_y \rangle |^2 \quad \text{and} \quad Q_{XY}^{[\rho, \sigma]}(x, y) = \mu_y | \langle e_x | f_y \rangle |^2 \quad (4.91)$$

mimic the Petz quantum divergence of the quantum states  $\rho$  and  $\sigma$ . Namely, they satisfy

$$\bar{D}_\alpha(\rho\|\sigma) = D_\alpha \left( P_{XY}^{[\rho, \sigma]} \parallel Q_{XY}^{[\rho, \sigma]} \right) \quad \text{for all } \alpha \geq 0. \quad (4.92)$$

Moreover, these distributions inherit some important properties of  $\rho$  and  $\sigma$ . For example,  $\rho \ll \sigma \iff P^{[\rho, \sigma]} \ll Q^{[\rho, \sigma]}$  and for product states we have

$$P^{[\rho \otimes \tau, \sigma \otimes \omega]} = P^{[\rho, \sigma]} \otimes P^{[\tau, \omega]}. \quad (4.93)$$

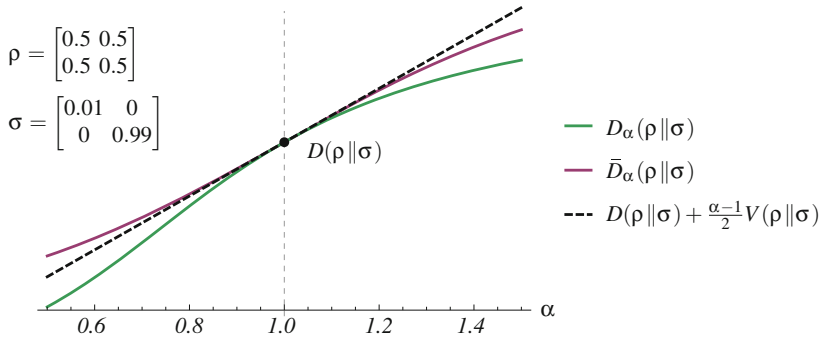


Fig. 4.2 Minimal and Petz quantum Rényi entropy around  $\alpha = 1$

Last but not least, since this representation is independent of  $\alpha$ , we are able to lift the convexity, monotonicity and limiting properties of  $\alpha \mapsto D_\alpha$  to the quantum regime—as a corollary of the respective classical properties.

**Corollary 4.3** *The function  $\alpha \mapsto \log \tilde{Q}_\alpha(\rho\|\sigma)$  is convex,  $\alpha \mapsto \tilde{D}_\alpha(\rho\|\sigma)$  is monotonically increasing, and*

$$\bar{D}_1(\rho\|\sigma) = \frac{\text{Tr}(\rho(\log \rho - \log \sigma))}{\text{Tr}(\rho)}. \tag{4.94}$$

So, in particular,  $\bar{D}_1(\rho\|\sigma) = \tilde{D}_1(\rho\|\sigma)$ . This means that these two curves are tangential at this point and their first derivatives agree (cf. Fig. 4.2).

**First Derivative at  $\alpha = 1$**

In fact, the Nussbaum–Szkola representation gives us a simple means to evaluate the first derivative of  $\alpha \mapsto \bar{D}_\alpha(\rho\|\sigma)$  and  $\alpha \mapsto \tilde{D}_\alpha(\rho\|\sigma)$  at  $\alpha = 1$ , which will turn out to be useful later.

In order to do this, let us first take a step back and evaluate the derivative for classical probability mass functions  $\rho_X, \sigma_X \in \mathcal{S}_o(X)$ . Substituting  $\alpha = 1 + \nu$  and introducing the *log-likelihood ratio* as a random variable  $Z(X) = \ln(\rho(X)/\sigma(X))$ , where  $X$  is distributed according to the law  $X \leftarrow \rho_X$ , we find

$$D_{1+\nu}(\rho_X\|\sigma_X) = \frac{1}{\nu} \log \sum_x \rho(x) \left( \frac{\rho(x)}{\sigma(x)} \right)^\nu = \frac{\log \mathbb{E}(e^{\nu Z})}{\nu} = \log(e) \frac{G(\nu)}{\nu}, \tag{4.95}$$

where  $G(\nu)$  is the cumulant generating function of  $Z$ .

Clearly,  $G(0) = 0$ . Moreover, using l'Hôpital's rule, its first derivative at  $\nu = 0$  is

$$\lim_{\nu \rightarrow 0} \left( \frac{d}{d\nu} \frac{G(\nu)}{\nu} \right) = \lim_{\nu \rightarrow 0} \frac{\nu G'(\nu) - G(\nu)}{\nu^2} \quad (4.96)$$

$$= \lim_{\nu \rightarrow 0} \frac{G'(\nu) + \nu G''(\nu) - G'(\nu)}{2\nu} = \frac{G''(0)}{2}, \quad (4.97)$$

which is one half of the second cumulant of  $Z$ . The second cumulant simply equals the second central moment, or variance, of the log-likelihood ratio  $Z$ .

$$G''(0) = \mathbb{E}((Z - \mathbb{E}(Z))^2) = \mathbb{E}(Z^2) - \mathbb{E}(Z)^2 \quad (4.98)$$

$$= \sum_x \rho(x) \left( \ln \frac{\rho(x)}{\sigma(x)} - \sum_x \rho(x) \ln \frac{\rho(x)}{\sigma(x)} \right)^2 =: V(\rho_X \| \sigma_X) / \log(e)^2. \quad (4.99)$$

Combining these steps, we have established that

$$\frac{d}{d\alpha} D_\alpha(\rho_X \| \sigma_X) \Big|_{\alpha=1} = \frac{1}{2\log(e)} V(\rho_X \| \sigma_X). \quad (4.100)$$

Now we can simply substitute the Nussbaum–Szkoła distributions to lift this result to the Petz quantum Rényi divergence, and thus also the minimal quantum Rényi divergence. We recover the following result [109]:

**Proposition 4.9** *Let  $\rho, \sigma \in \mathcal{S}_\circ(A)$  with  $\rho \ll \sigma$ . Then the functions  $\alpha \mapsto \tilde{D}_\alpha(\rho \| \sigma)$  and  $\alpha \mapsto \bar{D}_\alpha(\rho \| \sigma)$  are continuously differentiable at  $\alpha = 1$  and*

$$\frac{d}{d\alpha} \tilde{D}_\alpha(\rho \| \sigma) \Big|_{\alpha=1} = \frac{d}{d\alpha} \bar{D}_\alpha(\rho \| \sigma) \Big|_{\alpha=1} = \frac{1}{2\log(e)} V(\rho \| \sigma), \quad (4.101)$$

where  $V(\rho \| \sigma) := \text{Tr} \left( \rho (\log \rho - \log \sigma - D(\rho \| \sigma))^2 \right)$ .

The minimal and Petz quantum Rényi divergences are thus differentiable at  $\alpha = 1$  and in fact infinitely differentiable. Hence, by Taylor's theorem, for every interval  $[a, b]$  containing 1, there exist constants  $K \in \mathbb{R}_+$  such that, for all  $\alpha \in [a, b]$ , we have

$$\left| \bar{D}_\alpha(\rho \| \sigma) - D(\rho \| \sigma) - (\alpha - 1) \frac{1}{2\log(e)} V(\rho \| \sigma) \right| \leq K(\alpha - 1)^2. \quad (4.102)$$

The same statement naturally also holds if we replace  $\bar{D}_\alpha$  with  $\tilde{D}_\alpha$ . An example of the first-order Taylor series approximation is plotted in Fig. 4.2.

## 4.5 Background and Further Reading

Shannon was first to derive the definition of entropy axiomatically [144] and many have followed his footsteps since. We exclusively consider Rényi's approach [142] here, but a recent overview of different axiomatizations can be found in [40].

The Belavkin-Staszewski relative entropy [17] was considered a reasonable alternative to Umegaki's relative entropy [166] until Hiai and Petz [86] established the operational interpretation of Umegaki's definition in quantum hypothesis testing. The proof that joint convexity implies data-processing is rather standard and mimics a development for the relative entropy that is due to Uhlmann [163, 164] and Lindblad [110, 111]. The data-processing inequality for the quantum relative entropy has been shown in these works, building on previous work by Lieb and Ruskai [107] that established it for the partial trace. The data-processing inequality can be strengthened by including a remainder term that characterizes how well the channel can be recovered. This has been shown by Fawzi and Renner [53] for the partial trace (see also [25, 29] for refinements and simplifications of the proof). Recently these results were extended to general channels in [173] (see also [23]) and further refined in [149].

The max-divergence was first formally introduced by Datta [41], based on Renner's work [139] treating conditional entropy. However, the idea to define a quantum relative entropy via an operator inequality appears implicitly in earlier literature, for example in the work of Jain, Radhakrishnan, and Sen [94]. The minimal (or sandwiched) quantum Rényi divergence was formally introduced independently in [122, 175]. Some ideas resulting in the former work were already presented publicly in [54, 153], and partial results were published in [50, Th. 21, 121]. The initial works only proved a few properties of the divergence and left others as conjectures. Various other authors then contributed by showing data-processing for certain ranges of  $\alpha$  concurrently with Frank and Lieb [57]. Notably, Müller-Lennert et al. [122] already establishes data-processing for  $\alpha \in (1, 2]$  and conjectured it for all  $\alpha \geq \frac{1}{2}$ . Concurrently with [57], Beigi [15] provided a proof for data-processing for  $\alpha > 1$  and Mosonyi and Ogawa [119] provided the proof discussed above, which is also only valid for  $\alpha > 1$ . Their proof in turn uses some of Hayashi's ideas [75].

The minimal, maximal and Petz quantum Rényi divergence are by no means the only quantum generalizations of the Rényi divergence. For example, a two-parameter family of Rényi divergences proposed by Jaksic et al. [95] and further investigated by Audenaert and Datta [9] (see also [35, 84]) captures both the minimal and Petz quantum Rényi divergence.

Both quantum Rényi divergences discussed in this work have found applications beyond binary quantum hypothesis testing. In particular, the minimal quantum Rényi divergence has turned out to be a very useful tool in order to establish the strong converse property for various information theoretic tasks. Most prominently it led to a strong converse for classical communication over entanglement-breaking channels [175], the entanglement-assisted capacity [68], and the quantum capacity of dephasing channels [161]. Furthermore, the strong converse exponents for coding



over classical-quantum channels can be expressed in terms of the minimal quantum Rényi divergence [120]. The minimal quantum Rényi divergence of order 2 can also be used to derive various achievability results [16]. Besides this, the quantum Rényi divergences have also found applications in quantum thermodynamics, e.g. in the study of the second law of thermodynamics [30], and in quantum cryptography, e.g. in [115].

Finally, we note that many of the definitions discussed here are perfectly sensible for infinite-dimensional quantum systems. However, some of the proofs we presented here do not directly generalize to this setting. Ohyama and Petz's book [129] treats quantum entropies in the even more general algebraic setting. However, a comprehensive investigation of the minimal quantum Rényi divergence in the infinite-dimensional or algebraic setting is missing.

# Chapter 5

## Conditional Rényi Entropy

**Abstract** Conditional Entropies are measures of the uncertainty inherent in a system from the perspective of an observer who is given side information on the system. The system as well as the side information can be either classical or a quantum. The goal in this chapter is to define conditional Rényi entropies that are operationally significant measures of this uncertainty, and to explore their properties. Unconditional entropies are then simply a special case of conditional entropies where the side information is uncorrelated with the system under observation.

We want the conditional Rényi entropies to retain most of the properties of the conditional von Neumann entropy, which is by now well established in quantum information theory. Most prominently, we expect that they satisfy a data-processing inequality: we require that the uncertainty of the system never decreases when the quantum system containing side information undergoes a physical evolution. This can be ensured by defining Rényi entropies in terms of the Rényi divergence, in analogy with the case of conditional von Neumann entropy.

### 5.1 Conditional Entropy from Divergence

Let us first recall Shannon’s definition of conditional entropy. For a joint probability mass function  $\rho(x, y)$  with marginals  $\rho(x)$  and  $\rho(y)$ , the conditional Shannon entropy is given as

$$H(X|Y)_\rho = \sum_y \rho(y) H(X|Y=y)_\rho \tag{5.1}$$

$$= \sum_y \rho(y) \sum_x \rho(x|y) \log \frac{1}{\rho(x|y)} \tag{5.2}$$

$$= \sum_{x,y} \rho(x, y) \log \frac{\rho(y)}{\rho(x, y)} \tag{5.3}$$

$$= H(XY)_\rho - H(Y)_\rho, \tag{5.4}$$

where we used the conditional probability distribution  $\rho(x|y) = \rho(x, y)/\rho(y)$ , and the corresponding Shannon entropy,  $H(X|Y = y)_\rho$ . Such conditional distributions are ubiquitous in classical information theory, but it is not immediate how to generalize this concept to quantum information. Instead, we avoid this issue altogether by generalizing the expression in (5.4), which is also called the *chain rule* of the Shannon entropy. This yields the following definition for the quantum conditional entropy.

**Definition 5.1** For any bipartite state  $\rho_{AB} \in \mathcal{S}_o(AB)$ , we define the **conditional von Neumann entropy** of  $A$  given  $B$  for the state  $\rho_{AB}$  as

$$H(A|B)_\rho := H(AB)_\rho - H(B)_\rho \quad \text{where} \quad H(A)_\rho := -\text{Tr}(\rho_A \log \rho_A). \quad (5.5)$$

Here,  $H(A)_\rho$  is the von Neumann entropy [170] and simply corresponds to the Shannon entropy of the state's eigenvalues. One of the most remarkable properties of the von Neumann entropy is *strong subadditivity*. It states that for any tripartite state  $\rho_{ABC} \in \mathcal{S}_o(ABC)$ , we have

$$H(ABC)_\rho + H(B)_\rho \leq H(AB)_\rho + H(BC)_\rho \quad (5.6)$$

or, equivalently  $H(A|BC)_\rho \leq H(A|B)_\rho$ . The latter is an expression of another principle, the *data-processing inequality*. It states that any processing of the side information system, in this case taking a partial trace, can at most increase the uncertainty of  $A$ . Formally, for any  $\mathcal{E} \in \text{CPTP}(B, B')$  map we have

$$H(A|B)_\rho \geq H(A|B')_\tau, \quad \text{where} \quad \tau_{AB'} = \mathcal{E}(\rho_{AB}). \quad (5.7)$$

This property of the von Neumann entropy was first proven by Lieb and Ruskai [107]. It implies weak subadditivity, and the relation [6]

$$|H(A)_\rho - H(B)_\rho| \leq H(AB)_\rho \leq H(A)_\rho + H(B)_\rho. \quad (5.8)$$

The conditional entropy can be conveniently expressed in terms of Umegaki's relative entropy, namely

$$H(A|B)_\rho = H(AB)_\rho - H(B)_\rho \quad (5.9)$$

$$= -\text{Tr}(\rho_{AB} \log \rho_{AB}) + \text{Tr}(\rho_B \log \rho_B) \quad (5.10)$$

$$= -\text{Tr}(\rho_{AB}(\log \rho_{AB} - \log(I_A \otimes \rho_B))) \quad (5.11)$$

$$= -D(\rho_{AB} \| I_A \otimes \rho_B). \quad (5.12)$$

Here, we used that  $\log(I_A \otimes \rho_B) = I_A \otimes \log \rho_B$  to establish (5.11). Sometimes it is useful to rephrase this expression as an optimization problem. Based on (5.11) we

can introduce an auxiliary state  $\sigma_B \in \mathcal{S}_o(B)$  and write

$$H(A|B)_\rho = -\text{Tr}(\rho_{AB}(\log \rho_{AB} - I_A \otimes \log \sigma_B)) + \text{Tr}(\rho_B(\log \rho_B - \log \sigma_B)) \quad (5.13)$$

$$= -D(\rho_{AB} \| I_A \otimes \sigma_B) + D(\rho_B \| \sigma_B). \quad (5.14)$$

Since the latter divergence is always non-negative and equals zero if and only if  $\sigma_B = \rho_B$ , this yields the following expression for the conditional entropy:

$$H(A|B)_\rho = \max_{\sigma_B \in \mathcal{S}_o(B)} -D(\rho_{AB} \| I_A \otimes \sigma_B). \quad (5.15)$$

## 5.2 Definitions and Properties

In the case of quantum Rényi entropies, it is not immediate which of the relations (5.9), (5.12) or (5.15) should be used to define the conditional Rényi entropies. It has been found in the study of the classical special case (see, e.g. [55, 93]) that generalizations based on (5.9) have severe limitations, for example they generally do not satisfy a data-processing inequality. On the other hand, definitions based on the underlying divergence, as in (5.12) or (5.15), have proven to be very fruitful and lead to quantities with operational significance and useful mathematical properties.

Together with the two proposed quantum generalizations of the Rényi divergence,  $\tilde{D}_\alpha$  and  $\bar{D}_\alpha$ , this leads to a total of four different candidates for conditional Rényi entropies [122, 154, 155].

**Definition 5.2** For  $\alpha \geq 0$  and  $\rho_{AB} \in \mathcal{S}_o(AB)$ , we define the following **quantum conditional Rényi entropies** of  $A$  given  $B$  of the state  $\rho_{AB}$ :

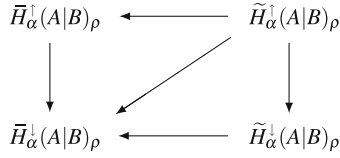
$$\bar{H}_\alpha^\downarrow(A|B)_\rho := -\bar{D}_\alpha(\rho_{AB} \| I_A \otimes \rho_B), \quad (5.16)$$

$$\bar{H}_\alpha^\uparrow(A|B)_\rho := \sup_{\sigma_B \in \mathcal{S}_o(B)} -\bar{D}_\alpha(\rho_{AB} \| I_A \otimes \sigma_B), \quad (5.17)$$

$$\tilde{H}_\alpha^\downarrow(A|B)_\rho := -\tilde{D}_\alpha(\rho_{AB} \| I_A \otimes \rho_B), \quad \text{and} \quad (5.18)$$

$$\tilde{H}_\alpha^\uparrow(A|B)_\rho := \sup_{\sigma_B \in \mathcal{S}_o(B)} -\tilde{D}_\alpha(\rho_{AB} \| I_A \otimes \sigma_B). \quad (5.19)$$

Note that for  $\alpha > 1$  the optimization over  $\sigma_B$  can always be restricted to  $\sigma_B$  with support equal to the support of  $\rho_B$ . Moreover, since small eigenvalues of  $\sigma_B$  lead to a large divergence, we can further restrict  $\sigma_B$  to a compact set of states with eigenvalues bounded away from 0. Since we are thus optimizing a continuous function over a compact set, we are justified in writing a maximum in the above



**Fig. 5.1** Overview of the different conditional entropies used in this paper. *Arrows* indicate that one entropy is larger or equal to the other for all states  $\rho_{AB} \in \mathcal{S}_\circ(AB)$  and all  $\alpha \geq 0$

definitions. Furthermore, pulling the optimization inside the logarithm, we see that these optimization problems are either convex (for  $\alpha > 1$ ) or concave (for  $\alpha < 1$ ).

Consistent with the notation of the preceding chapter, we also use  $\mathbb{H}_\alpha$  to refer to any of the four entropies and  $H_\alpha$  to refer to the respective classical quantities. More precisely, we use  $\mathbb{H}_\alpha$  only to refer to quantum conditional Rényi entropies that satisfy data-processing, which—as we will see in Sect. 5.2.3—means that  $\mathbb{H}_\alpha$  encompasses  $\bar{H}_\alpha$  for  $\alpha \in [0, 2]$  and  $\tilde{H}_\alpha$  for  $\alpha \in [\frac{1}{2}, \infty]$ .

For a trivial system  $B$ , we find that

$$\mathbb{H}_\alpha(A)_\rho = -D_\alpha(\rho_A \| I_A) = \frac{\alpha}{1-\alpha} \log \|\rho_A\|_\alpha. \quad (5.20)$$

reduces to the classical Rényi entropy of the eigenvalues of  $\rho_A$ . In particular, if  $\alpha = 1$ , we always recover the von Neumann entropy.

Finally, note that we use the symbols ‘ $\uparrow$ ’ and ‘ $\downarrow$ ’ to express the observation that

$$H_\alpha^\uparrow(A|B)_\rho \geq H_\alpha^\downarrow(A|B)_\rho \quad \text{and} \quad \tilde{H}_\alpha^\uparrow(A|B)_\rho \geq \tilde{H}_\alpha^\downarrow(A|B)_\rho \quad (5.21)$$

which follows trivially from the respective definitions. Furthermore, the Araki-Lieb-Thirring inequality in (4.87) yields the relations

$$\tilde{H}_\alpha^\uparrow(A|B)_\rho \geq H_\alpha^\uparrow(A|B)_\rho \quad \text{and} \quad \tilde{H}_\alpha^\downarrow(A|B)_\rho \geq H_\alpha^\downarrow(A|B)_\rho. \quad (5.22)$$

These relations are summarized in Fig. 5.1.

### Limits and Special Cases

Inheriting these properties from the corresponding divergences, all entropies are monotonically decreasing functions of  $\alpha$ , and we recover many interesting special cases in the limits  $\alpha \rightarrow \{0, 1, \infty\}$ .

For  $\alpha = 1$ , all definitions coincide with the usual von Neumann conditional entropy (5.12). For  $\alpha = \infty$ , two quantum generalizations of the conditional min-entropy emerge, both of which have been studied by Renner [139]. Namely,

$$\tilde{H}_\infty^\downarrow(A|B)_\rho = \sup \{ \lambda \in \mathbb{R} : \rho_{AB} \leq 2^{-\lambda} I_A \otimes \rho_B \} \quad \text{and} \quad (5.23)$$

$$\tilde{H}_\infty^\uparrow(A|B)_\rho = \sup \{ \lambda \in \mathbb{R} : \exists \sigma_B \in \mathcal{S}_\circ(B) \text{ such that } \rho_{AB} \leq 2^{-\lambda} I_A \otimes \sigma_B \}. \quad (5.24)$$

For  $\alpha = \frac{1}{2}$ , we find the conditional max-entropy studied by König et al. [101],<sup>1</sup>

$$\tilde{H}_{1/2}^\uparrow(A|B)_\rho = \sup_{\sigma_B \in \mathcal{S}_\circ(B)} \log F(\rho_{AB}, I_A \otimes \sigma_B). \quad (5.25)$$

For  $\alpha = 2$ , we find a quantum conditional collision entropy [139]:

$$\tilde{H}_2^\downarrow(A|B)_\rho = -\log \text{Tr} \left( \rho_{AB} \left( I_A \otimes \rho_B^{-\frac{1}{2}} \right) \rho_{AB} \left( I_A \otimes \rho_B^{-\frac{1}{2}} \right) \right). \quad (5.26)$$

For  $\alpha = 0$ , we find a generalization of the Hartley entropy [72], proposed in [139]:

$$\bar{H}_0^\uparrow(A|B)_\rho = \sup_{\sigma_B \in \mathcal{S}_\circ(B)} \log \text{Tr}(\{\rho_{AB} > 0\} I_A \otimes \sigma_B). \quad (5.27)$$

### 5.2.1 Alternative Expression for $\bar{H}_\alpha^\uparrow$

For the quantity  $\bar{H}_\alpha^\uparrow$  we find a closed-form expression for the optimal (minimal or maximal)  $\sigma_B$ . This yields an alternative expression for  $\bar{H}_\alpha^\uparrow$  as follows [145, 154].

**Lemma 5.1** *Let  $\alpha \in (0, 1) \cup (1, \infty)$  and  $\rho_{AB} \in \mathcal{S}(AB)$ . Then,*

$$\bar{H}_\alpha^\uparrow(A|B)_\rho = \frac{\alpha}{1-\alpha} \log \text{Tr} \left( \left( \text{Tr}_A(\rho_{AB}^\alpha) \right)^{\frac{1}{\alpha}} \right). \quad (5.28)$$

*Proof* Recall the definition

$$H_\alpha^\uparrow(A|B)_\rho = \sup_{\sigma_B \in \mathcal{S}_\circ(B)} \frac{1}{1-\alpha} \log \text{Tr}(\rho_{AB}^\alpha \sigma_B^{1-\alpha}) = \sup_{\sigma_B \in \mathcal{S}_\circ(B)} \frac{1}{1-\alpha} \log \text{Tr}(\text{Tr}_A(\rho_{AB}^\alpha) \sigma_B^{1-\alpha}). \quad (5.29)$$

This can immediately be lower bounded by the expression in (5.28) by substituting

$$\sigma_B^* = \frac{(\text{Tr}_A(\rho_{AB}^\alpha))^{\frac{1}{\alpha}}}{\text{Tr} \left( (\text{Tr}_A(\rho_{AB}^\alpha))^{\frac{1}{\alpha}} \right)} \quad (5.30)$$

for  $\sigma_B$ . It remains to show that this choice is optimal. For  $\alpha < 1$ , we employ the Hölder inequality in (3.5) for  $p = \frac{1}{\alpha}$ ,  $q = \frac{1}{1-\alpha}$ ,  $L = \text{Tr}_A(\rho_{AB}^\alpha)$  and  $K = \sigma_B^{1-\alpha}$  to find

---

<sup>1</sup>The notation  $H_{\min}(A|B)_{\rho|B} \equiv \tilde{H}_{\infty}^\downarrow(A|B)_\rho$  and  $H_{\min}(A|B)_\rho \equiv \tilde{H}_{\infty}^\uparrow(A|B)_\rho$  is widely used. The alternative notation  $H_{\max}(A|B)_\rho \equiv \tilde{H}_{1/2}^\uparrow(A|B)_\rho$  is often used too, for example in Chap. 6.

$$\mathrm{Tr}(\mathrm{Tr}_A(\rho_{AB}^\alpha)\sigma_B^{1-\alpha}) \leq \left( \mathrm{Tr}\left(\left(\mathrm{Tr}_A(\rho_{AB}^\alpha)\right)^\frac{1}{\alpha}\right) \right)^\alpha (\mathrm{Tr}(\sigma_B))^{1-\alpha}, \quad (5.31)$$

which yields the desired upper bound since  $\mathrm{Tr}(\sigma_B) = 1$ . For  $\alpha > 1$ , we instead use the reverse Hölder inequality (3.6). This leads us to (5.28) upon the same substitutions.  $\square$

In particular, note that (5.30) gives an explicit expression for the optimal  $\sigma_B$  in the definition of  $\bar{H}_\alpha^\uparrow$ . A similar closed-form expression for the optimal  $\sigma_B$  in the definition of  $\tilde{H}_\alpha^\uparrow$  is however not known.

### 5.2.2 Conditioning on Classical Information

We now analyze the behavior of  $\mathbb{D}_\alpha$  and  $\mathbb{H}_\alpha$  when applied to partly classical states. Formally, consider normalized classical-quantum states of the form  $\rho_{XA} = \sum_x \rho(x) |x\rangle\langle x| \otimes \hat{\rho}_A(x)$  and  $\sigma_{XA} = \sum_x \sigma(x) |x\rangle\langle x| \otimes \hat{\sigma}_A(x)$ . A straightforward calculation using Property (VI) shows that for two such states,

$$\mathbb{D}_\alpha(\rho_{XA} \parallel \sigma_{XA}) = \frac{1}{\alpha - 1} \log \left( \sum_x \rho(x)^\alpha \sigma(x)^{1-\alpha} \exp \left( (\alpha - 1) \mathbb{D}_\alpha(\rho_{h_A(x)} \parallel \sigma_{h_A(x)}) \right) \right). \quad (5.32)$$

In other words, the divergence  $\mathbb{D}_\alpha(\rho_{XA} \parallel \sigma_{XA})$  decomposes into the divergences  $\mathbb{D}_\alpha(\hat{\rho}_A(x) \parallel \hat{\sigma}_A(x))$  of the ‘conditional’ states. This leads to the following relations for conditional Rényi entropies.

**Proposition 5.1** *Let  $\rho_{ABY} = \sum_y \rho(y) \hat{\rho}_{AB}(y) \otimes |y\rangle\langle y| \in \mathcal{S}_\circ(ABY)$  and  $\alpha \in (0, 1) \cup (1, \infty)$ . Then, the conditional entropies satisfy*

$$\mathbb{H}_\alpha^\downarrow(A|BY)_\rho = \frac{1}{1-\alpha} \log \left( \sum_y \rho(y) \exp \left( (1-\alpha) \mathbb{H}_\alpha^\downarrow(A|B)_{\hat{\rho}(y)} \right) \right), \quad (5.33)$$

$$\mathbb{H}_\alpha^\uparrow(A|BY)_\rho = \frac{\alpha}{1-\alpha} \log \left( \sum_y \rho(y) \exp \left( \frac{1-\alpha}{\alpha} \mathbb{H}_\alpha^\uparrow(A|B)_{\hat{\rho}(y)} \right) \right). \quad (5.34)$$

(Here,  $\mathbb{H}_\alpha$  is a substitute for  $\tilde{H}_\alpha$  or  $\bar{H}_\alpha$ .)

*Proof* The first statement follows directly from (5.32) and the definition of the ‘ $\downarrow$ ’-entropy. To show the second statement, recall that by definition,

$$\mathbb{H}_\alpha^\uparrow(A|BY)_\rho = \max_{\sigma_{BY} \in \mathcal{S}_\circ(BY)} -\mathbb{D}_\alpha(\rho_{ABY} \parallel I_A \otimes \sigma_{BY}) \quad (5.35)$$

where the infimum is over all (normalized) states  $\sigma_{BY}$ , but due to data processing (we can measure the  $Y$ -register, which does not affect  $\rho_{ABY}$ ), we can restrict to states  $\sigma_{BY}$  with classical  $Y$ , i.e.  $\sigma_{BY} = \sum_y \sigma(y) |y\rangle\langle y| \otimes \hat{\sigma}_B(y)$ . Using the decomposition of  $\mathbb{D}_\alpha$  in (5.32), we then obtain

$$\begin{aligned} \mathbb{H}_\alpha^\uparrow(A|BY)_\rho &= \max_{\sigma_{BY}} -\frac{1}{\alpha-1} \log \left( \sum_y \rho(y)^\alpha \sigma(y)^{1-\alpha} \exp \left( (\alpha-1) \mathbb{D}_\alpha(\hat{\rho}_{AB}(y) \| I_A \otimes \hat{\sigma}_B(y)) \right) \right) \\ &= \max_{\{\sigma(y)\}_y} \frac{1}{1-\alpha} \log \left( \sum_y \rho(y)^\alpha \sigma(y)^{1-\alpha} \exp \left( (1-\alpha) \mathbb{H}_\alpha^\uparrow(A|B)_{\hat{\rho}(y)} \right) \right). \end{aligned} \quad (5.36)$$

Writing  $r_y = \rho(y) \exp\left(\frac{1-\alpha}{\alpha} \mathbb{H}_\alpha^\uparrow(A|B)_{\hat{\rho}(y)}\right)$ , and using straightforward Lagrange multiplier technique, one can show that the infimum is attained by the distribution  $\sigma(y) = r_y / \sum_z r_z$ . Substituting this into the above equation leads to the desired relation.  $\square$

In particular, considering a state  $\rho_{XY} = \rho(x, y) |x\rangle\langle x| \otimes |y\rangle\langle y|$ , we recover two notions of classical conditional Rényi entropy

$$H_\alpha^\downarrow(X|Y)_\rho = \frac{1}{1-\alpha} \log \left( \sum_y \sum_x \rho(y) \rho(x|y)^\alpha \right), \quad (5.37)$$

$$H_\alpha^\uparrow(X|Y)_\rho = \frac{\alpha}{1-\alpha} \log \left( \sum_y \rho(y) \left( \sum_x \rho(x|y)^\alpha \right)^{\frac{1}{\alpha}} \right), \quad (5.38)$$

where the latter was originally suggested by Arimoto [7].

### 5.2.3 Data-Processing Inequalities and Concavity

Let us first discuss some important properties that immediately follow from the respective properties of the underlying divergence. First, the conditional Rényi entropies satisfy a data-processing inequality.

**Corollary 5.1** *For any channel  $\mathcal{E} \in \text{CPTP}(B, B')$  with  $\tau_{AB'} = \mathcal{E}(\rho_{AB})$  for any state  $\rho_{AB} \in \mathcal{S}_o(AB)$ , we have*

$$\overline{\mathbb{H}}_\alpha(A|B)_\rho \leq \overline{\mathbb{H}}_\alpha(A|B')_\tau \quad \text{for } \alpha \in [0, 2] \quad (5.39)$$

$$\tilde{\mathbb{H}}_\alpha(A|B)_\rho \leq \tilde{\mathbb{H}}_\alpha(A|B')_\tau \quad \text{for } \alpha \geq \frac{1}{2}. \quad (5.40)$$

(Here,  $\overline{\mathbb{H}}_\alpha$  is a substitute for either  $\overline{H}_\alpha^\uparrow$  or  $\overline{H}_\alpha^\downarrow$ , and the same for  $\tilde{\mathbb{H}}_\alpha$ .)

In particular, these entropies thus satisfy strong subadditivity in the form



$$\mathbb{H}_\alpha(A|BC)_\rho \leq \mathbb{H}_\alpha(A|B)_\rho \quad (5.41)$$

for the respective ranges of  $\alpha$ .

Furthermore, it is easy to verify that these entropies are invariant under applications of local isometries on either the  $A$  or  $B$  systems. Moreover, for any sub-unital map  $\mathcal{F} \in \text{CPTP}(A, A')$  and  $\tau_{A'B} = \mathcal{F}(\rho_{AB})$ , we get

$$\overline{H}_\alpha^\downarrow(A'|B)_\tau = -\overline{D}(\tau_{A'B} \| I_{A'} \otimes \tau_B) \geq -\overline{D}(\tau_{A'B} \| \mathcal{F}(I_A) \otimes \tau_B) \quad (5.42)$$

$$\geq -\overline{D}(\rho_{AB} \| I_A \otimes \rho_B) = \overline{H}_\alpha^\downarrow(A|B) \quad (5.43)$$

and an analogous argument for the other entropies reveals  $\mathbb{H}_\alpha(A'|B)_\tau \geq \mathbb{H}_\alpha(A|B)_\rho$  for all entropies with data-processing. Hence, sub-unital maps on  $A$  do not decrease the uncertainty about  $A$ . However, note that the condition that the map be sub-unital is crucial, and counter-examples are abound if it is not.

Finally, as for the divergence itself, the above data-processing inequalities remain valid if the maps  $\mathcal{E}$  and  $\mathcal{F}$  are trace non-increasing and  $\text{Tr}(\mathcal{E}(\rho)) = \text{Tr}(\rho)$  and  $\text{Tr}(\mathcal{F}(\rho)) = \text{Tr}(\rho)$ , respectively.

As another consequence of the joint concavity of  $\overline{Q}_\alpha$  for  $\alpha < 1$ , we find that  $\rho \mapsto \overline{\mathbb{H}}_\alpha(A|B)_\rho$  is concave for all  $\alpha \in [0, 1]$ . Moreover it is quasi-concave for  $\alpha \in [1, 2]$ . Similarly  $\rho \mapsto \widetilde{\mathbb{H}}_\alpha(A|B)_\rho$  is concave for all  $\alpha \in [\frac{1}{2}, 1]$  and quasi-concave for  $\alpha > 1$ .

### 5.3 Duality Relations and Their Applications

We have now introduced four different quantum conditional Rényi entropies. Here we show that these definitions are in fact related and complement each other via duality relations. It is well known that, for any tripartite pure state  $\rho_{ABC}$ , the relation

$$H(A|B)_\rho + H(A|C)_\rho = 0 \quad (5.44)$$

holds. We call this a *duality relation* for the conditional entropy. To see this, simply write  $H(A|B)_\rho = H(\rho_{AB}) - H(\rho_B)$  and  $H(A|C)_\rho = H(\rho_{AC}) - H(\rho_C)$  and verify consulting the Schmidt decomposition that the spectra of  $\rho_{AB}$  and  $\rho_C$  as well as the spectra of  $\rho_B$  and  $\rho_{AC}$  agree. The significance of this relation is manifold—for example it turns out to be useful in cryptography where the information an adversarial party, let us say  $C$ , has about a quantum system  $A$ , can be estimated using local state tomography by two honest parties,  $A$  and  $B$ .

In the following, we are interested to see if such relations hold more generally for conditional Rényi entropies.

### 5.3.1 Duality Relation for $\bar{H}_\alpha^\downarrow$

It was shown in [155] that  $\bar{H}_\alpha^\downarrow$  indeed satisfies a duality relation.

**Proposition 5.2** *For any pure state  $\rho_{ABC} \in \mathcal{S}_o(ABC)$ , we have*

$$\bar{H}_\alpha^\downarrow(A|B)_\rho + \bar{H}_\beta^\downarrow(A|C)_\rho = 0 \quad \text{when } \alpha + \beta = 2, \alpha, \beta \in [0, 2]. \quad (5.45)$$

*Proof* By definition, we have  $\bar{H}_\alpha^\downarrow(A|B)_\rho = \frac{1}{1-\alpha} \log \bar{Q}_\alpha(\rho_{AB} \| I_A \otimes \rho_B)$ . Now, note that

$$\bar{Q}_\alpha(\rho_{AB} \| I_A \otimes \rho_B) = \text{Tr}(\rho_{AB}^\alpha \rho_B^{1-\alpha}) = \text{Tr}(\rho_{AB}^{\alpha-1} |\rho\rangle\langle\rho|_{ABC} \rho_B^{1-\alpha}) \quad (5.46)$$

$$= \text{Tr}(\rho_C^{\alpha-1} |\rho\rangle\langle\rho|_{ABC} \rho_{AC}^{1-\alpha}) = \text{Tr}(\rho_C^{\alpha-1} \rho_{AC}^{2-\alpha}). \quad (5.47)$$

The result then follows by substituting  $\alpha = 2 - \beta$ .  $\square$

Note that the map  $\alpha \mapsto \beta = 2 - \alpha$  maps the interval  $[0, 2]$ , where data-processing holds, onto itself. This is not surprising. Indeed, consider the Stinespring dilation  $\mathcal{U} \in \text{CPTP}(B, B'B'')$  of a quantum channel  $\mathcal{E} \in \text{CPTP}(B, B')$ . Then, for  $\rho_{ABC}$  pure,  $\tau_{AB'B''C} = \mathcal{U}(\rho_{ABC})$  is also pure and the above duality relation implies that

$$H_\alpha^\downarrow(A|B)_\rho \leq H_\alpha^\downarrow(A|B')_\tau \iff H_\beta^\downarrow(A|C)_\rho \geq H_\beta^\downarrow(A|B''C)_\tau. \quad (5.48)$$

Hence, data-processing for  $\alpha$  holds if and only if data-processing for  $\beta$  holds.

### 5.3.2 Duality Relation for $\tilde{H}_\alpha^\uparrow$

It was shown in [122] and [15] that a similar relation holds for  $\tilde{H}_\alpha^\uparrow$ , generalizing a well-known relation between the min- and max-entropies [101].

**Proposition 5.3** *For any pure state  $\rho_{ABC} \in \mathcal{S}_o(ABC)$ , we have*

$$\tilde{H}_\alpha^\uparrow(A|B)_\rho + \tilde{H}_\beta^\uparrow(A|C)_\rho = 0 \quad \text{when } \frac{1}{\alpha} + \frac{1}{\beta} = 2, \alpha, \beta \in \left[\frac{1}{2}, \infty\right]. \quad (5.49)$$

*Proof* Without loss of generality, we assume that  $\alpha > 1$  and  $\beta < 1$ . Since  $(0, 1) \ni \alpha' := \frac{\alpha-1}{\alpha} = -\frac{\beta-1}{\beta} =: -\beta'$ , it suffices to show that

$$\min_{\sigma_B \in \mathcal{S}_o(B)} \left( \tilde{Q}_\alpha(\rho_{AB} \| I_A \otimes \sigma_B) \right)^\frac{1}{\alpha} = \max_{\sigma_B \in \mathcal{S}_o(B)} \left( \tilde{Q}_\beta(\rho_{AB} \| I_A \otimes \sigma_B) \right)^\frac{1}{\beta}, \quad (5.50)$$

or, equivalently,  $\min_{\sigma_B \in \mathcal{S}_\circ(B)} \|\rho_{AB}^{1/2} \sigma_B^{-\alpha'} \rho_{AB}^{1/2}\|_\alpha = \max_{\tau_C \in \mathcal{S}_\circ(C)} \|\rho_{AC}^{1/2} \tau_C^{-\beta'} \rho_{AC}^{1/2}\|_\beta$ . Now, leveraging the Hölder and reverse Hölder inequalities in Lemma 3.1, we find for any  $M \in \mathcal{P}(A)$ ,

$$\|M\|_\alpha = \max \left\{ \text{Tr}(MN) : N \geq 0, \|N\|_{1/\alpha'} \leq 1 \right\} = \max_{\tau \in \mathcal{S}_\circ(A)} \text{Tr}(M\tau^{\alpha'}), \quad \text{and} \quad (5.51)$$

$$\|M\|_\beta = \min \left\{ \text{Tr}(MN) : N \geq 0, N \gg M, \|N^{-1}\|_{-1/\beta'} \leq 1 \right\} = \min_{\substack{\sigma \in \mathcal{S}_\circ(A) \\ \sigma \gg M}} \text{Tr}(M\sigma^{\beta'}). \quad (5.52)$$

In the last expression we can safely ignore operators  $\sigma \gg M$  since those will certainly not achieve the minimum. Substituting this into the above expressions, we find

$$\left\| \rho_{AB}^{1/2} \sigma_B^{-\alpha'} \rho_{AB}^{1/2} \right\|_\alpha = \max_{\tau_{AB} \in \mathcal{S}_\circ(AB)} \text{Tr} \left( \rho_{AB}^{1/2} \sigma_B^{-\alpha'} \rho_{AB}^{1/2} \tau_{AB}^{\alpha'} \right) \quad (5.53)$$

and, furthermore, choosing  $|\Psi\rangle \in \mathcal{P}(ABC)$  to be the unnormalized maximally entangled state with regards to the Schmidt bases of  $|\rho\rangle_{ABC}$  in the decomposition  $AB : C$ , we find

$$\max_{\tau_{AB} \in \mathcal{S}_\circ(AB)} \text{Tr} \left( \rho_{AB}^{1/2} \sigma_B^{-\alpha'} \rho_{AB}^{1/2} \tau_{AB}^{\alpha'} \right) = \max_{\tau_C \in \mathcal{S}_\circ(C)} \left\langle \Psi \left| \rho_{AB}^{1/2} \sigma_B^{-\alpha'} \rho_{AB}^{1/2} \otimes \tau_C^{\alpha'} \right| \Psi \right\rangle_{ABC} \quad (5.54)$$

$$= \max_{\tau_C \in \mathcal{S}_\circ(C)} \left\langle \rho \left| \sigma_B^{-\alpha'} \otimes \tau_C^{\alpha'} \right| \rho \right\rangle_{ABC}. \quad (5.55)$$

An analogous argument also reveals that

$$\left\| \rho_{AC}^{1/2} \tau_C^{-\beta'} \rho_{AC}^{1/2} \right\|_\beta = \min_{\sigma_B \in \mathcal{S}_\circ(B)} \left\langle \rho \left| \sigma_B^{\beta'} \otimes \tau_C^{-\beta'} \right| \rho \right\rangle_{ABC} = \min_{\sigma_B \in \mathcal{S}_\circ(B)} \left\langle \rho \left| \sigma_B^{-\alpha'} \otimes \tau_C^{\alpha'} \right| \rho \right\rangle_{ABC}. \quad (5.56)$$

At this points it only remains to show that the minimum over  $\sigma_B$  and the maximum over  $\tau_C$  can be interchanged. This can be verified using Sion's minimax theorem [146], noting that  $\langle \rho | \sigma_B^{-\alpha'} \otimes \tau_C^{\alpha'} | \rho \rangle_{ABC}$  is convex in  $\sigma_B$  and concave in  $\tau_C$ , and we are optimizing over a compact convex space.  $\square$

We again note that the map  $\alpha \mapsto \beta = \frac{\alpha}{2\alpha-1}$  maps  $[\frac{1}{2}, \infty]$  onto itself.

### 5.3.3 Duality Relation for $\bar{H}_\alpha^\uparrow$ and $\tilde{H}_\alpha^\downarrow$

The alternative expression in Lemma 5.1 leads us to the final duality relation, which establishes a surprising connection between two quantum Rényi entropies [154].

**Proposition 5.4** For any pure state  $\rho_{ABC} \in \mathcal{S}_o(ABC)$ , we have

$$\bar{H}_\alpha^\uparrow(A|B)_\rho + \tilde{H}_\beta^\downarrow(A|C)_\rho = 0 \quad \text{when } \alpha\beta = 1, \alpha, \beta \in [0, \infty]. \quad (5.57)$$

*Proof* First we note that  $\beta = \frac{1}{\alpha}$  and  $\frac{\alpha}{1-\alpha} = -\frac{1}{1-\beta}$ . Then, using the expression in Lemma 5.1, it remains to show that

$$\text{Tr}\left(\left(\text{Tr}_A(\rho_{AB}^\alpha)\right)^{\frac{1}{\alpha}}\right) = \text{Tr}\left(\left(\rho_C^{\alpha'} \rho_{AC} \rho_C^{\alpha'}\right)^{\frac{1}{\alpha}}\right), \quad \text{where } \alpha' = \frac{\alpha - 1}{2}. \quad (5.58)$$

In the following we show something stronger, namely that the operators

$$\text{Tr}_A(\rho_{AB}^\alpha) \quad \text{and} \quad \rho_C^{\alpha'} \rho_{AC} \rho_C^{\alpha'} \quad (5.59)$$

are unitarily equivalent. This is true since both of these operators are marginals—on  $B$  and  $AC$ —of the same tripartite rank-1 operator,  $\rho_C^{\alpha'} \rho_{ABC} \rho_C^{\alpha'}$ . To see that this is indeed true, note the first operator in (5.59) can be rewritten as

$$\text{Tr}_A(\rho_{AB}^\alpha) = \text{Tr}_A(\rho_{AB}^{\alpha'} \rho_{AB} \rho_{AB}^{\alpha'}) = \text{Tr}_{AC}(\rho_{AB}^{\alpha'} \rho_{ABC} \rho_{AB}^{\alpha'}) = \text{Tr}_{AC}(\rho_C^{\alpha'} \rho_{ABC} \rho_C^{\alpha'}). \quad (5.60)$$

The last equality can be verified using the Schmidt decomposition of  $\rho_{ABC}$  with regards to the partition  $AB:C$ .  $\square$

Again, note that the transformation  $\alpha \mapsto \beta = \frac{1}{\alpha}$  maps the interval  $[0, 2]$  where data-processing holds for  $\bar{\mathbb{H}}_\alpha$  to the interval  $[\frac{1}{2}, \infty]$  where data-processing holds for  $\tilde{\mathbb{H}}_\beta$ , and vice versa.

### 5.3.4 Additivity for Tensor Product States

One implication of the duality relation for  $\tilde{H}_\alpha^\uparrow$  is that it allows us to show additivity for this quantity. Namely, we can use it to show the following corollary.

**Corollary 5.2** For any product state  $\rho_{AB} \otimes \tau_{A'B'}$  and  $\alpha \in [\frac{1}{2}, \infty)$ , we have

$$\tilde{H}_\alpha^\uparrow(AA'|BB')_{\rho \otimes \tau} = \tilde{H}_\alpha^\uparrow(A|B)_\rho + \tilde{H}_\alpha^\uparrow(A'|B')_\tau. \quad (5.61)$$

*Proof* By definition of  $\tilde{H}_\alpha^\uparrow(AA'|BB')_{\rho \otimes \tau}$  we immediately find the following chain of inequalities:

$$\tilde{H}_\alpha^\uparrow(AA'|BB')_{\rho \otimes \tau} = \min_{\sigma_{BB'} \in \mathcal{S}(BB')} \tilde{D}_\alpha(\rho_{AB} \otimes \tau_{A'B'} \| I_{AA'} \otimes \sigma_{BB'}) \quad (5.62)$$

$$\leq \min_{\substack{\sigma_B \in \mathcal{S}(B), \\ \omega_{B'} \in \mathcal{S}(B')}} \tilde{D}_\alpha(\rho_{AB} \otimes \tau_{A'B'} \| I_A \otimes \sigma_B \otimes I_{A'} \otimes \omega_{B'}) \quad (5.63)$$

$$= \tilde{H}_\alpha^\uparrow(A|B)_\rho + \tilde{H}_\alpha^\uparrow(A'|B')_\tau. \quad (5.64)$$

To establish the opposite inequality we introduce purifications  $\rho_{ABC}$  of  $\rho_{AB}$  and  $\tau_{A'B'C'}$  of  $\tau_{A'B'}$  and choose  $\beta$  such that  $\frac{1}{\alpha} + \frac{1}{\beta} = 2$ . Then, an instance of the above inequality (5.62)–(5.64) reads

$$\tilde{H}_\beta^\uparrow(AA'|CC')_{\rho \otimes \tau} \leq \tilde{H}_\beta^\uparrow(A|C)_\rho + \tilde{H}_\beta^\uparrow(A'|C')_\tau. \quad (5.65)$$

The duality relation in Proposition 5.3 then yields  $\tilde{H}_\alpha^\uparrow(AA'|BB')_{\rho \otimes \tau} \geq \tilde{H}_\alpha^\uparrow(A|B)_\rho + \tilde{H}_\alpha^\uparrow(A'|B')_\tau$ , concluding the proof.  $\square$

Finally, note that the corresponding additivity relations for  $\tilde{H}_\alpha^\downarrow$  and  $\bar{H}_\alpha^\downarrow$  are evident from the respective definition. Additivity for  $\bar{H}_\alpha^\uparrow$  in turn follows directly from the explicit expression established in Lemma 5.1.

### 5.3.5 Lower and Upper Bounds on Quantum Rényi Entropy

The above duality relations also yield relations between different conditional Rényi entropies for arbitrary mixed states [154].

**Corollary 5.3** *Let  $\rho_{AB} \in \mathcal{S}_\circ(AB)$ . Then, the following holds for  $\alpha \in [\frac{1}{2}, \infty]$ :*

$$\tilde{H}_\alpha^\uparrow(A|B)_\rho \leq \bar{H}_{2-\frac{1}{\alpha}}^\uparrow(A|B)_\rho, \quad \bar{H}_\alpha^\uparrow(A|B)_\rho \leq \bar{H}_{2-\frac{1}{\alpha}}^\downarrow(A|B)_\rho, \quad (5.66)$$

$$\tilde{H}_\alpha^\downarrow(A|B)_\rho \leq \tilde{H}_{2-\frac{1}{\alpha}}^\downarrow(A|B)_\rho, \quad \tilde{H}_\alpha^\downarrow(A|B)_\rho \leq \bar{H}_{2-\frac{1}{\alpha}}^\downarrow(A|B)_\rho. \quad (5.67)$$

*Proof* Consider an arbitrary purification  $\rho_{ABC} \in \mathcal{S}(ABC)$  of  $\rho_{AB}$ . The relations of Fig. 5.1, for any  $\gamma \geq 0$ , applied to the marginal  $\rho_{AC}$  are given as

$$\tilde{H}_\gamma^\uparrow(A|C)_\rho \geq \tilde{H}_\gamma^\downarrow(A|C)_\rho \geq \bar{H}_\gamma^\downarrow(A|C)_\rho, \quad \text{and} \quad (5.68)$$

$$\tilde{H}_\gamma^\uparrow(A|C)_\rho \geq \bar{H}_\gamma^\uparrow(A|C)_\rho \geq \bar{H}_\gamma^\downarrow(A|C)_\rho. \quad (5.69)$$

We then substitute the corresponding dual entropies according to the duality relations in Sect. 5.3, which yields the desired inequalities upon appropriate new parametrization.  $\square$

Some special cases of these inequalities are well known and have operational significance. For example, (5.67) for  $\alpha = \infty$  states that  $\tilde{H}_\infty^\uparrow(A|B)_\rho \leq \tilde{H}_2^\downarrow(A|B)_\rho$ ,

which relates the conditional min-entropy in (5.24) to the conditional collision entropy in (5.26). To understand this inequality more operationally we rewrite the conditional min-entropy as its dual semi-definite program [101] (see also Chap. 6),

$$\tilde{H}_\infty^\uparrow(A|B)_\rho = \min_{\mathcal{E} \in \text{CPTP}(B, A')} -\log(d_A F(\psi_{AA'}, \mathcal{E}(\rho_{AB}))), \quad (5.70)$$

where  $A'$  is a copy of  $A$  and  $\psi_{AA'}$  is the maximally entangled state on  $A : A'$ . Now, the above inequality becomes apparent since the conditional collision entropy can be written as [21]

$$\tilde{H}_2^\downarrow(A|B)_\rho = -\log(d_A F(\phi_{AA'}, \mathcal{E}^{\text{pg}}(\rho_{AB}))), \quad (5.71)$$

where  $\mathcal{E}^{\text{pg}}$  denotes the pretty good recovery map of Barnum and Knill [13].

Finally, (5.66) for  $\alpha = \frac{1}{2}$  yields  $\tilde{H}_{1/2}^\uparrow(A|B)_\rho \leq \bar{H}_0^\uparrow(A|B)_\rho$ , which relates the quantum conditional max-entropy in (5.25) to the quantum conditional generalization of the Hartley entropy in (5.27).

### Dimension Bounds

First, note two particular inequalities from Corollary 5.3:

$$\tilde{H}_\infty^\downarrow(A|B)_\rho \leq \bar{H}_2^\downarrow(A|B)_\rho \quad \text{and} \quad \tilde{H}_{1/2}^\uparrow(A|B)_\rho \leq \bar{H}_0^\uparrow(A|B)_\rho. \quad (5.72)$$

From this and the monotonicity in  $\alpha$ , we find that all conditional entropies (that satisfy the data-processing inequality) can be upper and lower bounded as follows.

$$\tilde{H}_\infty^\downarrow(A|B)_\rho \leq \mathbb{H}_\alpha(A|B)_\rho \leq \bar{H}_0^\uparrow(A|B)_\rho. \quad (5.73)$$

Thus, in order to find upper and lower bounds on quantum Rényi entropies it suffices to investigate these two quantities.

**Lemma 5.2** *Let  $\rho_{AB} \in \mathcal{S}_\circ(AB)$ . Then the following holds:*

$$-\log \min\{\text{rank}(\rho_A), \text{rank}(\rho_B)\} \leq \mathbb{H}_\alpha(A|B)_\rho \leq \log \text{rank}(\rho_A). \quad (5.74)$$

*Moreover,  $\mathbb{H}_\alpha(A|B)_\rho \geq 0$  if  $\rho_{AB}$  is separable.*

*Proof* Without loss of generality (due to invariance under local isometries) we assume that  $\rho_A$  and  $\rho_B$  have full rank. The upper bound follows since  $\bar{H}_0^\uparrow(A|B)_\rho \leq H_0(A)_\rho = \log d_A$ . Similarly, we find  $H_\infty^\downarrow(A|B)_\rho = -\bar{H}_0^\uparrow(A|C)_\rho \geq -H_0(A)_\rho = -\log d_A$  by taking into account an arbitrary purification  $\rho_{ABC}$  of  $\rho_{AB}$ . On the other hand, for any decomposition  $\rho_{AB} = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i|$  into pure states, quasi-concavity of  $\mathbb{H}_\alpha$  (which is a direct consequence of the quasi-convexity of  $\mathbb{D}_\alpha$ ) yields

$$H_{\infty}^{\downarrow}(A|B)_{\rho} \geq \min_i H_{\infty}^{\downarrow}(A|B)_{\phi_i} = \min_i -H_0(A)_{\phi_i} \geq -\log d_B. \quad (5.75)$$

This concludes the proof of the first statement.

For separable states, we may write

$$\rho_{AB} = \sum_k p_k \sigma_A^k \otimes \tau_B^k \leq \sum_k p_k I_A \otimes \tau_B^k = I_A \otimes \rho_B, \quad (5.76)$$

and, hence,  $H_{\infty}^{\downarrow}(A|B)_{\rho} = \sup\{\lambda \in \mathbb{R} : \rho_{AB} \leq \exp(-\lambda)I_A \otimes \rho_B\} \geq 0$ .  $\square$

## 5.4 Chain Rules

The chain rule,  $H(AB|C) = H(A|BC) + H(B|C)$ , is fundamentally important in many applications because it allows us to see the entropy of a system as the sum of the entropies of its parts. However,  $\mathbb{H}_{\alpha}(AB|C) = \mathbb{H}_{\alpha}(A|BC) + \mathbb{H}_{\alpha}(B|C)$ , generally does not hold for  $\alpha \neq 1$ . Nonetheless, there exist weaker statements that we can prove.

For a first such statement, we note that for any  $\rho_{ABC} \in \mathcal{S}_{\circ}(ABC)$ , the inequality

$$\rho_{BC} \leq \exp\left(-\tilde{H}_{\infty}^{\downarrow}(B|C)_{\rho}\right) I_B \otimes \rho_C \quad (5.77)$$

holds by definition of  $\tilde{H}_{\infty}^{\downarrow}$ . Hence, using the dominance relation of the Rényi divergence, we find

$$\bar{H}_{\alpha}^{\downarrow}(A|BC)_{\rho} = -\bar{D}_{\alpha}(\rho_{ABC} \| I_A \otimes \rho_{BC}) \quad (5.78)$$

$$\leq -\bar{D}_{\alpha}(\rho_{ABC} \| I_{AB} \otimes \rho_C) - H_{\infty}^{\downarrow}(B|C)_{\rho}, \quad (5.79)$$

or, equivalently  $\bar{H}_{\alpha}^{\downarrow}(AB|C)_{\rho} \geq \bar{H}_{\alpha}^{\downarrow}(A|BC)_{\rho} + \tilde{H}_{\infty}^{\downarrow}(B|C)_{\rho}$ . Using an analogous argument we get the same statement also for  $\tilde{H}_{\alpha}$ .

**Proposition 5.5** *For any state  $\rho_{ABC} \in \mathcal{S}_{\circ}(ABC)$ , we have*

$$\mathbb{H}_{\alpha}^{\downarrow}(AB|C)_{\rho} \geq \mathbb{H}_{\alpha}^{\downarrow}(A|BC)_{\rho} + \tilde{H}_{\infty}^{\downarrow}(B|C)_{\rho}. \quad (5.80)$$

Several other variations of the chain rule can now be established using the duality relations, for example

$$\bar{H}_{\alpha}^{\uparrow}(AB|C)_{\rho} \leq \bar{H}_0^{\uparrow}(A|BC)_{\rho} + \bar{H}_{\alpha}^{\uparrow}(B|C)_{\rho}. \quad (5.81)$$

Next, let us try to find a chain rule that only involves entropies of the ‘ $\uparrow$ ’ type. For this purpose, we follow the above argument but start with the fact that

$$\rho_{BC} \leq \exp\left(-\tilde{H}_\infty^\uparrow(B|C)_\rho\right) I_B \otimes \sigma_C \quad (5.82)$$

for some  $\sigma_C \in \mathcal{S}_o(C)$ . This yields the relation

$$\tilde{H}_\alpha^\uparrow(AB|C)_\rho \geq \tilde{H}_\alpha^\uparrow(A|BC)_\rho + \tilde{H}_\infty^\uparrow(B|C)_\rho \quad (5.83)$$

and we can use the inequality in (5.67) to remove the remaining ‘ $\downarrow$ ’. This leads to

$$\tilde{H}_\alpha^\uparrow(AB|C)_\rho \geq \tilde{H}_\beta^\uparrow(A|BC)_\rho + \tilde{H}_\infty^\uparrow(B|C)_\rho, \quad \alpha = 2 - \frac{1}{\beta}. \quad (5.84)$$

This result is a special case of a beautiful set of chain rules for  $\tilde{H}_\alpha^\uparrow$  that were recently established by Dupuis [49].

**Theorem 5.1** *Let  $\rho_{ABC} \in \mathcal{S}(ABC)$  and  $\alpha, \beta, \gamma \in (\frac{1}{2}, 1) \cup (1, \infty)$  such that  $\frac{\alpha}{\alpha-1} = \frac{\beta}{\beta-1} + \frac{\gamma}{\gamma-1}$ . Then, if  $(\alpha-1)(\beta-1)(\gamma-1) > 0$ ,*

$$H_\alpha^\uparrow(AB|C)_\rho \geq H_\beta^\uparrow(A|BC)_\rho + H_\gamma^\uparrow(B|C)_\rho, \quad (5.85)$$

*and the inequality is reversed if  $(\alpha-1)(\beta-1)(\gamma-1) < 0$ .*

The proof in [49] is outside the scope of this book (see also Beigi [15]). The chain rules for the von Neumann entropy follow as a limit of the above relation. For example, if we choose  $\beta = \gamma = 1 + 2\varepsilon$  so that  $\alpha = \frac{1+2\varepsilon}{1+\varepsilon}$  for a small parameter  $\varepsilon \rightarrow 0$ , we recover the relation

$$H(AB|C)_\rho \geq H(A|BC)_\rho + H(B|C)_\rho. \quad (5.86)$$

The opposite inequality follows by choosing  $\beta = \gamma = 1 - 2\varepsilon$ .

Finally, we want to stress that slightly stronger chain rules are sometimes possible when the underlying state has structure.

### Entropy of Classical Information

We explore this with the example of classical and coherent-classical quantum states, which arise when we purify classical systems. For concreteness, consider a state  $\rho \in \mathcal{S}_\bullet(XAB)$  that is classical on  $X$ , and a purification of the form

$$\rho_{XX'ABC} := \sum_{x,x'} |x'\rangle\langle x|_X \otimes |x'\rangle\langle x|_{X'} \otimes |\rho(x')\rangle\langle \rho(x)|_{ABC}, \quad (5.87)$$



where  $\rho_{ABC}(x)$  is a purification of  $\rho_{AB}(x)$ . We say that  $\rho_{XX'ABC}$  is *coherent-classical* between  $X$  and  $X'$ : if one of these systems is traced out the remaining states are isomorphic and classical on  $X$  or  $X'$ , respectively.

**Lemma 5.3** *Let  $\rho \in \mathcal{S}_\bullet(XX'AB)$  be coherent-classical between  $X$  and  $X'$ . Then,*

$$\mathbb{H}_\alpha^\uparrow(XA|X'B)_\rho \leq \mathbb{H}_\alpha^\uparrow(A|XX'B)_\rho \quad \text{and} \quad \tilde{\mathbb{H}}_\alpha(XA|B)_\rho \geq \tilde{\mathbb{H}}_\alpha(A|B)_\rho. \quad (5.88)$$

The second statement reveals that classical information has non-negative entropy, regardless of the nature of the state on  $AB$ . (Note that Lemma 5.2 already established this fact for the case where  $A$  is trivial.)

*Proof* We will establish the first inequality for all conditional Rényi entropies of the type ‘ $\uparrow$ ’. The second inequality then follows by the respective duality relations, and a relabelling  $B \leftrightarrow C$ .

Let  $\alpha < 1$  such that  $\mathbb{Q}_\alpha$  is jointly concave the data-processing inequality ensures that  $\mathbb{Q}_\alpha$  is non-decreasing under TPCP maps. Then define the projector  $\Pi_{XX'} = \sum_x |x\rangle\langle x|_X \otimes |x\rangle\langle x|_{X'}$ . Clearly,  $\rho_{XX'AB} = \Pi_{XX'}\rho_{XX'AB}\Pi_{XX'}$ . Hence, for any  $\sigma \in \mathcal{S}_\circ(X'B)$ , the data-processing inequality yields

$$\mathbb{Q}_\alpha(\rho_{XX'AB} \| I_{XA} \otimes \sigma_{X'B}) \leq \mathbb{Q}_\alpha(\rho_{XX'AB} \| I_A \otimes \Pi_{XX'}(I_{X'} \otimes \sigma_{X'B})\Pi_{XX'}) \quad (5.89)$$

$$\leq \max_{\sigma \in \mathcal{S}_\circ(XX'B)} \mathbb{Q}_\alpha(\rho_{XX'AB} \| I_A \otimes \sigma_{XX'B}), \quad (5.90)$$

where we used that  $\text{Tr}(\Pi_{XX'}(I_{X'} \otimes \sigma_{X'B})\Pi_{XX'}) = \text{Tr}(\sigma_{X'B}) = 1$ . We conclude that the desired statement holds for  $\alpha < 1$ , and for  $\alpha \geq 1$  an analogous argument with opposite inequalities applies.  $\square$

Finally, the following result gives dimension-dependent bounds on how much information a classical register can contain.

**Lemma 5.4** *Let  $\rho \in \mathcal{S}_\bullet(XAB)$  be classical on  $X$ . Then,*

$$\mathbb{H}_\alpha^\uparrow(XA|B)_\rho \leq \mathbb{H}_\alpha^\uparrow(A|XB) + \log d_X. \quad (5.91)$$

*Proof* Simply note that for any  $\sigma_B \in \mathcal{S}_\circ(B)$ , we have

$$\mathbb{D}_\alpha(\rho_{XAB} \| I_{XA} \otimes \sigma_B) = \mathbb{D}_\alpha(\rho_{XAB} \| I_A \otimes (\pi_X \otimes \sigma_B)) - \log d_X \quad (5.92)$$

$$\geq \min_{\sigma_{XB} \in \mathcal{S}_\circ(XB)} \mathbb{D}_\alpha(\rho_{XAB} \| I_A \otimes \sigma_{XB}) - \log d_X. \quad (5.93)$$

$\square$

For example, combining the above two lemmas, we find that

$$\tilde{H}_\alpha^\uparrow(A|B)_\rho \leq \tilde{H}_\alpha^\uparrow(AX|B)_\rho \leq \tilde{H}_\alpha^\uparrow(A|BX)_\rho + \log d_X. \quad (5.94)$$

## 5.5 Background and Further Reading

Strong subadditivity (5.6) was first conjectured by Lanford and Robinson in [104]. Its first proof by Lieb and Ruskai [107] is one of the most celebrated results in quantum information theory. The original proof is based on Lieb's theorem [106]. Simpler proofs were subsequently presented by Nielsen and Petz [126] and Ruskai [143], amongst others. In this book we proved this statement indirectly via the data-processing inequality for the relative entropy, which in turns follows by continuity from the data-processing inequality for the Rényi divergence in Chap. 4. We also provide an elementary proof in Appendix.

The classical version of  $H_\alpha^\uparrow$  was introduced by Arimoto for an evaluation of the guessing probability [7]. Gallager used  $H_\alpha^\uparrow$  to upper bound the decoding error probability of a random coding scheme for data compression with side-information [64]. More recently, the classical and the classical-quantum special cases of  $\bar{H}_\alpha^\uparrow$  were investigated by Hayashi (see, for example, [79]).

The quantum conditional Rényi entropy  $\bar{H}_\alpha^\downarrow$  was first studied in [155]. We note that the expression for  $\bar{H}_\alpha^\uparrow$  in Lemma 5.1 can be derived using a quantum Sibson's identity, first proposed by Sharma and Warsi [145]. On the other hand, the quantum Rényi entropy  $\tilde{H}_\alpha^\uparrow$  was proposed in [153] and investigated in [122], whereas  $\tilde{H}_\alpha^\downarrow$  is first considered in [154].

It is an open question whether the inequalities in Corollary 5.3 also hold for the Rényi divergences themselves. Relatedly, Mosonyi [118] used a converse of the Araki-Lieb-Thirring trace inequality due to Audenaert [8] to find a converse to the ordering relation  $\bar{D}_\alpha(\rho\|\sigma) \geq \tilde{D}_\alpha(\rho\|\sigma)$ , namely

$$\tilde{D}_\alpha(\rho\|\sigma) \geq \alpha \bar{D}_\alpha(\rho\|\sigma) + \log \text{Tr}(\rho^\alpha) + (\alpha - 1) \log \|\sigma\|. \quad (5.95)$$

In this book we focus our attention on conditional Rényi entropies, but similar techniques can also be used to explore Rényi generalizations of the mutual information [68, 80] and conditional mutual information [24].

# Chapter 6

## Smooth Entropy Calculus

**Abstract** Smooth Rényi entropies are defined as optimizations (either minimizations or maximization) of Rényi entropies over a set of close states. For many applications it suffices to consider just two smooth Rényi entropies: the smooth min-entropy acts as a representative of all conditional Rényi entropies with  $\alpha > 1$ , whereas the smooth max-entropy acts as a representative for all Rényi entropies with  $\alpha < 1$ . These two entropies have particularly nice properties and can be expressed in various different ways, for example as semi-definite optimization problems. Most importantly, they give rise to an entropic (and fully quantum) version of the asymptotic equipartition property, which states that both the (regularized) smooth min- and max-entropies converge to the conditional von Neumann entropy for iid product states. This is because smoothing implicitly allows us to restrict our attention to a typical subspace where all conditional Rényi entropies coincide with the von Neumann entropy. Furthermore, we will see that the smooth entropies inherit many properties of the underlying Rényi entropies.

### 6.1 Min- and Max-Entropy

This section develops a variety of useful alternative expressions for the min- and max-entropies,  $\tilde{H}_\infty^\uparrow$  and  $\tilde{H}_{1/2}^\uparrow$ . In particular, we express both the min- and the max-entropy in terms of semi-definite programs.

#### 6.1.1 Semi-Definite Programs

Optimization problems that can be formulated as semi-definite programs are particularly interesting because they have a rich structure and efficient numerical solvers. Here we present a formulation of semi-definite programs that has a very symmetric structure, following Watrous' lecture notes [171].

**Definition 6.1** A semi-definite program (SDP) is a triple  $\{K, L, \mathcal{E}\}$ , where  $K \in \mathcal{L}^\dagger(A)$ ,  $L \in \mathcal{L}^\dagger(B)$  and  $\mathcal{E} \in \mathcal{L}(\mathcal{L}(A), \mathcal{L}(B))$  is a super-operator from  $A$  to  $B$  that preserves self-adjointness. The following two optimization problems are associated with the semi-definite program:

<u>primal problem</u>	<u>dual problem</u>	
minimize : $\text{Tr}(KX)$	maximize : $\text{Tr}(LY)$	(6.1)
subject to : $\mathcal{E}(X) \geq L$	subject to : $\mathcal{E}^\dagger(Y) \leq K$	
$X \in \mathcal{P}(A)$	$Y \in \mathcal{P}(B)$	

We call an operator  $X \in \mathcal{P}(A)$  primal feasible if it satisfies  $\mathcal{E}(X) \geq L$ . Similarly, we say that  $Y \in \mathcal{P}(B)$  is dual feasible if  $\mathcal{E}^\dagger(Y) \leq K$ . Moreover, we denote the optimal solution of the primal problem by  $a$  and the optimal solution of the dual problem by  $b$ . Formally, we define

$$a = \inf \{ \text{Tr}(LX) : X \in \mathcal{P}(A), \mathcal{E}(X) \geq L \} \quad (6.2)$$

$$b = \sup \{ \text{Tr}(KY) : Y \in \mathcal{P}(B), \mathcal{E}^\dagger(Y) \leq K \}. \quad (6.3)$$

The following two statements are true for any SDP and provide a relation between the primal and dual problem. The first fact is called *weak duality*, and the second statement is also known as Slater's condition for *strong duality*.

Weak Duality: We have  $a \geq b$ .

Strong Duality: If  $a$  is finite and there exists an operator  $Y > 0$  such that  $\mathcal{E}^\dagger(Y) < K$ , then  $a = b$  and there exists a primal feasible  $X$  such that  $\text{Tr}(KX) = a$ .

For a proof we defer to [171]. As an immediate consequence, this implies that every dual feasible operator  $Y$  provides a lower bound of  $\text{Tr}(LY)$  on  $a$  and every primal feasible operator  $X$  provides an upper bound of  $\text{Tr}(KX)$  on  $b$ .

### 6.1.2 The Min-Entropy

We first recall the expression for  $\tilde{H}_\infty^\uparrow$  in (5.24), which we will simply call *min-entropy* in this chapter. We extend the definition to include sub-normalized states [139].

**Definition 6.2** Let  $\rho_{AB} \in \mathcal{S}_\bullet(AB)$ . The **min-entropy** of  $A$  conditioned on  $B$  of the state  $\rho_{AB}$  is

$$H_{\min}(A|B)_\rho = \sup_{\sigma_B \in \mathcal{S}_\bullet(B)} \sup \{ \lambda \in \mathbb{R} : \rho_{AB} \leq \exp(-\lambda) I_A \otimes \sigma_B \}. \quad (6.4)$$

Let us take a closer look at the inner supremum first. First, note that there exists a feasible  $\lambda$  if and only if  $\sigma_B \gg \rho_B$ . However, if this condition on the support is satisfied, then using the generalized inverse, we find that

$$\lambda_* = -\log \left\| \sigma_B^{-\frac{1}{2}} \rho_{AB} \sigma_B^{-\frac{1}{2}} \right\|_{\infty} \quad (6.5)$$

is feasible and achieves the maximum. The min-entropy can thus alternatively be written as

$$H_{\min}(A|B)_{\rho} = \max_{\sigma_B} -\log \left\| \sigma_B^{-\frac{1}{2}} \rho_{AB} \sigma_B^{-\frac{1}{2}} \right\|_{\infty}, \quad (6.6)$$

where we use the generalized inverse and the maximum is taken over all  $\sigma_B \in \mathcal{S}_{\bullet}(B)$  with  $\sigma_B \gg \rho_B$ . We can also reformulate (6.4) as a semi-definite program.

For this purpose, we include the factor  $\exp(-\lambda)$  in  $\sigma_B$  and allow  $\sigma_B$  to be an arbitrary positive semi-definite operator. The min-entropy can then be written as

$$H_{\min}(A|B)_{\rho} = -\log \min \left\{ \text{Tr}(\sigma_B) : \sigma_B \in \mathcal{P}(B) \wedge \rho_{AB} \leq I_A \otimes \sigma_B \right\}. \quad (6.7)$$

In particular, we consider the following semi-definite optimization problem for the expression  $\exp(-H_{\min}(A|B)_{\rho})$ , which has an efficient numerical solver.

**Lemma 6.1** *Let  $\rho_{AB} \in \mathcal{S}_{\bullet}(AB)$ . Then, the following two optimization problems satisfy strong duality and both evaluate to  $\exp(-H_{\min}(A|B)_{\rho})$ .*

primal problem	dual problem	
minimize : $\text{Tr}(\sigma_B)$	maximize : $\text{Tr}(\rho_{AB} X_{AB})$	(6.8)
subject to : $I_A \otimes \sigma_B \geq \rho_{AB}$	subject to : $\text{Tr}_A[X_{AB}] \leq I_B$	
$\sigma_B \geq 0$	$X_{AB} \geq 0$	

*Proof* Clearly, the dual problem has a finite solution; in fact, we always have  $\text{Tr}[\rho_{AB} X_{AB}] \leq \text{Tr} X_{AB} \leq d_B$ . Furthermore, there exists a  $\sigma_B > 0$  with  $I_A \otimes \sigma_B > \rho_{AB}$ . Hence, strong duality applies and the values of the primal and dual problems are equal.  $\square$

Let us investigate the dual problem next. We can replace the inequality in the condition  $X_B \leq I_B$  by an equality since adding a positive part to  $X_{AB}$  only increases  $\text{Tr}(\rho_{AB} X_{AB})$ . Hence,  $X_{AB}$  can be interpreted as a Choi-Jamiolkowski state of a unital CP map (cf. Sect. 2.6.4) from  $\mathcal{H}_{A'}$  to  $\mathcal{H}_B$ . Let  $\mathcal{E}^{\dagger}$  be that map, then

$$\exp(-H_{\min}(A|B)_{\rho}) = \max_{\mathcal{E}^{\dagger}} \text{Tr}(\rho_{AB} \mathcal{E}^{\dagger}(\Psi_{AA'})) = d_A \max_{\mathcal{E}} \text{Tr}(\mathcal{E}[\rho_{AB}] \psi_{AA'}), \quad (6.9)$$

where the second maximization is over all  $\mathcal{E} \in \text{CPTP}(B, A')$ , i.e. all maps whose adjoint is completely positive and unital from  $A'$  to  $B$ . The fully entangled state

$\psi_{AA'} = \Psi_{AA'}/d_A$  is pure and normalized and if  $\rho_{AB} \in \mathcal{S}_\circ(AB)$  is normalized as well, we can rewrite the above expression in terms of the fidelity [101]

$$H_{\min}(A|B)_\rho = -\log \left( d_A \max_{\mathcal{E} \in \text{CPTP}(B,A')} F(\mathcal{E}(\rho_{AB}), \psi_{AA'}) \right) \geq -\log d_A. \quad (6.10)$$

(Note that  $\psi$  is defined as the fully entangled in an arbitrary but fixed basis of  $\mathcal{H}_A$  and  $\mathcal{H}_{A'}$ . The expression is invariant under the choice of basis, since the fully entangled states can be converted into each other by an isometry appended to  $\mathcal{E}$ .)

Alternatively, we can interpret  $X_{AB}$  as the Choi-Jamiołkowski state of a TP-CPM map from  $\mathcal{H}_{B'}$  to  $\mathcal{H}_A$ , leading to

$$H_{\min}(A|B)_\rho = -\log \left( d_B \max_{\mathcal{E} \in \text{CPTP}(B',A)} \text{Tr}(\rho_{AB} \mathcal{E}(\psi_{BB'})) \right) \geq -\log d_B. \quad (6.11)$$

### 6.1.3 The Max-Entropy

We use the following definition of the max-entropy, which coincides with  $\tilde{H}_{1/2}^\uparrow$  in the case where  $\rho_{AB}$  is normalized.

**Definition 6.3** Let  $\rho_{AB} \in \mathcal{S}_\bullet(AB)$ . The max-entropy of  $A$  conditioned on  $B$  of the state  $\rho_{AB}$  is

$$H_{\max}(A|B)_\rho := \max_{\sigma_B \in \mathcal{S}_\bullet(B)} \log F(\rho_{AB}, I_A \otimes \sigma_B). \quad (6.12)$$

Clearly, the maximum is taken for a normalized state in  $\mathcal{S}_\circ(B)$ . However, note that the fidelity term is not linear in  $\sigma_B$ , and thus this cannot directly be interpreted as an SDP. This can be overcome by introducing an arbitrary purification  $\rho_{ABC}$  of  $\rho_{AB}$  and applying Uhlmann's theorem, which yields

$$\exp(H_{\max}(A|B)_\rho) = d_A \max_{\tau_{ABC} \in \mathcal{S}_\bullet(ABC)} \langle \rho_{ABC} | \tau_{ABC} | \rho_{ABC} \rangle, \quad (6.13)$$

where  $\tau_{ABC}$  has marginal  $\tau_{AB} = \pi_A \otimes \sigma_B$  for some  $\sigma_B \in \mathcal{S}_\bullet(B)$ . This is the dual problem of a semi-definite program.

**Lemma 6.2** Let  $\rho_{AB} \in \mathcal{S}_\bullet(AB)$ . Then, the following two optimization problems satisfy strong duality and both evaluate to  $\exp(H_{\max}(A|B)_\rho)$ .

primal problem	dual problem	
minimize : $\mu$	maximize : $\text{Tr}(\rho_{ABC} Y_{ABC})$	(6.14)
subject to : $\mu I_B \geq \text{Tr}_A(Z_{AB})$	subject to : $\text{Tr}_C(Y_{ABC}) \leq I_A \otimes \sigma_B$	
$Z_{AB} \otimes I_C \geq \rho_{ABC}$	$\text{Tr}(\sigma_B) \leq 1$	
$Z_{AB} \geq 0, \mu \geq 0$	$Y_{ABC} \geq 0, \sigma_B \geq 0.$	

*Proof* The dual problem has a finite solution,  $\text{Tr}(Y_{ABC}) \leq d_A$ , and hence the maximum cannot exceed  $d_A$ . There are also primal feasible points with  $Z_{AB} \otimes I_C > \rho_{ABC}$  and  $I_B > Z_B$ .  $\square$

The primal problem can be rewritten by noting that the optimization over  $\mu$  corresponds to evaluating the operator norm of  $Z_B$ .

$$H_{\max}(A|B)_\rho = \log \min \left\{ \|Z_B\|_\infty : Z_{AB} \otimes I_C \geq \rho_{ABC}, Z_{AB} \in \mathcal{P}(AB) \right\}. \quad (6.15)$$

To arrive at this SDP we introduced a purification of  $\rho_{AB}$ , and consequently (6.15) depends on  $\rho_{ABC}$  as well. This can be avoided by choosing a different SDP for the fidelity.

**Lemma 6.3** *For all  $\rho_{AB} \in \mathcal{S}_\bullet(AB)$ , we have*

$$\exp(H_{\max}(A|B)_\rho) = \inf_{Y_{AB} > 0} \text{Tr}(\rho_{AB} Y_{AB}^{-1}) \|Y_B\|_\infty. \quad (6.16)$$

This can be interpreted as the Alberti form [1] of the max-entropy. Its proof is based on an SDP formulation of the fidelity due to Watrous [172] and Killoran [98].

*Proof* From [98, 172] we learn that  $\max_{\sigma_B \in \mathcal{S}(B)} \sqrt{F(\rho_{AB}, I_A \otimes \sigma_B)}$  equals the dual problem of the following SDP:

primal problem	dual problem	
minimize : $\text{Tr}(\rho_{AB} Y_{AB}) + \gamma$	maximize : $\frac{1}{2} (\text{Tr} X_{12} + \text{Tr} X_{21})$	(6.17)
subject to : $\gamma I_B \geq \text{Tr}_A(Y_{22})$	subject to : $X_{11} \leq \rho_{AB}$	
$\begin{pmatrix} Y_{11} & 0 \\ 0 & Y_{22} \end{pmatrix} \geq \frac{1}{2} \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$	$X_{22} \leq I_A \otimes \sigma_B$	
$Y_{11} \geq 0, Y_{22} \geq 0, \gamma \geq 0$	$\text{Tr}(\sigma_B) \leq 1$	
	$\begin{pmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{pmatrix} \geq 0, \sigma_B \geq 0.$	

Strong duality holds. The primal program can be simplified by noting that  $\begin{pmatrix} Y_{11} & 0 \\ 0 & Y_{22} \end{pmatrix} \geq \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}$  holds if and only if  $\sqrt{Y_{22}}Y_{11}\sqrt{Y_{22}} \geq I$ . This allows us to simplify the primal problem and we find

$$\max_{\sigma_B \in \mathcal{S}(B)} \sqrt{F(\rho_{AB}, I_A \otimes \sigma_B)} = \inf_{Y_{AB} > 0} \frac{1}{2} \text{Tr}(\rho_{AB} Y_{AB}^{-1}) + \frac{1}{2} \|Y_B\|_\infty. \quad (6.18)$$

Now, by the arithmetic geometric mean inequality, we have

$$\frac{1}{2} \text{Tr}(\rho_{AB} Y_{AB}^{-1}) + \frac{1}{2} \|Y_B\|_\infty \geq \sqrt{\text{Tr}(\rho_{AB} Y_{AB}^{-1}) \|Y_B\|_\infty} = \frac{1}{2} \text{Tr}(\rho_{AB} (c Y_{AB})^{-1}) + \frac{1}{2} \|c Y_B\|_\infty \quad (6.19)$$

$$\geq \inf_{Y_{AB} > 0} \frac{1}{2} \text{Tr}(\rho_{AB} Y_{AB}^{-1}) + \frac{1}{2} \|Y_B\|_\infty. \quad (6.20)$$

Here,  $c$  is chosen such that  $\frac{1}{c} \text{Tr}(\rho_{AB} Y_{AB}^{-1}) = c \|Y_B\|_\infty$ , such that the arithmetic geometric mean inequality becomes an equality. Therefore we have

$$\max_{\sigma_B \in \mathcal{S}(B)} \sqrt{F(\rho_{AB}, I_A \otimes \sigma_B)} = \inf_{Y_{AB} > 0} \sqrt{\text{Tr}(\rho_{AB} Y_{AB}^{-1}) \|Y_B\|_\infty} \quad (6.21)$$

and the desired equality follows.  $\square$

This can be used to prove upper bounds on the max-entropy. For example, the quantity  $\bar{H}_0^\uparrow(A|B)_\rho$ —which is sometimes used instead of the max-entropy [139]—is an upper bound on  $H_{\max}(A|B)_\rho$ .

$$\bar{H}_0^\uparrow(A|B)_\rho = \log \max_{\sigma_B \in \mathcal{S}_\bullet(B)} \text{Tr}(\{\rho_{AB} > 0\} I_A \otimes \sigma_B) \geq H_{\max}(A|B)_\rho. \quad (6.22)$$

This follows from Lemma 6.3 by the choice  $Y_{AB} = \{\rho_{AB} > 0\} + \varepsilon I_{AB}$  with  $\varepsilon \rightarrow 0$ , which yields the projector onto the support of  $\rho_{AB}$ . Furthermore, we have

$$\| \text{Tr}_A(\{\rho_{AB} > 0\}) \|_\infty = \max_{\sigma_B \in \mathcal{S}_\bullet(B)} \text{Tr}(\{\rho_{AB} > 0\} I_A \otimes \sigma_B). \quad (6.23)$$

### Min- and Max-Entropy Duality

Finally, the max-entropy can be expressed as a min-entropy of the purified state using the duality relation in Proposition 5.3, which for this special case was first established by König et al. [101].

**Lemma 6.4** *Let  $\rho \in \mathcal{S}_\bullet(ABC)$  be pure. Then,  $H_{\max}(A|B)_\rho = -H_{\min}(A|C)_\rho$ .*



*Proof* We have already seen in Proposition 5.3 that this relation holds for normalized states. The lemma thus follows from the observation that

$$H_{\min}(A|B)_\rho = H_{\min}(A|B)_{\tilde{\rho}} - \log t, \quad \text{and} \quad H_{\max}(A|B)_\rho = H_{\min}(A|B)_{\tilde{\rho}} + \log t \quad (6.24)$$

for any  $\rho_{AB} \in \mathcal{S}_\bullet(AB)$  and  $\tilde{\rho}_{AB} \in \mathcal{S}_\circ(AB)$  with  $\rho_{AB} = t\tilde{\rho}_{AB}$ .  $\square$

### 6.1.4 Classical Information and Guessing Probability

First, let us specialize some of the results in Proposition 5.1 to the min- and max-entropy. In the limit  $\alpha \rightarrow \infty$  and at  $\alpha = \frac{1}{2}$ , we find that

$$H_{\min}(A|BY)_\rho = -\log \left( \sum_y \rho(y) \exp \left( -H_{\min}(A|B)_{\hat{\rho}(y)} \right) \right), \quad (6.25)$$

$$H_{\max}(A|BY)_\rho = \log \left( \sum_y \rho(y) \exp \left( H_{\max}(A|B)_{\hat{\rho}(y)} \right) \right). \quad (6.26)$$

#### Guessing Probability

The classical min-entropy  $H_{\min}(X|Y)_\rho$  can be interpreted as a *guessing probability*. Consider an observer with access to  $Y$ . What is the probability that this observer guesses  $X$  correctly, using his optimal strategy? The optimal strategy of the observer is clearly to guess that the event with the highest probability (conditioned on his observation) will occur. As before, we denote the probability distribution of  $x$  conditioned on a fixed  $y$  by  $\rho(x|y)$ . Then, the guessing probability (averaged over the random variable  $Y$ ) is given by

$$\sum_y \rho(y) \max_x \rho(x|y) = \exp \left( -H_{\min}(X|Y)_\rho \right). \quad (6.27)$$

It was shown by König et al. [101] that this interpretation of the min-entropy extends to the case where  $Y$  is replaced by a quantum system  $B$  and the allowed strategies include arbitrary measurements of  $B$ .

Consider a classical-quantum state  $\rho_{XB} = \sum_x |x\rangle\langle x| \otimes \rho_B(x)$ . For states of this form, the min-entropy simplifies to

$$\exp \left( -H_{\min}(X|B)_\rho \right) = \max_{\mathcal{E} \in \text{CPTP}(B, X')} \left\langle \Psi \left| \sum_x |x\rangle\langle x|_X \otimes \mathcal{E}(\rho_B(x)) \right| \Psi \right\rangle_{XX'} \quad (6.28)$$

$$= \max_{\mathcal{E} \in \text{CPTP}(B, X')} \sum_x \langle x | \mathcal{E}(\rho_B(x)) | x \rangle_{X'}. \quad (6.29)$$

The latter expression clearly reaches its maximum when  $\mathcal{E}$  has classical output in the basis  $\{|x\rangle_{X'}\}_x$ , or in other words, when  $\mathcal{E}$  is a measurement map of the form  $\mathcal{E} : \rho_B \mapsto \sum_y \text{Tr}(\rho_B M_y) |y\rangle\langle y|$  for a POVM  $\{M_y\}_y$ . We can thus equivalently write

$$\exp(-H_{\min}(X|B)_\rho) = \max_{\{M_y\}_y \text{ a POVM}} \sum_y \text{Tr}(M_y \rho_B(y)). \quad (6.30)$$

Moreover, let  $\{\tilde{M}_y\}$  be a measurement that achieves the maximum in the above expression and define  $\tau(x, y) = \text{Tr}(\tilde{M}_y \rho_B(x))$  as the probability that the true value is  $x$  and the observer's guess is  $y$ . Then,

$$\exp(-H_{\min}(X|B)_\rho) = \sum_y \text{Tr}(\tilde{M}_y \rho_B(y)) \quad (6.31)$$

$$\leq \sum_y \max_x \text{Tr}(\tilde{M}_y \rho_B(x)) = \exp(-H_{\min}(X|Y)_\tau), \quad (6.32)$$

and this is in fact an equality by the data-processing inequality. Thus, it is evident that  $H_{\min}(X|B)_\rho = H_{\min}(X|Y)_\tau$  can be achieved by a measurement on  $B$ .

## 6.2 Smooth Entropies

The smooth entropies of a state  $\rho$  are defined as optimizations over the min- and max-entropies of states  $\tilde{\rho}$  that are close to  $\rho$  in *purified distance*. Here, we define the purified distance and the smooth min- and max-entropies and explore some properties of the smoothing.

### 6.2.1 Definition of the $\varepsilon$ -Ball

We introduce sets of  $\varepsilon$ -close states that will be used to define the smooth entropies.

**Definition 6.4** Let  $\rho \in \mathcal{S}_\bullet(A)$  and  $0 \leq \varepsilon < \sqrt{\text{Tr}(\rho)}$ . We define the  $\varepsilon$ -ball of states in  $\mathcal{S}_\bullet(A)$  around  $\rho$  as

$$\mathcal{B}^\varepsilon(A; \rho) := \{\tau \in \mathcal{S}_\bullet(A) : P(\tau, \rho) \leq \varepsilon\}. \quad (6.33)$$

Furthermore, we define the  $\varepsilon$ -ball of pure states around  $\rho$  as  $\mathcal{B}_*^\varepsilon(A; \rho) := \{\tau \in \mathcal{B}^\varepsilon(A; \rho) : \text{rank}(\tau) = 1\}$ .

For the remainder of this chapter, we will assume that  $\varepsilon$  is sufficiently small so that  $\varepsilon < \sqrt{\text{Tr } \rho}$  is always satisfied. Furthermore, if it is clear from the context which system is meant, we will omit it and simply use the notation  $\mathcal{B}(\rho)$ . We now list some properties of this  $\varepsilon$ -ball, in addition to the properties of the underlying purified distance metric.

- i. The set  $\mathcal{B}^\varepsilon(A; \rho)$  is compact and convex.
- ii. The ball grows monotonically in the smoothing parameter  $\varepsilon$ , namely  $\varepsilon < \varepsilon' \implies \mathcal{B}^\varepsilon(A; \rho) \subset \mathcal{B}^{\varepsilon'}(A; \rho)$ . Furthermore,  $\mathcal{B}^0(A; \rho) = \{\rho\}$ .

## 6.2.2 Definition of Smooth Entropies

The *smooth entropies* are now defined as follows.

**Definition 6.5** Let  $\rho_{AB} \in \mathcal{S}_\bullet(AB)$  and  $\varepsilon \geq 0$ . Then, we define the  $\varepsilon$ -**smooth min- and max-entropy** of  $A$  conditioned on  $B$  of the state  $\rho_{AB}$  as

$$H_{\min}^\varepsilon(A|B)_\rho := \max_{\tilde{\rho}_{AB} \in \mathcal{B}^\varepsilon(\rho_{AB})} H_{\min}(A|B)_{\tilde{\rho}} \quad \text{and} \quad (6.34)$$

$$H_{\max}^\varepsilon(A|B)_\rho := \min_{\tilde{\rho}_{AB} \in \mathcal{B}^\varepsilon(\rho_{AB})} H_{\max}(A|B)_{\tilde{\rho}}. \quad (6.35)$$

Note that the extrema can be achieved due to the compactness of the  $\varepsilon$ -ball (cf. Property i.). We usually use  $\tilde{\rho}$  to denote the state that achieves the extremum. Moreover, the smooth min-entropy is monotonically increasing in  $\varepsilon$  and the smooth max-entropy is monotonically decreasing in  $\varepsilon$  (cf. Property ii.). Furthermore,

$$H_{\min}^0(A|B)_\rho = H_{\min}(A|B)_\rho \quad \text{and} \quad H_{\max}^0(A|B)_\rho = H_{\max}(A|B)_\rho. \quad (6.36)$$

If  $\rho_{AB}$  is normalized, the optimization problems defining the smooth min- and max-entropies can be formulated as SDPs. To see this, note that the restrictions on the smoothed state  $\tilde{\rho}$  are linear in the purification  $\rho_{ABC}$  of  $\rho_{AB}$ . In particular, consider the condition  $P(\rho, \tilde{\rho}) \leq \varepsilon$  on  $\tilde{\rho}$ , or, equivalently,  $F_*^2(\rho, \tilde{\rho}) \geq 1 - \varepsilon^2$ . If  $\rho_{ABC}$  is normalized, then the squared fidelity can be expressed as  $F_*^2(\rho, \tilde{\rho}) = \text{Tr } \rho_{ABC} \tilde{\rho}_{ABC}$ .

We give the primal of the SDP for  $\exp(-H_{\min}^\varepsilon(A|B)_\rho)$  as an example. This SDP is parametrized by an (arbitrary) purification  $\rho_{ABC} \in \mathcal{S}_\circ(ABC)$ .

primal problem

$$\begin{aligned}
& \text{minimize : } \text{Tr}(\sigma_B) \\
& \text{subject to : } I_A \otimes \sigma_B \geq \text{Tr}_C(\tilde{\rho}_{ABC}) \\
& \quad \text{Tr}(\tilde{\rho}_{ABC}) \leq 1 \\
& \quad \text{Tr}(\tilde{\rho}_{ABC}\rho_{ABC}) \geq 1 - \varepsilon^2 \\
& \quad \tilde{\rho}_{ABC} \in \mathcal{S}(ABC), \sigma_B \in \mathcal{P}(B)
\end{aligned} \tag{6.37}$$

This program allows us to efficiently compute the smooth min-entropy as long as the involved Hilbert space dimensions are small.

### 6.2.3 Remarks on Smoothing

For both the smooth min- and max-entropy, we can restrict the optimization in Definition 6.5 to states in the support of  $\rho_A \otimes \rho_B$ .

**Proposition 6.1** *Let  $\rho_{AB} \in \mathcal{S}_\bullet(AB)$  and  $0 \leq \varepsilon < \sqrt{\text{Tr}(\rho_{AB})}$ . Then, there exist respective states  $\tilde{\rho}_{AB} \in \mathcal{B}^\varepsilon(\rho_{AB})$  in the support of  $\rho_A \otimes \rho_B$  such that*

$$H_{\min}^\varepsilon(A|B)_\rho = H_{\min}(A|B)_{\tilde{\rho}} \quad \text{or} \quad H_{\max}^\varepsilon(A|B)_\rho = H_{\max}(A|B)_{\tilde{\rho}}. \tag{6.38}$$

*Proof* Let  $\rho_{ABC}$  be any purification of  $\rho_{AB}$ . Moreover, let  $\Pi_{AB} = \{\rho_A > 0\} \otimes \{\rho_B > 0\}$  be the projector onto the support of  $\rho_A \otimes \rho_B$ .

For the min-entropy, first consider any state  $\tilde{\rho}'_{AB} \in \mathcal{B}^\varepsilon(\rho_{AB})$  that achieves the maximum in Definition 6.5. Then, there exists a  $\sigma'_B \in \mathcal{S}_\circ(B)$  with  $H_{\min}^\varepsilon(A|B)_\rho = -\log \text{Tr}(\sigma'_B)$  such that

$$\tilde{\rho}'_{AB} \leq I_A \otimes \sigma'_B \implies \underbrace{\Pi_{AB}\tilde{\rho}'_{AB}\Pi_{AB}}_{=: \tilde{\rho}_{AB}} \leq \{\rho_A > 0\} \otimes \underbrace{\{\rho_B > 0\}\sigma'_B\{\rho_B > 0\}}_{=: \sigma_B}. \tag{6.39}$$

Moreover,  $\tilde{\rho}_{AB} \in \mathcal{B}^\varepsilon(\rho_{AB})$  since the purified distance contracts under trace non-increasing maps, and  $\text{Tr}(\sigma_B) \leq \text{Tr}(\sigma'_B)$ . We conclude that  $\tilde{\rho}_{AB}$  must be optimal.

For the max-entropy, again we start with any state  $\tilde{\rho}'_{AB} \in \mathcal{B}^\varepsilon(\rho_{AB})$  that achieves the maximum in Definition 6.5. Then, using  $\tilde{\rho}_{AB}$  as defined above

$$\max_{\sigma'_B \in \mathcal{S}_\circ(B)} F(\tilde{\rho}_{AB}, I_A \otimes \sigma'_B) = \max_{\sigma_B \in \mathcal{S}_\circ(B)} F(\Pi_{AB}\tilde{\rho}'_{AB}\Pi_{AB}, I_A \otimes \sigma'_B) \tag{6.40}$$

$$= \max_{\sigma_B \in \mathcal{S}_\circ(B)} F(\tilde{\rho}'_{AB}, \{\rho_A > 0\} \otimes \{\rho_B > 0\}\sigma'_B\{\rho_B > 0\}) \tag{6.41}$$

$$\leq \max_{\sigma_B \in \mathcal{S}_\bullet(B)} F(\tilde{\rho}'_{AB}, I_A \otimes \sigma_B). \tag{6.42}$$

Hence,  $H_{\max}(A|B)_{\tilde{\rho}} \leq H_{\max}(A|B)_{\tilde{\rho}'}$ , concluding the proof.  $\square$

Note that these optimal states are not necessarily normalized. In fact, it is in general not possible to find a normalized state in the support of  $\rho_A \otimes \rho_B$  that achieves the optimum. Allowing sub-normalized states, we avoid this problem and as a consequence the smooth entropies are invariant under embeddings into a larger space.

**Corollary 6.1** *For any state  $\rho_{AB} \in \mathcal{S}_\bullet(AB)$  and isometries  $U : A \rightarrow A'$  and  $V : B \rightarrow B'$ , we have*

$$H_{\min}^e(A|B)_\rho = H_{\min}^e(A'|B')_\tau, \quad H_{\max}^e(A|B)_\rho = H_{\max}^e(A'|B')_\tau \quad (6.43)$$

where  $\tau_{A'B'} = (U \otimes V)\rho_{AB}(U \otimes V)^\dagger$ .

On the other hand, if  $\rho$  is normalized, we can always find normalized optimal states if we embed the systems  $A$  and  $B$  into large enough Hilbert spaces that allow smoothing outside the support of  $\rho_A \otimes \rho_B$ . For the min-entropy, this is intuitively true since adding weight in a space orthogonal to  $A$ , if sufficiently diluted, will neither affect the min-entropy nor the purified distance.

**Lemma 6.5** *There exists an embedding from  $A$  to  $A'$  and a normalized state  $\hat{\rho}_{A'B} \in \mathcal{B}^e(\rho_{A'B})$  such that  $H_{\min}(A'|B)_{\hat{\rho}} = H_{\min}^e(A|B)_\rho$ .*

*Proof* Let  $\{\tilde{\rho}_{AB}, \sigma_B\}$  be such that they maximize the smooth min-entropy  $\lambda = H_{\min}^e(A|B)_\rho$ , i.e. we have  $\tilde{\rho}_{AB} \leq \exp(-\lambda)I_A \otimes \sigma_B$ . Then we embed  $A$  into an auxiliary system  $A'$  with dimension  $d_A + d_{\tilde{A}}$  to be defined below. The state  $\hat{\rho}_{A'B} = \tilde{\rho}_{AB} \oplus (1 - \text{Tr}(\tilde{\rho}))\pi_{\tilde{A}} \otimes \sigma_B$ , satisfies

$$\hat{\rho}_{A'B} = \tilde{\rho}_{AB} \oplus (1 - \text{Tr}(\tilde{\rho}))\pi_{\tilde{A}} \otimes \sigma_B \leq \exp(-\lambda)(I_A \oplus I_{\tilde{A}}) \otimes \sigma_B \quad (6.44)$$

if  $\exp(\lambda)(1 - \text{Tr}(\tilde{\rho})) \leq \exp(\lambda) \leq d_{\tilde{A}}$ . Hence, if  $d_{\tilde{A}}$  is chosen large enough, we have  $H_{\min}(A'|B)_{\hat{\rho}} \geq \lambda$ . Moreover,  $F_*(\hat{\rho}, \rho) = F_*(\tilde{\rho}, \rho)$  is not affected by adding the orthogonal subspace.  $\square$

For the max-entropy, a similar statement can be derived using the duality of the smooth entropies.

### Smoothing Classical States

Finally, smoothing respects the structure of the state  $\rho$ , in particular if some subsystems are classical then the optimal state  $\tilde{\rho}$  will also be classical on these systems.

**Lemma 6.6** *For both  $H_{\min}^e(AX|BY)_\rho$  and  $H_{\max}^e(AX|BY)_\rho$ , there exist an optimizer  $\tilde{\rho}_{AXBY} \in \mathcal{B}^e(\rho_{AXBY})$  that is classical on  $X$  and  $Y$ .*

*Proof* Consider the pinching maps  $\mathcal{P}_X(\cdot) = \sum_x |x\rangle\langle x| \cdot |x\rangle\langle x|$  and  $\mathcal{P}_Y$  defined analogously. Since these are CPTP and unital, we immediately find that  $H_{\min}^e(AX|BY)_{\tilde{\rho}} \leq H_{\min}^e(AX|BY)_{\tilde{\rho}}$  for any state  $\tilde{\rho}'_{AXBY}$  and  $\tilde{\rho}_{AXBY} = \mathcal{P}_X \otimes \mathcal{P}_Y(\tilde{\rho}'_{AXBY})$  of the desired

form. Since  $\rho_{AXBY}$  is invariant under this pinching, the state  $\tilde{\rho}$  lies in  $\mathcal{B}^\varepsilon(\rho)$  if  $\tilde{\rho}'$  lies in the ball. Hence,  $\tilde{\rho}$  must be optimal.

For the max-entropy, we follow the argument in the proof of the previous lemma, leveraging on Lemma 3.3. Using the state  $\tilde{\rho}$  from above, this yields

$$\max_{\sigma'_{BY} \in \mathcal{S}_\circ(B)} F(\tilde{\rho}_{AXBY}, I_{AX} \otimes \sigma'_{BY}) = \max_{\sigma'_{BY} \in \mathcal{S}_\circ(B)} F(\tilde{\rho}'_{AXBY}, \mathcal{P}_X(I_{AX}) \otimes \mathcal{P}_Y(\sigma'_{BY})) \quad (6.45)$$

$$\leq \max_{\sigma_{BY} \in \mathcal{S}_\circ(B)} F(\tilde{\rho}'_{AXBY}, I_{AX} \otimes \sigma_{BY}). \quad (6.46)$$

Hence,  $H_{\max}(AX|BY)_{\tilde{\rho}} \leq H_{\max}(AX|BY)_{\tilde{\rho}'}$ , concluding the proof.  $\square$

### 6.3 Properties of the Smooth Entropies

The smooth entropies inherit many properties of the respective underlying unsmoothed Rényi entropies, including data-processing inequalities, duality relations and chain rules.

#### 6.3.1 Duality Relation and Beyond

The duality relation in Lemma 6.4 extends to smooth entropies.

**Proposition 6.2** *Let  $\rho \in \mathcal{S}_\bullet(ABC)$  be pure and  $0 \leq \varepsilon < \sqrt{\text{Tr}(\rho)}$ . Then,*

$$H_{\max}^\varepsilon(A|B)_\rho = -H_{\min}^\varepsilon(A|C)_\rho. \quad (6.47)$$

*Proof* According to Corollary 6.1, the smooth entropies are invariant under embeddings, and we can thus assume without loss of generality that the spaces  $B$  and  $C$  are large enough to entertain purifications of the optimal smoothed states, which are in the support of  $\rho_A \otimes \rho_B$  and  $\rho_A \otimes \rho_C$ , respectively. Let  $\tilde{\rho}_{AB}$  be optimal for the max-entropy, then

$$H_{\max}^\varepsilon(A|B)_\rho = H_{\max}(A|B)_{\tilde{\rho}} \geq \min_{\tilde{\rho} \in \mathcal{B}_*^\varepsilon(\rho_{ABC})} H_{\max}(A|B)_{\tilde{\rho}} \quad (6.48)$$

$$= \min_{\tilde{\rho} \in \mathcal{B}_*^\varepsilon(\rho_{ABC})} -H_{\min}(A|C)_{\tilde{\rho}} \geq \min_{\tilde{\rho} \in \mathcal{B}^\varepsilon(\rho_{AC})} -H_{\min}(A|C)_{\tilde{\rho}} = -H_{\min}^\varepsilon(A|C)_\rho. \quad (6.49)$$

And, using the same argument starting with  $H_{\min}^\varepsilon(A|C)_\rho$ , we can show the opposite inequality.  $\square$

Due to the monotonicity in  $\alpha$  of the Rényi entropies the min-entropy cannot exceed the max-entropy for normalized states. This result extends to smooth entropies [116, 169].

**Proposition 6.3** *Let  $\rho \in \mathcal{S}_\circ(AB)$  and  $\varphi, \vartheta \geq 0$  such that  $\varphi + \vartheta < \frac{\pi}{2}$ . Then,*

$$H_{\min}^{\sin(\varphi)}(A|B)_\rho \leq H_{\max}^{\sin(\vartheta)}(A|B)_\rho + 2 \log \frac{1}{\cos(\varphi + \vartheta)}. \quad (6.50)$$

*Proof* Set  $\varepsilon = \sin(\varphi)$ . According to Lemma 6.5, there exists an embedding  $A'$  of  $A$  and a normalized state  $\tilde{\rho}_{A'B} \in \mathcal{B}^\varepsilon(\rho_{A'B})$  such that  $H_{\min}(A'|B)_{\tilde{\rho}} = H_{\min}^\varepsilon(A|B)_\rho$ . In particular, there exists a state  $\sigma_B \in \mathcal{S}_\circ(B)$  such that  $\tilde{\rho}_{A'B} \leq \exp(-\lambda)I_{A'} \otimes \sigma_B$  with  $\lambda = H_{\min}^\varepsilon(A|B)_\rho$ . Thus, letting  $\bar{\rho}_{A'B} \in \mathcal{B}^{\sin(\vartheta)}(\rho_{A'B})$  be a state that minimizes the smooth max-entropy, we find

$$H_{\max}^{\varepsilon'}(A|B)_\rho = H_{\max}(A'|B)_{\tilde{\rho}} \geq -D_{1/2}(\bar{\rho}_{A'B} \| I_{A'} \otimes \sigma_B) \quad (6.51)$$

$$\geq \lambda - D_{1/2}(\bar{\rho}_{A'B} \| \tilde{\rho}_{A'B}) = \lambda + \log(1 - P(\bar{\rho}_{A'B}, \tilde{\rho}_{A'B})^2) \quad (6.52)$$

$$\geq H_{\min}^\varepsilon(A|B)_\rho + \log(1 - \sin(\varphi + \vartheta)^2). \quad (6.53)$$

In the final step we used the triangle inequality in (3.58) to find  $P(\bar{\rho}_{A'B}, \tilde{\rho}_{A'B}) \leq \sin(\varphi + \vartheta)$ .  $\square$

Proposition 6.3 implies that smoothing states that have similar min- and max-entropies has almost no effect. In particular, let  $\rho_{AB} \in \mathcal{S}_\circ(AB)$  with  $H_{\min}(A|B)_\rho = H_{\max}(A|B)_\rho$ . Then,

$$H_{\min}^\varepsilon(A|B)_\rho \leq H_{\max}(A|B)_\rho - \log(1 - \varepsilon^2) = H_{\min}(A|B)_\rho - \log(1 - \varepsilon^2). \quad (6.54)$$

This inequality is tight and the smoothed state  $\tilde{\rho} = (1 - \varepsilon^2)\rho_{\mathcal{B}^\varepsilon}(\rho)$  reaches equality. An analogous relation can be derived for the smooth max-entropy.

### 6.3.2 Chain Rules

Similar to the conditional Rényi entropies, we also provide a collection of inequalities that replace the chain rule of the von Neumann entropy. These chain rules are different in that they introduce an additional correction term in  $O(\log \frac{1}{\varepsilon})$  that does not appear in the results of the previous chapter.

**Theorem 6.1** *Let  $\rho \in \mathcal{S}_\bullet(ABC)$  and  $\varepsilon, \varepsilon', \varepsilon'' \in [0, 1)$  with  $\varepsilon > \varepsilon' + 2\varepsilon''$ . Then,*

$$H_{\min}^\varepsilon(AB|C)_\rho \geq H_{\min}^{\varepsilon'}(A|BC)_\rho + H_{\min}^{\varepsilon''}(B|C)_\rho - g(\delta), \quad (6.55)$$

$$H_{\min}^{\varepsilon'}(AB|C)_\rho \leq H_{\min}^\varepsilon(A|BC)_\rho + H_{\max}^{\varepsilon''}(B|C)_\rho + 2g(\delta), \quad (6.56)$$

$$H_{\min}^{\varepsilon'}(AB|C)_\rho \leq H_{\max}^{\varepsilon''}(A|BC)_\rho + H_{\min}^\varepsilon(B|C)_\rho + 3g(\delta), \quad (6.57)$$

where  $g(\delta) = -\log(1 - \sqrt{1 - \delta^2})$  and  $\delta = \varepsilon - \varepsilon' - 2\varepsilon''$ .

See [169] for a proof. Using the duality relation for smooth entropies on (6.55), (6.56) and (6.57), we also find the chain rules

$$H_{\max}^\varepsilon(AB|C)_\rho \leq H_{\max}^{\varepsilon'}(A|BC)_\rho + H_{\max}^{\varepsilon''}(B|C)_\rho + g(\delta), \quad (6.58)$$

$$H_{\max}^{\varepsilon'}(AB|C)_\rho \geq H_{\min}^{\varepsilon''}(A|BC)_\rho + H_{\max}^\varepsilon(B|C)_\rho - 2g(\delta), \quad (6.59)$$

$$H_{\max}^{\varepsilon'}(AB|C)_\rho \geq H_{\max}^\varepsilon(A|BC)_\rho + H_{\min}^{\varepsilon''}(B|C)_\rho - 3g(\delta). \quad (6.60)$$

### Classical Information

Sometimes the following alternative bounds restricted to classical information are very useful. The first result asserts that the entropy of a classical register is always non-negative and bounds how much entropy it can contain.

**Lemma 6.7** *Let  $\varepsilon \in [0, 1)$  and  $\rho \in \mathcal{S}_\bullet(XAB)$  be classical on  $X$ . Then,*

$$H_{\min}^\varepsilon(A|B)_\rho \leq H_{\min}^\varepsilon(XA|B)_\rho \leq H_{\min}^\varepsilon(A|B)_\rho + \log d_X \quad \text{and} \quad (6.61)$$

$$H_{\max}^\varepsilon(A|B)_\rho \leq H_{\max}^\varepsilon(XA|B)_\rho \leq H_{\max}^\varepsilon(A|B)_\rho + \log d_X. \quad (6.62)$$

We are also concerned with the maximum amount of information a classical register  $X$  can contain about a quantum state  $A$ .

**Lemma 6.8** *Let  $\varepsilon \in [0, 1)$  and  $\rho \in \mathcal{S}_\bullet(AYB)$  be classical on  $Y$ . Then,*

$$H_{\min}^\varepsilon(A|YB)_\rho \geq H_{\min}^\varepsilon(A|B)_\rho - \log d_Y \quad \text{and} \quad (6.63)$$

$$H_{\max}^\varepsilon(A|YB)_\rho \geq H_{\max}^\varepsilon(A|B)_\rho - \log d_Y. \quad (6.64)$$

We omit the proofs of the above statements, but note that they can be derived from (5.94) together with the fact that the states achieving the optimum for the smooth entropies retain the classical-quantum structure (cf. Lemma 6.6).



### 6.3.3 Data-Processing Inequalities

We expect measures of uncertainty of the system  $A$  given side information  $B$  to be non-decreasing under local physical operations (e.g., measurements or unitary evolutions) applied to the  $B$  system. Furthermore, in analogy to the conditional Rényi entropies, we expect that the uncertainty of the system  $A$  does not decrease when a sub-unital map is executed on the  $A$  system.

**Theorem 6.2** *Let  $\rho_{AB} \in \mathcal{S}_\bullet(AB)$  and  $0 \leq \varepsilon < \sqrt{\text{Tr}(\rho)}$ . Moreover, let  $\mathcal{E} \in \text{CPTP}(A, A')$  be sub-unital, and let  $\mathcal{F} \in \text{CPTP}(B, B')$ . Then, the state  $\tau_{A'B'} = (\mathcal{E} \otimes \mathcal{F})(\rho_{AB})$  satisfies*

$$H_{\min}^\varepsilon(A|B)_\rho \leq H_{\min}^\varepsilon(A'|B')_\tau \quad \text{and} \quad H_{\max}^\varepsilon(A|B)_\rho \leq H_{\max}^\varepsilon(A'|B')_\tau. \quad (6.65)$$

*Proof* The data-processing inequality for the min-entropy follows from the respective property of the unsmoothed conditional Rényi entropy. We have

$$H_{\min}^\varepsilon(A|B)_\rho = H_\infty^\uparrow(A|B)_{\tilde{\rho}} \leq H_\infty^\uparrow(A'|B')_{\tilde{\tau}} \leq H_{\min}^\varepsilon(A'|B')_\tau. \quad (6.66)$$

Here,  $\tilde{\rho}_{AB}$  is a state maximizing the smooth min-entropy and  $\tilde{\tau}_{AB} = (\mathcal{E} \otimes \mathcal{F})(\tilde{\rho}_{AB})$  lies in  $\mathcal{B}^\varepsilon(\tau_{A'B'})$ .

To prove the result for the max-entropy, we take advantage of the Stinespring dilation of  $\mathcal{E}$  and  $\mathcal{F}$ . Namely, we introduce the isometries  $U : AA'A''$  and  $V : BB'B''$  and the state  ${}_{A'A''B''} = (U \otimes V)\rho_{AB}(U^\dagger \otimes V^\dagger)$  of which  ${}_{A'B'}$  is a marginal. Let  $\tilde{\tau} \in \mathcal{B}^\varepsilon({}_{A'A''B''})$  be the state that minimizes the smooth max-entropy  $H_{\max}^\varepsilon(A'|B')_\tau$ . Then,

$$H_{\max}^\varepsilon(A'|B')_\tau = \max_{\sigma_{B'} \in \mathcal{S}_\circ(B')} \log F^2(\tilde{\tau}_{A'B'}, I_{A'} \otimes \sigma_{B'}) \quad (6.67)$$

$$\geq \max_{\sigma_{B'} \in \mathcal{S}_\circ(B')} \log F^2(\tilde{\tau}_{A'B'}, \text{Tr}_{A''} \Pi_{A'A''} \otimes \sigma_{B'}). \quad (6.68)$$

We introduced the projector  $\Pi_{A'A''} = UU^\dagger$  onto the image of  $U$ , which exhibits the following property due to the fact that  $\mathcal{E}$  is sub-unital:

$$\text{Tr}_{A''}(\Pi_{A'A''}) = \text{Tr}_{A''}(UI_AU^\dagger) = \mathcal{E}(I_A) \leq I_{A'}. \quad (6.69)$$

The inequality in (6.68) is then a result of the fact that the fidelity is non-increasing when an argument  $A$  is replaced by a smaller argument  $B \leq A$ . Next, we use the monotonicity of the fidelity under partial trace to bound (6.68) further.

$$H_{\max}^{\varepsilon}(A'|B')_{\tau} \geq \max_{\sigma_{B'B''} \in \mathcal{S}_{\circ}(B'B')} \log F^2(\tilde{\tau}_{A'A''B'B''}, \Pi_{A'A''} \otimes \sigma_{B'B''}) \quad (6.70)$$

$$= \max_{\sigma_{B'B''} \in \mathcal{S}_{\circ}(B'B')} \log F^2(\Pi_{A'A''} \tilde{\tau}_{A'A''B'B''} \Pi_{A'A''}, I_{A'A''} \otimes \sigma_{B'B''}) \quad (6.71)$$

$$= H_{\max}(A'A''|B'B'')_{\hat{\tau}}. \quad (6.72)$$

Finally, we note that  $\hat{\tau}_{A'A''B'B''} = \Pi_{A'A''} \tilde{\tau}_{A'A''B'B''} \Pi_{A'A''} \in \mathcal{B}^{\varepsilon}(\rho_{A'A''B'B''})$  due to the monotonicity of the purified distance under trace non-increasing maps. Hence, we established  $H_{\max}^{\varepsilon}(A'|B')_{\tau} \geq H_{\max}^{\varepsilon}(A'A''|B'B'')_{\tau} = H_{\max}^{\varepsilon}(A|B)_{\rho}$ , where the last equality follows due to the invariance of the max-entropy under local isometries.  $\square$

### Functions on Classical Registers

Let us now consider a state  $\rho_{XAB}$  that is classical on  $X$ . We aim to show that applying a classical function on the register  $X$  cannot increase the smooth entropies  $AX$  given  $B$ , even if this operation is not necessarily sub-unital. In particular, for the min-entropy this corresponds to the intuitive statement that it is always at least as hard to guess the input of a function than it is to guess its output.

**Proposition 6.4** *Let  $\rho_{XAB} = \sum_x p_x |x\rangle\langle x|_X \otimes \hat{\rho}_{AB}(x)$  be classical on  $X$ . Furthermore, let  $\varepsilon \in [0, 1)$  and let  $f : XZ$  be a function. Then, the state  $\tau_{ZAB} = \sum_x p_x |f(x)\rangle\langle f(x)|_Z \otimes \hat{\rho}_{AB}(x)$  satisfies*

$$H_{\min}^{\varepsilon}(ZA|B)_{\tau} \leq H_{\min}^{\varepsilon}(XA|B)_{\rho} \quad \text{and} \quad H_{\max}^{\varepsilon}(ZA|B)_{\tau} \leq H_{\max}^{\varepsilon}(XA|B)_{\rho}. \quad (6.73)$$

*Proof* A possible Stinespring dilation of  $f$  is given by the isometry  $U : |x\rangle_X \mapsto |x\rangle_{X'} \otimes |f(x)\rangle_Z$  followed by a partial trace over  $X'$ . Applying  $U$  on  $\rho_{XAB}$ , we get

$$\tau_{X'ZAB} := U \rho_{XAB} U^{\dagger} = \sum_x p_x |x\rangle\langle x|_{X'} \otimes |f(x)\rangle\langle f(x)|_Z \otimes \hat{\rho}_{AB}(x) \quad (6.74)$$

which is classical on  $X'$  and  $Z$  and an extension of  $ZAB$ . Hence, the invariance under isometries of the smooth entropies (cf. Corollary 6.1) in conjunction with Proposition 6.8 implies

$$H_{\min}^{\varepsilon}(XA|B)_{\rho} = H_{\min}^{\varepsilon}(X'ZA|B)_{\tau} \geq H_{\min}^{\varepsilon}(ZA|B)_{\tau}. \quad (6.75)$$

An analogous argument applies for the smooth max-entropy.  $\square$

## 6.4 Fully Quantum Asymptotic Equipartition Property

Smooth entropies give rise to an entropic (and fully quantum) version of the asymptotic equipartition property (AEP), which states that both the (regularized) smooth min- and max-entropies converge to the conditional von Neumann entropy for iid product states. The classical special case of this, which is usually not expressed in terms of entropies (see, e.g., [38]), is a workhorse of classical information theory and similarly the quantum AEP has already found many applications.

The entropic form of the AEP explains the crucial role of the von Neumann entropy to describe information theoretic tasks. While operational quantities in information theory (such as the amount of extractable randomness, the minimal length of compressed data and channel capacities) can naturally be expressed in terms of smooth entropies in the one-shot setting, the von Neumann entropy is recovered if we consider a large number of independent repetitions of the task.

Moreover, the entropic approach to asymptotic equipartition lends itself to a generalization to the quantum setting. Note that the traditional approach, which considers the AEP as a statement about (conditional) probabilities, does not have a natural quantum generalization due to the fact that we do not know a suitable generalization of conditional probabilities to quantum side information. Figure 6.1 visualizes the intuitive idea behind the entropic AEP.

### 6.4.1 Lower Bounds on the Smooth Min-Entropy

For the sake of generality, we state our results here in terms of the *smooth relative max-divergence*, which we define for any  $\rho \in \mathcal{S}_\bullet(A)$  and  $\sigma \in \mathcal{S}(A)$  as

$$D_{\max}^\varepsilon(\rho\|\sigma) := \min_{\tilde{\rho} \in \mathcal{B}^\varepsilon(\rho)} D_\infty(\tilde{\rho}\|\sigma). \quad (6.76)$$

The following gives an upper bound on the smooth relative max-entropy [45, 155].

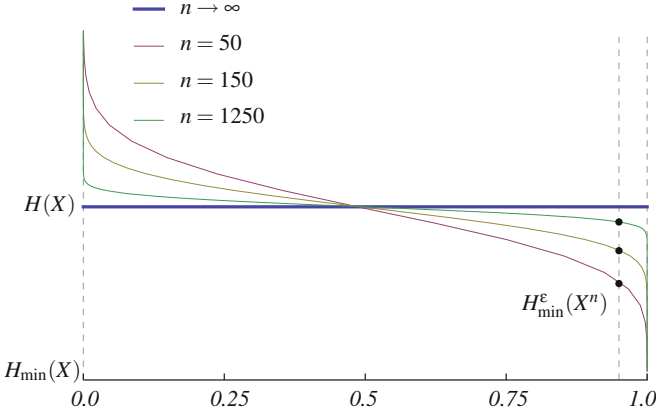
**Lemma 6.9** *Let  $\rho \in \mathcal{S}_\bullet(A)$ ,  $\sigma \in \mathcal{S}(A)$  and  $\lambda \in (-\infty, D_{\max}(\rho\|\sigma)]$ . Then,*

$$D_{\max}^\varepsilon(\rho\|\sigma) \leq \lambda, \quad \text{where } \varepsilon = \sqrt{2 \operatorname{Tr}(\Sigma) - \operatorname{Tr}(\Sigma)^2} \quad (6.77)$$

*and  $\Sigma = \{\rho > \exp(\lambda)\sigma\}(\rho - \exp(\lambda)\sigma)$ , i.e. the positive part of  $\rho - \exp(\lambda)\sigma$ .*

The proof constructs a smoothed state  $\tilde{\rho}$  that reduces the smooth relative max-divergence relative to  $\sigma$  by removing the subspace where  $\rho$  exceeds  $\exp(\lambda)\sigma$ .

*Proof* We first choose  $\tilde{\rho}$ , bound  $D_{\max}^\varepsilon(\tilde{\rho}\|\sigma)$ , and then show that  $\tilde{\rho} \in \mathcal{B}^\varepsilon(\rho)$ . We use the abbreviated notation  $\Lambda := \exp(\lambda)\sigma$  and set



**Fig. 6.1 Emergence of Typical Set.** We consider  $n$  independent Bernoulli trials with  $p = 0.2$  and denote the probability that an event  $x^n$  (a bit string of length  $n$ ) occurs by  $P_n(x^n)$ . The plot shows the surprisal rate,  $-\frac{1}{n} \log P_n(x^n)$ , over the cumulated probability of the events sorted such that events with high surprisal are on the *left*. The curves for  $n = \{50, 100, 500, 2500\}$  converge to the von Neumann entropy,  $H(X) \approx 0.72$  as  $n$  increases. This indicates that, for large  $n$ , most (in probability) events are close to typical (i.e. they have surprisal rate close to  $H(X)$ ). The min-entropy,  $H_{\min}(X) \approx 0.32$ , constitutes the minimum of the curves while the max-entropy,  $H_{\max}(X) \approx 0.85$ , is upper bounded by their maximum. Moreover, the respective  $\varepsilon$ -smooth entropies,  $\frac{1}{n} H_{\min}^\varepsilon(X^n)$  and  $\frac{1}{n} H_{\max}^\varepsilon(X^n)$ , can be approximately obtained by cutting off a probability  $\varepsilon$  from each side of the  $x$ -axis and taking the minima or maxima of the remaining curve. Clearly, the  $\varepsilon$ -smooth entropies converge to the von Neumann entropy as  $n$  increases

$$\tilde{\rho} := G\rho G^\dagger, \quad \text{where } G := \Lambda^{1/2}(\Lambda + \Sigma)^{-1/2}, \quad (6.78)$$

where we use the generalized inverse. From the definition of  $\Sigma$ , we have  $\rho \leq \Lambda + \Sigma$ ; hence,  $\tilde{\rho} \leq \Lambda$  and  $D_{\max}(\tilde{\rho}|\sigma) \leq \lambda$ .

Let  $|\rho\rangle$  be a purification of  $\rho$ , then  $(G \otimes I)|\rho\rangle$  is a purification of  $\tilde{\rho}$  and, using Uhlmann’s theorem, we find a bound on the (generalized) fidelity:

$$\sqrt{F_*(\tilde{\rho}, \rho)} \geq |\langle \rho | G | \rho \rangle| + \sqrt{(1 - \text{Tr}(\rho))(1 - \text{Tr}(\tilde{\rho}))} \quad (6.79)$$

$$\geq \Re(\text{Tr}(G\rho)) + 1 - \text{Tr}(\rho) = 1 - \text{Tr}((I - \tilde{G})\rho), \quad (6.80)$$

where we introduced  $\tilde{G} = \frac{1}{2}(G + G^\dagger)$  and  $\Re$  denotes the real part. This can be simplified further by noting that  $G$  is a contraction. To see this, we multiply  $\Lambda \leq \Lambda + \Sigma$  with  $(\Lambda + \Sigma)^{-1/2}$  from left and right to get

$$G^\dagger G = (\Lambda + \Sigma)^{-1/2} \Lambda (\Lambda + \Sigma)^{-1/2} \leq I. \quad (6.81)$$

Furthermore,  $\tilde{G} \leq I$ , since  $\|\tilde{G}\| \leq 1$  by the triangle inequality and  $\|G\| = \|G^\dagger\| \leq 1$ .

$$\mathrm{Tr}((I - \bar{G})\rho) \leq \mathrm{Tr}(\Lambda + \Sigma) - \mathrm{Tr}(\bar{G}(\Lambda + \Sigma)) \quad (6.82)$$

$$= \mathrm{Tr}(\Lambda + \Sigma) - \mathrm{Tr}((\Lambda + \Sigma)^{1/2} \Lambda^{1/2}) \leq \mathrm{Tr}(\Sigma), \quad (6.83)$$

where we used  $\rho \leq \Lambda + \Sigma$  and  $\sqrt{\Lambda + \Sigma} \geq \sqrt{\Lambda}$ . The latter inequality follows from the operator monotonicity of the square root function. Finally, using the above bounds, the purified distance between  $\tilde{\rho}$  and  $\rho$  is bounded by

$$P(\tilde{\rho}, \rho) = \sqrt{1 - F_*(\tilde{\rho}, \rho)} \leq \sqrt{1 - (1 - \mathrm{Tr}(\Sigma))^2} = \sqrt{2 \mathrm{Tr}(\Sigma) - \mathrm{Tr}(\Sigma)^2}. \quad (6.84)$$

Hence, we verified that  $\tilde{\rho} \in \mathcal{B}^\varepsilon(\rho)$ , which concludes the proof.

In particular, this means that for a fixed  $\varepsilon \in [0, 1)$  and  $\rho \ll \sigma$ , we can always find a finite  $\lambda$  such that Lemma 6.9 holds. To see this, note that  $\varepsilon(\lambda) = \sqrt{2 \mathrm{Tr}(\Sigma) - \mathrm{Tr}(\Sigma)^2}$  is continuous in  $\lambda$  with  $\varepsilon(D_{\max}(\rho \parallel \sigma)) = 0$  and  $\lim_{\lambda \rightarrow -\infty} \varepsilon(\lambda) = 1$ .

Our main tool for proving the fully quantum AEP is a family of inequalities that relate the smooth max-divergence to quantum Rényi divergences for  $\alpha \in (1, \infty)$ .

**Proposition 6.5** *Let  $\rho \in \mathcal{S}_o(A)$ ,  $\sigma \in \mathcal{S}(A)$ ,  $0 < \varepsilon < 1$  and  $\alpha \in (1, \infty)$ . Then,*

$$D_{\max}^\varepsilon(\rho \parallel \sigma) \leq \mathbb{D}_\alpha(\rho \parallel \sigma) + \frac{g(\varepsilon)}{\alpha - 1}, \quad (6.85)$$

where  $g(\varepsilon) = -\log(1 - \sqrt{1 - \varepsilon^2})$  and  $\mathbb{D}_\alpha$  is any quantum Rényi divergence.

*Proof* If  $\rho \not\ll \sigma$  the bound holds trivially, so for the following we have  $\rho \ll \sigma$ . Furthermore, since the divergences are invariant under isometries we can assume that  $\sigma > 0$  is invertible.

We then choose  $\lambda$  such that Lemma 6.9 holds for the  $\varepsilon$  specified above. Next, we introduce the operator  $X = \rho - \exp(\lambda)\sigma$  with eigenbasis  $\{|e_i\rangle\}_{i \in S}$ . The set  $S^+ \subseteq S$  contains the indices  $i$  corresponding to positive eigenvalues of  $X$ . Hence,  $\{X \geq 0\}X\{X \geq 0\} = \Sigma$  as defined in Lemma 6.9. Furthermore, let  $r_i = \langle e_i | \rho | e_i \rangle \geq 0$  and  $s_i = \langle e_i | \sigma | e_i \rangle > 0$ . It follows that

$$\forall i \in S^+ : r_i - \exp(\lambda)s_i \geq 0 \quad \text{and, thus,} \quad \frac{r_i}{s_i} \exp(-\lambda) \geq 1. \quad (6.86)$$

For any  $\alpha \in (1, \infty)$ , we bound  $\mathrm{Tr}(\Sigma) = 1 - \sqrt{1 - \varepsilon^2}$  as follows:

$$1 - \sqrt{1 - \varepsilon^2} = \text{Tr}(\Sigma) = \sum_{i \in S^+} r_i - \exp(\lambda) s_i \leq \sum_{i \in S^+} r_i \quad (6.87)$$

$$\leq \sum_{i \in S^+} r_i \left( \frac{r_i}{s_i} \exp(-\lambda) \right)^{\alpha-1} \leq \exp(-\lambda(\alpha-1)) \sum_{i \in S} r_i^\alpha s_i^{1-\alpha}. \quad (6.88)$$

Hence, taking the logarithm and dividing by  $\alpha - 1 > 0$ , we get

$$\lambda \leq \frac{1}{\alpha-1} \log \left( \sum_{i \in S} r_i^\alpha s_i^{1-\alpha} \right) + \frac{1}{\alpha-1} \log \frac{1}{1 - \sqrt{1 - \varepsilon^2}}. \quad (6.89)$$

Next, we use the data-processing inequality of the Rényi divergences. We use the measurement CPTP map  $\mathcal{M} : X \mapsto \sum_{i \in S} |e_i\rangle\langle e_i| X |e_i\rangle\langle e_i|$  to obtain

$$\mathbb{D}_\alpha(\rho \| \sigma) \geq D_\alpha(\mathcal{M}(\rho) \| \mathcal{M}(\sigma)) = \frac{1}{\alpha-1} \log \left( \sum_{i \in S} r_i^\alpha s_i^{1-\alpha} \right). \quad (6.90)$$

We conclude the proof by substituting this into (6.89) and applying Lemma 6.9.  $\square$

We also note here that  $g(\varepsilon)$  can be bounded by simpler expressions. For example,  $1 - \sqrt{1 - \varepsilon^2} \geq \frac{1}{2}\varepsilon^2$  using a second order Taylor expansion of the expression around  $\varepsilon = 0$  and the fact that the third derivative is non-negative. This is a very good approximation for small  $\varepsilon$ . Hence, (6.85) can be simplified to [155]

$$D_{\max}^\varepsilon(\rho \| \sigma) \leq \mathbb{D}_\alpha(\rho \| \sigma) + \frac{1}{\alpha-1} \log \frac{2}{\varepsilon^2}. \quad (6.91)$$

Proposition 6.5 is of particular interest when applied to the smooth conditional min-entropy. In this case, let  $\rho_{AB} \in \mathcal{S}_\bullet(AB)$  and  $\sigma_B$  be of the form  $I_A \otimes \sigma_B$ . Then, for any  $\alpha \in (1, \infty)$ , we have

$$H_{\min}^\varepsilon(A|B)_\rho \geq \mathbb{H}_\alpha(A|B)_\rho - \frac{g(\varepsilon)}{\alpha-1}, \quad (6.92)$$

where we again take  $\mathbb{H}_\alpha$  to be any conditional Rényi entropy whose underlying divergence satisfies the data-processing inequality. The duality relation for the smooth min- and max-entropies (cf. Proposition 6.2) and the Rényi entropies (cf. Sect. 5.3) yield a corresponding dual relation for the max-entropy.

## 6.4.2 The Asymptotic Equipartition Property

In this section we now apply Proposition 6.5 to two sequences  $\{\rho^n\}_n$  and  $\{\sigma^n\}_n$  of product states of the form

$$\rho^n = \bigotimes_{i=1}^n \rho_i, \quad \sigma^n = \bigotimes_{i=1}^n \sigma_i, \quad \text{with } \rho_i, \sigma_i \in \mathcal{S}_o(A) \quad (6.93)$$

where we assume for mathematical simplicity that the marginal states  $\rho_i$  and  $\sigma_i$  are taken from a finite subset of  $\mathcal{S}_o(A)$ . Proposition 6.5 then yields

$$\frac{1}{n} D_{\max}^\varepsilon(\rho^n \|\sigma^n) \leq \frac{1}{n} \sum_{i=1}^n \tilde{D}_\alpha(\rho_i, \sigma_i) + \frac{g(\varepsilon)}{n(\alpha - 1)}. \quad (6.94)$$

We can further bound the smooth max-divergence in Proposition 6.5 using the Taylor series expansion for the Rényi divergence in (4.101). This means that there exists a constant  $C$  such that, for all  $\alpha \in (1, 2]$  and all  $\rho_i$  and  $\sigma_i$ , we have<sup>1</sup>

$$\tilde{D}_\alpha(\rho_i \|\sigma_i) \leq D(\rho_i \|\sigma_i) + (\alpha - 1) \frac{\log(e)}{2} V(\rho_i \|\sigma_i) + (\alpha - 1)^2 C, \quad (6.95)$$

It is often not necessary to specify the constant  $C$  in the above expression. However, it is possible to give explicit bounds, which is done, for example, in [155]. Substituting the above into (6.94) and setting  $\alpha = 1 + \frac{1}{\sqrt{n}}$  yields

$$\frac{1}{n} D_{\max}^\varepsilon(\rho^n \|\sigma^n) \leq \frac{1}{n} \sum_{i=1}^n D(\rho_i \|\sigma_i) + \frac{1}{\sqrt{n}} \left( g(\varepsilon) + \frac{\log(e)}{2} \frac{1}{n} \sum_{i=1}^n V(\rho_i \|\sigma_i) \right) + \frac{C}{n}. \quad (6.96)$$

Hence, in particular for the iid case where  $\rho_i = \rho$  and  $\sigma_i = \sigma$  for all  $i$ , we find:

**Theorem 6.3** *Let  $\rho \in \mathcal{S}_o(A)$  and  $\sigma \in \mathcal{S}(B)$  and  $\varepsilon \in (0, 1)$ . Then,*

$$\lim_{n \rightarrow \infty} \left\{ \frac{1}{n} D_{\max}^\varepsilon(\rho^{\otimes n} \|\sigma^{\otimes n}) \right\} \leq D(\rho \|\sigma). \quad (6.97)$$

This is the main ingredient of our proof of the AEP below.

### Direct Part

In this section, we are mostly interested in the application of Theorem 6.3 to conditional min- and max-entropies. Here, for any state  $\rho_{AB} \in \mathcal{S}_o(AB)$ , we choose  $\sigma_{AB} = I_A \otimes \rho_B$ . Clearly,

$$H_{\min}^\varepsilon(A^n | B^n)_{\rho^{\otimes n}} \geq -D_{\max}^\varepsilon(\rho_{AB}^{\otimes n} \|\sigma_{AB}^{\otimes n}) \quad (6.98)$$

<sup>1</sup>Here we use that  $\rho_i$  and  $\sigma_i$  are taken from a finite set, so that we can choose  $C$  uniformly.

Thus, by Theorem 6.3, we have

$$\lim_{n \rightarrow \infty} \left\{ \frac{1}{n} H_{\min}^{\varepsilon}(A^n | B^n)_{\rho^{\otimes n}} \right\} \geq \lim_{n \rightarrow \infty} \left\{ -\frac{1}{n} D_{\max}^{\varepsilon}(\rho_{AB}^{\otimes n} \| \sigma_{AB}^{\otimes n}) \right\} \quad (6.99)$$

$$= -D(\rho_{AB} \| \sigma_{AB}) = H(A|B)_{\rho}. \quad (6.100)$$

This and the dual of this relation leads to the following corollary, which is the *direct part* of the AEP.

**Corollary 6.2** *Let  $\rho_{AB} \in \mathcal{S}_{\circ}(AB)$  and  $0 < \varepsilon < 1$ . Then, the smooth entropies of the i.i.d. product state  $\rho_{A^n B^n} = \rho_{AB}^{\otimes n}$  satisfy*

$$\lim_{n \rightarrow \infty} \left\{ \frac{1}{n} H_{\min}^{\varepsilon}(A^n | B^n)_{\rho} \right\} \geq H(A|B)_{\rho} \quad \text{and} \quad (6.101)$$

$$\lim_{n \rightarrow \infty} \left\{ \frac{1}{n} H_{\max}^{\varepsilon}(A^n | B^n)_{\rho} \right\} \leq H(A|B)_{\rho}. \quad (6.102)$$

### Converse Part

To prove asymptotic convergence, we will also need converse bounds. For  $\varepsilon = 0$ , the converse bounds are a consequence of the monotonicity of the conditional Rényi entropies in  $\alpha$ , i.e.  $H_{\min}(A|B)_{\rho} \leq H(A|B)_{\rho} \leq H_{\max}(A|B)_{\rho}$  for normalized states  $\rho_{AB} \in \mathcal{S}_{\circ}(AB)$ . For  $\varepsilon > 0$ , similar bounds can be derived based on the continuity of the conditional von Neumann entropy in the state [2]. However, such bounds do not allow a statement of the form of Corollary 6.2 as the deviation from the von Neumann entropy scales as  $nf(\varepsilon)$ , where  $f(\varepsilon) \rightarrow 0$  only for  $\varepsilon \rightarrow 0$ . (See, for example, [155] for such a weak converse bound.) This is not sufficient for some applications of the asymptotic equipartition property.

Here, we prove a tighter bound, which relies on the bound between smooth max-entropy and smooth min-entropy established in Proposition 6.3. Employing this in conjunction with (6.101) and (6.102) establishes the converse AEP bounds. Let  $0 < \varepsilon < 1$ . Then, using any smoothing parameter  $0 < \varepsilon' < 1 - \varepsilon$ , we bound

$$\frac{1}{n} H_{\min}^{\varepsilon}(A^n | B^n)_{\rho} \leq \frac{1}{n} H_{\max}^{\varepsilon'}(A^n | B^n)_{\rho} + \frac{1}{n} \log \frac{1}{1 - (\varepsilon + \varepsilon')^2}. \quad (6.103)$$

The corresponding statement for the smooth max-entropy follows analogously. Starting from (6.103) we then apply the same argument that led to Corollary 6.2 in order to establish the following *converse part* of the AEP.



**Corollary 6.3** *Let  $\rho_{AB} \in \mathcal{S}_o(AB)$  and  $0 \leq \varepsilon < 1$ . Then, the smooth entropies of the i.i.d. product state  $\rho_{A^n B^n} = \rho_{AB}^{\otimes n}$  satisfy*

$$\lim_{n \rightarrow \infty} \left\{ \frac{1}{n} H_{\min}^\varepsilon(A^n | B^n)_\rho \right\} \leq H(A|B)_\rho \quad \text{and} \quad (6.104)$$

$$\lim_{n \rightarrow \infty} \left\{ \frac{1}{n} H_{\max}^\varepsilon(A^n | B^n)_\rho \right\} \geq H(A|B)_\rho. \quad (6.105)$$

These converse bounds are particularly important to bound the smooth entropies for large smoothing parameters. In this form, the AEP implies strong converse statements for many information theoretic tasks that can be characterized by smooth entropies in the one-shot setting.

### Second Order

It is in fact possible to derive more refined bounds here, in analogy with the second-order refinement for Stein's lemma encountered in Sect. 7.1. First we note that from the above arguments we can deduce that the second-order term scales as

$$D_{\max}^\varepsilon(\rho^{\otimes n} \| \sigma^{\otimes n}) = nD(\rho \| \sigma) + O(\sqrt{n}). \quad (6.106)$$

and thus it suggests itself to try to find an exact expression for the  $O(\sqrt{n})$  term.<sup>2</sup> One finds that the second-order expansion of  $D_{\max}^\varepsilon(\rho^{\otimes n} \| \sigma^{\otimes n})$  is given as [157]

$$D_{\max}^\varepsilon(\rho^{\otimes n} \| \sigma^{\otimes n}) = nD(\rho \| \sigma) - \sqrt{nV(\rho \| \sigma)} \Phi^{-1}(\varepsilon^2) + O(\log n), \quad (6.107)$$

where  $\Phi$  is the cumulative (normal) Gaussian distribution function. A more detailed discussion of this is outside the scope of this book and we defer to [157] instead.

## 6.5 Background and Further Reading

This chapter is largely based on [152, Chaps.4–5]. The exposition here is more condensed compared to [152]. On the other hand, some results are revisited and generalized in light of a better understanding of the underlying conditional Rényi entropies.

The origins of the smooth entropy calculus can be found in classical cryptography, for example the work of Cachin [32]. Renner and Wolf [141] first introduced the classical special case of the formalism used in this book. The formalism was then generalized to the quantum setting by Renner and König [140] in order to investigate randomness extraction against quantum adversaries in cryptography [99]. Based on

<sup>2</sup>Analytic Bounds on the second-order term were also investigated in [11].

this initial work, Renner [139] then defined conditional smooth entropies in the quantum setting. He chose  $\widetilde{H}_\infty^\uparrow$  as the min-entropy (as we do here as well) and he chose  $\widetilde{H}_0^\uparrow$  as the max entropy. Later König, Renner and Schaffner [101] discovered that  $\widetilde{H}_{1/2}^\uparrow$  naturally complements the min-entropy due to the duality relation between the two quantities. Consequently, the max-entropy is defined as  $\widetilde{H}_{1/2}^\uparrow$  in most recent work. (Notably, at the time the structure of conditional Rényi entropies as discussed in this book, in particular the duality relation, was only known in special cases.) Moreover, Renner [139] initially used a metric based on the trace distance to define the  $\varepsilon$ -ball of close states. However, in order for the duality relation to hold for smooth min- and max-entropies, it was later found that the purified distance [156] is more appropriate.

The chain rules were derived by Vitanov et al. [168, 169], based on preliminary results in [20, 160]. The specialized chain rules for classical information in Lemmas 6.7 and 6.8 were partially developed in [138, 176], and extended in [152].

A first achievability bound for the quantum AEP for the smooth min-entropy was established in Renner's thesis [139]. However, the quantum AEP presented here is due to [152, 155]; it is conceptually simpler and leads to tighter bounds as well as a strong converse statement. It is also noteworthy that a hallmark result of quantum information theory, the strong sub-additivity of the von Neumann entropy 5.6, can be derived from elementary principles using the AEP [14].

The smooth min-entropy of classical-quantum states has operational meaning in randomness extraction, as will be discussed in some detail in Sect. 7.3. Decoupling is a natural generalization of randomness extraction to the fully quantum setting (see Dupuis' thesis [48] for a comprehensive overview), and was initially studied in the context of state merging by Horodecki, Oppenheim and Winter [90]. Decoupling theorems can also be expressed in the one-shot setting, where the (fully quantum) smooth min-entropy  $H_{\min}^\varepsilon(A|B)$  attains operational significance [19, 49, 150]. Smooth entropies have been used to characterize various information theoretic tasks in the one-shot setting, for example in [42–44, 138]. The framework has also been used to investigate the relation between randomness extraction and data compression with side information [136]. Smooth entropies have also found various applications in quantum thermodynamics, for example they are used to derive a thermodynamical interpretation of negative conditional entropy [47].

We have restricted our attention to finite-dimensional quantum systems here, but it is worth noting that the definitions of the smooth min- and max-entropies can be extended without much trouble to the case where the side information is modeled by an infinite-dimensional Hilbert space [60] or a general von Neumann algebra [22]. Many of the properties discussed here extend to these strictly more general settings. However, general chain rules and an entropic asymptotic equipartition property are not yet established in the most general algebraic setting [22].

# Chapter 7

## Selected Applications

**Abstract** This chapter gives a taste of the applications of the mathematical toolbox discussed in this book. The discussion of binary hypothesis testing is crucial because it provides an operational interpretation for the two quantum generalizations of the Rényi divergence we treated in this book. This belatedly motivates our specific choice. Entropic uncertainty relations provide a compelling application of conditional Rényi entropies and their properties, in particular the duality relation. Finally, smooth entropies were originally invented in the context of cryptography, and the Leftover Hashing Lemma reveals why this definition has proven so useful.

### 7.1 Binary Quantum Hypothesis Testing

As mentioned before, the Petz and the minimal quantum Rényi divergence both find operational significance in binary quantum hypothesis testing. We thus start by surveying binary hypothesis testing for quantum states. However, the proofs of the statements in this section are outside the scope of this book, and we will refer to the published primary literature instead.

Let us consider the following binary hypothesis testing problem. Let  $\rho, \sigma \in \mathcal{S}_\circ(A)$  be two states. The *null-hypothesis* is that a certain preparation procedure leaves system  $A$  in the state  $\rho$ , whereas the *alternate hypothesis* is that it leaves it in the state  $\sigma$ . If this preparation is repeated independently  $n \in \mathbb{N}$  times, we consider the following two hypotheses.

Null Hypothesis: The state of  $A^n$  is  $\rho^{\otimes n}$ .

Alternate Hypothesis: The state of  $A^n$  is  $\sigma^{\otimes n}$ .

A *hypothesis test* for this setup is an event  $T_n \in \mathcal{P}_\bullet(A^n)$  that indicates that the null-hypothesis is correct. The *error of the first kind*,  $\alpha_n(T_n)$ , is defined as the probability that we wrongly conclude that the alternate hypothesis is correct even if the state is  $\rho^{\otimes n}$ . It is given by

$$\alpha_n(T_n; \rho) := \text{Tr}(\rho^{\otimes n}(I_{A^n} - T_n)). \tag{7.1}$$

Conversely, the error of the second kind,  $\beta_n(T_n)$ , is defined as the probability that we wrongly conclude that the null hypothesis is correct even if the state is  $\sigma^{\otimes n}$ . It is given by

$$\beta_n(T_n; \sigma) := \text{Tr}(\sigma^{\otimes n} T_n). \quad (7.2)$$

### 7.1.1 Chernoff Bound

We now want to understand how these errors behave for large  $n$  if we choose an optimal test. Let us first minimize the average of these two errors (assuming equal priors) over all hypothesis tests, which leads us to the well known distinguishing advantage (cf. Sect. 3.2).

$$\begin{aligned} \min_{T_n \in \mathcal{P}_\bullet(A^n)} \frac{1}{2} (\alpha_n(T_n; \rho) + \beta_n(T_n; \sigma)) &= \frac{1}{2} + \frac{1}{2} \min_{T_n \in \mathcal{P}_\bullet(A^n)} \text{Tr}(T_n(\sigma^{\otimes n} - \rho^{\otimes n})) \\ &= \frac{1}{2} (1 - \Delta(\rho^{\otimes n}, \sigma^{\otimes n})). \end{aligned} \quad (7.3)$$

However, this expression is often not very useful in itself since we do not know how  $\Delta(\rho^{\otimes n}, \sigma^{\otimes n})$  behaves as  $n$  gets large. This is answered by the quantum Chernoff bound which states that the expression in (7.3) drops exponentially fast in  $n$  (unless  $\rho = \sigma$ , of course). The exponent is given by the quantum Chernoff bound [10,127]:

**Theorem 7.1** *Let  $\rho, \sigma \in \mathcal{S}_\circ(A)$ . Then,*

$$\lim_{n \rightarrow \infty} -\frac{1}{n} \log \min_{T_n \in \mathcal{P}_\bullet(A^n)} \frac{1}{2} (\alpha_n(T_n; \rho) + \beta_n(T_n; \sigma)) = \max_{0 \leq s \leq 1} -\log \bar{Q}_s(\rho \| \sigma). \quad (7.4)$$

This gives a first operational interpretation of the Petz quantum Rényi divergence for  $\alpha \in (0, 1)$ .

Note that the exponent on the right-hand side is negative and symmetric in  $\rho$  and  $\sigma$ . The objective function is also strictly convex in  $s$  and hence the minimum is unique unless  $\rho = \sigma$ . The negative exponent is also called the *Chernoff distance* between  $\rho$  and  $\sigma$ , defined as

$$\xi_C(\rho, \sigma) := - \min_{0 \leq s \leq 1} \log \bar{Q}_s(\rho \| \sigma) = \max_{0 \leq s \leq 1} (1 - s) \bar{D}_s(\rho \| \sigma). \quad (7.5)$$

In particular, we have  $\xi_C(\rho, \sigma) \leq D(\rho \| \sigma)$  since  $(1 - s) \leq 1$  in (7.5).

### 7.1.2 Stein's Lemma

In the Chernoff bound we treated the two kind of errors (of the first and second kind) symmetrically, but this is not always desirable. Let us thus in the following consider sequences of tests  $\{T_n\}_n$  such that  $\beta_n(T_n; \sigma) \leq \varepsilon_n$  for some sequence of  $\{\varepsilon_n\}_n$  with  $\varepsilon_n \in [0, 1]$ . We are then interested in the quantities

$$\alpha_n^*(\varepsilon_n; \rho, \sigma) := \min \left\{ \alpha_n(T_n; \sigma) : T_n \in \mathcal{P}_\bullet(A^n) \wedge \beta_n(T_n, \rho) \leq \varepsilon_n \right\}. \quad (7.6)$$

Let us first consider the sequence  $\varepsilon_n = \exp(-nR)$ . Quantum Stein's lemma now tells us that  $D(\rho\|\sigma)$  is a critical rate for  $R$  in the following sense [86, 128].

**Theorem 7.2** *Let  $\rho, \sigma \in \mathcal{S}_\circ(A)$  with  $\rho \ll \sigma$ . Then,*

$$\lim_{n \rightarrow \infty} \alpha_n^*(\exp(-nR); \rho, \sigma) = \begin{cases} 0 & \text{if } R < D(\rho\|\sigma) \\ 1 & \text{if } R > D(\rho\|\sigma) \end{cases}. \quad (7.7)$$

This establishes the operational interpretation of Umegaki's quantum relative entropy. In fact, the respective convergence to 0 and 1 is exponential in  $n$ , as we will see below. An alternative formulation of Stein's lemma states that, for any  $\varepsilon \in (0, 1)$ , we have

$$\lim_{n \rightarrow \infty} -\frac{1}{n} \log \min \left\{ \beta_n(T_n; \sigma) : T_n \in \mathcal{P}_\bullet(A^n) \wedge \alpha_n(T_n, \rho) \leq \varepsilon \right\} = D(\rho\|\sigma). \quad (7.8)$$

#### 7.1.2.1 Second Order Refinements for Stein's Lemma

A natural question then is to investigate what happens if  $-\log \varepsilon_n \approx nD(\rho\|\sigma)$  plus some small variation that grows slower than  $n$ . This is covered by the second order refinement of quantum Stein's lemma [105, 157].

**Theorem 7.3** *Let  $\rho, \sigma \in \mathcal{S}_\circ(A)$  with  $\rho \ll \sigma$  and  $r \in \mathbb{R}$ . Then,*

$$\lim_{n \rightarrow \infty} \alpha_n^*(\exp(-nD(\rho\|\sigma) - \sqrt{nr}); \rho, \sigma) = \Phi \left( \frac{r}{\sqrt{V(\rho\|\sigma)}} \right), \quad (7.9)$$

where  $\Phi$  is the cumulative (normal) Gaussian distribution function.

These works also consider a slightly different formulation of the problem in the spirit of (7.8), and establish that

$$\begin{aligned} & -\log \min \left\{ \beta_n(T_n; \sigma) : T_n \in \mathcal{P}_\bullet(A^n) \wedge \alpha_n(T_n, \rho) \leq \varepsilon \right\} \\ & = nD(\rho\|\sigma) + \sqrt{nV(\rho\|\sigma)} \Phi^{-1}(\varepsilon) + O(\log n). \end{aligned} \quad (7.10)$$

### 7.1.3 Hoeffding Bound and Strong Converse Exponent

Another refinement of quantum Stein's lemma concerns the speed with which the convergence to zero occurs in (7.7) if  $R < D(\rho\|\sigma)$ . The quantum Hoeffding bound shows that this convergence is exponentially fast in  $n$ , and reveals the optimal exponent [76, 123]:

**Theorem 7.4** *Let  $\rho, \sigma \in \mathcal{S}_o(A)$  and  $0 \leq R < D(\rho\|\sigma)$ . Then,*

$$\lim_{n \rightarrow \infty} -\frac{1}{n} \log \alpha_n^*(\exp(-nR); \rho, \sigma) = \sup_{s \in (0,1)} \left\{ \frac{1-s}{s} (\bar{D}_s(\rho\|\sigma) - R) \right\}. \quad (7.11)$$

This yields a second operational interpretation of Petz' quantum Rényi divergence.

A similar investigation can be performed in the regime when  $R > D(\rho\|\sigma)$ , and this time we find that the convergence to one is exponentially fast in  $n$ . The strong converse exponent is given by [119]:

**Theorem 7.5** *Let  $\rho, \sigma \in \mathcal{S}_o(A)$  with  $\rho \ll \sigma$  and  $R > D(\rho\|\sigma)$ . Then,*

$$\lim_{n \rightarrow \infty} -\frac{1}{n} \log \left( 1 - \alpha_n^*(\exp(-nR); \rho, \sigma) \right) = \sup_{s > 1} \left\{ \frac{s-1}{s} (R - \tilde{D}_s(\rho\|\sigma)) \right\}. \quad (7.12)$$

This establishes an operational interpretation of the minimal quantum Rényi divergence for  $\alpha \in (1, \infty)$ .

## 7.2 Entropic Uncertainty Relations

The uncertainty principle [81] is one of quantum physics' most intriguing phenomena. Here we are concerned with preparation uncertainty, which states that an observer who has only access to classical memory cannot predict the outcomes of two incompatible measurements with certainty. Uncertainty is naturally expressed in

terms of entropies, and in fact entropic uncertainty relations (URs) have found many applications in quantum information theory, specifically in quantum cryptography.

Let us now formalize a first entropic UR. For this purpose, let  $\{|\phi_x\rangle\}_x$  and  $\{|\vartheta_y\rangle\}_y$  be two ONBs on a system  $A$  and  $\mathcal{M}_X \in \text{CPTP}(A, X)$  and  $\mathcal{M}_Y \in \text{CPTP}(A, Y)$  the respective measurement maps. Then, Maassen and Uffink's entropic UR [112] states that, for any initial state  $\rho_A \in \mathcal{S}_o(A)$ , we have

$$H_\alpha(X)_{\mathcal{M}_X(\rho)} + H_\beta(Y)_{\mathcal{M}_Y(\rho)} \geq -\log c, \quad \text{where } c = \max_{x,y} |\langle \phi_x | \vartheta_y \rangle|^2 \quad (7.13)$$

is the *overlap* of the two ONBs and the parameters of the conditional Rényi entropy,  $\alpha, \beta \in [\frac{1}{2}, \infty)$ , satisfy  $\frac{1}{\alpha} + \frac{1}{\beta} = 2$ . In the following we generalize this relation to conditional entropies and quantum side information.

### 7.2.1 Tripartite Uncertainty Relation

First, note that an observer with quantum side information that is maximally entangled with  $A$  can predict the outcomes of both measurements perfectly (see, for instance, the discussion in [20]). This can be remedied by considering two different observers—in which case the monogamy of entanglement comes to our rescue. We find that the most natural generalization of the Maassen-Uffink relation is stated for a tripartite quantum system  $ABC$  where  $A$  is the system being measured and  $B$  and  $C$  are two systems containing side information [37, 122].

**Theorem 7.6** *Let  $\rho_{ABC} \in \mathcal{S}(ABC)$  and  $\alpha, \beta \in [\frac{1}{2}, \infty]$  with  $\frac{1}{\alpha} + \frac{1}{\beta} = 2$ . Then,*

$$\tilde{H}_\alpha^\uparrow(X|B)_{\mathcal{M}_X(\rho)} + \tilde{H}_\beta^\uparrow(Y|C)_{\mathcal{M}_Y(\rho)} \geq -\log c, \quad (7.14)$$

*with  $c$  defined in (7.13).*

*Proof* We prove this statement for a pure state  $\rho_{ABC}$  and the general statement then follows by the data-processing inequality. By the duality relation in Proposition 5.3, it suffices to show that

$$\tilde{H}_\alpha^\uparrow(X|B)_{\mathcal{M}_X(\rho)} \geq \tilde{H}_\alpha^\uparrow(Y|Y'B)_{\mathcal{U}_Y(\rho)} - \log c, \quad (7.15)$$

where  $\text{CPTP}(A, YY') \ni \mathcal{U}_Y : \rho_A \mapsto \sum_{y,y'} \langle \vartheta_y | \rho_A | \vartheta_{y'} \rangle |y\rangle\langle y'|_Y \otimes |y\rangle\langle y'|_{Y'}$  is the map corresponding to the Stinespring dilation unitary of  $\mathcal{M}_Y$ . Let us now verify (7.15). We have

$$\tilde{H}_\alpha^\uparrow(Y|Y'B)_{\mathcal{U}_Y(\rho)} = \max_{\sigma_{Y'B} \in \mathcal{S}_\circ(Y'B)} -\tilde{D}_\alpha(\mathcal{U}_Y(\rho_{AB}) \| I_Y \otimes \sigma_{Y'B}) \quad (7.16)$$

$$\leq \max_{\sigma_{Y'B} \in \mathcal{S}_\circ(Y'B)} -\tilde{D}_\alpha(\rho_{AB} \| \mathcal{U}_Y^{-1}(I_Y \otimes \sigma_{Y'B})) \quad (7.17)$$

$$\leq \max_{\sigma_{Y'B} \in \mathcal{S}_\circ(Y'B)} -\tilde{D}_\alpha(\mathcal{M}_X(\rho_{AB}) \| \mathcal{M}_X(\mathcal{U}_Y(I_Y \otimes \sigma_{Y'B}))). \quad (7.18)$$

The first inequality follows by the data-processing inequality pinching the states so that they are block-diagonal with regards to the image of  $\mathcal{U}_Y$  and its complement. We can then disregard the block outside the image since  $\mathcal{U}_Y(\rho_{AB})$  has no weight there using the mean Property (VI). The second inequality is due to data-processing with  $\mathcal{M}_X$ . Now, note that for every  $\sigma_{Y'B}$ , we have

$$\mathcal{M}_X(\mathcal{U}_Y(I_Y \otimes \sigma_{Y'B})) = \sum_y \mathcal{M}_X(|\vartheta_y\rangle\langle\vartheta_y|_A) \otimes \langle y|_{Y'} \sigma_{Y'B} |y\rangle_{Y'} \quad (7.19)$$

$$= \sum_{x,y} |\langle \phi_x | \vartheta_y \rangle|^2 |x\rangle\langle x|_X \otimes \langle y|_{Y'} \sigma_{Y'B} |y\rangle_{Y'} \quad (7.20)$$

$$\leq c \sum_{x,y} |x\rangle\langle x|_X \otimes \langle y|_{Y'} \sigma_{Y'B} |y\rangle_{Y'} = c I_X \otimes \sigma_B. \quad (7.21)$$

Substituting this into (7.18) yields the desired inequality.

## 7.2.2 Bipartite Uncertainty Relation

Based on the tripartite UR in Theorem 7.6, we can now explore bipartite URs with only one side information system. To establish such an UR, we start from (7.15) and use the chain rule in Theorem 5.1 to find

$$\tilde{H}_\alpha^\uparrow(X|B)_{\mathcal{M}_X(\rho)} \geq \tilde{H}_\gamma^\uparrow(YY'|B)_{\mathcal{U}_Y(\rho)} - H_\beta^\uparrow(Y'|B)_{\mathcal{U}_Y(\rho)} - \log c, \quad (7.22)$$

where we chose  $\beta, \gamma \geq \frac{1}{2}$  such that

$$\frac{\gamma}{\gamma-1} = \frac{\alpha}{\alpha-1} + \frac{\beta}{\beta-1} \quad \text{and} \quad (\alpha-1)(\beta-1)(\gamma-1) < 0. \quad (7.23)$$

Then, using the fact that the marginals on  $YB$  and  $Y'B$  of the state  $\mathcal{U}_Y(\rho_{AB}) \in \mathcal{S}_\circ(YY'B)$  are equivalent and that the conditional entropies are invariant under local isometries, we conclude that



$$\tilde{H}_\alpha^\uparrow(X|B)_{\mathcal{M}_X(\rho)} + \tilde{H}_\beta^\uparrow(Y|B)_{\mathcal{M}_Y(\rho)} \geq \tilde{H}_\gamma^\uparrow(A|B)_\rho + \log \frac{1}{c}. \quad (7.24)$$

Interesting limiting cases include  $\alpha = 2$ ,  $\beta \rightarrow \frac{1}{2}$ , and  $\gamma \rightarrow \infty$  as well as  $\alpha, \beta, \gamma \rightarrow 1$ .

Clearly, variations of this relation can be shown using different conditional entropies or chain rules. However, all bipartite URs share the property that on the right-hand side of the inequality there appears a conditional entropy of the state  $\rho_{AB}$  prior to measurement. This quantity can be negative in the presence of entanglement, and in particular for the case of a maximally entangled state the term on the right-hand side becomes negative or zero and the bound thus trivial.

## 7.3 Randomness Extraction

One of the main applications of the smooth entropy framework is in cryptography, in particular in *randomness extraction*, the art of extracting uniform randomness from a biased source. Here the smooth min-entropy of a classical system characterizes the amount of uniformly random key that can be extracted such that it is independent of the side information. More precisely, we consider a source that outputs a classical system  $Z$  about which there exists *side information*  $E$ —potentially quantum—and ask how much uniform randomness,  $S$ , can be extracted from  $Z$  such that it is independent of the side information  $E$ .

### 7.3.1 Uniform and Independent Randomness

The quality of the extracted randomness is measured using the trace distance to a perfect secret key, which is uniform on  $S$  and product with  $E$ . Namely, we consider the distance

$$\Delta(S|E)_\rho := \Delta(\rho_{SE}, \pi_S \otimes \rho_E), \quad (7.25)$$

where  $\pi_S$  is the maximally mixed state. Due to the operational interpretation of the trace distance as a distinguishing advantage, a small  $\Delta$  implies that the extracted random variable cannot be distinguished from a uniform and independent random variable with probability more than  $\frac{1}{2}(1 + \Delta)$ . This viewpoint is at the root of universally composable security frameworks (see, e.g., [33, 167]), which ensure that a secret key satisfying the above property can safely be employed in any (composable secure) protocol requiring a secret key.

A probabilistic protocol  $\mathcal{F}$  extracting a key  $S$  from  $Z$  using a random seed  $F$  is comprised of the following:

- A set  $\mathcal{F} = \{f\}$  of functions  $f : Z \rightarrow S$  which are in one-to-one correspondence with the standard basis elements  $|f\rangle$  of  $F$ .

- A probability mass function  $\tau \in \mathcal{S}_o(F)$ .

The protocol then applies a function  $f \in \mathcal{F}$  at random (according to the value in  $F$ ) on the input  $Z$  to create the key  $S$ . Clearly, this process can be summarized by a classical channel  $\mathcal{F} \in \text{CPTP}(Z, SF)$ . More explicitly, we start with a classical-quantum state  $\rho_{ZE}$  of the form

$$\rho_{ZE} = \sum_z |z\rangle\langle z|_Z \otimes \rho_E(z) = \sum_z \rho(z) |z\rangle\langle z|_Z \otimes \hat{\rho}_E(z), \quad \hat{\rho}_E(z) \in \mathcal{S}_o(E). \quad (7.26)$$

The protocol will transform this state into  $\rho_{SEF} = (\mathcal{F}_{Z \rightarrow SF} \otimes \mathcal{I}_E)(\rho_{ZE})$ , where

$$\rho_{SEF} = \sum_f \tau(f) \hat{\rho}_{SE}(f) \otimes |f\rangle\langle f|_F, \quad \text{and} \quad (7.27)$$

$$\hat{\rho}_{SE}(f) = \sum_s |s\rangle\langle s|_S \otimes \sum_z \delta_{s,f(z)} \rho_E(z) \quad (7.28)$$

is the state produced when  $f$  is applied to the  $Z$  system of  $\rho_{ZE}$ .

For such protocols, we then require that the average distance

$$\sum_f \tau(f) \Delta(S|E)_{\rho_f} = \Delta(S|EF)_{\rho} \quad (7.29)$$

is small, or, equivalently, we require that the extracted randomness is independent of the seed  $F$  as well as  $E$ . This is called the strong extractor regime in classical cryptography, and clearly independence of  $F$  is crucial as otherwise the extractor could simply output the seed. A randomness extractor of the above form that satisfies the security criterion  $\Delta(S|EF)_{\rho} \leq \varepsilon$  is said to be  $\varepsilon$ -secret.

Finally, the maximal number of bits of uniform and independent randomness that can be extracted from a state  $\rho_{ZE}$  is then defined as  $\log_2 \ell^\varepsilon(Z|E)_{\rho}$ , where

$$\ell^\varepsilon(Z|E)_{\rho} := \max \{ \ell \in \mathbb{N} : \exists \mathcal{F} \text{ s.t. } d_S = \ell \wedge \mathcal{F} \text{ is } \varepsilon\text{-secret} \}. \quad (7.30)$$

The classical Leftover Hash Lemma [91, 92, 114] states that the amount of extractable randomness is at least the min-entropy of  $Z$  given  $E$ . In fact, since hashing is an entirely classical process, one might expect that the physical nature of the side information is irrelevant and that a purely classical treatment is sufficient. This is, however, not true in general. For example, the output of certain extractor functions may be partially known if side information about their input is stored in a quantum device of a certain size, while the same output is almost uniform conditioned on any side information stored in a classical system of the same size. (See [65] for a concrete example and [100] for a more general discussion of this topic.)

### 7.3.2 Direct Bound: Leftover Hash Lemma

A particular class of protocols that can be used to extract uniform randomness is based on two-universal hashing [36]. A two-universal family of hash functions, in the language of the previous section, satisfies

$$\Pr_{F \leftarrow \tau} [F(z) = F(z')] = \sum_f \tau(f) \delta_{f(z), f(z')} = \frac{1}{d_S} \quad \forall z \neq z'. \quad (7.31)$$

Using two-universal hashing, Renner [139] established the following bound.

**Proposition 7.1** *Let  $\rho \in \mathcal{S}(ZE)$ . For every  $\ell \in \mathbb{N}$ , there exists a randomness extractor as prescribed above such that*

$$\Delta(S|EF)_\rho \leq \exp\left(\frac{1}{2}(\log \ell - H_{\min}(Z|E)_\rho)\right). \quad (7.32)$$

We provide a proof that simplifies the original argument. We also note that instead of  $H_{\min}$  one can write  $\bar{H}_2^\uparrow$  to get a tighter bound in (7.32).

*Proof* We set  $d_S = \ell$ . Using the notation of the previous section, we have

$$\Delta(S|EF)_\rho = \sum_f \tau(f) \|\hat{\rho}_{SE}(f) - \pi_S \otimes \rho_E\|_1. \quad (7.33)$$

We note that  $\hat{\rho}_E(f) = \rho_E$  does not depend on  $f$ . Then, by Hölder's inequality, for any  $\sigma \in \mathcal{S}_\circ(E)$  such that  $\sigma_E \gg \rho_E^f$  for all  $f$ , we have

$$\|\hat{\rho}_{SE}(f) - \pi_S \otimes \rho_E\|_1 = \|\sigma_E^{\frac{1}{2}} \sigma_E^{-\frac{1}{2}} (\hat{\rho}_{SE}(f) - \pi_S \otimes \rho_E)\|_1 \quad (7.34)$$

$$\leq \|I_S \otimes \sigma_E^{\frac{1}{2}}\|_2 \cdot \|\sigma_E^{-\frac{1}{2}} (\hat{\rho}_{SE}(f) - \pi_S \otimes \rho_E)\|_2 \quad (7.35)$$

$$= \sqrt{d_S \operatorname{Tr}(\sigma_E^{-1} (\hat{\rho}_{SE}(f) - \pi_S \otimes \rho_E)^2)}. \quad (7.36)$$

Hence, Jensen's inequality applied to the square root function yields

$$(\Delta(S|EF)_\rho)^2 \leq d_S \sum_f \tau(f) \operatorname{Tr}(\sigma_E^{-1} (\hat{\rho}_{SE}(f) - \pi_S \otimes \rho_E) (\hat{\rho}_{SE}(f) - \pi_S \otimes \rho_E)) \quad (7.37)$$

$$= \sum_f \tau(f) \operatorname{Tr}(\sigma_E^{-1} \hat{\rho}_{SE}(f) \hat{\rho}_{SE}(f)) - \frac{1}{d_S} \operatorname{Tr}(\sigma_E^{-1} \rho_E^2), \quad (7.38)$$

where we used that  $\pi_S = \frac{1}{d_S} I_S$ . Next, by the definition of  $\hat{\rho}_{SE}(f)$  in (7.28), we find

$$\sum_f \tau(f) \text{Tr} \left( \sigma_E^{-1} \hat{\rho}_{SE}(f) \hat{\rho}_{SE}(f) \right) \quad (7.39)$$

$$= \sum_{f, z, z'} \tau(f) \delta_{f(z), f(z')} \text{Tr} \left( \sigma_E^{-1} \rho_E(z) \rho_E(z') \right) \quad (7.40)$$

$$= \sum_{z \neq z'} \frac{1}{d_S} \text{Tr} \left( \sigma_E^{-1} \rho_E(z) \rho_E(z') \right) + \sum_z \text{Tr} \left( \sigma_E^{-1} \rho_E(z) \rho_E(z) \right) \quad (7.41)$$

$$= \frac{1}{d_S} \text{Tr} \left( \sigma_E^{-1} \rho_E^2 \right) + \left( 1 - \frac{1}{d_S} \right) \text{Tr} \left( \sigma_E^{-1} \rho_{ZE}^2 \right). \quad (7.42)$$

Substituting this into (7.38), we observe that two terms cancel, and maximizing over  $\sigma_E$  we find

$$\Delta(S|EF)_\rho \leq \sqrt{d_S \exp(-\bar{H}_2^\uparrow(Z|E)_\rho)}, \quad (7.43)$$

where we used the definition of  $\bar{H}_2^\uparrow(Z|E)_\rho$  and optimized over all  $\sigma_B$ . The desired bound then follows since  $\bar{H}_2^\uparrow(Z|E)_\rho \geq H_{\min}(Z|E)_\rho$  according to Corollary 5.3.  $\square$

From the definition of  $\ell^\varepsilon(Z|E)_\rho$  we can then directly deduce that

$$\log \ell^\varepsilon(Z|E)_\rho \geq \tilde{H}_2^\uparrow(Z|E)_\rho - 2 \log \frac{1}{\varepsilon} \geq H_{\min}(Z|E)_\rho - 2 \log \frac{1}{\varepsilon}. \quad (7.44)$$

This can then be generalized using the smoothing technique as follows:

**Corollary 7.1** *The same statement as in Proposition 7.1 holds with*

$$\Delta(S|EF)_\rho \leq \exp \left( \frac{1}{2} (\log \ell - H_{\min}^\varepsilon(Z|E)_\rho) \right) + 2\varepsilon. \quad (7.45)$$

*Proof* Let  $\tilde{\rho}_{ZE}$  be a state maximizing  $H_{\min}^\varepsilon(Z|E)_\rho = H_{\min}(Z|E)_{\tilde{\rho}}$ . Then, Proposition 7.1 yields

$$\Delta(S|EF)_{\tilde{\rho}} \leq \exp \left( \frac{1}{2} (\log \ell - H_{\min}^\varepsilon(Z|E)_\rho) \right). \quad (7.46)$$

Moreover, employing the triangle inequality twice, we find that  $\Delta(S|EF)_\rho \leq \Delta(S|EF)_{\tilde{\rho}} + 2\varepsilon$ .  $\square$

This result can also be written in the following form:

$$\log \ell^\varepsilon(Z|E)_\rho \geq H_{\min}^{\varepsilon_1}(Z|E)_\rho - 2 \log \frac{1}{\varepsilon_2}, \quad \text{where } \varepsilon = 2\varepsilon_1 + \varepsilon_2. \quad (7.47)$$

Note that the protocol families discussed above work on any state  $\rho_{ZE}$  with sufficiently high min-entropy, i.e. they do not take into account other properties of the state. Next, we will see that these protocols are essentially optimal.

### 7.3.3 Converse Bound

We prove a converse bound by contradiction. Assume for the sake of the argument that we have an  $\varepsilon$ -good protocol that extracts  $\log \ell > H_{\min}^{\varepsilon'}(Z|E)_\rho$  bits of randomness, where  $\varepsilon' = \sqrt{2\varepsilon - \varepsilon^2}$ . Then, due to Proposition 6.4 we know that applying a function on  $Z$  cannot increase the smooth min-entropy, thus

$$\forall f \in F : H_{\min}^{\varepsilon'}(S|E)_{\rho^f} \leq H_{\min}^{\varepsilon'}(Z|E)_\rho < \log \ell. \quad (7.48)$$

This in turn implies that  $\sum \tau(f) \Delta(S|E)_{\rho^f} > \varepsilon$  as the following argument shows. The above inequality as well as the definition of the smooth min-entropy implies that all states  $\tilde{\rho}$  with

$$P(\tilde{\rho}_{SE}, \rho_{SE}^f) \leq \varepsilon' \quad \text{or} \quad \Delta(\tilde{\rho}_{SE}, \rho_{SE}^f) \leq \varepsilon \quad (7.49)$$

necessarily satisfy  $H_{\min}(S|E)_{\tilde{\rho}} < \log \ell$ . (The latter statement follows from the Fuchs–van de Graaf inequalities in Lemma 3.5.) In particular, these close states can thus not be of the form  $\pi_S \otimes \rho_E$ , because such states have min-entropy  $\log \ell$ . Thus,  $\Delta(S|E)_{\rho^f} > \varepsilon$ .

Since this contradicts our initial assumption that the protocol is  $\varepsilon$ -good, we have established the following converse bound:

$$\log \ell^\varepsilon(Z|E)_\rho \leq H_{\min}^{\varepsilon'}(Z|E)_\rho. \quad (7.50)$$

Collecting (7.47) and (7.50), we arrive at the following theorem.

**Theorem 7.7** *Let  $\rho_{ZE} \in \mathcal{S}_\bullet(ZE)$  be classical on  $Z$  and let  $\varepsilon \in (0, 1)$ . Then,*

$$H_{\min}^{\varepsilon'}(Z|E)_\rho - 2 \log \frac{1}{\delta} \leq \log \ell^\varepsilon(Z|E)_\rho \leq H_{\min}^{\varepsilon''}(Z|E)_\rho, \quad (7.51)$$

for any  $\delta \in (0, \varepsilon)$ ,  $\varepsilon' = \frac{\varepsilon - \delta}{2}$ , and  $\varepsilon'' = \sqrt{2\varepsilon - \varepsilon^2}$ .

We have thus established that the extractable uniform and independent randomness is characterized by the smooth min-entropy, in the above sense. One could now analyze this bound further by choosing an  $n$ -fold iid product state and then apply the AEP to find the asymptotics of  $\frac{1}{n} \log \ell^\varepsilon(Z^n|E^n)_{\rho^{\otimes n}}$  for large  $n$ . More precisely,

using (6.107) we can verify that the upper and lower bounds on this quantity agree in the first order but disagree in the second order. In particular, the dependence on  $\varepsilon$  is qualitatively different in the upper and lower bound. Thus, one could certainly argue that the bounds in Theorem 7.7 are not as tight as they should be in the asymptotic limit. We omit a more detailed discussion of this here (see [157] instead) since most applications consider the task of randomness extraction only in the one-shot setting where the resource state is unstructured.

## 7.4 Background and Further Reading

The quantum Chernoff bound has been established by Nussbaum and Szkolá [127] (converse) and Audenaert et al. [10] (achievability). Quantum Stein's Lemma was shown by Hiai and Petz [86] (achievability and weak converse) and Ogawa and Nagaoka [128] (strong converse). Its second order refinement was proven independently by Li [105] and in [157]. The quantum Hoeffding bound was established by Hayashi [76] (achievability) and Nagaoka [123] (converse). Audenaert et al. [12] provide a good review of these results. The optimal strong converse exponent was recently established by Mosonyi and Ogawa [119].

The limiting cases  $\alpha = \beta = 1$  and  $\alpha \rightarrow \infty, \beta \rightarrow \frac{1}{2}$  of the tripartite Maassen-Uffink entropic UR in Theorem 7.6 were first shown by Berta et al. [20] and in [159], respectively. The former was first conjectured and proven in a special case by Renes and Boileau [137] and extended to infinite-dimensional systems [56, 61]. Here we follow a simplified proof strategy due to Coles et al. [37]. The exact result presented here can be found in [122]. Tripartite URs in the spirit of Sect. 7.2 can also be shown for smooth min- and max-entropies, both for the case of discrete observables in [159], and for the case of continuous observables (e.g. position and momentum) by Furrer et al. [61]. These entropic URs lie at the core of security proofs for quantum key distribution [62, 158].

There exist other protocol families that extract the min-entropy against quantum adversaries, for example based on almost two-universal hashing [160] or Trevisan's extractors [46]. These families are considered mainly because they need a smaller seed or can be implemented more efficiently than two-universal hashing.

# Appendix

## Some Fundamental Results in Matrix Analysis

One of the main technical ingredients of our derivations are the properties of operator monotone and concave functions. While a comprehensive discussion of their properties is outside the scope of this book, we will provide an elementary proof of the Lieb–Ando Theorem in (2.50) and the joint convexity of relative entropy, which lie at the heart of our derivations.

### Preparatory Lemmas

We follow the proof strategy of Ando [4], although highly specialized to the problem at hand. We restrict our attention to finite-dimensional positive definite matrices here and start with the following well-known result:

**Lemma A.1** *Let  $A, B$  be positive definite, and  $X$  linear. We have*

$$\begin{pmatrix} A & X \\ X^\dagger & B \end{pmatrix} \geq 0 \iff A \geq XB^{-1}X^\dagger. \quad (\text{A.1})$$

*Proof* Since the matrix  $\begin{pmatrix} I & -XB^{-1} \\ 0 & I \end{pmatrix}$  is invertible, we find that  $\begin{pmatrix} A & X \\ X^\dagger & B \end{pmatrix} \geq 0$  holds if and only if

$$0 \leq \begin{pmatrix} I & -XB^{-1} \\ 0 & I \end{pmatrix} \begin{pmatrix} A & X \\ X^\dagger & B \end{pmatrix} \begin{pmatrix} I & 0 \\ -B^{-1}X^\dagger & I \end{pmatrix} = \begin{pmatrix} A - XB^{-1}X^\dagger & 0 \\ 0 & B \end{pmatrix}, \quad (\text{A.2})$$

from which the assertion follows. □

From this we can then derive two elementary results:

**Lemma A.2** *The map  $(A, B) \mapsto BA^{-1}B$  is jointly convex and the map  $(A, B) \mapsto (A^{-1} + B^{-1})^{-1}$  is jointly concave.*

The latter expression is proportional to the matrix harmonic mean  $A!B = 2(A^{-1} + B^{-1})^{-1}$ , and its joint concavity was first shown in [3].

*Proof* Let  $A_1, A_2, B_1, B_2$  be positive definite. Then, by Lemma A.1, for any  $\lambda \in [0, 1]$ , we have

$$0 \leq \lambda \begin{pmatrix} A_1 & B_1 \\ B_1 & B_1 A_1^{-1} B_1 \end{pmatrix} + (1 - \lambda) \begin{pmatrix} A_2 & B_2 \\ B_2 & B_2 A_2^{-1} B_2 \end{pmatrix} \quad (\text{A.3})$$

$$= \begin{pmatrix} \lambda A_1 + (1 - \lambda) A_2 & \lambda B_1 + (1 - \lambda) B_2 \\ \lambda B_1 + (1 - \lambda) B_2 & \lambda B_1 A_1^{-1} B_1 + (1 - \lambda) B_2 A_2^{-1} B_2 \end{pmatrix} \quad (\text{A.4})$$

and, invoking Lemma A.1 once again, we conclude that

$$\begin{aligned} & \lambda B_1 A_1^{-1} B_1 + (1 - \lambda) B_2 A_2^{-1} B_2 \\ & \geq (\lambda B_1 + (1 - \lambda) B_2) (\lambda A_1 + (1 - \lambda) A_2)^{-1} (\lambda B_1 + (1 - \lambda) B_2), \end{aligned} \quad (\text{A.5})$$

establishing joint convexity of the first map.

To investigate the second map, we use a Woodbury matrix identity,

$$(A^{-1} + B^{-1})^{-1} = B - B(A + B)^{-1}B, \quad (\text{A.6})$$

which can be verified by multiplying both sides with  $A^{-1} + B^{-1}$  from either side and simplifying the resulting expression. To conclude the proof, we note that  $B(A + B)^{-1}B$  is jointly convex due to the first statement and the fact that  $A + B$  is linear in  $A$  and  $B$ .  $\square$

As a simple corollary of this we find that  $A \mapsto A^{-1}$  and  $B \mapsto B^2$  are convex.

## Proof of Lieb–Ando Theorem

Let us now state Lieb and Ando's results [4, 106].

**Theorem A.1** *The map  $(A, B) \mapsto A^\alpha \otimes B^{1-\alpha}$  on positive definite operators is jointly concave for  $\alpha \in (0, 1)$  and jointly convex for  $\alpha \in (-1, 0) \cup (1, 2)$ .*

*Proof* Using contour integration one can verify that  $\int_0^\infty (1 + \lambda)^{-1} \lambda^{\alpha-1} d\lambda = \pi \sin(\alpha\pi)^{-1}$  for  $\alpha \in (0, 1)$ . By the change of variable  $\lambda \rightarrow \mu = t\lambda$ , we then find the following integral representation for all  $\alpha \in (0, 1)$  and  $t > 0$ :



$$t^\alpha = \frac{\sin(\alpha\pi)}{\pi} \int_0^\infty \frac{t}{\mu+t} \mu^{\alpha-1} d\mu. \quad (\text{A.7})$$

Let us now first consider the case  $\alpha \in (0, 1)$ . Using (A.7), we write

$$A^\alpha \otimes B^{1-\alpha} = (A \otimes B^{-1})^{\alpha-1} \cdot A \otimes I \quad (\text{A.8})$$

$$= \frac{\sin(\alpha\pi)}{\pi} \int_0^\infty (\mu I \otimes I + A \otimes B^{-1})^{-1} A \otimes I \mu^{\alpha-1} d\mu. \quad (\text{A.9})$$

Thus, it suffices to show joint concavity for every term in the integrand, i.e. for the map

$$(A, B) \mapsto (\mu I \otimes I + A \otimes B^{-1})^{-1} A \otimes I = (\mu A^{-1} \otimes I + I \otimes B^{-1})^{-1} \quad (\text{A.10})$$

and all  $\mu \geq 0$ . This is a direct consequence of the second statement of Lemma A.2.

Next, we consider the case  $\alpha \in (1, 2)$ . We again write this as

$$A^\alpha \otimes B^{1-\alpha} = (A \otimes B^{-1})^{\alpha-1} \cdot A \otimes I \quad (\text{A.11})$$

$$= \frac{\sin((\alpha-1)\pi)}{\pi} \int_0^\infty (A \otimes B^{-1})(\mu I \otimes I + A \otimes B^{-1})^{-1} A \otimes I \mu^{\alpha-2} d\mu. \quad (\text{A.12})$$

The integrand here simplifies to

$$(A \otimes B^{-1})(\mu I \otimes I + A \otimes B^{-1})^{-1} A \otimes I = A \otimes I (\mu I \otimes B + A \otimes I)^{-1} A \otimes I. \quad (\text{A.13})$$

However, the first statement of Lemma A.2 asserts that the latter expression is jointly convex in the arguments  $A \otimes I$  and  $\mu I \otimes B + A \otimes I$ . And, moreover, since they are linear in  $A$  and  $B$ , it follows that the integrand is jointly convex for all  $\mu \geq 0$ . The remaining case follows by symmetry.  $\square$

The joint convexity and concavity of the trace functional in (2.50) now follows by the argument presented in Sect. 2.5, which allows to write

$$\text{Tr}(A^\alpha K B^{1-\alpha} K^\dagger) = \langle \Psi | K^\dagger A^\alpha \otimes (B^T)^{1-\alpha} K | \Psi \rangle. \quad (\text{A.14})$$

This thus gives us a compact proof of Lieb's Concavity Theorem and Ando's Convexity Theorem. Finally, we can also relax the condition that  $A$  and  $B$  are positive definite by choosing  $A' = A + \varepsilon I$  and  $B' = B + \varepsilon I$  and taking the limit  $\varepsilon \rightarrow 0$ . Choosing  $K = I$ , we find that this limit exists as long as we require that  $B \gg A$  if  $\alpha > 1$ .

## Joint Convexity of Relative Entropy

As a bonus we will use the above techniques to show that the relative entropy is jointly convex, thereby providing a compact proof of strong sub-additivity.

**Theorem A.2** *The map  $(A, B) \mapsto A \log(A) \otimes I - A \otimes \log(B)$  is jointly convex.*

*Proof* It suffices to prove this statement for the natural logarithm. We will use the representation

$$\ln(t) = \int_0^\infty \frac{1}{\mu + 1} - \frac{1}{\mu + t} d\mu \quad (\text{A.15})$$

Using this integral representation, we then write

$$A \ln(A) \otimes I - A \otimes \ln(B) = \ln(A \otimes B^{-1}) \cdot A \otimes I \quad (\text{A.16})$$

$$= \int_0^\infty \frac{A \otimes I}{\mu + 1} - (\mu I \otimes I + A \otimes B^{-1})^{-1} \cdot A \otimes I d\mu \quad (\text{A.17})$$

$$= \int_0^\infty \frac{A \otimes I}{\mu + 1} - (\mu A^{-1} \otimes I + I \otimes B^{-1})^{-1} d\mu. \quad (\text{A.18})$$

Invoking Lemma A.2, we can check that the integrand is jointly convex for all  $\mu \geq 0$ .  $\square$

As an immediate corollary, we find that

$$D(\rho \parallel \sigma) = \text{Tr}(\rho \log \rho - \rho \log \sigma) = \langle \Psi | \rho \log \rho \otimes I - \rho \otimes \log \sigma^T | \Psi \rangle \quad (\text{A.19})$$

is jointly convex in  $\rho$  and  $\sigma$ . This in turn implies the data-processing inequality for the relative entropy using Uhlmann's trick as discussed in Proposition 4.2. In particular, we find strong subadditivity if we apply the data-processing inequality for the partial trace:

$$H(ABC)_\rho - H(BC)_\rho = D(\rho_{ABC} \parallel I_A \otimes \rho_{BC}) \quad (\text{A.20})$$

$$\leq D(\rho_{AB} \parallel I_A \otimes \rho_B) = H(AB)_\rho - H(B)_\rho. \quad (\text{A.21})$$

# References

1. P.M. Alberti, A note on the transition probability over  $C^*$ -algebras. *Lett. Math. Phys.* **7**, 25–32 (1983). doi:[10.1007/BF00398708](https://doi.org/10.1007/BF00398708)
2. R. Alicki, M. Fannes, Continuity of quantum conditional information. *J. Phys. A: Math. Gen.* **37**(5), L55–L57 (2004). doi:[10.1088/0305-4470/37/5/L01](https://doi.org/10.1088/0305-4470/37/5/L01)
3. W. Anderson, R. Duffin, Series and parallel addition of matrices. *J. Math. Anal. Appl.* **26**(3), 576–594 (1969). doi:[10.1016/0022-247X\(69\)90200-5](https://doi.org/10.1016/0022-247X(69)90200-5)
4. T. Ando, Concavity of certain maps on positive definite matrices and applications to Hadamard products. *Linear Algebra Appl.* **26**, 203–241 (1979)
5. H. Araki, On an inequality of Lieb and Thirring. *Lett. Math. Phys.* **19**(2), 167–170 (1990). doi:[10.1007/BF01045887](https://doi.org/10.1007/BF01045887)
6. H. Araki, E.H. Lieb, Entropy inequalities. *Commun. Math. Phys.* **18**(2), 160–170 (1970)
7. S. Arimoto, Information measures and capacity of order alpha for discrete memoryless channels. *Colloq. Math. Soc. János Bolya* **16**, 41–52 (1975)
8. K.M.R. Audenaert, On the Araki-Lieb-Thirring inequality. *Int. J. Inf. Syst. Sci.* **4**(1), 78–83 (2008). [arXiv:math/0701129](https://arxiv.org/abs/math/0701129)
9. K.M.R. Audenaert, N. Datta,  $\alpha$ -z-relative Rényi entropies. *J. Math. Phys.* **56**, 022202 (2015). doi:[10.1063/1.4906367](https://doi.org/10.1063/1.4906367)
10. K.M.R. Audenaert, L. Masanes, A. Acín, F. Verstraete, Discriminating states: the quantum Chernoff bound. *Phys. Rev. Lett.* **98**(16), 160501 (2007). doi:[10.1103/PhysRevLett.98.160501](https://doi.org/10.1103/PhysRevLett.98.160501)
11. K.M.R. Audenaert, M. Mosonyi, F. Verstraete, Quantum state discrimination bounds for finite sample size. *J. Math. Phys.* **53**(12), 122205 (2012). doi:[10.1063/1.4768252](https://doi.org/10.1063/1.4768252)
12. K.M.R. Audenaert, M. Nussbaum, A. Szkoła, F. Verstraete, Asymptotic error rates in quantum hypothesis testing. *Commun. Math. Phys.* **279**(1), 251–283 (2008). doi:[10.1007/s00220-008-0417-5](https://doi.org/10.1007/s00220-008-0417-5)
13. H. Barnum, E. Knill, Reversing quantum dynamics with near-optimal quantum and classical fidelity. *J. Math. Phys.* **43**(5), 2097 (2002). doi:[10.1063/1.1459754](https://doi.org/10.1063/1.1459754)
14. N.J. Beaudry, R. Renner, An intuitive proof of the data processing inequality. *Quantum Inf. Comput.* **12**(5&6), 0432–0441 (2012). [arXiv:1107.0740](https://arxiv.org/abs/1107.0740)
15. S. Beigi, Sandwiched Rényi divergence satisfies data processing inequality. *J. Math. Phys.* **54**(12), 122202 (2013). doi:[10.1063/1.4838855](https://doi.org/10.1063/1.4838855)
16. S. Beigi, A. Gohari, Quantum achievability proof via collision relative entropy. *IEEE Trans. Inf. Theory* **60**(12), 7980–7986 (2014). doi:[10.1109/TIT.2014.2361632](https://doi.org/10.1109/TIT.2014.2361632)
17. V.P. Belavkin, P. Staszewski,  $C^*$ -algebraic generalization of relative entropy and entropy. *Ann. Henri Poincaré* **37**(1), 51–58 (1982)

18. C.H. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computer, Systems and Signal Processing* (IEEE, Bangalore, 1984) pp. 175–179
19. M. Berta, Single-shot quantum state merging. Master’s thesis, ETH Zurich (2008). [arXiv:0912.4495](https://arxiv.org/abs/0912.4495)
20. M. Berta, M. Christandl, R. Colbeck, J.M. Renes, R. Renner, The uncertainty principle in the presence of quantum memory. *Nat. Phys.* **6**(9), 659–662 (2010). doi:[10.1038/nphys1734](https://doi.org/10.1038/nphys1734)
21. M. Berta, P.J. Coles, S. Wehner, Entanglement-assisted guessing of complementary measurement outcomes. *Phys. Rev. A* **90**(6), 062127 (2014). doi:[10.1103/PhysRevA.90.062127](https://doi.org/10.1103/PhysRevA.90.062127)
22. M. Berta, F. Furrer, V.B. Scholz, The smooth entropy formalism on von Neumann algebras (2011). [arXiv:1107.5460](https://arxiv.org/abs/1107.5460)
23. M. Berta, M. Lemm, M.M. Wilde, Monotonicity of quantum relative entropy and recoverability (2014). [arXiv:1412.4067](https://arxiv.org/abs/1412.4067)
24. M. Berta, K. Seshadreesan, M. Wilde, Rényi generalizations of the conditional quantum mutual information. *J. Math. Phys.* **56**(2), 022205 (2015). doi:[10.1063/1.4908102](https://doi.org/10.1063/1.4908102)
25. M. Berta, M. Tomamichel, The fidelity of recovery is multiplicative. [arXiv:1502.07973](https://arxiv.org/abs/1502.07973)
26. R. Bhatia, *Matrix Analysis*, Graduate Texts in Mathematics (Springer, New York, 1997)
27. R. Bhatia, *Positive Definite Matrices*, Princeton Series in Applied Mathematics (Princeton University Press, Princeton, 2007)
28. L. Boltzmann, Weitere Studien über das Wärmegleichgewicht unter Gasmolekülen. *Sitzungsberichte der Akademie der Wissenschaften zu Wien* **66**, 275–370 (1872)
29. F.G.S.L. Brandão, A.W. Harrow, J. Oppenheim, S. Strelchuk, Quantum conditional mutual information, reconstructed states, and state redistribution (2014). [arXiv:1411.4921](https://arxiv.org/abs/1411.4921)
30. F.G.S.L. Brandao, M. Horodecki, N.H.Y. Ng, J. Oppenheim, S. Wehner, The second laws of quantum thermodynamics. *Proc. Natl Acad. Sci. U S A* **112**(11), 3275–3279 (2014). doi:[10.1073/pnas.1411728112](https://doi.org/10.1073/pnas.1411728112)
31. D. Bures, An extension of Kakutani’s theorem on infinite product measures to the tensor product of semifinite  $\omega^*$ -algebras. *Trans. Am. Math. Soc.* **135**, 199–212 (1969). doi:[10.1090/S0002-9947-1969-0236719-2](https://doi.org/10.1090/S0002-9947-1969-0236719-2)
32. C. Cachin, Entropy measures and unconditional security in cryptography. Ph.D. thesis, ETH Zurich (1997)
33. R. Canetti, Universally composable security: a new paradigm for cryptographic protocols. *Proc. IEEE FOCS*, pp. 136–145 (2001). doi:[10.1109/SFCS.2001.959888](https://doi.org/10.1109/SFCS.2001.959888)
34. E. Carlen, Trace Inequalities and Quantum Entropy, in *Entropy and the Quantum*, vol. 529, Contemporary Mathematics, ed. by R. Sims, D. Ueltschi (AMS, Providence, 2010), 73 p
35. E.A. Carlen, R.L. Frank, E.H. Lieb, Some operator and trace function convexity theorems (2014). [arXiv:1409.0564](https://arxiv.org/abs/1409.0564)
36. J.L. Carter, M.N. Wegman, Universal classes of hash functions. *J. Comput. Syst. Sci.* **18**(2), 143–154 (1979). doi:[10.1016/0022-0000\(79\)90044-8](https://doi.org/10.1016/0022-0000(79)90044-8)
37. P.J. Coles, R. Colbeck, L. Yu, M. Zwolak, Uncertainty relations from simple entropic properties. *Phys. Rev. Lett.* **108**(21), 210405 (2012). doi:[10.1103/PhysRevLett.108.210405](https://doi.org/10.1103/PhysRevLett.108.210405)
38. T.M. Cover, J.A. Thomas, *Elements of Information Theory* (Wiley, New York, 1991). doi:[10.1002/047174882X](https://doi.org/10.1002/047174882X)
39. I. Csiszár, Eine informationstheoretische Ungleichung und ihre Anwendung auf den Beweis der Ergodizität von Markoffschen Ketten. *Magy. Tud. Akad. Mat. Kutato Int. Kozl* **8**, 85–108 (1963)
40. I. Csiszár, Axiomatic characterizations of information measures. *Entropy* **10**, 261–273 (2008). doi:[10.3390/e10030261](https://doi.org/10.3390/e10030261)
41. N. Datta, Min- and max-relative entropies and a new entanglement monotone. *IEEE Trans. Inf. Theory* **55**(6), 2816–2826 (2009). doi:[10.1109/TIT.2009.2018325](https://doi.org/10.1109/TIT.2009.2018325)
42. N. Datta, M.-H. Hsieh, One-shot entanglement-assisted quantum and classical communication. *IEEE Trans. Inf. Theory* **59**(3), 1929–1939 (2013). doi:[10.1109/TIT.2012.2228737](https://doi.org/10.1109/TIT.2012.2228737)
43. N. Datta, F. Leditzky, A limit of the quantum Rényi divergence. *J. Phys. A: Math. Theor.* **47**(4), 045304 (2014). doi:[10.1088/1751-8113/47/4/045304](https://doi.org/10.1088/1751-8113/47/4/045304)

44. N. Datta, M. Mosonyi, M.-H. Hsieh, F.G.S.L. Brandao, A smooth entropy approach to quantum hypothesis testing and the classical capacity of quantum channels. *IEEE Trans. Inf. Theory* **59**(12), 8014–8026 (2013). doi:[10.1109/TIT.2013.2282160](https://doi.org/10.1109/TIT.2013.2282160)
45. N. Datta, R. Renner, Smooth entropies and the quantum information spectrum. *IEEE Trans. Inf. Theory* **55**(6), 2807–2815 (2009). doi:[10.1109/TIT.2009.2018340](https://doi.org/10.1109/TIT.2009.2018340)
46. A. De, C. Portmann, T. Vidick, R. Renner, Trevisan’s extractor in the presence of quantum side information. *SIAM J. Comput.* **41**(4), 915–940 (2012). doi:[10.1137/100813683](https://doi.org/10.1137/100813683)
47. L. del Rio, J. Åberg, R. Renner, O. Dahlsten, V. Vedral, The thermodynamic meaning of negative entropy. *Nature* **474**(7349), 61–63 (2011). doi:[10.1038/nature10123](https://doi.org/10.1038/nature10123)
48. F. Dupuis, The decoupling approach to quantum information theory. Ph.D. thesis, Université de Montréal (2009). [arXiv:1004.1641](https://arxiv.org/abs/1004.1641)
49. F. Dupuis, Chain rules for quantum Rényi entropies. *J. Math. Phys.* **56**(2), 022203 (2015). doi:[10.1063/1.4907981](https://doi.org/10.1063/1.4907981)
50. F. Dupuis, O. Fawzi, S. Wehner, Achieving the limits of the noisy-storage model using entanglement sampling, in *Proceedings of the CRYPTO*, ed. by R. Canetti, J.A. Garay. LNCS, vol. 8043 (Springer, New York, 2013), pp. 326–343. doi:[10.1007/978-3-642-40084-1](https://doi.org/10.1007/978-3-642-40084-1)
51. A.K. Ekert, Quantum cryptography based on Bell’s theorem. *Phys. Rev. Lett.* **67**(6), 661–663 (1991). doi:[10.1103/PhysRevLett.67.661](https://doi.org/10.1103/PhysRevLett.67.661)
52. P. Faist, F. Dupuis, J. Oppenheim, R. Renner, The minimal work cost of information processing. *Nat. Commun.* **6**, 7669 (2015). doi:[10.1038/ncomms8669](https://doi.org/10.1038/ncomms8669)
53. O. Fawzi, R. Renner, Quantum conditional mutual information and approximate Markov chains (2014). [arXiv:1410.0664](https://arxiv.org/abs/1410.0664)
54. S. Fehr, On the conditionl Rényi entropy (2013). <http://www.statslab.cam.ac.uk/biid2013/>
55. S. Fehr, S. Berens, On the conditional Rényi entropy. *IEEE Trans. Inf. Theory* **60**(11), 6801–6810 (2014)
56. R.L. Frank, E.H. Lieb, Extended quantum conditional entropy and quantum uncertainty inequalities. *Commun. Math. Phys.* **323**(2), 487–495 (2013). doi:[10.1007/s00220-013-1775-1](https://doi.org/10.1007/s00220-013-1775-1)
57. R.L. Frank, E.H. Lieb, Monotonicity of a relative Rényi entropy. *J. Math. Phys.* **54**(12), 122201 (2013). doi:[10.1063/1.4838835](https://doi.org/10.1063/1.4838835)
58. C.A. Fuchs, Distinguishability and accessible information in quantum theory. Ph.D. thesis, University of New Mexico (1996). [arXiv:quant-ph/9601020v1](https://arxiv.org/abs/quant-ph/9601020v1)
59. C.A. Fuchs, J. van de Graaf, Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Trans. Inf. Theory* **45**(4), 1216–1227 (1999). doi:[10.1109/18.761271](https://doi.org/10.1109/18.761271)
60. F. Furrer, J. Åberg, R. Renner, Min- and max-entropy in infinite dimensions. *Commun. Math. Phys.* **306**(1), 165–186 (2011). doi:[10.1007/s00220-011-1282-1](https://doi.org/10.1007/s00220-011-1282-1)
61. F. Furrer, M. Berta, M. Tomamichel, V.B. Scholz, M. Christandl, Position-momentum uncertainty relations in the presence of quantum memory. *J. Math. Phys.* **55**, 122205 (2014). doi:[10.1063/1.4903989](https://doi.org/10.1063/1.4903989)
62. F. Furrer, T. Franz, M. Berta, A. Leverrier, V.B. Scholz, M. Tomamichel, R.F. Werner, Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks. *Phys. Rev. Lett.* **109**(10), 100502 (2012). doi:[10.1103/PhysRevLett.109.100502](https://doi.org/10.1103/PhysRevLett.109.100502)
63. R.G. Gallager, *Information Theory and Reliable Communication* (Wiley, New York, 1968)
64. R.G. Gallager, Source coding with side information and universal coding, in *Proceedings of the IEEE ISIT*, vol. 21 (IEEE, Ronneby, 1976)
65. D. Gavinsky, J. Kempe, I. Kerenidis, R. Raz, R. de Wolf, Exponential separation for one-way quantum communication complexity, with applications to cryptography, in *Proceedings of the ACM STOC* (ACM Press, Providence, 2007), pp. 516–525. [arXiv:quant-ph/0611209v3](https://arxiv.org/abs/quant-ph/0611209v3)
66. J.W. Gibbs, On the equilibrium of heterogeneous substances. *Trans. Conn. Acad. Arts Sci.* **3**, 108–248 (1876)
67. A. Gilchrist, N. Langford, M. Nielsen, Distance measures to compare real and ideal quantum processes. *Phys. Rev. A* **71**(6), 062310 (2005). doi:[10.1103/PhysRevA.71.062310](https://doi.org/10.1103/PhysRevA.71.062310)

68. M.K. Gupta, M.M. Wilde, Multiplicativity of completely bounded p-norms implies a strong converse for entanglement-assisted capacity. *Commun. Math. Phys.* **334**(2), 867–887 (2015). doi:[10.1007/s00220-014-2212-9](https://doi.org/10.1007/s00220-014-2212-9)
69. T. Han, S. Verdú, Approximation theory of output statistics. *IEEE Trans. Inf. Theory* **39**(3), 752–772 (1993). doi:[10.1109/18.256486](https://doi.org/10.1109/18.256486)
70. T.S. Han, *Information-Spectrum Methods in Information Theory*, Applications of Mathematics (Springer, New York, 2002)
71. F. Hansen, G.K. Pedersen, Jensen’s operator inequality. *Bull. Lond. Math. Soc.* **35**(4), 553–564 (2003)
72. R.V.L. Hartley, Transmission of information. *Bell Syst. Tech. J.* **7**(3), 535–563 (1928)
73. M. Hayashi, Asymptotics of quantum relative entropy from representation theoretical viewpoint. *J. Phys. A: Math. Gen.* **34**(16), 3413–3419 (1997). doi:[10.1088/0305-4470/34/16/309](https://doi.org/10.1088/0305-4470/34/16/309)
74. M. Hayashi, Optimal sequence of quantum measurements in the sense of Stein’s lemma in quantum hypothesis testing. *J. Phys. A: Math. Gen.* **35**(50), 10759–10773 (2002). doi:[10.1088/0305-4470/35/50/307](https://doi.org/10.1088/0305-4470/35/50/307)
75. M. Hayashi, *Quantum Information—An Introduction* (Springer, Berlin, 2006)
76. M. Hayashi, Error exponent in asymmetric quantum hypothesis testing and its application to classical-quantum channel coding. *Phys. Rev. A* **76**(6), 062301 (2007). doi:[10.1103/PhysRevA.76.062301](https://doi.org/10.1103/PhysRevA.76.062301)
77. M. Hayashi, Second-order asymptotics in fixed-length source coding and intrinsic randomness. *IEEE Trans. Inf. Theory* **54**(10), 4619–4637 (2008). doi:[10.1109/TIT.2008.928985](https://doi.org/10.1109/TIT.2008.928985)
78. M. Hayashi, Information spectrum approach to second-order coding rate in channel coding. *IEEE Trans. Inf. Theory* **55**(11), 4947–4966 (2009). doi:[10.1109/TIT.2009.2030478](https://doi.org/10.1109/TIT.2009.2030478)
79. M. Hayashi, Large deviation analysis for quantum security via smoothing of Rényi entropy of order 2 (2012). [arXiv:1202.0322](https://arxiv.org/abs/1202.0322)
80. M. Hayashi, M. Tomamichel, Correlation detection and an operational interpretation of the Rényi mutual information (2014). [arXiv:1408.6894](https://arxiv.org/abs/1408.6894)
81. W. Heisenberg, Über den Anschaulichen Inhalt der Quantentheoretischen Kinematik und Mechanik. *Z. Phys.* **43**(3–4), 172–198 (1927)
82. K.E. Hellwig, K. Kraus, Pure operations and measurements. *Commun. Math. Phys.* **11**(3), 214–220 (1969). doi:[10.1007/BF01645807](https://doi.org/10.1007/BF01645807)
83. K.E. Hellwig, K. Kraus, Operations and measurements II. *Commun. Math. Phys.* **16**(2), 142–147 (1970). doi:[10.1007/BF01646620](https://doi.org/10.1007/BF01646620)
84. F. Hiai, Concavity of certain matrix trace and norm functions (2012). [arXiv:1210.7524](https://arxiv.org/abs/1210.7524)
85. F. Hiai, M. Mosonyi, D. Petz, C. Bény, Quantum f-divergences and error correction. *Rev. Math. Phys.* **23**(07), 691–747 (2011). doi:[10.1142/S0129055X11004412](https://doi.org/10.1142/S0129055X11004412)
86. F. Hiai, D. Petz, The proper formula for relative entropy and its asymptotics in quantum probability. *Commun. Math. Phys.* **143**(1), 99–114 (1991). doi:[10.1007/BF02100287](https://doi.org/10.1007/BF02100287)
87. F. Hiai, D. Petz, *Introduction to Matrix Analysis and Applications* (Springer, New York, 2014). doi:[10.1007/978-3-319-04150-6](https://doi.org/10.1007/978-3-319-04150-6)
88. A.S. Holevo, *Quantum Systems, Channels, Information* (De Gruyter, Berlin, 2012). doi:[10.1515/9783110273403](https://doi.org/10.1515/9783110273403)
89. M. Horodecki, P. Horodecki, R. Horodecki, Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A* **223**(1–2), 1–8 (1996). doi:[10.1016/S0375-9601\(96\)00706-2](https://doi.org/10.1016/S0375-9601(96)00706-2)
90. M. Horodecki, J. Oppenheim, A. Winter, Partial quantum information. *Nature* **436**(7051), 673–676 (2005). doi:[10.1038/nature03909](https://doi.org/10.1038/nature03909)
91. R. Impagliazzo, L.A. Levin, M. Luby, Pseudo-random generation from one-way functions, in *Proceedings of the ACM STOC* (ACM Press, Providence, 1989), pp. 12–24. doi:[10.1145/73007.73009](https://doi.org/10.1145/73007.73009)
92. R. Impagliazzo, D. Zuckerman, How to recycle random bits, in *Proceedings of the IEEE Symposium on Foundations of Computer Science*, pp. 248–253 (1989). doi:[10.1109/SFCS.1989.63486](https://doi.org/10.1109/SFCS.1989.63486)

93. M. Iwamoto, J. Shikata, Information theoretic security for encryption based on conditional Rényi entropies (2013). <http://eprint.iacr.org/2013/440>
94. R. Jain, J. Radhakrishnan, P. Sen, Privacy and interaction in quantum communication complexity and a theorem about the relative entropy of quantum states, in *Proceedings of the FOCS*, pp. 429–438, IEEE Computer Society, Vancouver (2002). doi:[10.1109/SFCS.2002.1181967](https://doi.org/10.1109/SFCS.2002.1181967)
95. V. Jaksic, Y. Ogata, Y. Pautrat, C.A. Pillet, Entropic fluctuations in quantum statistical mechanics—an introduction, in *Quantum Theory from Small to Large Scales: Lecture Notes of the Les Houches Summer School*, vol. 95 (Oxford University Press, Oxford, 2012)
96. A. Jamiokowski, Linear transformations which preserve trace and positive semidefiniteness of operators. *Rep. Math. Phys.* **3**(4), 275–278 (1972)
97. R. Jozsa, Fidelity for mixed quantum states. *J. Mod. Opt.* **41**(12), 2315–2323 (1994). doi:[10.1080/09500349414552171](https://doi.org/10.1080/09500349414552171)
98. N. Killoran, Entanglement quantification and quantum benchmarking of optical communication devices. Ph.D. thesis, University of Waterloo (2012)
99. R. König, U.M. Maurer, R. Renner, On the power of quantum memory. *IEEE Trans. Inf. Theory* **51**(7), 2391–2401 (2005). doi:[10.1109/TIT.2005.850087](https://doi.org/10.1109/TIT.2005.850087)
100. R. König, R. Renner, Sampling of min-entropy relative to quantum knowledge. *IEEE Trans. Inf. Theory* **57**(7), 4760–4787 (2011). doi:[10.1109/TIT.2011.2146730](https://doi.org/10.1109/TIT.2011.2146730)
101. R. König, R. Renner, C. Schaffner, The operational meaning of min- and max-entropy. *IEEE Trans. Inf. Theory* **55**(9), 4337–4347 (2009). doi:[10.1109/TIT.2009.2025545](https://doi.org/10.1109/TIT.2009.2025545)
102. F. Kubo, T. Ando, Means of positive linear operators. *Math. Ann.* **246**(3), 205–224 (1980). doi:[10.1007/BF01371042](https://doi.org/10.1007/BF01371042)
103. S. Kullback, R.A. Leibler, On information and sufficiency. *Ann. Math. Stat.* **22**(1), 79–86 (1951). doi:[10.1214/aoms/1177729694](https://doi.org/10.1214/aoms/1177729694)
104. O.E. Lanford, D.W. Robinson, Mean entropy of states in quantum-statistical mechanics. *J. Math. Phys.* **9**(7), 1120 (1968). doi:[10.1063/1.1664685](https://doi.org/10.1063/1.1664685)
105. K. Li, Second-order asymptotics for quantum hypothesis testing. *Ann. Stat.* **42**(1), 171–189 (2014). doi:[10.1214/13-AOS1185](https://doi.org/10.1214/13-AOS1185)
106. E.H. Lieb, Convex trace functions and the Wigner-Yanase-Dyson conjecture. *Adv. Math.* **11**(3), 267–288 (1973). doi:[10.1016/0001-8708\(73\)90011-X](https://doi.org/10.1016/0001-8708(73)90011-X)
107. E.H. Lieb, M.B. Ruskai, Proof of the strong subadditivity of quantum-mechanical entropy. *J. Math. Phys.* **14**(12), 1938 (1973). doi:[10.1063/1.1666274](https://doi.org/10.1063/1.1666274)
108. E.H. Lieb, W.E. Thirring, Inequalities for the moments of the eigenvalues of the Schrödinger Hamiltonian and their relation to sobolev inequalities, in *The Stability of Matter: From Atoms to Stars*, chapter III, (Springer, New York, 2005), pp. 205–239. doi:[10.1007/3-540-27056-6\\_16](https://doi.org/10.1007/3-540-27056-6_16)
109. S.M. Lin, M. Tomamichel, Investigating properties of a family of quantum Rényi divergences. *Quantum Inf. Process.* **14**(4), 1501–1512 (2015). doi:[10.1007/s11128-015-0935-y](https://doi.org/10.1007/s11128-015-0935-y)
110. G. Lindblad, Expectations and entropy inequalities for finite quantum systems. *Commun. Math. Phys.* **39**(2), 111–119 (1974). doi:[10.1007/BF01608390](https://doi.org/10.1007/BF01608390)
111. G. Lindblad, Completely positive maps and entropy inequalities. *Commun. Math. Phys.* **40**(2), 147–151 (1975). doi:[10.1007/BF01609396](https://doi.org/10.1007/BF01609396)
112. H. Maassen, J. Uffink, Generalized entropic uncertainty relations. *Phys. Rev. Lett.* **60**(12), 1103–1106 (1988). doi:[10.1103/PhysRevLett.60.1103](https://doi.org/10.1103/PhysRevLett.60.1103)
113. K. Matsumoto, A new quantum version of f-divergence (2014). [arXiv:1311.4722](https://arxiv.org/abs/1311.4722)
114. J. McInnes, Cryptography using weak sources of randomness. Technical report, University of Toronto (1987)
115. C.A. Miller, Y. Shi, Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices (2014). [arXiv:1402.0489](https://arxiv.org/abs/1402.0489)
116. C. Morgan, A. Winter, Pretty strong converse for the quantum capacity of degradable channels. *IEEE Trans. Inf. Theory* **60**(1), 317–333 (2014). doi:[10.1109/TIT.2013.2288971](https://doi.org/10.1109/TIT.2013.2288971)
117. T. Morimoto, Markov processes and the H-theorem. *J. Phys. Soc. Jpn.* **18**(3), 328–331 (1963). doi:[10.1143/JPSJ.18.328](https://doi.org/10.1143/JPSJ.18.328)

118. M. Mosonyi, Rényi divergences and the classical capacity of finite compound channels (2013). [arXiv:1310.7525](#)
119. M. Mosonyi, T. Ogawa, Quantum hypothesis testing and the operational interpretation of the quantum Rényi relative entropies. *Commun. Math. Phys.* **334**(3), 1617–1648 (2014). doi:[10.1007/s00220-014-2248-x](#)
120. M. Mosonyi, T. Ogawa, Strong converse exponent for classical-quantum channel coding (2014). [arXiv:1409.3562](#)
121. M. Müller-Lennert, Quantum relative Rényi entropies. Master thesis, ETH Zurich (2013)
122. M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, M. Tomamichel, On quantum Rényi entropies: a new generalization and some properties. *J. Math. Phys.* **54**(12), 122203 (2013). doi:[10.1063/1.4838856](#)
123. H. Nagaoka, The converse part of the theorem for quantum Hoeffding bound (2006). [arXiv:quant-ph/0611289](#)
124. H. Nagaoka, M. Hayashi, An information-spectrum approach to classical and quantum hypothesis testing for simple hypotheses. *IEEE Trans. Inf. Theory* **53**(2), 534–549 (2007). doi:[10.1109/TIT.2006.889463](#)
125. M.A. Nielsen, I. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000)
126. M.A. Nielsen, D. Petz, A simple proof of the strong subadditivity inequality. *Quantum Inf. Comput.* **5**(6):507–513 (2005). [arXiv:quant-ph/0408130](#)
127. M. Nussbaum, A. Szkoła, The Chernoff lower bound for symmetric quantum hypothesis testing. *Ann. Stat.* **37**(2), 1040–1057 (2009). doi:[10.1214/08-AOS593](#)
128. T. Ogawa, H. Nagaoka, Strong converse and Stein’s lemma in quantum hypothesis testing. *IEEE Trans. Inf. Theory* **46**(7), 2428–2433 (2000). doi:[10.1109/18.887855](#)
129. M. Ohya, D. Petz, *Quantum Entropy and Its Use* (Springer, Heidelberg, 1993)
130. R. Penrose, A generalized inverse for matrices. *Math. Proc. Camb. Philos. Soc.* **51**(3), 406 (1955). doi:[10.1017/S0305004100030401](#)
131. A. Peres, Separability criterion for density matrices. *Phys. Rev. Lett.* **77**(8), 1413–1415 (1996). doi:[10.1103/PhysRevLett.77.1413](#)
132. D. Petz, Quasi-entropies for finite quantum systems. *Rep. Math. Phys.* **23**, 57–65 (1984)
133. Y. Polyanskiy, H.V. Poor, S. Verdú, Channel coding rate in the finite blocklength regime. *IEEE Trans. Inf. Theory* **56**(5), 2307–2359 (2010). doi:[10.1109/TIT.2010.2043769](#)
134. A. Rastegin, Relative error of state-dependent cloning. *Phys. Rev. A* **66**(4), 042304 (2002). doi:[10.1103/PhysRevA.66.042304](#)
135. A.E. Rastegin, Sine distance for quantum states (2006). [arXiv:quant-ph/0602112](#)
136. J.M. Renes, Duality of privacy amplification against quantum adversaries and data compression with quantum side information. *Proc. R. Soc. A* **467**(2130), 1604–1623 (2010). doi:[10.1098/rspa.2010.0445](#)
137. J.M. Renes, J.-C. Boileau, Physical underpinnings of privacy. *Phys. Rev. A* **78**(3), 032335 (2008). doi:[10.1103/PhysRevA.78.032335](#)
138. J.M. Renes, R. Renner, One-shot classical data compression with quantum side information and the distillation of common randomness or secret keys. *IEEE Trans. Inf. Theory* **58**(3), 1985–1991 (2012). doi:[10.1109/TIT.2011.2177589](#)
139. R. Renner, Security of quantum key distribution. Ph.D. thesis, ETH Zurich (2005). [arXiv:quant-ph/0512258](#)
140. R. Renner, R. König, Universally composable privacy amplification against quantum adversaries, in *Proceedings of the TCC*. LNCS, vol. 3378, pp. 407–425. Cambridge University Press, Cambridge (2005). doi:[10.1007/978-3-540-30576-7\\_22](#)
141. R. Renner, S. Wolf, Smooth Rényi entropy and applications, in *Proceedings of the ISIT* (IEEE, Chicago, 2004), pp. 232–232. doi:[10.1109/ISIT.2004.1365269](#)
142. A. Rényi, On measures of information and entropy, in *Proceedings of the Symposium on Mathematical Statistics and Probability* (University of California Press, Berkeley, 1961), pp. 547–561



143. M.B. Ruskai, Another short and elementary proof of strong subadditivity of quantum entropy. *Rev. Math. Phys.* **60**(1), 1–12 (2007). doi:[10.1016/S0034-4877\(07\)00019-5](https://doi.org/10.1016/S0034-4877(07)00019-5)
144. C. Shannon, A mathematical theory of communication. *Bell Syst. Tech. J.* **27**, 379–423 (1948)
145. N. Sharma, N.A. Warsi, Fundamental bound on the reliability of quantum information transmission. *Phys. Rev. Lett.* **110**(8), 080501 (2013). doi:[10.1103/PhysRevLett.110.080501](https://doi.org/10.1103/PhysRevLett.110.080501)
146. M. Sion, On general minimax theorems. *Pac. J. Math.* **8**, 171–176 (1958)
147. W.F. Stinespring, Positive functions on  $C^*$ -algebras. *Proc. Am. Math. Soc.* **6**, 211–216 (1955). doi:[10.1090/S0002-9939-1955-0069403-4](https://doi.org/10.1090/S0002-9939-1955-0069403-4)
148. V. Strassen, Asymptotische Abschätzungen in Shannons Informationstheorie, in *Transactions of the Third Prague Conference on Information Theory*, pp. 689–723, Prague (1962)
149. D. Sutter, M. Tomamichel, A.W. Harrow, Strengthened monotonicity of relative entropy via Pinched Petz recovery map (2015). [arXiv:1507.00303](https://arxiv.org/abs/1507.00303)
150. O. Szechr, F. Dupuis, M. Tomamichel, R. Renner, Decoupling with unitary approximate two-designs. *New J. Phys.* **15**(5), 053022 (2013). doi:[10.1088/1367-2630/15/5/053022](https://doi.org/10.1088/1367-2630/15/5/053022)
151. V.Y.F. Tan, Asymptotic estimates in information theory with non-vanishing error probabilities. *Found. Trends Commun. Inf. Theory* **10**(4), 1–184 (2014). doi:[10.1561/01000000086](https://doi.org/10.1561/01000000086)
152. M. Tomamichel, A framework for non-asymptotic quantum information theory. Ph.D. thesis, ETH Zurich (2012). [arXiv:1203.2142](https://arxiv.org/abs/1203.2142)
153. M. Tomamichel, Smooth entropies: a tutorial with focus on applications in cryptography (2012). <http://2012.qcrypt.net/>
154. M. Tomamichel, M. Berta, M. Hayashi, Relating different quantum generalizations of the conditional Rényi entropy. *J. Math. Phys.* **55**(8), 082206 (2014). doi:[10.1063/1.4892761](https://doi.org/10.1063/1.4892761)
155. M. Tomamichel, R. Colbeck, R. Renner, A fully quantum asymptotic equipartition property. *IEEE Trans. Inf. Theory* **55**(12), 5840–5847 (2009). doi:[10.1109/TIT.2009.2032797](https://doi.org/10.1109/TIT.2009.2032797)
156. M. Tomamichel, R. Colbeck, R. Renner, Duality between smooth min- and max-entropies. *IEEE Trans. Inf. Theory* **56**(9), 4674–4681 (2010). doi:[10.1109/TIT.2010.2054130](https://doi.org/10.1109/TIT.2010.2054130)
157. M. Tomamichel, M. Hayashi, A hierarchy of information quantities for finite block length analysis of quantum tasks. *IEEE Trans. Inf. Theory* **59**(11), 7693–7710 (2013). doi:[10.1109/TIT.2013.2276628](https://doi.org/10.1109/TIT.2013.2276628)
158. M. Tomamichel, C.C.W. Lim, N. Gisin, R. Renner, Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **3**, 634 (2012). doi:[10.1038/ncomms1631](https://doi.org/10.1038/ncomms1631)
159. M. Tomamichel, R. Renner, Uncertainty relation for smooth entropies. *Phys. Rev. Lett.* **106**(11), 110506 (2011). doi:[10.1103/PhysRevLett.106.110506](https://doi.org/10.1103/PhysRevLett.106.110506)
160. M. Tomamichel, C. Schaffner, A. Smith, R. Renner, Leftover hashing against quantum side information. *IEEE Trans. Inf. Theory* **57**(8), 5524–5535 (2011). doi:[10.1109/TIT.2011.2158473](https://doi.org/10.1109/TIT.2011.2158473)
161. M. Tomamichel, M.M. Wilde, A. Winter, Strong converse rates for quantum communication (2014). [arXiv:1406.2946](https://arxiv.org/abs/1406.2946)
162. C. Tsallis, Possible generalization of Boltzmann-Gibbs statistics. *J. Stat. Phys.* **52**(1–2), 479–487 (1988). doi:[10.1007/BF01016429](https://doi.org/10.1007/BF01016429)
163. A. Uhlmann, Endlich-Dimensionale Dichtematrizen II. *Wiss. Z. Karl-Marx-Univ. Leipzig, Math-Nat.* **22**:139–177 (1973)
164. A. Uhlmann, Relative entropy and the Wigner-Yanase-Dyson-Lieb concavity in an interpolation theory. *Commun. Math. Phys.* **54**(1), 21–32 (1977). doi:[10.1007/BF01609834](https://doi.org/10.1007/BF01609834)
165. A. Uhlmann, The transition probability for states of star-algebras. *Ann. Phys.* **497**(4), 524–532 (1985)
166. H. Umegaki, Conditional expectation in an operator algebra. *Kodai Math. Sem. Rep.* **14**, 59–85 (1962)
167. D. Unruh, Universally composable quantum multi-party computation, in *Proceedings of the EUROCRYPT*. LNCS, vol. 6110 (Springer, New York, 2010), pp. 486–505. doi:[10.1007/978-3-642-13190-5](https://doi.org/10.1007/978-3-642-13190-5)
168. A. Vitanov, Smooth min- and max-entropy calculus: chain rules. Master’s thesis, ETH Zurich (2011)

169. A. Vitanov, F. Dupuis, M. Tomamichel, R. Renner, Chain rules for smooth min- and max-entropies. *IEEE Trans. Inf. Theory* **59**(5), 2603–2612 (2013). doi:[10.1109/TIT.2013.2238656](https://doi.org/10.1109/TIT.2013.2238656)
170. J. von Neumann, *Mathematische Grundlagen der Quantenmechanik* (Springer, Berlin, 1932)
171. J. Watrous, *Theory of quantum information*, Lecture Notes (2008). <http://www.cs.uwaterloo.ca/~watrous/quant-info/>
172. J. Watrous, Simpler semidefinite programs for completely bounded norms (2012). [arXiv:1207.5726](https://arxiv.org/abs/1207.5726)
173. M.M. Wilde, Recoverability in quantum information theory. [arXiv:1505.04661](https://arxiv.org/abs/1505.04661)
174. M.M. Wilde, *Quantum Information Theory* (Cambridge University Press, Cambridge, 2013)
175. M.M. Wilde, A. Winter, D. Yang, Strong converse for the classical capacity of entanglement-breaking and Hadamard channels via a Sandwiched Rényi relative entropy. *Commun. Math. Phys.* **331**(2), 593–622 (2014). doi:[10.1007/s00220-014-2122-x](https://doi.org/10.1007/s00220-014-2122-x)
176. S. Winkler, M. Tomamichel, S. Hengli, R. Renner, Impossibility of growing quantum bit commitments. *Phys. Rev. Lett.* **107**(9), 090502 (2011). doi:[10.1103/PhysRevLett.107.090502](https://doi.org/10.1103/PhysRevLett.107.090502)