# Security of Continuous-Variable Quantum Key Distribution and Aspects of Device-Independent Security

Von der Fakultät für Mathematik und Physik
der Gottfried Wilhelm Leibniz Universität Hannover
zur Erlangung des Grades

Doktor der Naturwissenschaften
-Dr. rer. nat.-

genehmigte Dissertation
von

**M. Sc. Fabian Furrer**

geboren am 24.04.1982 in Zürich, Schweiz

**2012**

| | |
|---|---|
| **Referent:** | Prof. Dr. Reinhard F. Werner |
| **Koreferent:** | Prof. Dr. Renato Renner |
| **Koreferent:** | Prof. Dr. Elmar Schrohe |
| **Tag der Promotion:** | 9. November 2012 |

# Abstract

Quantum key distribution is the art of distributing a secure key between remote parties by using quantum communication. The major goal from a theoretical perspective is to prove that, under well-specified assumptions, no information about the key has been leaked during the task. In this thesis, we extend information theoretic tools for proving security of quantum key distribution protocols from finite-dimensional to continuous-variable systems, present a complete finite-key security analysis for a squeezed state protocol and address questions related to device-independent security. Conceptually, it can be subdivided into three main parts.

The first part is devoted to an extension of the smooth min- and max-entropies to the algebraic approach to quantum mechanics in which observables are the fundamental objects and described by the theory of von Neumann algebras. The smooth entropy formalism was introduced to analyze one-shot information theory, which is crucial to studying the security of quantum key distribution. We generalize various properties of these entropies and extend the characterization of privacy amplification and data compression to the situation, in which the side-information is modeled by an arbitrary observable algebra. We further derive an entropic uncertainty relation with quantum side-information for position and momentum observables for both finite and infinite measurement precision.

In the second part, the optimal characterization of the extractable secure key length by the smooth min-entropy for one-way classical post-processing is extended to continuous-variable systems. The obtained key is composable secure and the formalism allows the inclusion of finite-key effects due to finite rounds of quantum communication in a protocol. Using this result, we obtain the first quantitative finite-key analysis proving security against coherent attacks for a continuous-variable protocol where squeezed states are measured via homodyne detection. A positive key rate is obtained for experimentally challenging but achievable parameters. The security proof is based on the application of the entropic uncertainty relation for smooth min- and max-entropies. The key rate is compared with the one obtained under the assumptions of collective attacks.

The third part addresses a fundamental question of device-independent security. We investigate the ability of a correlation table to offer perfect security, meaning that the outcomes of the honest parties are statistically uncorrelated with the outcomes of any measurement an eavesdropper could perform. It turns out that such correlation tables are exactly the ones which are extremal in the convex set of all correlation tables. Motivated by this link, we follow an algebraic approach to construct methods to verify extremality and present a continuous family of extremal correlation tables in the case of two parties with two binary measurements each. Furthermore, we elaborate on the peculiar situation where the correlation table uniquely determines the quantum state and the observable.



**Keywords:** Smooth Min- and Max-Entropies, Continuous-Variable Quantum Key Distribution, Device-Independent Security

# Zusammenfassung

Quanten Schlüssel Verteilung beschreibt den Vorgang, einen sicheren Schlüssel an räumlich getrennte Parteien zu verteilen mit Hilfe von Quantenkommunikation. Die Herausforderung aus Sicht der Theorie ist es zu beweisen, dass wenn gewisse Annahmen erfüllt sind, keine Information über den Schlüssel nach auSSen dringen konnte. In dieser Arbeit, erweitern wir informationstheoretische Methoden der die Sicherheitsanalyse von Quanten Schlüssel Verteilungsprotokollen, die auf endlich dimensionalen Systemen basieren, zu solchen, die auf kontinuierlichen Variablen Systemen basieren. Wir präsentieren weiter einen konkreten Sicherheitsbeweis für ein Protokoll, das auf gequetschten Lichtzuständen basiert und behandeln fundamentale Fragen von geräteunabhängiger Sicherheit. Konzeptuell, besteht die Arbeit aus drei Hauptteilen.

Der erste Teil beschäftigt sich mit der Erweiterung der Smooth Min- und Max-Entropien auf eine algebraische Beschreibung der Quanten Mechanik, in der Observablen eine fundamentale Rolle zukommt und die mittels der Theorie von von Neumann Algebren beschrieben wird. Die Smooth Min- und Max-Entropien sind eingeführt worden, um Einzelschussinformationstheorie zu beschreiben, was notwendig ist um Sicherheit von Quanten Schlüssel Verteilung zu studieren. Wir verallgemeinern verschiedene Eigenschaften dieser Entropien und erweitern die Charakterisierungen von Sicherheitsverstärkung und Datenkompression, wobei die Zusatzinformation mittels allgemeiner Observablenalgebren modelliert wird. Wir leiten weiter eine entropische Unschärferelation mit Quatenzusatzinformation für Ort und Impuls Observablen her für endliche und unendlich genaue Messauflösung her.

Im zweiten Teil, wird die optimale Charakterisierung der extrahierbaren Schlüssellänge durch die Smooth Min-Entropie für klassische Einwegnachverarbeitung für kontinuierliche Variablen Systeme gezeigt. Der so erzeuge Schlüssel ist sicher kombinierbar und der Formalismus erlaubt es, die Effekte aufgrund endlicher Quantenkommunikation zu berücksichtigen. Mit Hilfe dieses Resultats, präsentieren wir die erste quantitative Sicherheitsanalyse die Sicherheit gegen allgemeine Attacke liefert für ein Protokoll mit kontinuierliche Variablen Systemen, in dem gequetschte Zustände mit homodyner Detektion gemessen werden. Eine positive Schlüsselrate ist mit den heutigen Technologien möglich wenn auch anspruchsvoll. Der Sicherheitsbeweis baut auf der Unschärferelation auf. Wir vergleichen die Schlüsselrate auch mit derjenigen die man unter Annahme von kollektiven Attacken errechnet.

Der dritte Teil analysiert eine grundsätzliche Frage von geräteunabhängiger Sicherheit. Wir fragen nämlich was die Eigenschaften einer Korrelationstabelle ist, die Sicherheit garantiert in dem Sinne, dass sie statistisch unabhängig von den Ausgängen all möglicher Messungen ist, die ein potentieller Lauscher machen könnte. Es zeigt sich, dass solche Korrelationstabellen diejenigen sind, die in der Menge aller möglichen extremal sind. Motiviert durch diesen Zusammenhang, benützen wir algebraische Methoden, um Extremalität zu verifizieren und konstruieren eine kontinuierliche Familie von extremalen Punkten für den Fall von zwei Partein mit je zwei binären Messungen. Wir analysieren zudem den Spezialfall, in dem die Korrelationstabelle den Zustande und die Messungen eindeutig bestimmt.



**Schlagwörter:** Smooth Min- und Max-Entropien, Kontinuierliche Variablen Quantenschlüsselverteilung, Geräteunabhängige Sicherheit

# Acknowledgments

First of all, I would like to thank my supervisor Prof. Dr. Reinhard Werner for guiding me through my PhD. He had always time for me for questions and interesting and stimulating discussions. His huge knowledge helped me to always see the big pictures behind the scientific questions.

I am also indebted to Prof. Dr. Stephanie Wehner who was an amazing host during my visit at the Center of Quantum Technology in Singapore. I was profiting a lot from the interesting and prolific collaboration with her. I enjoyed many interesting and illuminative discussions with her and also the members of her group who warmly welcomed me. I'm further very grateful to Prof. Dr. Iordanis Kerenidis for the very inspiring and interesting discussions we had at CQT in Singapore.

Furthermore, I would like to thank Prof. Dr. Renato Renner who hosted me during my visit in Zurich. He also inspired and motivated me to work on the topics presented in this thesis and his research results are reflected at many places in this work.

Moreover, I would like to thank the Graduierten Kollege 1463 and his members for the appealing research environment they provided me during my PhD in Hannover. I enjoyed interesting talks, seminars and discussions about various topics in theoretical physics and mathematics. A special thanks goes to my co-advisor Prof. Dr. Elmar Schrohe who always had time for questions.

I'm very grateful the amazing research atmosphere in the quantum information group in Hannover. For that, I thank all the members of the group I have met during my PhD in Hannover. Especially, my office neighbors Robert Matjeschk and Fabian Transchel with whom I enjoyed many illuminative discussions. A special thank is also going to Prof. Dr. Tobias Osborne who was always motivating me with his passion for physics. He further had always time for explanations and discussion I could profit tremendously.

Very important for my great time during my PhD and especially the work I present in this thesis are all my co-authors: Volkher Scholz, Torsten Franz, Mario Berta, Marco Tomamichel, Johan Aberg, Anthony Leverrier, Renato Renner and Reinhard Werner. I thank all of you for the uncountable interesting and illuminating discussions, all your effort and, last but not least, the passion we all share for science. Without you this work presented in this thesis would not have been possible.

I also thank Tobias Eberle and Vitus Händchen from Quantum Interferometry Group of Prof. Dr. Roman Schnabel at the Albert-Einstein-Institute for explaining me the experimental side of continuous-variable quantum key distribution.

Special thanks for helping me in the writing process of this thesis goes to Torsten Franz, Jörg Duhme, Volkher Scholz, Sarah Harrison, Sönke Schmidt, Corsin Pfister, Ashley Milsted, Christoph Cedzich. Thanks for all the time you have invested together with me in this thesis.

Finally, I like to thank the most precious people in my life, Midori Masuzawa and my parents Maria and Roger Furrer for supporting me during my PhD and for all what they did for me in the past.

# Contents

# 1. Introduction

## 1.1. Outline

This section provides a short guideline to this thesis including a detailed outline of the structure of the work. It should help a reader to get an overview about the content presented in this thesis. Moreover, it should enable readers which are familiar with the topics to find quickly the particular results. This work combines material already presented in [FFW11, BFS11, FFB$^+$11] and [FAR11, Sect. 8]. The content of Chapter 5 is not yet publicly available and presented in this thesis for the first time. In the main text, we omit the explicit reference to the aforementioned papers and preprints and instead the connection between the different topics in this thesis and the references is given in the outline presented below. The conclusion and outlook corresponding to the different topics are collected at the very end of this thesis in Chapter 8.

We start in Sections 1.2, 1.3 and 1.4 with a basic and non-technical introduction to the main topics addressed in this thesis. The idea is to discuss the basic notions and historical developments essential to put the presented results into a bigger picture. Section 1.2 provides an overview about algebraic approaches to model quantum mechanics. Therein also a description of the Hilbert space formalism is presented. In Section 1.3, we discuss the role of entropy measures in information theory by considering simple examples. It starts with the Shannon and von Neumann entropy and proceeds with a discussion of smooth entropies used in the one-shot regime. We close the introduction in Section 1.4 with a preliminary discussion about quantum key distribution focused on security aspects and its connection to entropies, where we also discuss the idea behind device-independent quantum key distribution.

Chapter 2 gives an introduction to C*- and von Neumann algebras. The goal is to set the notation and discuss the mathematical tools used in this thesis. In Chapter 3, we translate concepts from quantum information theory usually described in the language of Hilbert spaces to the language of von Neumann algebras. This is based on own work presented in [BFS11]. The first part, Section 3.1, is a repetition of the basic operator algebra formalism of quantum mechanics. In Section 3.2, we define multipartite quantum systems and the purification of a state on a von Neumann algebra. Section 3.4 generalizes the purified distance from [TCR10] to von Neumann algebras.

With the preliminary results from the previous chapter at hand, we can define and analyze the smooth entropies on von Neumann algebras in Chapter 4 (based on own work from [BFS11] and [FAR11, Section 6]). Section 4.2 contains the definition of the conditional min- and max-entropies. In Section 4.3 the smooth versions thereof are defined. The rest of this chapter is devoted to translate properties and interpretations

of the smooth and non-smooth min- and max-entropies known for finite-dimensional quantum systems to the case of arbitrary quantum systems modeled by von Neumann algebras. Important for further chapters are the uncertainty relation with quantum side-information, Section 4.7, and the result on randomness extraction in the presence of a quantum adversary given in Section 4.8.

Chapter 5 addresses the uncertainty relation for position and momentum operators. We first introduce the differential conditional min- and max-entropies in Section 5.2. The main result is the approximation of the differential min- and max-entropies of continuous outcome measurements by their discrete counterparts when increasing the measurement precision (see Section 5.2.2). The entropic uncertainty relation with quantum side information for position and momentum measurements of finite and infinite precision are discussed in Section 5.3.

In Chapter 6, we use the results derived in the previous two chapters to prove security for a continuous-variable squeezed state protocol against arbitrary quantum attacks (Theorem 6.3.1)(based on own work from [FFB$^+$11]). We start in Section 6.2.1 by stating the composable security definitions and give a general formula for a secure key length in terms of the smooth min-entropy. This key length is then computed for a continuous-variable protocol which is based on quadrature measurements of a two-mode squeezed state (see Section 6.3.1). The security analysis against arbitrary quantum attacks presented in Section 6.3.3 is based on the entropic uncertainty relation with quantum side-information as derived and discussed in the previous two chapters. For comparison, the key length is computed against collective attacks in Section 6.3.4.

A question from device-independent quantum key distribution is addressed and analyzed in Chapter 7 [FFW11]. Section 7.2 aims to introduce the framework suitable to study questions for a device-independent scenario. In Section 7.3, we connect the security question in a quantum key distribution protocol to a geometric property of the correlations of the measurement outcomes, namely, being extremal in the set of all possible quantum correlations [FFW11]. Strategies how to find, or to check whether correlations are extremal are then discussed in Section 7.4.

The thesis ends with a summary of the obtained results and a discussion of future questions in Chapter 8, which is separated according to the three main topics.

## 1.2. Model of Quantum Mechanics

The mathematical formalism of quantum mechanics was developed in the first half of the 19th century. Heisenberg together with Born and Jordan invented the matrix mechanic formalism in 1925 to describe the kinematics of electrons in an atom [Hei25, BJ25, BHJ25]. The main idea was to describe the position and momentum of electrons by selfadjoint operators $Q_i$ and $P_i$ $(i = 1, .., n)$ satisfying the canonical commutation relations $[P_i, P_j] = [Q_i, Q_j] = 0$ and $[P_i, Q_j] = -i\delta_{ij}\hbar$. The obtained results agreed with the quantization rules of Bohr and Sommerfeld proposed at the beginning of the 19th century to explain the deviation of the experimental data with the theory of classical mechanics.

In parallel, Schrödinger developed the wave mechanics [Sch26a, Sch26b], which was also able to reproduce the energy quantization rules for the hydrogen atom. The

idea of Schrödinger was to replace the stationary Hamilton-Jacobi equation by a variational principle. The result was a prescription how to derive a wave equation from the classical Hamiltonian function by replacing the conjugated phase space variables $q_i$ and $p_i$ by the multiplication operator and the derivative $-i\hbar\frac{\partial}{\partial q_i}$. The absolute square of the wave function (solution of the wave equation) was later interpreted by Born as the probability distribution of the position measurement [Bor26].

The equivalence of the matrix mechanic and wave equation formalism was realized soon and a unified mathematical framework was developed based on operators on a Hilbert space. The wave mechanic corresponds then to a irreducible representation of position and momentum operators obeying the canonical commutation relations on the Hilbert space $L^2(\mathbb{R}^n)$. Furthermore, it turned out that for finitely many pairs of canonically conjugated operators $Q_i$ and $P_i$ this is the only irreducible representation up to unitary equivalence [Sto30, vN31].

Let us briefly summarize the mathematical formalism of Hilbert space quantum mechanics by means of a generic experiment described by the three steps: preparation, evolution and measurement. With a preparation, we associate a density operator or state[1] $\rho$ on a Hilbert space $\mathcal{H}$, that is, $\rho$ is a bounded operator on $\mathcal{H}$ admitting a spectral decomposition

$$\rho = \sum_{k=1} \lambda_k |\psi_k\rangle\langle\psi_k| \tag{1.1}$$

with eigenvalues $\lambda_k \geq 0$ satisfying $\sum_k \lambda_k = 1$ and orthogonal normalized eigenvectors $\psi_k \in \mathcal{H}$. More formally, $\rho$ is a positive trace-class operator with $\mathrm{Tr}\rho = 1$. Note that in general, different preparation devices can lead to the same density matrix.[2] A state of finest preparation in which all but one $\lambda_k$ in Equation (1.1) are zero is called a pure state. A state which is not pure is called mixed since it can be modeled as the mixture (convex combination) of states of finest preparation. A measurement device with possible outputs $\{x_k\}_{k=1}^N$ is associated with a set of positive operators $\{E_k\}_{k=1}^N$ on $\mathcal{H}$ satisfying[3]

$$\sum_{k=1}^{N} E_k = \mathbb{1}\,. \tag{1.2}$$

Such a set is referred to as a positive operator valued measure (POVM) or an observable (c.f. [Dav76]). It is called projective or sharp if all the operators are projections. The theory determines the probability distribution $\{p_k\}$ of the outcomes $\{x_k\}$ given that the system is prepared in a state $\rho$, via

$$p_k = \mathrm{Tr}\rho\, E_k\,. \tag{1.3}$$

One commonly identifies projective observables with selfadjoint operators where the spectrum represents the possible outcomes and the positive projection valued measure in the spectral decomposition the measurement operators. Hence, applying the

[1] Later on, we use the terminology state for the functional on $\mathcal{B}(\mathcal{H})$ which is induced by $\rho$ via $a \mapsto \mathrm{Tr}\rho\, a$. In an algebraic approach these objects cannot be identified in general.

[2] One has to carefully distinguish the concept of a preparation device and the density operator [Kra83].

[3] For simplicity we consider here only measurement devices with a finite number of outcomes.

aforementioned rules, the expectation value of the obserbable corresponding to the selfadjoint operator $\mathcal{O}$ can be computed by $\langle \mathcal{O} \rangle_\rho = \mathrm{Tr} \rho \mathcal{O}$.

A general and not necessarily reversible evolution is associated with a completely positive map $\mathcal{E} : \mathcal{B}(\mathcal{H}) \to \mathcal{B}(\mathcal{H})$ satisfying $\mathcal{E}(\mathbb{1}) = \mathbb{1}$, which is called a quantum channel in the following.[4] We use the Heisenberg picture in which the evolution is applied to the measurement operators, that is, it maps the observable $\{E_k\}_{k=1}^N$ onto the observable $\{\mathcal{E}(E_k)\}_{k=1}^N$. Hence, the set $\{\mathcal{E}(E_k)\}_{k=1}^N$ describes the transformed measurement operators before the evolution of the system.

Motivated by this description of quantum mechanics, von Neumann started to study subalgebras of operators on a Hilbert space [vN29], which led to the notion of weakly*-closed subalgebras, nowadays called von Neumann algebras. It was shown that such subalgebras were sufficient to enclose the projection valued measures of the spectral decompositions of all normal operators. In fact, as realized later, it is sufficient to consider the commutative norm-closed $*$-algebras generated by the normal operators to analyze its spectral properties (see, e.g., [Seg47]). The study of norm-closed subalgebras (C*-algebras) was initialized by Gelfand and Neumark [GN43]. It turned out that a simple condition, namely, that $\|A^*A\| = \|A\|^2$, was sufficient to characterize general closed subalgebras of bounded operators on a Hilbert space. The theory of C*-algebras was further developed by Segal and used to give an axiomatic description of quantum mechanics [Seg47]. He also observed the tight connection between states and representations of a C*-algebra which is discussed in Section 2.1.2. Since then, the theory of operator algebras emerged as an independent discipline in modern mathematics.

The theory of C*- and von Neumann algebras in physics turned out to be necessary for systems described infinitely many pairs of canonical commuting operators $Q_i$ and $P_i$. In that case there exist no unique irreducible representation anymore. This problem appears for instance in the thermodynamic limit or in quantum field theory (see e.g. [BR79, BR81, Haa92] and references therein). In quantum statistical mechanics the different representations of the C*-algebras are associated with different phases of the material. In particular, an equilibrium state in the thermodynamic limit induces a concrete representation. The von Neumann algebra is then obtained by taking the weak* closure.

The fundamental object in an algebraic approach to quantum mechanics is the algebra generated by the observables of the physical system. A C*-algebra $\mathcal{A}$ captures the abstract mathematical structure of the observables independent of the representation on a particular Hilbert space. States on a C*-algebra are linear positive functionals $\omega : \mathcal{A} \to \mathbb{C}$ and the expectation of an observable $A$ is given in analogy to the Hilbert space quantum mechanics by $\omega(A)$. The C*-algebra approach for instances allows to study general properties induced by simple relations between the

[4] For a definition of completely positive see Section 3.1. An example of a quantum channel is the (reversible) time evolution of a closed system. It is induced by a selfadjoint operator $H$, the Hamiltonian, and the quantum channel at time t is given by $\mathcal{E}_t(A) = U(t)^* A U(t)$, where $U(t) = \exp(-iHt)$.

measurement observables. This is for instance used in Section 7 to analyze properties of general correlation experiments.

Von Neumann algebras are usually used if one is interested in particular representations of C*-algebra on a Hilbert space. They are obtained by taking the weak*-closure of a C*-algebra. Constructively, this means that for any sequence of observables $\{A_i\}$ for which $\omega(A_i)$ is a convergent sequence for any state $\omega$, we add the observable $A$ corresponding to the limit point. This is physically reasonable and provides analytical simplifications. It for instance allows to work in a representation in which all the states are pure that is given by vector states of the underlying Hilbert space.

Compared to the Hilbert space quantum mechanics, the use of the algebraic approach brings the advantage that symmetries of the physical system can naturally be incorporated in the description. Let us assume that the physical system or the state one is interested in, is invariant under the symmetry group $G$. This is mathematically modelled by a unitary group representation of $G$ acting on the set of bounded operators on the Hilbert space associated with the system. Hence, all the relevant observables have to be invariant under the action of the unitary group representation. But the set of invariant operators form a subalgebra which can be weakly closed to obtain the von Neumann algebra generated by the relevant observables.

## 1.3. Entropies in Quantum Information Theory

Quantum information theory studies how quantum systems and features thereof can be beneficially used to perform information theoretic or computational tasks. One important question is if and to which extend implementations based on quantum systems can outperform their classical counterparts. In order to quantify the performance of such tasks entropy measures play a fundamental role. This idea goes back to the beginning of classical information theory initialized by a seminal work of Shannon [Sha48]. In this work he addressed questions of how to quantify the uncertainty of an information source and put it in relation with the capacity of a channel. A classical source is in general described by a random variable $X$ assumed to take values in a finite alphabet $\mathcal{X}$ and distributed according to a probability distribution $\{p_x\}_{x\in\mathcal{X}}$. The measure of uncertainty introduced in [Sha48] is nowadays called Shannon entropy and defined as

$$\mathrm{H}(X)_p = -\sum_{x\in\mathcal{X}} p_x \log p_x. \tag{1.4}$$

One usually measures information in bits so the logarithm log in the definition of the entropy is taken with base 2. The quantity has the property that if the source ejects always the same output the entropy is zero. The maximal value is given by $\log|\mathcal{X}|$ and attained for the uniform distribution. The Shannon entropy can be axiomatically derived from a set of properties expected to hold for an uncertainty measure [Sha48, Rén60].

The Shannon entropy can be seen as the expectation value of the information function $-\log p_k$ and as such, the law of large numbers implies that

$$-\frac{1}{n}\log(p_{x_1}p_{x_2}...p_{x_n}) \to \mathrm{H}(X)_p \quad (n\to\infty)$$

if the values $x_i$ are generated by an independent and identically distributed (i.i.d.) source characterized by $\{p_x\}_{x=1}^d$. Output strings $(x_1, ..., x_n)$ for which $p_{x_1}p_{x_2}...p_{x_n} \approx 2^{n\mathrm{H}(X)_p}$ are called typical and the number of them is approximately $2^{n\mathrm{H}(X)_p}$ [CT91]. This is thus directly connected to coding problems in the sense that the number of bits per signal (rate) which has to be stored without losing information of a source is given by $\mathrm{H}(X)_p$ [Sha48, CT91]. This holds in the asymptotic limit which denotes the limit of infinite repetitions ($n \to \infty$) of an i.i.d. source under the constraint that the probability that an error occurs tends to zero. The performance in this asymptotic limit is called rate. The asymptotic limit of most of the classical information theoretic problems like various versions of data compression and channel codings can be characterized by the Shannon entropy [Sha48, CT91].

Similar questions can now be addressed in a quantum setting. A quantum system $A$ is characterized by a Hilbert space $\mathcal{H}_A$ and the source by a density matrix $\rho_A$ on $\mathcal{H}_A$.[5] The quantum counterpart of the Shannon entropy is the von Neumann entropy first introduced in quantum statistical physics

$$\mathrm{H}(A)_\rho = -\mathrm{Tr}\rho_A \log \rho_A \,. \tag{1.5}$$

It can be interpreted as the minimization of the Shannon entropy over all outcome distributions obtained by rank one measurement (see for instance [NC00, Wil11]). Schumacher proved that in the asymptotic limit, similar to the classical case, the numbers of qubits[6] per signal needed to encode an i.i.d. source characterized by $\rho_A$ is roughly $\mathrm{H}(A)_\rho$ [Sch95]. An i.i.d. quantum source is a resource which produces in each run the same state $\rho_A$ which is uncorrelated to all the others. Hence, after $n$ runs, we end up with the n-fold tensor product state $\rho_A^{\otimes n} = \rho_A \otimes ... \otimes \rho_A$ on the Hilbert space $\mathcal{H}_A^{\otimes n}$. For large $n$ there exists now a typical subspace $\mathcal{K}$ of $\mathcal{H}_A^{\otimes n}$ with dimension $2^{n\mathrm{H}(A)_\rho}$ such that the projection of $\rho_A^{\otimes n}$ onto $\mathcal{K}$ fails with small probability which goes to zero as $n$ tends to infinity [Sch95].

An important role in information theory plays side information which describes the instant that one has certain pre-knowledge about the source. In the classical case such a situation can be modeled by considering two correlated random variables $X$ and $Y$ jointly distributed according to $p(x, y)$ on $\mathcal{X} \times \mathcal{Y}$. Here, $X$ characterizes the source and $Y$ our pre-knowledge. The distribution of the source $X$ conditioned on the even that the value $y$ is known is simply the conditional distribution $p(x|y) = p(x, y)/p_Y(y)$, where $p_Y(y) = \sum_x p(x, y)$ is the probability distribution of $Y$. For instance, if $X$ and $Y$ are maximally correlated $p(x, y) = 1/(|\mathcal{X}|)\delta_{xy}$ then the value $y$ completely determines the value of $x$ described by $p(x|y) = \delta_{xy}$. Let us consider again the coding problem of how many bits of information one has to store in order to recover the output of the source $X$ given that we know $Y$. Thus, we have to count the number of typical sequences for $n$ repetitions of the i.i.d. event distributed

[5] We use the letters $X$, $Y$ and $Z$ to denote classical systems and $A$, $B$ and $C$ for quantum systems. In order to avoid technical issues, we use here the Hilbert space description of quantum mechanics.

[6] A qubit is a quantum system with two degrees of freedom like for instance a spin-1/2 system or the polarization of a photon.

according to $p(x, y)$. Let us separate the events first according to the value of $Y$. Since $n$ is large, the number of events where $y$ occurs is given by $p_Y(y)n$ which can then be reliably encoded by compression to approximately $2^{p_Y(y)nH(X|Y=y)}$ bits, where $H(X|Y = y)$ is the Shannon entropy of the conditional probability distribution $p(x|y)$. Hence, the total average number of bits can be computed to be

$$\frac{1}{n} \log \Big( \prod_y 2^{p_Y(y)nH(Y)_{p_X}} \Big) = \sum_y p_Y(y) H(X|Y = y) \; . \tag{1.6}$$

The right hand side is the expectation value of the entropy of $X$ with respect to $Y$ and defines the conditional Shannon entropy $H(X|Y)$. A simple computation shows that it can be rewritten as $H(X|Y) = H(XY) - H(Y)$. This suggests that in the asymptotic limit the information behaves "additive". The conditional Shannon entropy characterizes the coding problem of correlated sources known as the Slepian-Wolf theorem [SW71], or the capacity of noisy classical channels [Sha48].

This motivates to define the quantum conditional entropy in a similar fashion. Let $A$ and $B$ be two quantum systems modeled on Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, and $\rho_{AB}$ a joint state on $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. We define the conditional von Neumann entropy by

$$\mathrm{H}(A|B)_\rho = \mathrm{H}(AB)_\rho - \mathrm{H}(B)_\rho \, , \tag{1.7}$$

where $\mathrm{H}(AB)_\rho$ and $\mathrm{H}(B)_\rho$ denote the von Neumann entropies of $\rho_{AB}$ and $\rho_B$. This definition can also be used for hybrid models consisting of quantum and classical degrees of freedom. For that, one embeds the classical system $X$ into a Hilbert space $\mathcal{H}_X = \mathrm{span}\{|x\rangle \;\; x \in \mathcal{X}\}$, where $\{|x\rangle\}_{x\in\mathcal{X}}$ is an orhthonormal basis. A probability distribution $p(x)$ over $x$ is then mapped to the quantum state $\rho_X = \sum_x p(x)|x\rangle\langle x|$ which is diagonal with respect to the basis $|x\rangle$. It is easy to see that the Shannon entropy of $p(x)$ is equal to the von Neumann entropy of $\rho_X$. The embedding can be extended to hybrid systems containing a classical part $X$ and a quantum part $A$ characterized by ensembles $(p(x), \rho_A^x)$ and written as states on a Hilbert space by $\rho_{XA} = \sum_x p(x)|x\rangle\langle x| \otimes \rho_A^x$. In the asymptotic limit, the conditional entropy $\mathrm{H}(X|A)$ characterizes for instance the coding problem if the side-information is encoded in the quantum states $\{\rho_A^x\}$ [DW03]. Moreover, it determines the rate by which classical information can be sent through a quantum channel via the Holevo-Schumacher-Westmoreland theorem [SW97, Hol98]. The fully quantum conditional entropy $H(A|B)$ is related to quantum stage merging [HOW05, HOW06].

The simplifying assumption to consider the limit of infinite repetitions of an i.i.d. resource used in the asymptotic limit are justified for many scenarios. But there are exceptions in which a non-asymptotic treatment is necessary. This is for instance the case if one analyzes the security of cryptographic protocols where these assumptions can offer loop holes for possible attacks. It is thus important to have information measures which characterize the single use of a source, the so-called one-shot scenario. Possible measures are the $\alpha$-Rényi entropies which satisfy, like the Shannon entropy, properties expected from an uncertainty measure [Rén60]. For

a quantum state $\rho_A$ and $\alpha \in [0, \infty]$, they are defined by[7]

$$H_\alpha(A)_\rho = \frac{1}{1-\alpha} \log \mathrm{Tr} \rho^\alpha \,, \tag{1.8}$$

where the cases $\alpha = 1, \infty$ are defined as the corresponding limit. In the case $\alpha = 1$, we retrieve the von Neumann entropy and $\alpha = \infty$ corresponds to the min-entropy $H_{\min}(A)_\rho = -\log \|\rho_A\|$.

The min-entropy appeared in connection with randomness extraction in [ILL89], where also the operational concept of entropy smoothing was introduced (c.f. [CM96]).[8] The idea was extended to a more abstract concept of smooth conditional Rényi entropies by Renner and Wolf [RW04] and applied to randomness extraction and channel coding in the one-shot regime. The idea behind entropy smoothing is that in a one-shot regime, the success is only defined up to some error probability. Let us for instance consider the task of randomness extraction, where one starts with a random variable $X$ which should be compressed to a smaller alphabet such that the new variable is uniformly distributed. In general, complete uniformity is not achievable but one can make the probability $\epsilon$ that a malicious party can distinguish it from the uniform distribution arbitrary small. In particular, the statistical distance to uniform is $\epsilon$ if one compresses $X$ to

$$\ell \approx \mathrm{H}_{\min}(X) - O(\log \frac{1}{\epsilon}) \tag{1.9}$$

bits [ILL89].

In [RW04], they showed that a further optimization of the min-entropy over probability distributions, which cannot be distinguished from the original one with probability higher than $\epsilon'$, preserves the desired properties of the entropy measure and leads in the asymptotic limit to the von Neumann entropy. This so-called $\epsilon'$-smooth min-entropy quantifies now the extractable key length $\ell$ in Equation (1.9) with an error $\epsilon+\epsilon'$. It further holds that the $\epsilon$-smooth min-entropy deviates from all Rényi entropies with $\alpha > 1$ only in a term logarithmic in $1/\epsilon$ and thus, concerning operational questions, unifies the properties of all these entropies [RW04]. Same results has been obtained for classical data compression using the $\alpha = 0$ Rényi-entropy [BS94, RW04] (c.f. Section 4.9). As a counterpart to the smooth min-entropy emerged the smooth max-entropy which, from an operational view point, unifies the properties of the Rényi entropies of order $\alpha < 1$.

The concept of smooth entropies was generalized to the quantum and the classical-quantum hybrid setting in [Ren05] and subsequently further analayzed and developed in [KRS09, TCR10]. In particular, a pair of smooth entropies where introduced, the so-called smooth min- and max-entropy, where the min-entropy of a classical random variable belongs to the $\alpha = \infty$ and the (new) max-entropy to the $\alpha = 1/2$ Rény entropy [KRS09].[9] Optimal one-shot characterization of data compression or randomness extraction with quantum side-information and quantum

[7] They were first defined by Rényi for classical systems [Rén60]. The classical version are obtained by embedding the classical system into a quantum system as described before.

[8] Similar results were developed independently in [BBR88].

[9] Renner introduced in [Ren05] the max-entropy as the $\alpha = 0$ Rényi entropy.

state merging by smooth conditional min- and max-entropies (see Definition 4.3.2) are presented in [RR12, Ren05, TSSR10, Ber08]. It was shown that the smooth min- and max-entropy converge in the asymptotic limit to the von Neumann entropy [Ren05, TCR10] (c.f. Section 4.5.3), by which the results discussed before are retrieved.

In Chapter 4, we discuss the smooth min- and max-entropy from a more algebraic point of view by using the von Neumann algebra generated by the observables as the fundamental object. So far they were mostly considered for finite-dimensional quantum systems except in [Fur09] where a functional analytic approach has been used to analyze these entropies in separable Hilbert spaces. There an approximation was presented, which allowed to carry over results from the finite-dimensional to the infinite-dimensional setting (c.f. Section 4.5.2). From a theory point of view, this has the downside that it does not illuminated the algebraic properties of these entropies. But since the min-entropy is essentially determined by the positivity structure (c.f. Definition 4.2.1) on the von Neumann algebra an algebraic approach seems to be natural.

In operator algebra many studies of entropy measures started from the concept of relative entropies between two states relevant in hypothesis testing (see e.g. [HP91, OP93] and references therein). Araki defined the relative entropy for two states in a von Neumann algebra via the modular operator [Ara75]. Petz generalized the concept to the so-called quasi-entropies [Pet85, Pet86] by considering arbitrary operator concave functions of the modular operator. In contrast, the min-entropy leads to a concept of a relative max-entropy [MD09] which can be written as the norm of the non-commutative Radon-Nykodim derivative. Hence, the min-entropy cannot be reduced to the study of quasi-entropies and thus, requires new techniques.

## 1.4. Quantum Key Distribution

The insight that properties of a quantum system can offer security of a key distribution protocol which does not rely on computational assumptions, goes back to a seminal paper by Bennet and Brassard in 1984 [BB84].[10] It can be seen as one of the first applications where quantum features prove to overcome limitations inherent in any classical implementation. Quantum key distribution (QKD) denotes the task to distribute a random bit string between two remote parties Alice and Bob by means of quantum and classical communication which is secure against eavesdropping of a third party called Eve (see [SBPC$^+$09] for a survey). The idea why quantum communication offers security is based on the principle that any interaction of Eve with the quantum channel introduces a disturbance of the system [KSW08] which can be detected. One can differ between two main categories of protocols depending on how the quantum system is distributed. In the case where Alice prepares the state, sends it to Bob whereupon he performs a measurement, is called a prepare and measure protocol [BB84]. Another approach introduced by Ekert in [Eke91] is based on the preparation of an entangled state which is then distributed between Alice and

[10] The first idea to use quantum features goes back to Wiesner in 1983 [Wie84], who proposed quantum money to enable security against counterfeiting.

Bob who subsequently measure it. Such protocols are referred to as entanglement based protocols and its conversion to prepare and measure protocols is discussed in [BBM92].

The security analysis of entanglement based QKD protocols can for instance be reduced to the distillation of maximally entangled qubits (singlets). In that case the security can be inferred from the monogamy property of entanglement (see e.g., [SP00, TKI03]). Other arguments using more information theoretical arguments are based on the idea of the uncertainty principle [May96, Koa06, TLGR12]. For both approaches, it is important how one quantifies the security of the generated key. For long time, one considered a small accessible information $\mathrm{I}_{\mathrm{ac}}(S:E)$ between the key $S$ and the quantum system $E$ as sufficient.[11] But as shown lately in [KRBM07], this security definition is not composobale, which means that the key can become insecure if used in another protocol like for instance one-time pad encryption of a message.[12] Composable security definitions has been presented in [BOHL$^+$05, RK05, Ren05].

Using one-way classical post processing consisting of error correction (see Section 4.9) and privacy amplification (see Section 4.8), the optimal lower bound on the number of extractable composable secure bits can be characterized in terms of the smooth min-entropy [Ren05]:[13]

$$\ell \approx \mathrm{H}_{\min}^{\epsilon}(\mathrm{X_A}|\mathrm{E})_{\omega} - \mathrm{leak}_{\mathrm{EC}} - \mathrm{O}(\log \frac{1}{\epsilon'}) \,.$$

Here, $\mathrm{leak}_{\mathrm{EC}}$ denotes the number of bits leaked in the error correction phase and $\epsilon$ ,$\epsilon'$ determine the failure probability of the protocol. This connects the problem of proving security of the generated key to the challenging task of finding a lower bound on the smooth min-entropy only based on the measured data during the protocol.

In order to estimate the knowledge of an eavesdropper (which is for instance linked in Equation (1.4) to estimate $\mathrm{H}_{\min}^{\epsilon}(\mathrm{X_A}|\mathrm{E})_{\omega}$), one usually restricts the power of the considered attacks. The most common restriction is that Eve is limited to apply always the same attack to each quantum signal.[14] If Eve's output of such an attack is classical then one calls it an individual attack. If Eve's output is a quantum state which she can store in a quantum memory and measure at any stage of the protocol (even after the protocol ended and conditioned on further information), one talks about collective attacks. The most general attacks in which Eve is only limited by the law of quantum mechanics are called coherent attacks.

In the simplest case of individual attacks the problem of composability is similar as in the purely classical situation, and a bound on the accessible information is sufficient [CK78]. The collective case corresponds to an i.i.d. quantum source. Starting with Equation (1.4), one can then use the asymptotic equipartition property of

[11] The accessible information $\mathrm{I}_{\mathrm{ac}}(S:E)$ is defined as the mutual information $\mathrm{I}(S:M(E)) = \mathrm{H}(S) - \mathrm{H}(S|M(E))$ optimized over the possible measurements $M$ of Eve's system.

[12] Note that a QKD protocol only generates a secure key between Alice and Bob which then enables the encryption of a message in order to send it securely from one party to the other. Hence, a QKD protocol which is not composable secure is redundant.

[13] Note that one can also use the smooth Rényi entropy of order 2 to characterize the key length [KGR05, RGK05, AKMB11]

[14] With quantum signal, we denote the subsystem which leads to one measurement outcome.

the min-entropy [Ren05, TCR09] to obtain a bound on the smooth min-entropy by the von Neumann entropy of a single copy of the i.i.d. source. In the asymptotic limit one then finds the Devetak-Winter rate first proven in [DW05]. In the case of coherent attacks, one can use the exponential de Finetti theorem [Ren07] or the post-selection technique [CKR09] to extend security against collective attacks of a permutation symmetric protocol to security against coherent attacks. This reduces the finite-key length compared to collective attacks by a term which vanishes in the asymptotic limit and thus, shows that the Devetak-Winter rate also specifies the asymptotic key rate secure against coherent attacks. A more direct way to proof security against coherent attacks for BB84 like protocols was presented in [TLGR12] based on an uncertainty relation with quantum side information for smooth min- and max-entropies proved by Tomamichel and Renner in [TR11]. Another finite-key security proof for the BB84 protocol is presented in [HT11b].

An important alternative to discrete protocols using quantum systems with a finite number of degrees of freedom are continuous-variable protocols where the information is encoded in the quadratures of the electromagnetic field. They are usually based on the distribution of Gaussian states which are generally easier to prepare than single photon states used in discrete variable protocols. The quadrature measurements via homodyne or heterodyne detection can be implemented efficiently which leads to a high data acquisition and avoids photon counters offering possible loopholes [LAM$^+$11]. Furthermore, they offer the possibility to use standard telecom technologies. For further readings see for instance the latest survey in [WPGP$^+$12].

One drawback of continuous-variable systems is that the quantum system has to be model by an infinite-dimensional Hilbert space which rises additional technical difficulties in security proofs. One of the first security proofs was given in [GP01] for a squeezed state protocol based on entanglement distillation, which provided security against coherent attacks. But it has the disadvantage that the protocol is experimentally not feasible with nowadays technology and no explicit finite-key rate was computed. Other security proofs relied on the assumption that the formulas for the key rates explicitly derived for finite-dimensional quantum systems, like the one in Equation (1.4), also hold for continuous-variable systems (see [SBPC$^+$09, WLB$^+$04] for references).

Another problem is that the de Finetti theorem [Ren07] and the post-selection technique [CKR09] do not directly apply to infinite-dimensional systems [CKMR07]. An extension of the exponential de Finetti theorem to infinite-dimensional systems is presented in [RC09] via an "energy" bound constraining the relevant system to a finite-dimensional subspace. Unfortunately, this technique applied to continuous-variable protocols lead to very pessimistic bounds.[15] Nevertheless, it shows that in the asymptotic limit the optimal key rate secure against coherent attacks is equal to the one secure against collective attacks.

In usual security proofs one trusts the measurement devices and sometimes also the

[15] In [Ped08], the conditions required to apply [RC09] are analyzed. It turns out that it is hard to satisfy all the conditions at the same time. Moreover, the solution presented in [Ped08] is not robust in the experimental parameters.

source. This means that one assumes that the measurement devices in an experiment can be accurately modeled by certain observables. But often, this contains already simplifications and thus, offers loopholes for possible attacks. It is now possible to infer security of a quantum key distribution protocol solely on the foot of the measured correlations,[16] which is called device-independent security. The idea behind is that the violation of a Bell inequality forbids a local hidden variable model, which implies that the randomness of the measurement outcomes of the remote parties cannot be generated locally. Hence, an eavesdropper can never hold a complete description of the generated outcomes. First results go back to Mayers and Yao [MY98] for the noiseless case. Security against a non-signaling adversary was proven in [BHK05] against individual attacks. A more recent result shows security against collective attacks based on the violation of the Clauser-Horne-Shimony-Holt (CHSH) inequality [ABG$^+$07]. This was then generalized to the case of coherent attacks under the assumption of commuting measurement devices [MPA11, HR10]. See also [HÏ0] for a survey and further readings.

A fundamental question which arises in this context is whether one can characterize the property of correlation which enables security in the sense that they are statistically independent of any measurement of an eavesdropper.[17] This is a question about monogamy of correlations which was also discussed in the setting of non-signaling theories in [BLM$^+$05]. The correlation leading to a maximal violation of the CHSH inequality can be shown to be secure in this sense (c.f. [BKP06]). The reason is that the only quantum system which generates such correlation is essentially a singlet state together with rotated Pauli $Z$ and $X$ measurements for both parties [Tsi85]. Since this implies that the state is necessarily pure, any extension to a third party must be of product form and thus leads to uncorrelated measurement outcomes.

## 1.5. Contributions

This thesis starts with an extension of the smooth min- and max-entropies, $\mathrm{H}_{\min}^{\epsilon}(A|B)$ and $\mathrm{H}_{\max}^{\epsilon}(A|B)$, to an algebraic approach to quantum mechanics. We model the quantum systems by the von Neumann algebra generated by the physical observables. This paths the way to consider non-asymptotic information theory with quantum systems requiring infinite-dimensions, as for example continuous-variable systems. We show that many properties of the finite-dimensional smooth min- and max-entropies remain true in this more general framework. For instance, we analyze the behavior of these entropies for i.i.d. quantum resources and show that they still approximate the von Neumann entropy in the asymptotic limit (see Theorem 4.5.3). For the non-smooth conditional min-entropy $\mathrm{H}_{\min}(A|B)$ with finite-dimensional $A$ system and general $B$ system, we employ a Hahn-Banach extension theorem for positive functionals to recover the interpretation of $\mathrm{H}_{\min}(A|B)$ as maximal achievable quantum correlations by local operations (Theorem 4.6.4). In the case where the $A$ system is classical this results in an intuitive interpretation of the min-entropy as

[16] Note that the detection loophole still remains in this setting [GM87, Lar98].

[17] During this thesis, we use "secure" for different aspects. But in the main text, we clearly define what we mean by a secure key or a secure correlation table.

the optimal guessing probability. Similar results concerning the operational interpretation of the non-smooth max-entropy as the decoupling accuracy are proven in Theorem 4.6.6.

We consider the problem of privacy amplification against an adversary with side-information modeled on a general infinite-dimensional system. This is the crucial result by which the generalization of the key length formula for quantum key distribution in (1.4) to continuous-variable systems is obtained. We prove a similar characterization of the optimal extractable secure key length by the smooth min-entropy as in the finite-dimensional case (see Theorem 4.8.3). The proof is different to the ones given in the finite-dimensional case, have no straightforward generalization. We further consider the task of data compression with side-information modeled by a general von Neumann algebra. Using the formalism of von Neumann algebras brings the advantage that one is able to restrict the possible observables instead of considering all measurement operators in a Hilbert space. We show that the optimal characterization by the smooth max-entropy from the finite-dimensional case remains true in this more general framework (see Theorem 4.9.2).

A further important result is the generalization of the entropic uncertainty relation with quantum side-information for smooth min- and max-entropies (see Theorem 4.7.1). This relation is used to studying the uncertainty of position and momentum-like observables with arbitrary measurement precisions. In order to study the case of infinite precision, which leads to a continuous distribution, we define the differential conditional min- and max-entropies.[18] We show that this differential min- and max-entropies can be approximated by their discrete counterparts by letting the spacing go to zero. This approximation result, together with the uncertainty relation for the discrete min- and max-entropy, results to a tight entropic uncertainty relation with quantum side-information for continuous position and momentum measurements.

Based on the previous result on privacy amplification, we show that the key length formula in (1.4) also holds in the case of continuous-variable systems. Using the approximation of the von Neumann entropy by the smooth entropies of i.i.d. quantum resources, we set the Devetak-Winter formula for the asymptotic key rate on rigorous footing for continuous-variable protocols. We then consider a two-mode squeezed state protocol and present a security proof against coherent attacks based on the entropic uncertainty relation with quantum side-information inspired by the one for the BB84 protocol presented in [TLGR12]. We numerically compute the finite-key rate and show that for a two-mode squeezed state with squeezing strength experimentally demonstrated in [EHD$^+$11b], a non-vanishing key rate is obtained (see Figure 6.2). We also compute the key length given in Equation (1.4) under the assumptions of collective attacks by the help of the asymptotic equipartition property of the smooth min-entropy.

[18] Note that the term "differential" refers to the situation where first system $A$ is modeled by a continuous variable. The situation that the side-information $B$ is described by a continuous variable is included from the beginning since we consider general von Neumann algebras for the $B$ system.

In the last part of this thesis, we characterize the secure quantum correlations which have the property that they are uncorrelated with outcomes of any measurement an eavesdropper can perform. Considering the convex set of all quantum correlation tables, we show that such secure correlation tables are exactly the extremal ones. This illustrates the properties, which have to be satisfied by a correlation table to be useful for a device-independent quantum key distribution protocol. We further show that whenever an extremal correlation table determines the state and the observables uniquely, also all other measurements generated by the observables of the honest parties are independent of the outcomes of a measurement of an eavesdropper.

We introduce the universal C*-algebra corresponding to a general correlation experiment to study properties of correlation tables. In the particular case of $N$ parties with 2 binary-measurements each, it is given by the $N$-fold tensor product of the algebra of two projections. For this algebra the representation theory is well understood, which crucially simplifies problems like for instance to verify that a correlation table is extremal. The knowledge about the irreducible representations of the algebra is then also employed to construct for the case of $N = 2$ parties an explicit continuously parameterized family of extremal correlation tables including the one which maximizes the CHSH inequality.

# 2. Preliminaries

We use the framework of C*- and von Neumann algebras to model quantum mechanics. The theory of C*-algebras corresponds to the abstract theory of closed subalgebras of the set of bounded operators on a Hilbert space. These subalgebras are thought of as being generated by the possible observables of the physical system. An introduction to operator algebras from a physics perspective can be found in [BR79, BR81]. For a nice mathematical introduction see for instance [Mur90] while for further readings, we refer to the comprehensive series by Takesaki [Tak01, Tak02a, Tak02b].

We start with a short introduction to C*-algebras. The aim is to give the basic definitions and set the notation. Special emphasis is put on the Gelfand-Naimark-Siegel construction (see Section 2.1.2), which is used to show the equivalence of the abstract definition of a C*-algebra and norm closed subalgebras of the set of bounded operators on a Hilbert space. Section 2.2 is devoted to the discussion of a special class of C*-algebras, namely, the von Neumann algebras. These are obtained by closing the C*-algebra with respect to taking expectation values in the sense of quantum mechanics. Von Neumann algebras have more structure which turns out to be useful in the following.

## 2.1. C*-Algebras

### 2.1.1. Basic Definitions.

This part aims to set the notation used in the following and to give a self-contained introduction to C*-algebras. We refer to the first chapters in [BR79] for more details and proves. A $*$-*algebra* $\mathcal{A}$ is an algebra over the field $\mathbb{C}$ with an involution $*$ satisfying $A^{**} = A$, $(AB)^* = B^*A^*$, and $(\lambda A + B)^* = \bar{\lambda}A^* + B^*$ for any $A, B \in \mathcal{A}$ and $\lambda \in \mathbb{C}$. If a norm on a $*$-algebra $\mathcal{A}$ is defined for which $\mathcal{A}$ is complete, then $\mathcal{A}$ is called a *Banach* $*$-*algebra*.

**Definition 2.1.1.** *A Banach* $*$*-algebra* $\mathcal{A}$ *is called a C*-algebra if* $\|AA^*\| = \|A\|^2$ *for all* $A \in \mathcal{A}$*. Moreover, if* $\mathcal{A}$ *contains the identity element* $\mathbb{1}$ *it is called unital.*

From now on, we always assume that the C*-algebra is unital. Let $\mathcal{H}$ be a Hilbert space and $\mathcal{B}(\mathcal{H})$ the bounded (or equivalently continuous) operators on $H$ with respect to the usual operator norm

$$\|A\|_\infty = \sup_{\psi \in \mathcal{H}} \frac{\|A\psi\|}{\|\psi\|} \ (A \in \mathcal{B}(\mathcal{H}))\,. \tag{2.1}$$

In the following we omit the indication of the norm and simply write $\|A\|$ instead of $\|A\|_\infty$. It is easy to check that $\|AA^*\| = \|A\|^2$ and thus, $\mathcal{B}(\mathcal{H})$ is a C*-algebra. From

this it follows that each norm closed $*$-subalgebra of $\mathcal{B}(\mathcal{H})$ is a C*-algebra. As we discuss later the converse is also true, namely, that each C*-algebra is isomorphic to a norm closed $*$-subalgebra of $\mathcal{B}(\mathcal{H})$ (see Theorem 2.1.4).

An element $A$ in a C*-algebra $\mathcal{A}$ is called selfadjoint if $A^* = A$ and a subalgebra $\tilde{A} \subset \mathcal{A}$ is called selfadjoint if it is closed under the involution. An important role among the selfadjoint operators is played by the positive elements $A \geq 0$ in $\mathcal{A}$, which are defined through the property that there exists an operator $B \in \mathcal{A}$ such that $A = B^*B$. The set of all positive elements $\mathcal{A}_+$ defines a closed convex cone in $\mathcal{A}$. Recall that a cone $C$ is defined as a set for which $c \in C$ implies $\lambda c \in C$ for any $\lambda \geq 0$. We denote by $A \leq B$ the fact that $B - A \geq 0$, which defines a partial order relation in $\mathcal{A}$. Note that every selfadjoint operator can be composed into $A = A_+ - A_-$ where $A_+, A_-$ are positive. Furthermore, each operator can be written as $A = A_1 + iA_2$ for $A_1$, $A_2$ selfadjoint operators. Hence, the complex linear span of the positive operators forms the entire C*-algebra $\mathcal{A}$.

In order to obtain the structure theorem for C*-algebras saying that they can be represented as closed subalgebras of the set of all bounded operators on a suitable Hilbert space, the concept of states on a C*-algebra is crucial. Let us consider the dual space $\mathcal{A}^*$ of $\mathcal{A}$ consisting of all continuous functional from $\mathcal{A}$ to $\mathbb{C}$. An element $\omega \in \mathcal{A}^*$ is called positive and denoted by $\omega \geq 0$ if $\omega(A) \geq 0$ for all $A \geq 0$. We call now $\omega \in \mathcal{A}^*$ a *state* if $\omega \geq 0$ and $\omega(\mathbb{1}) = 1$. The set of all states is denoted by $\mathcal{S}_*(\mathcal{A})$. A state $\omega \in \mathcal{S}_*(\mathcal{A})$ satisfies the Cauchy-Schwarz inequality, that is,

$$|\omega(A^*B)|^2 \leq \omega(A^*A)\omega(B^*B) \;\; \forall A, B \in \mathcal{A}. \tag{2.2}$$

The positivity structure on $\mathcal{A}^*$ also induces a partial ordering via $\omega \geq \sigma$ if $\sigma - \omega \geq 0$. A state $\omega$ is called *pure* if $\sigma \leq \omega$ implies $\sigma = \lambda\omega$ for all $\sigma \geq 0$. $\mathcal{S}_*(\mathcal{A})$ is then given as the weak* closure of the convex envelope of all pure states in $\mathcal{S}_*(\mathcal{A})$.

A *$*$-homomorphism* is a linear map between two C*-algebras $\pi : \mathcal{A}_1 \to \mathcal{A}_2$ such that $\pi(AB) = \pi(A)\pi(B)$ and $\pi(A^*) = \pi(A)^*$. A *representation* of a C*-algebra $\mathcal{A}$ is a $*$-homomorphism into the set of bounded operators on a Hilbert space $\mathcal{B}(\mathcal{H})$. A representation is always a contraction, that is, $\|\pi(A)\| \leq \|A\|$. This implies that it is always continuous and that the image of $\mathcal{A}$ under a representation is always a closed subalgebra of $\mathcal{B}(\mathcal{H})$. We call a representation *faithful* if it is injective, that is, $\ker \pi = \{0\}$. It follows that a representation is faithful if and only if it is isometric. A representation $\pi$ of $\mathcal{A}$ is called *nondegenerated* if there exists no $\psi \in \mathcal{H} \setminus \{0\}$ such that $\pi(A)\psi = 0$ for all $A \in \mathcal{A}$. Each representation can be turned into a direct sum of a nondegenerated and a trivial representation. A vector $\psi \in \mathcal{H}$ is called *cyclic* for a set $U \subset \mathcal{B}(\mathcal{H})$ if $\{A\psi \mid A \in U\}$ is dense in $\mathcal{H}$. A triple $(\mathcal{H}, \pi, \psi)$ consisting of a representation $\pi$ of $\mathcal{A}$ on $\mathcal{H}$ and a vector $\psi \in \mathcal{H}$ which is cyclic for $\pi(\mathcal{A})$ is called a *cyclic representation* of $\mathcal{A}$. Note that a cyclic representation is always nondegenerated.

### 2.1.2. The GNS Representation

We are now going to show that for each C*-algebra $\mathcal{A}$ we can find a Hilbert space $\mathcal{H}$ such that $\mathcal{A}$ is isomorphic to a closed subalgebra of $\mathcal{B}(\mathcal{H})$. The main tool will be the Gelfand, Naimark and Segal (GNS) construction, which assigns to each state a cyclic

representation. Since it provides a powerful method of obtaining representations and is a widely established tool in operator theory, we give the detailed construction. The main result is the following.

**Theorem 2.1.2.** *Let $\mathcal{A}$ be a C*-algebra and $\omega \in \mathcal{S}(\mathcal{A})$. Then there exists a cyclic representation $(\mathcal{H}, \pi, \xi_\omega)$ of $\mathcal{A}$ such that $\omega(A) = \langle \xi_\omega \,|\pi(A)\xi_\omega \rangle$. Moreover, the representation is unique up to unitary equivalences.*

The proof is given by an explicit construction (see e.g., [BR79, Theorem 2.3.16] or [Mur90, Chapter 3.4]).

*Proof.* Consider $\mathcal{A}$ as a vector space over $\mathbb{C}$ and define the sesquilinear and positive semi-definite form $\langle A \,|B \rangle = \omega(A^*B)$. The set $N = \{C \in \mathcal{A} \,|\, \omega(C^*C) = 0\}$ defines a left-sided ideal in $\mathcal{A}$, that is, $AC \in N$ for all $A \in \mathcal{A}$ and $C \in N$. The quotient $\tilde{\mathcal{H}} = \mathcal{A}/N$ is therefore well defined and forms together with $\langle \cdot \,|\cdot \rangle$ a pre-Hilbert space. By completion this space can be turned into a Hilbert space which we denote by $\mathcal{H}$. To avoid confusion, we denote by $\psi_\mathcal{A}$ the vector in $\mathcal{H}$ which corresponds to $A \in \mathcal{A}$. We define now the representation of $\mathcal{A}$ on the dense subspace $\tilde{\mathcal{H}}$ via $\pi(A)\psi_B = \psi_{AB}$. This operator is bounded on $\tilde{\mathcal{H}}$ since

$$\|\pi(\mathcal{A})\psi_B\| = \|\psi_{AB}\| = \omega(B^*A^*AB) \leq \|A\|^2\omega(B^*B) = \|A\|^2\|\psi_B\|$$

for any $A, B \in \mathcal{A}$. Hence, the closure of the operator $\pi(A)$ on $\mathcal{H}$ defines a bounded operator on $\mathcal{H}$. The fact that $\pi$ satisfies the requirement of a representation can be checked by simple calculations on the dense subspace $\tilde{\mathcal{H}}$. Finally, we define $\xi_\omega = \psi_\mathbb{1}$ and find that $\langle \xi_\omega \,|\pi(A)\xi_\omega \rangle = \omega(A)$. It is clear that $\xi_\omega$ is cyclic for $\pi(\mathcal{A})$.

It remains to show uniqueness. Let $(\mathcal{H}, \pi, \xi_\omega)$ and $(\mathcal{H}', \pi', \xi'_\omega)$ be two cyclic representations of $\mathcal{A}$. We define the linear map $V$ on $\tilde{\mathcal{H}}$ via $V\pi(A)\xi_\omega = \pi'(A)\xi'_\omega$. Since for any $A, B \in \mathcal{A}$

$$\langle V\pi(A)\xi_\omega \,|V\pi(B)\xi_\sigma \rangle = \langle \pi'(A)\xi'_\omega \,|\pi'(B)\xi'_\omega \rangle = \omega(A^*B) = \langle \pi(A)\xi_\omega \,|\pi(B)\xi_\sigma \rangle ,$$

we have that $V$ defines a unitary map on a dense subspace on $\mathcal{H}$. But this operator can be unitarily extended to $\mathcal{H}$. □

We proceed by linking pure states with irreducible representations. Let $\mathcal{H}$ be an arbitrary Hilbert space and $S$ a subspace of $\mathcal{B}(\mathcal{H})$. A subspace $V \subset \mathcal{H}$ satisfying $SV \subset V$ is called invariant subspace of $S$. We call a set $S$ irreducible if the only invariant subspaces of $S$ are $\mathcal{H}$ and $\{0\}$. A representation $\pi$ of $\mathcal{A}$ on $\mathcal{H}$ is called irreducible if $\pi(A)$ is irreducible. The commutant $S'$ of $S$ is defined as the set $S' = \{A \in \mathcal{B}(\mathcal{H}) \,|\, [A, B] = 0 \,\forall\, B \in S\}$. Note that the commutant forms a closed subalgebra of $\mathcal{B}(\mathcal{H})$, that is a C*-algebra, which contains at least multiples of the identity. An important result which connects the two notions is the following:$S$ is irreducible if and only if $S'$ consists just of multiple of the identity. A proof of this statement can be found in [BR79, Proposition 2.3.8].

**Proposition 2.1.3.** *Let $\mathcal{A}$ be a C*-algebra and $\omega \in \mathcal{S}(\mathcal{A})$. Then, the GNS representation $(\mathcal{H}, \pi, \xi_\omega)$ of $\omega$ is irreducible if and only if $\omega$ is pure.*

The proof (see [BR79, Theorem 2.3.19]) exploits the fact that for any state which satisfies $\sigma \leq \lambda\omega$ there exists a positive operator $H_\sigma$ in $\pi(\mathcal{A})'$ such that $\sigma(A) = \langle \xi_\omega \, | \pi(A) H_\sigma \xi_\sigma \rangle$ with $\|H_\sigma\| \leq 1$. The operator $h_\sigma = \sqrt{H_\sigma}$ is also called the non-commutative Radon-Nikodym derivative of $\sigma$ with respect to $\omega$ and will be discussed later.

Let us conclude this chapter with the structure theorem for C*-algebras.

**Theorem 2.1.4.** *Every C*-algebra is isomorphic to a closed selfadjoint subalgebra of bounded operators on a Hilbert space.*

The proof follows by considering the direct sum representation over all possible states on $\mathcal{A}$. In order to show that the representation is faithful or equivalently isometric one uses the fact that for each $A \in \mathcal{A}$ there exists a state $\omega$ such that $\omega(A^*A) = \|A\|^2$. The latter result is obtained via the Hahn-Banach theorem on Banach spaces (see e.g., [BR79, Theorem 2.3.22A]). For a complete proof we refer to [BR79, Theorem 2.1.10].

## 2.2. Von Neumann Algebras

Von Neumann algebras are selfadjoint $*$-subalgebras of $\mathcal{B}(\mathcal{H})$ which are closed under quantum mechanical expectation values (see Section 3.1 for an introduction to quantum mechanics). In mathematical terminology, this means that the $*$-subalgebra is $\sigma$-weakly closed (see Definition 2.2.1 below). Historically, their investigation initialized by von Neumann [vN29] started earlier than the one of general C*-algebras. From a technical perspective, the importance of von Neumann algebras is due to the fact that they contain the spectral projections of any selfadjoint operator of the algebra. Since the algebra is spanned by the selfadjoint operators the information about the spectral projections determines the algebra itself. Dependent on the properties of these projections a factor of a von Neumann algebra is called of type $I$, $II$, $III$, and each type is again further categorized into subtypes. Type $I_n$ is the full algebra of operators on a n-dimensional Hilbert space and $I_\infty$ corresponds to the full algebra of operators on an infinite-dimensional Hilbert space. The type $II$ factors are the ones which admit a unique finite (type $I_1$) or semifinite (type $II_\infty$) trace, but which are not of type $I$. Type $III$ factors contain no finite projection which are not equal to the zero-projection. See [BR79, Tak01] for a detailed description of types of von Neumann algebras.

In the following we review the basic definitions and provide the technicalities used in the proceeding chapters. We start with the definition of a von Neumann algebra and introduce the set of normal states. In a next section, we discuss the standard form of a von Neumann algebra which allows to represent each normal state as a vector state in a cone of a suitable Hilbert space. This provides a helpful tool to prove several statements in Chapter 4. We conclude this section by introducing the non-commutative Radon-Nikodym derivation.

### 2.2.1. Three Equivalent Definitions

There are three equivalent ways to define a von Neumann algebra. One is topological in nature and the other two are more algebraical. We start by discussing various

topologies on $\mathcal{B}(\mathcal{H})$ for a Hilbert space $\mathcal{H}$. We denote by $\tau(\mathcal{H})$ the set of trace class (also called nuclear) operators in $\mathcal{B}(\mathcal{H})$ for which the trace is finite. Furthermore, we let $\mathcal{K}(\mathcal{H})$ be the set of compact operators. Note that both sets are ideals in $\mathcal{B}(\mathcal{H})$ and that the relations $\mathcal{K}(\mathcal{H})^* = \tau(\mathcal{H})$ and $\tau(\mathcal{H})^* = \mathcal{B}(\mathcal{H})$ hold [RS78]. Here, $S^*$ stands for the dual space of $S$ and should not be confused with the one used for the involution. We introduce different locally convex topologies on $\mathcal{B}(\mathcal{H})$ induced by different set of seminorms.

**Definition 2.2.1.** *Let $\mathcal{H}$ be a Hilbert space.*

- *The locally convex topology on $\mathcal{B}(\mathcal{H})$ induced by the seminorms $A \mapsto |\langle \psi | A\psi \rangle|$ for $\psi \in \mathcal{H}$ is called the weak operator topology.*
- *The locally convex topology on $\mathcal{B}(\mathcal{H})$ induced by the seminorms $A \mapsto |\eta(A)|$ for $\eta \in \tau(\mathcal{H})$ is called the $\sigma$-weak or weak* topology.*
- *The locally convex topology on $\mathcal{B}(\mathcal{H})$ induced by the seminorms $A \mapsto \|A\psi\|$ for $\psi \in \mathcal{H}$ is called the strong operator topology.*
- *The locally convex topology on $\mathcal{B}(\mathcal{H})$ induced by the seminorms $A \mapsto \left(\sum_{k=1}^{\infty} \|A\psi_k\|^2\right)^{1/2}$ for $\psi_k \in \mathcal{H}$ such that $\sum_k \|\psi_k\| < \infty$ is called the $\sigma$-strong topology.*

Every convex subset $\mathcal{C}$ of $\mathcal{B}(\mathcal{H})$ has the following property: $\mathcal{C}$ is $\sigma$-weakly closed if and only if it is $\sigma$-strongly closed. Furthermore, if $\mathcal{B}_r(\mathcal{H})$ defines the ball of radius $r$, then equivalent are $\mathcal{C}$ is $\sigma$-weakly closed, $\mathcal{C} \cap \mathcal{B}_r(\mathcal{H})$ is weakly operator closed for any $r > 0$, and $\mathcal{C} \cap \mathcal{B}_r(\mathcal{H})$ is strongly operator closed for any $r > 0$.

We give now the algebraical definition of a von Neumann algebras and state their equivalent topological characterization.

**Definition 2.2.2.** *Let $\mathcal{H}$ be a Hilbert space. A von Neumann algebra $\mathcal{M}$ acting on $\mathcal{H}$ is a $*$-subalgebra $\mathcal{M} \subset \mathcal{B}(\mathcal{H})$ which satisfies $\mathcal{M}'' = \mathcal{M}$.*

In the following $\mathcal{M}$ denotes always a von Neumann algebra. It is easy to see that if $A \in \mathcal{M}$ then also $A_+$, $A_-$ and $|A|$. We call $\mathcal{Z}(\mathcal{M}) = \mathcal{M} \cap \mathcal{M}'$ the *center of* $\mathcal{M}$ and $\mathcal{M}$ a *factor* if $\mathcal{Z}(\mathcal{M})$ consists only of multiples of the identity. Each von Neumann algebra can be decomposed into the direct some of factors [Tak01, Chapter V, Theorem 1.19]. This is easily obtained by taking a maximal family $\{p_i\}$ of orthogonal projections in the center of $\mathcal{M}$, for which one finds that $\mathcal{M} = \bigoplus_i p_i \mathcal{M} p_i$.

For any subset $\mathcal{C} \subset \mathcal{B}(\mathcal{H})$ the commutant $\mathcal{C}'$ is closed in all topologies defined in Definition 2.2.1. Hence, a von Neumann algebra $\mathcal{M}$ is closed with respect to these locally convex topologies. The converse is called the double commutant theorem.

**Theorem 2.2.3.** *Let $\mathcal{A}$ be a nondegenerated, selfadjoint subalgebra of $\mathcal{B}(\mathcal{H})$. Then we have that $\mathcal{A}$ is a von Neumann algebra, i.e., $\mathcal{A}'' = \mathcal{A}$ if and only if $\mathcal{A}$ is $\sigma$-weakly closed.*

The details as well as the proof can for instance be found in [BR79, Chapter 2.4.2] or [Mur90, Chapter 4.1].

The last definition is due to Sakai and can be stated in the category of C*-algebras. A von Neumann algebra $\mathcal{M}$ is a $C^*$-algebra with the property that it is the dual space of a Banach space. Due to historical reasons this is also called a $W^*$-algebra. The Banach space $\mathcal{N}(\mathcal{M})$ such that $\mathcal{N}(\mathcal{M})^* = \mathcal{M}$, often denoted by $\mathcal{M}_*$, is called the predual of $\mathcal{M}$. Let us consider for simplicity $\mathcal{M} = \mathcal{B}(\mathcal{H})$ for a Hilbert space $\mathcal{H}$. Then, according to the discussion before, we know that $\mathcal{N}(\mathcal{M}) = \tau(\mathcal{H})$ the set of trace class operators on $\mathcal{H}$ which is of course a Banach space as it is the dual space of the compact operators. Furthermore, it consists exactly of the $\sigma$-weakly continuous functionals on $\mathcal{M}$. The same holds now for arbitrary von Neumann algebras. Namely, the set $\mathcal{N}(\mathcal{M})$ is the set of all $\sigma$-weakly continuous functionals on $\mathcal{M}$ equipped with the norm inherited from $\mathcal{M}^*$. According to the Hahn-Banach theorem it is also clear that for each $\omega \in \mathcal{N}(\mathcal{M})$ exists a $\rho \in \tau(\mathcal{H})$ such that

$$\omega_\rho(x) = \mathrm{Tr}(\rho x) = \omega(x) \; \forall x \in \mathcal{M}\,. \tag{2.3}$$

The cone of positive elements in $\mathcal{N}(\mathcal{M}) \subset \mathcal{M}^*$ is denoted by $\mathcal{N}^+(\mathcal{M})$ and elements in $\mathcal{N}^+(\mathcal{M})$ are called normal. It is worth to mention that $\|\omega\| = \omega(\mathbb{1})$ for all $\omega \in \mathcal{N}^+(\mathcal{M})$. We call functionals $\omega \in \mathcal{N}^+(\mathcal{M})$ with the property $\|\omega\| \leq 1$ subnormalized states and denote the set of all subnormalized states by $\mathcal{S}_\leq(\mathcal{M})$. Moreover, we say that $\omega \in \mathcal{S}_\leq(\mathcal{M})$ is a normalized state if $\|\omega\| = 1$, and set $\mathcal{S}(\mathcal{M}) = \{\omega \in \mathcal{S}_\leq(\mathcal{M}) : \|\omega\| = 1\}$.[1] Since each positive functional in $\mathcal{N}(\mathcal{M})$ admits a positive extension to whole $\mathcal{B}(\mathcal{H})$, there exists for every $\omega \in \mathcal{S}_\leq(\mathcal{M})$ a positive trace class operator $\rho$ such that (2.3) holds. Such an operator $\rho$ is called a density matrix.

Given two commuting von Neumann algebras $\mathcal{M}$ and $\hat{\mathcal{M}}$ acting on the same Hilbert space $\mathcal{H}$, we define the von Neumann algebra generated by $\mathcal{M}$ and $\hat{\mathcal{M}}$ as $\mathcal{M} \vee \hat{\mathcal{M}} = (\mathcal{M} \cup \hat{\mathcal{M}})''$, where $\mathcal{M} \cup \hat{\mathcal{M}} = \mathrm{span}\{\mathrm{xy}\ ;\ \mathrm{x} \in \mathcal{M}\,, \mathrm{y} \in \hat{\mathcal{M}}\}$. According to the bicommutant theorem [BR79, Lemma 2.4.11], $\mathcal{M} \vee \hat{\mathcal{M}}$ is just the $\sigma$-weak closure of $\mathcal{M} \cup \hat{\mathcal{M}}$.

### 2.2.2. The Standard Form of a von Neumann Algebra

The standard form a von Neumann algebra $\mathcal{M}$ refers to a uniquely defined faithful representation $\pi$ of $\mathcal{M}$ on $\mathcal{H}$ for which a self-dual cone $\mathcal{P} \subset \mathcal{H}$ exists which contains for any normal state $\omega$ on $\mathcal{M}$ a vector representative in $\mathcal{P}$, that is, a vector $\xi_\omega \in \mathcal{P}$ with the property that

$$\omega(a) = \langle \xi_\omega \, | a \xi_\omega \, \rangle$$

for all $a \in \mathcal{M}$. It further admits a unitary involution $J$, that is, an anti linear isometry with $J^2 = \mathbb{1}$ which connects $\mathcal{M}$ with its commutator via $J\mathcal{M}J = \mathcal{M}'$ and leaves the cone invariant, $J\xi = \xi$ for all $\xi \in \mathcal{P}$. Since the representation is faithful we simply identified $\pi(\mathcal{M})$ and $\mathcal{M}$.

**Definition 2.2.4.** *A standard form of a von Neumann algebra $\mathcal{M}$ is a tuple $(\mathcal{H}, \pi, J, \mathcal{P})$ consisting of a Hilbert space $\mathcal{H}$, a faithful representation $\pi$ of $\mathcal{M}$ on $\mathcal{H}$, an unitary involution $J$, called modular conjugation, and a self-dual cone $\mathcal{P} \subset \mathcal{H}$ satisfying (i)*

[1] Note the ambiguity between the definitions of states for a C*-algebra and for a von Neumann algebra. This is because we only consider normal states as physical relevant states for von Neumann algebras.

*$J\mathcal{M}J = \mathcal{M}'$, (ii) $J\xi = \xi$ for all $\xi \in \mathcal{P}$, (iii) $aJaJ\mathcal{P} \subset \mathcal{P}$ for all $a \in \mathcal{M}$ and (iv) $JaJ = a*$ for all $a \in \mathcal{Z}(\mathcal{M})$. Here, we identified $\mathcal{M}$ with $\pi(\mathcal{M})$.*

It holds that every von Neumann algebra exists a Standard form. This follows from the fact that every von Neumann algebra $\mathcal{M}$ admits a faithful semi-finite normal weight [Tak02a, Chapter VII, Theorem 2.7] and that the GNS construction with respects to this weight generates a standard form of $\mathcal{M}$. The modular conjugation is obtained by identifying $\mathcal{M}$ with the von Neumann algebra generated by the left Hilbert algebra associated to the faithful semi-finite normal weight. For further readings see [Tak02a] or for the Tomita-Takesaki modular theory also [BR79].

### 2.2.3. Noncommutative Radon-Nikodym Derivative

A non-commutative Radon-Nikodym Derivative derivative is the generalization of the concept of the Radon-Nikodym derivative from measure theory, which can be interpreted as the theory of states and weights on abelian von Neumann algebras, to non-commutative von Neumann algebras. Sakai proved in [Sak65] that for two normal positive functionals $\omega$ and $\sigma$ on a von Neumann algebra $\mathcal{M}$, where $\sigma$ majorazes $\omega$ (i.e., $\omega \leq \lambda\sigma$ for an appropriate $\lambda \geq 0$) holds that there exists a $t \geq 0$ in $\mathcal{M}$ with $\omega(a) = \sigma(tat)$ for any $a \in \mathcal{M}$.

Let $(\pi_\omega, \mathcal{H}_\omega, |\xi_\omega\rangle)$ and $(\pi_\sigma, \mathcal{H}_\sigma, |\xi_\sigma\rangle)$ be cyclic representations of $\mathcal{M}$ with $\xi_\omega$ and $\xi_\sigma$ vector representatives of $\omega$ and $\sigma$. We then define the linear and bounded operator $D : \mathcal{H}_\sigma \to \mathcal{H}_\omega$ via $D\pi_\sigma(a)|\xi_\sigma\rangle = \pi_\omega|\xi_\omega\rangle$. A straightforward computation shows that $D\pi_\sigma(a) = \pi_\omega(a)D$ for all $a \in \mathcal{M}$. We further find that

$$\|D^*D\| = \sup_{a\in\mathcal{M}} \frac{\langle \pi_\sigma(a)\xi_\sigma \,|D^*D\,\pi_\sigma(a)\,\xi_\sigma\,\rangle}{\langle \pi_\sigma(a)\xi_\sigma \,|\pi_\sigma(a)\,\xi_\sigma\,\rangle} = \sup_{a\in\mathcal{M}} \frac{\omega(a^*a)}{\sigma(a^*a)}\,.$$

Let us define the max-relative entropy of $\omega$ with respect to $\sigma$ by

$$\mathrm{D}_{\max}\left(\omega \,||\, \sigma\right) = \inf\left\{\mu \in \mathbb{R} : \omega \leq 2^\mu \cdot \sigma\right\}\ .$$

We then easily find that

$$\log\|D^*D\| = \mathrm{D}_{\max}\left(\omega \,||\, \sigma\right). \tag{2.4}$$

We call $D$ the non-commutative Radon Nykodim derivative of $\omega$ with respect to $\sigma$.

Let us consider now a finite ensemble of normal positive functionals $\omega^x \in \mathcal{N}^+(\mathcal{M})$ enumerated $x \in X$ where $X$ denotes a finite alphabet. Assume that $\sigma \in \mathcal{N}^+(\mathcal{M}_E)$ such that $\omega_E^x \leq \sigma$ for all $x \in X$ and set further $\omega = \sum_x \omega^x$. We use the notation above and let $D_x$ and $D$ be the non-commutative Radon Nykodim derivatives of $\omega^x$ and $\omega$ with respect to $\sigma$. It then follows that

$$\begin{aligned}\langle \pi_\sigma(a)\xi_\sigma \,|\pi_\sigma(b) \sum_{x\in X} D_x^*D_x\xi_\sigma\,\rangle &= \sum_{x\in X} \langle D_x\xi_\sigma \,|\pi_\sigma(a^*b)D_x\xi_\sigma\,\rangle = \sum_x \omega_E^x(a^*b)\\ &= \omega(a^*b)\\ &= \langle \pi_\sigma(a)\xi_\sigma \,|\pi_\sigma(b)D^*D\xi_\tau\,\rangle\,,\end{aligned}$$

for all $a$, $b \in \mathcal{M}$. Using that $(\pi_\sigma, \mathcal{H}_\sigma, |\xi_\sigma\rangle)$ is cyclic we obtain

$$\pi_\sigma(a) \sum_{x \in X} D_x^* D_x \xi_\sigma = \pi_\sigma(a) D^* D \xi_\sigma \,, \tag{2.5}$$

for any $a \in \mathcal{M}$.

# 3. Quantum Information Theory on von Neumann Algebras

This chapter aims to discuss the language and techniques which are used while working with general von Neumann algebras instead of all bounded operators on a Hilbert space. We assume that the reader is familiar with the standard Hilbert space formulation of quantum mechanics and quantum information theory and place emphasis on the peculiarities for von Neumann algebras. This section is of importance for Chapter 4 where the smooth entropies are discussed.

## 3.1. The Formalism of Quantum Mechanics

With every physical system we associate a von Neumann algebra $\mathcal{M} \subset \mathcal{B}(\mathcal{H})$ which contains the possible observables. An *observable* is given by a positive operator valued measure (POVM), which consists of a measurable space $(X, \Sigma)$ with $\sigma$-algebra $\Sigma$ defining the values of the possible outcomes together with a $\sigma$-additive function $E : \Sigma \to \mathcal{M}_+$ such that $E(X) = \mathbb{1}$. In the following the possible outcomes are chosen such that $X \subset \mathbb{R}^n$. We call an observable projective (or sharp) if the POVM is a projective-valued measure. By spectral theory, every selfadjoint operator gives rise to a projective observable. Since we consider general properties of a quantum mechanical system, we do not specify which observables in $\mathcal{M}$ are physically relevant meaning that they correspond to a property of the system which can be measured in an experiment. We call an apparatus which measures the observalbe $E$ a *measurement* of the observable $E$.

The *state of a physical system* modeled on a von Neumann algebra $\mathcal{M}$ is given by an element $\omega \in \mathcal{S}(\mathcal{M})$, that is, a normal positive functional on $\mathcal{M}$ such that $\omega(\mathbb{1}) = 1$. In the case of $\mathcal{M} = \mathcal{B}(\mathcal{H})$, we also write $\mathcal{S}(\mathcal{H})$ instead of $\mathcal{S}(\mathcal{M})$ and use the identification with density matrices $\omega_\rho(a) = \mathrm{Tr}\rho a$ (see Eq. (2.3)). If the state of the system is $\omega$, then the measurement distribution of the POVM $E$ is given by $\omega(\mathrm{dE(x)})$. We are mostly considering the case of a finite number of outcomes $X = \{1, 2, ..., n\}$ with the point measure in which an observable is given by a set of positive operators $E = \{E_x\}$ with $\sum_x E_x = \mathbb{1}$. Then, the probability to measure outcome $x$ is $\omega(E_x)$. Let $\mathcal{M}$ act on $\mathcal{H}$. We then call a state $\omega_\xi(a) = \langle \xi \, | a\xi \, \rangle$ with $\xi \in \mathcal{H}$ a vector state and denote it by $|\xi\rangle$. Note that in the case where $\mathcal{M}$ is not $\mathcal{B}(\mathcal{H})$ the vector $\xi \in \mathcal{H}$ is not uniquely determined by $\omega_\xi$ and in general not pure. Moreover, as seen in section 2.2.2, the standard form of a von Neumann algebra $\mathcal{M}$ is such that every state is a vector state.

In the language of von Neumann algebras, evolutions are naturally defined in the

Heisenberg picture. For example if one considers a quantum system with Hamiltonian $H$, we have that the spectral projections of $H$ lies in $\mathcal{M}$. Hence, the time evolution operator $U(t) = \exp itH$ is in $\mathcal{M}$ and the map $t \mapsto U(t)AU(t)^*$ for $A \in \mathcal{M}$ defines an endomorphism from $\mathcal{M}$ onto $\mathcal{M}$. If the system is in interaction with its environment and the interaction is not explicitly included in the model, the evolution are described by completely positive, unital, linear maps between possibly different von Neumann algebras $\mathcal{E} : \mathcal{M}_B \to \mathcal{M}_A$. Such a map is called a *quantum channel* (see for instance [Dav76, Pau02] for more details).

**Definition 3.1.1.** *Let $\mathcal{A}$ and $\mathcal{B}$ be unital C*-algebras. A map $\phi : \mathcal{A} \to \mathcal{B}$ is called* unital *if $\phi(\mathbb{1}) = \mathbb{1}$ and* positive *if $\phi(\mathcal{A}_+) \subset \mathcal{B}_+$. The map $\phi$ is called completely positive if the extension $\phi \otimes \mathrm{id} : \mathcal{A} \otimes M_n \to \mathcal{B} \otimes M_n$ is positive for all $n \in \mathbb{N}$. Here, $M_n$ denotes the matrix algebra $\mathcal{B}(\mathbb{C}^n)$ and $\phi \otimes \mathrm{id}(\sum_k a_k \otimes x_k) = \sum_k \phi(a_k) \otimes x_k$.*

Note that a unital positive map between C*-algebras is always a contraction (i.e. $\|\phi(A)\| \leq \|A\|$) and $\|\phi\| = \|\phi(\mathbb{1})\|$ [Pau02, Cor 2.9].

## 3.2. Multipartite Systems and the Concept of Purification

Let us consider two physical systems denoted by A and B which are space like separated. If such systems are modeled by von Neumann algebras $\mathcal{M}_A$ and $\mathcal{M}_B$ on the same Hilbert space, then they necessarily commute because of the non-signaling principle. The composite system is then described by the von Neumann algebra $\mathcal{M}_{AB} = \mathcal{M}_A \vee \mathcal{M}_A$. In the case where the two systems are modeled on different Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, we consider the natural embedding of $\mathcal{M}_A$ and $\mathcal{M}_B$ into $\mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and describe the compostion again by $\mathcal{M}_A \vee \mathcal{M}_B$. This construction is naturally generalized to more than two parties. We indicate the subsystems by subscripts, that is, $\omega_{ABC}$ denotes a state on a multipartite system $\mathcal{M}_{ABC}$ and $\omega_{AB}$ is the restriction of $\omega_{ABC}$ onto $\mathcal{M}_{AB}$.

The concept of a purification is standard in quantum information theory [NC00]. The goal is to generalize the notion of a purification for systems described on a general von Neumann algebra. If one considers a state $\omega_A$ on a type I factor $\mathcal{M}_A = \mathcal{B}(\mathcal{H}_A)$, one calls any vector state $|\phi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ for suitable $\mathcal{H}_B$ with restriction onto $\mathcal{H}_A$ equal to $\omega_A$ a purification of $\omega_A$. Let us denote the state corresponding to $|\phi\rangle$ by $\omega_{AB}$. This extension has the property that it is a pure state on $\mathcal{M}_A \vee \mathcal{M}_B$ where $\mathcal{M}_B = \mathcal{M}_A' = \mathcal{B}(\mathcal{H}_B)$. A pure state has the property that any further extension is uncorrelated [Tak02a, Section IV, Lemma 4.11]: if $\tilde{\omega} \in \mathcal{S}(\tilde{\mathcal{M}})$ with $\mathcal{M} \subset \tilde{\mathcal{M}}$ and $\tilde{\omega}$ restricted to $\mathcal{M}$ is a pure state $\omega$ on $\mathcal{M}$, then it follows that $\tilde{\omega}(xy) = \tilde{\omega}(x)\tilde{\omega}(y)$ for all $x \in \mathcal{M}$ and $y \in \mathcal{M}' \cap \tilde{\mathcal{M}}$.

For a general von Neumann algebra it is not possible to find always an extension of a state such that it can be understood as a pure state on a bipartite system $\mathcal{M}_A \vee \mathcal{M}_B$. This is only possible if the state is a factor state, that is, its GNS-construction is a factor [Wor72]. In order to see this, let us consider a state $\omega_A$ on $\mathcal{M}_A$ for which the GNS construction $(\mathcal{H}, \Pi, \xi)$ is not a factor. Denoting $\pi(\mathcal{M}_A)$ again by $\mathcal{M}_A$ and $\mathcal{M}_B = \mathcal{M}_A'$, we consider the restriction of $\omega_\xi$ onto $\mathcal{M}_A \vee \mathcal{M}_B$ denoted by $\omega_{AB}$. Since this is also a GNS representation of $\omega_{AB}$ and $(\mathcal{M}_A \vee \mathcal{M}_B)'$ is not trivial because $\mathcal{Z}(\mathcal{M}_A) \subset (\mathcal{M}_A \vee \mathcal{M}_B)'$, Proposition 2.1.3 tells us that the state is not pure

on $\mathcal{M}_A \vee \mathcal{M}_B$. Nevertheless $\omega_\xi$ defines a pure state on $\mathcal{B}(\mathcal{H})$. We therefore use the following weaker definition of a purification, which still ensures that it contains the maximal amount of correlations accessible by another space like separated party.

**Definition 3.2.1.** *Let $\mathcal{M}$ be a von Neumann algebra and $\omega \in \mathcal{S}_\leq(\mathcal{M})$. A purification of $\omega$ is defined as a triple $(\pi, \mathcal{H}, |\xi\rangle)$, where $\pi$ is a representation of $\mathcal{M}$ on a Hilbert space $\mathcal{H}$, and $\xi \in \mathcal{H}$ is such that $\omega(x) = \langle \xi \, | \pi(x) \xi \, \rangle$ for all $x \in \mathcal{M}$. Moreover, we call $\pi(\mathcal{M})$ the relevant and $\pi(\mathcal{M})'$ the complementary system of the purification $(\pi, \mathcal{H}, |\xi\rangle)$.*

We first note that by the GNS-construction, every state admits a purification. Furthermore, that the notion coincides with the standard terminology for type I von Neumann algebras. For simplicity, we say that $\omega_{A'B}$ is a purification of $\omega_A \in \mathcal{S}_\leq(\mathcal{M}_A)$, if there exists a purification $(\pi, \mathcal{H}, |\xi\rangle)$ of $\omega_A$ such that $\mathcal{M}_{A'} = \pi(\mathcal{M}_A)$, $\mathcal{M}_B = \pi(\mathcal{M}_A)'$ and $\omega_{A'B}(x) = \langle \xi \, | x \xi \, \rangle$ for all $x \in \mathcal{M}_{A'B}$. As discussed before, such a purification $\omega_{A'B}$ is in general not a pure state on $\mathcal{M}_{A'B}$, although the vector state $\omega_\xi(x) = \langle \xi \, | x \xi \, \rangle$ on $\mathcal{B}(\mathcal{H})$ is. Another important property of a purification $(\pi, \mathcal{H}, |\xi\rangle)$ of $\omega_A \in \mathcal{S}(\mathcal{M}_A)$ is that $\pi$ is not required to be faithful on the entire $\mathcal{M}_A$ but only on the part 'seen' by the state $\omega_A$. This means that $\mathcal{M}_A$ is in general not isomorphic to $\pi(\mathcal{M}_A)$ and the systems cannot be identified, wherefore we denoted $\pi(\mathcal{M}_A)$ by A' instead of A. Beside the mathematical convenience, this is justified because a purification is just a theoretical construct without direct physical relevance, and can therefore chosen to be state dependent.[1] Recall also the standard form of a von Neumann algebra introduced in Section 2.2.2, which says that there exists a representation in which all states are purified.

A purification is of course not unique, but they are all connected by partial isometries. This property will assure that the concept is compatible with the definition of the entropies.

**Lemma 3.2.2.** *Let $\mathcal{M}$ be a von Neumann algebra, $\omega \in \mathcal{S}_\leq(\mathcal{M})$, and $(\pi_i, \mathcal{H}_i, |\xi_i\rangle)$ with $i = 1, 2$ two purifications of $\omega$. Then there exists a partial isometry $V : \mathcal{H}_1 \to \mathcal{H}_2$ such that $V|\xi_1\rangle = |\xi_2\rangle$ and $V$ intertwines with the representations $\pi_i$, that is, $V\pi_1(x) = \pi_2(x)V$ for all $x \in \mathcal{M}$.*

*Proof.* We construct an explicit partial isometry $V$. Define $V$ on $\{\pi_1(x)|\xi_1\rangle : x \in \mathcal{M}\}$ via $V\pi_1(x)|\xi_1\rangle = \pi_2(x)|\xi_2\rangle$. This defines $V$ uniquely on the closed subspace $\mathcal{H}_1^\omega \subset \mathcal{H}_1$ given by the closure of $\{\pi_1(x)|\xi_1\rangle : x \in \mathcal{M}\}$. On the orthogonal complement of $\mathcal{H}_1^\omega$, we set $V$ equal to zero. One can now verify that the constructed $V$ satisfies the required properties. □

## 3.3. Classical-Quantum States

A classical system is described by a classical random variable $X$. For the sake of simplicity, we restrict our attention to the case where the random variable can only

[1] In finite dimension, a purification is often chosen to be state dependent as well. Given a density operator $\rho_A$ on a Hilbert space $\mathcal{H}_A$, a purification of $\rho_A$ is a rank one density operator $\rho_{A'B}$ on some Hilbert space $\mathcal{H}_{A'} \otimes \mathcal{H}_B$, such that $\rho_{A'} = \rho_A$. But note that $|A| \geq |A'| \geq \text{rank}(\rho_A)$, and not necessarily $|A'| = |A|$.

takes values in a countable set which, for convenience, is also denoted by $X$. An extension to continuous alphabets is given in Section 5.2.1. A classical random variable $X$ can be associated to the abelian von Neumann algebra of bounded complex valued functions on $X$, denoted by $\ell^\infty(X) = \ell^\infty(X, \mathbb{C})$. Elements $\lambda$ in $\ell^\infty(X)$ can be represented as sequences $(\lambda_x)_{x\in X}$ with $\lambda_x \in \mathbb{C}$, and the norm is the supremum norm $\|\lambda\|_\infty = \sup_x |\lambda_x|$. We often use the abbreviation $\ell^\infty_{|X|}$ for $\ell^\infty(X)$ justified by the simple fact that $\ell^\infty(X)$ is isomorphic to $\ell^\infty(Y)$ if $X$ and $Y$ have the same cardinality. The set of normal states on $\ell^\infty(X)$ is formed by positive and absolutely converging sequences $(p_x)$ in $\ell^1(X) = \ell^1_{|X|}$ satisfying $\sum_x p_x = 1$. Hence, a state defines a probability distribution of $X$. Henceforth, we usually use the symbols $X$, $Y$, $Z$ to denote classical systems.

A bipartite system consisting of a classical part $X$ and a quantum part $B$, is then described by the von Neumann algebra $\mathcal{M}_{XB} = \ell^\infty_{|X|} \otimes \mathcal{M}_B$. This can be identified with the set of sequences $(a_x)_{x\in X}$, $a_x \in \mathcal{M}_B$, equipped with the norm

$$\|(a_x)\|_{\ell^\infty(\mathcal{M}_B)} = \sup_{x\in X} \|a_x\|_{\mathcal{M}_B} \ , \tag{3.1}$$

denoted by $\ell^\infty_{|X|}(\mathcal{M}_B)$ or also $\ell^\infty(X, \mathcal{M}_B)$. The set of normal functionals on $\ell^\infty_{|X|}\otimes\mathcal{M}_B$ is consequently $\ell^1_{|X|} \otimes \mathcal{N}(\mathcal{M}_B)$. States on $\ell^\infty_{|X|} \otimes \mathcal{M}_B$ are called classical quantum (cq-) states, and can be written as $\omega_{XB} = (\omega^x_B)_{x\in X}$, where $\omega^x_B \in \mathcal{S}_\leq(\mathcal{M}_B)$ such that $\omega_{XB}(a) = \sum_x \omega^x_B(a_x)$ for all $a = (a_x) \in \mathcal{M}_{XB}$. The norm inherited from $\ell^1_{|X|} \otimes \mathcal{N}(\mathcal{M}_B)$ is then given by

$$\|(\omega^x)\|_{\ell^1(\mathcal{N}(\mathcal{M}_B))} = \sum_{x\in X} \|\omega^x\|_{\mathcal{N}(\mathcal{M}_B)} \ . \tag{3.2}$$

Note that $\ell^\infty_{|X|} \otimes \mathcal{M}_B$ can be identified with $\bigoplus_{x\in X} \mathcal{M}_B$, and that states can also be written as $\omega_{XB} = \oplus_{x\in X}\omega^x_B$. Hence, we can think of $\ell^\infty_{|X|}(\mathcal{M}_B)$ as embedded into the quantum system $M_{|X|}(\mathcal{M}_B)$ as the algebra of diagonal matrices with entries in $\mathcal{M}_B$. This allows us to embed classical systems into quantum systems described by a matrix algebra. More concretely, let $\{|x\rangle\}_{x\in X}$ be an orthonormal basis which spans the Hilbert space $\mathcal{H}_X$. We denote by $e_x$ the state which corresponds to the density matrix $|x\rangle\langle x|$ and thus satisfies $e_x(|y\rangle\langle y|) = \delta_{xy}$. We identify a classical quantum state $\omega_{XB} = (\omega^x_B)$ with the state on $\mathcal{B}(\mathcal{H}_X) \otimes \mathcal{M}_B$ given by

$$\sum_x e_x \otimes \omega^x_B \tag{3.3}$$

which we also denote by $\omega_{XB}$. The operators $(a_x)$ of the classical quantum systems $\ell^\infty_{|X|} \otimes \mathcal{M}_B$ are then consistently identified by $\sum |x\rangle\langle x| \otimes a_x$ such that $\sum_x e_x \otimes \omega^x_B(\sum |x\rangle\langle x| \otimes a_x) = \sum_x \omega^x_B(a_x)$.

Cq-states can be interpreted as post-measurement states, where the outcome is treated as a random variable. Since we consider only measurements with finite alphabets, the classical part of the resulting cq-state is finite. Let us assume that we start with a bipartite state $\omega_{AB} \in \mathcal{S}(\mathcal{M}_{AB})$ on which we perform a measurement

on the system $A$ represented by the observable $\{E_x\}_{x\in X} \subset \mathcal{M}_A$. The normalized post-measurement states on $\mathcal{M}_B$ conditioned on the outcome $x \in X$, are described by $\frac{1}{\omega_B^x(\mathbb{1})}\omega_B^x$, where $\omega_B^x(a) = \omega_{AB}(E_x a)$ for all $a \in \mathcal{M}_B$. Note that $\omega_B^x(\mathbb{1})$ is just the probability to measure the outcome $x$. Hence, if we treat the outcome as a random variable, the post-measurement state is the cq-state $\omega_{XB} = (\omega_B^x)_{x\in X}$. The map $\omega_{AB} \mapsto (\omega_B^x)_{x\in X}$ describes a quantum channel from $\mathcal{M}_A$ to the classical output space $\ell_{|X|}^\infty$. Conversely, for any cq-state $\omega_{XB} = (\omega_B^x)_{x\in X}$ on $\mathcal{M}_{XB}$, we can find a state $\omega_{AB} \in \mathcal{S}(\mathcal{M}_A \vee \mathcal{M}_B)$ with suitable $\mathcal{M}_A$ and an observable $\{E_x\} \subset \mathcal{M}_A$, which give rise to $\omega_{XB}$. The measurement operators $E_x$ can for instance be chosen as the non-commutative Radon-Nikodym derivative of $\omega_B^x$ with respect to $\sum_x \omega_B^x$ (see Sectoin 2.2.3).

## 3.4. Distance Measures on the State Space

Distance measures on $\mathcal{S}(\mathcal{M})$ or $\mathcal{S}_\leq(\mathcal{M})$ are important tools to quantify how close two different states are. The common distance measure on $\mathcal{S}(\mathcal{M})$ is the one induced by the norm on $\mathcal{S}(\mathcal{M})$ via $d(\omega,\eta) = \frac{1}{2}\|\omega - \eta\|$. For type I factors $\mathcal{M} = \mathcal{B}(\mathcal{H})$ it is usually referred to as the trace distance, since for any $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ we get $\|\omega_\rho - \omega_\sigma\| = \|\rho - \sigma\|_1 = \mathrm{Tr}|\rho - \sigma|$. The advantage of this distance measure is its operational interpretation as the success probability to distinguish the two states with the optimal measurement.

The trace distance is often hard to compute and it is sometimes easier (especially if one of the states is pure) to use the fidelity to quantify the closeness of states. The fidelity or generalized transition probability was introduced and discussed for von Neumann algebras by Bures in [Bur69]. We define the fidelity according to Uhlmann [Uhl76] as

$$F_{\mathcal{M}}(\omega,\sigma) = \sup_\pi |\langle \xi_\omega^\pi | \xi_\sigma^\pi \rangle|^2, \tag{3.4}$$

where the supremum runs over all representations $\pi$ of $\mathcal{M}$ for which, simultaneously, purifications $|\xi_\omega^\pi\rangle$ and $|\xi_\sigma^\pi\rangle$ of $\omega$ and $\sigma$ exists. In the sequel, the subscript $\mathcal{M}$ denoting the von Neumann algebra is omitted if it is clear from the context. Furthermore, if $\mathcal{M} \subset \mathcal{B}(\mathcal{H})$ and $\omega$ a vector state state on $\mathcal{M}$ represented by $|\xi_\omega\rangle \in \mathcal{H}$, we define $F_{\mathcal{M}}(|\xi_\omega\rangle, \sigma) = F_{\mathcal{M}}(\omega,\sigma)$. If one chooses a particular representation $\pi$ on $\mathcal{H}$ in which $\omega, \sigma$ can be represented as vector states, and one takes arbitrary representatives $|\xi_\omega\rangle, |\xi_\sigma\rangle \in \mathcal{H}$ of them, the fidelity can be expressed as [Alb83]

$$F(\omega,\sigma) = \sup_{U\in\pi(\mathcal{M})'} |\langle \xi_\omega | U\xi_\sigma \rangle|^2 \ , \tag{3.5}$$

where the supremum is taken over unitaries $U$ in $\pi(\mathcal{M})'$. Since the optimization can be extended over the $\sigma$-weakly compact set of all $U$ with $\|U\| \leq 1$, and the map $U \mapsto \langle \xi_\omega, U\xi_\sigma\rangle$ is $\sigma$-weakly continuous, we know that the supremum is attained. Note that the optimization over all unitaries in the commutant is equivalent to the optimization over all possible purifications of $\sigma$ in $\mathcal{H}$. From this it follows that $F_{\mathcal{B}(\mathcal{H})}(|\psi\rangle, |\phi\rangle) = |\langle\psi|\phi\rangle|^2$ for all $|\psi\rangle, |\phi\rangle \in \mathcal{H}$. Another important property of the fidelity is the monotonic behavior under a quantum channel $\mathcal{E}$ [Alb83]

$$F(\omega,\sigma) \leq F(\mathcal{E}(\omega), \mathcal{E}(\sigma)) \ . \tag{3.6}$$

As a special case, we obtain that $F_{\mathcal{M}}(\omega,\sigma) \geq F_{\mathcal{N}}(\omega,\sigma)$ for $\mathcal{M} \subset \mathcal{N}$.

Based on the fidelity one can define distance measures, like for instance the Bures distance [Bur69] which is obtained via

$$\inf_{\pi} \| |\xi\rangle_{\omega} - |\xi\rangle_{\sigma} \| = \sqrt{\omega(\mathbb{1}) + \sigma(\mathbb{1}) - 2\sqrt{F(\rho,\omega)}}$$

where the infimum on the left hand side runs over all representation in which vector states for $\rho$ and $\omega$ exists. The obtained metric is known as the Bures distance.

**Generalized Fidelity and Purified Distance.** In the following we extend the concept of the generalized fidelity as introduced for finite-dimensional Hilbert spaces in [TCR10] to general von Neumann algebras. This quantity will then be used to define another metric on $\mathcal{S}_{\leq}(\mathcal{M})$, which turns out to be suitable in the context of smooth entropies. We start by introducing the concept of a *projective embedding* of a von Neumann algebra. Let $\mathcal{M},\mathcal{N}$ be two von Neumann algebras. We say that $\mathcal{N}$ admits a projective embedding of $\mathcal{M}$, denoted by $\mathcal{M} \curvearrowright \mathcal{N}$, if there exists a projector p in $\mathcal{N}$ such that $p\mathcal{N}p$ is isomorphic to $\mathcal{M}$.[2] Note that this is equivalent to the existence of a projector $p$ in $\mathcal{N}$ and a faithful representation $\pi$ of $\mathcal{M}$ into $\mathcal{N}$ such that $\pi(\mathcal{M}) = (\mathbb{1}-p) \oplus p\mathcal{N}p$. This concept allows us to interpret subnormalized states as the result of an incomplete measurement. In particular, given $\omega \in \mathcal{S}_{\leq}(\mathcal{M})$ and $\mathcal{M} \curvearrowright \mathcal{N}$ with $\mathcal{M} \cong p\mathcal{N}p$, there exists an extended state $\bar{\omega} \in \mathcal{S}(\mathcal{N})$ such that $\bar{\omega}(pxp) = \omega(x)$ for $x \in \mathcal{N}$, where we identified $\mathcal{M}$ and $p\mathcal{N}p$.[3] We then interpret each measurement in $\mathcal{M}$ as incomplete and complete it by adding the no event $(\mathbb{1}-p)$, which leads to the same results as considering the state $\omega$ on $\mathcal{M}$. Based on the concept of a projecting embedding, the generalized fidelity can now be defined similarly as in the finite-dimensional case [TCR10].

**Definition 3.4.1.** *Let $\mathcal{M}$ be a von Neumann algebra, and $\omega,\sigma \in \mathcal{S}_{\leq}(\mathcal{M})$. The generalized fidelity between $\sigma$ and $\omega$ is defined as*

$$\mathcal{F}_{\mathcal{M}}(\omega,\sigma) = \sup_{\mathcal{M}\curvearrowright\mathcal{N}} \sup_{\bar{\omega},\bar{\sigma}\in\mathcal{S}(\mathcal{N})} F_{\mathcal{N}}(\bar{\sigma},\bar{\omega}) \ , \tag{3.7}$$

*where the second supremum runs over all extended normalized states on $\mathcal{N}$ such that $\bar{\omega}(p \cdot p)$ on $p\mathcal{N}p \cong \mathcal{M}$ corresponds to $\omega$ and similarly for $\bar{\sigma}$.*

Due to $\mathcal{M} \curvearrowright \mathcal{M} \oplus \mathbb{C}$, the generalized fidelity can be simplified as follows [TCR10].

**Lemma 3.4.2.** *Let $\mathcal{M}$ be a von Neumann algebra, and $\omega,\sigma \in \mathcal{S}_{\leq}(\mathcal{M})$. Then*

$$\mathcal{F}_{\mathcal{M}}(\omega,\sigma)^{\frac{1}{2}} = F_{\hat{\mathcal{M}}}(\hat{\omega},\hat{\sigma})^{\frac{1}{2}} = F_{\mathcal{M}}(\omega,\sigma)^{\frac{1}{2}} + (1-\omega(\mathbb{1}))^{\frac{1}{2}}(1-\sigma(\mathbb{1}))^{\frac{1}{2}} \ , \tag{3.8}$$

*where $\hat{\mathcal{M}} = \mathcal{M} \oplus \mathbb{C}$, $\hat{\omega} = \omega \oplus (1-\omega(\mathbb{1}))$ and $\hat{\sigma} = \sigma \oplus (1-\sigma(\mathbb{1}))$.*

[2] Note that if $\mathcal{M} \subset \mathcal{B}(\mathcal{H})$ and $V : \mathcal{H} \to \mathcal{H}'$ is an isometry, it follows that $\mathcal{M} \curvearrowright \mathcal{B}(\mathcal{H}')$ with the projector $p = VV^*$ [TCR10].

[3] Choose for instance $\bar{\omega}(x) = \omega(pxp) + \sigma((\mathbb{1}-p)x(\mathbb{1}-p))$ with $\sigma \in \mathcal{S}_{\leq}(\mathcal{N})$ such that $\sigma(\mathbb{1}-p) = 1-\omega(p)$.

*Proof.* The proof for finite-dimensional Hilbert spaces is given in [TCR10, Lemma 3]. Let $\mathcal{N}$ be such that $\mathcal{M}\curvearrowright\mathcal{N}$ with $p$ the corresponding projector such that $\mathcal{M}\cong p\mathcal{N}p$. Furthermore let $\bar{\omega},\bar{\sigma}$ be extensions of $\omega,\sigma$ on $\mathcal{N}$ satisfying the required properties. According to the definition of the fidelity we have that $F_{\mathcal{N}}(\bar{\omega},\bar{\sigma}) = \sup|\langle\xi^{\pi}_{\bar{\omega}}|\xi^{\pi}_{\bar{\sigma}}\rangle|^2$, where the supremum runs over all representations admitting a purification of $\bar{\omega},\bar{\sigma}$. Now note that all such representations $\pi$ are also representations of $\mathcal{M}$, that $\xi^{\pi}_{\omega} = \pi(p)\xi^{\pi}_{\bar{\omega}}$ is a purification of $\omega$, and that the same also holds for $\xi^{\pi}_{\sigma} = \pi(p)\xi^{\pi}_{\bar{\sigma}}$. We can then use the Cauchy-Schwarz inequality to compute

$$\begin{aligned}|\langle\xi^{\pi}_{\bar{\omega}}|\xi^{\pi}_{\bar{\sigma}}\rangle| &= |\langle\xi^{\pi}_{\omega}|\xi^{\pi}_{\sigma}\rangle| + |\langle(\mathbb{1}-p)\xi^{\pi}_{\bar{\omega}}|(\mathbb{1}-p)\xi^{\pi}_{\bar{\sigma}}\rangle| \\ &\leq |\langle\xi^{\pi}_{\omega}|\xi^{\pi}_{\sigma}\rangle| + \sqrt{\|(\mathbb{1}-p)\xi^{\pi}_{\bar{\omega}}\|\|(\mathbb{1}-p)\xi^{\pi}_{\bar{\sigma}}\|} \\ &\leq |\langle\xi^{\pi}_{\omega}|\xi^{\pi}_{\sigma}\rangle| + \sqrt{(1-\omega(\mathbb{1}))(1-\sigma(\mathbb{1}))}\,.\end{aligned}$$

Since this holds for all $\pi$, we have that $\mathcal{F}_{\mathcal{N}}(\bar{\omega},\bar{\sigma})^{\frac{1}{2}} \leq F_{\mathcal{M}}(\omega,\sigma)^{\frac{1}{2}} + (1-\omega(\mathbb{1}))^{\frac{1}{2}}(1-\sigma(\mathbb{1}))^{\frac{1}{2}}$ for all $\mathcal{N}$ such that $\mathcal{M}\curvearrowright\mathcal{N}$ and all suitable $\bar{\omega},\bar{\sigma}$ on $\mathcal{N}$. Hence, we get

$$\mathcal{F}_{\mathcal{M}}(\omega,\sigma)^{\frac{1}{2}} \leq F_{\mathcal{M}}(\omega,\sigma)^{\frac{1}{2}} + (1-\omega(\mathbb{1}))^{\frac{1}{2}}(1-\sigma(\mathbb{1}))^{\frac{1}{2}}\ .$$

Finally it is easy to check that the specific choice $\hat{\mathcal{M}}$ together with $\hat{\omega}$ and $\hat{\sigma}$ achieves equality. □

The purified distance is defined as follows [TCR10].

**Definition 3.4.3.** *Let $\mathcal{M}$ be a von Neumann algebra, and $\omega,\sigma\in\mathcal{S}_{\leq}(\mathcal{M})$. The purified distance between $\omega$ and $\sigma$ is defined as*[4]

$$\mathcal{P}_{\mathcal{M}}(\omega,\sigma) = \sqrt{1-\mathcal{F}_{\mathcal{M}}(\omega,\sigma)}\ . \tag{3.9}$$

Like for the fidelity, we omit the indication of the von Neumann algebra whenever it is clear from the context and write $\mathcal{P}_{\mathcal{M}}(\omega,\sigma) = \mathcal{P}_{\mathcal{M}}(|\xi\rangle,\sigma)$ if $|\xi\rangle$ is a purification of $\omega$. For $\mathcal{P}(\omega,\sigma)\leq\epsilon$ we also use the notation $\omega\approx_{\epsilon}\sigma$, and say that $\omega$ and $\sigma$ are $\epsilon$-close. A detailed discussion of the properties of the purified distance can be found in [TCR10]. Although their scope is restricted to finite-dimensional Hilbert spaces, most of the properties follow in the same way for the more general setting of von Neumann algebras. It is for instance easy to see that the purified distance defines a metric on $\mathcal{S}_{\leq}(\mathcal{M})$. The following Lemma shows the equivalence to the norm distance on $\mathcal{N}(\mathcal{M})$.

**Lemma 3.4.4.** *Let $\mathcal{M}$ be a von Neumann algebra, and $\omega,\sigma\in\mathcal{S}_{\leq}(\mathcal{M})$. Then*

$$\sqrt{\|\omega-\sigma\|+|\omega(\mathbb{1})-\sigma(\mathbb{1})|} \geq \mathcal{P}_{\mathcal{M}}(\sigma,\omega) \geq \frac{1}{2}\big(\|\omega-\sigma\|+|\omega(\mathbb{1})-\sigma(\mathbb{1})|\big)\ . \tag{3.10}$$

[4] The name purified distance comes from the finite-dimensional case, where the purified distance between two states corresponds to the minimal trace norm between purifications. It is straightforward to see that the same result also holds in the case of a von Neumann algebra, namely, $\mathcal{P}_{\mathcal{M}}(\omega,\sigma) = \frac{1}{2}\inf_{\pi}\||\xi^{\pi}_{\omega}\rangle\langle\xi^{\pi}_{\omega}| - |\xi^{\pi}_{\sigma}\rangle\langle\xi^{\pi}_{\sigma}|\|_1$, where the infimum runs over all representations of $\mathcal{M}$ in which $\omega$ and $\sigma$ have a vector representation denoted by $|\xi^{\pi}_{\omega}\rangle$ and $|\xi^{\pi}_{\sigma}\rangle$, respectively.

*Proof.* The proof follows directly from the inequalities

$$1 - \sqrt{F(\omega,\sigma)} \leq \frac{1}{2}\|\omega - \sigma\| \leq \sqrt{1 - F(\omega,\sigma)} \ .$$

shown in [Bur69] and [Uhl76]. See [TCR10] for more details. □

An important property which follows directly from the way how the generalized fidelity is defined, is the monotonicity under completely positive, contractions.

**Lemma 3.4.5.** *Let $\mathcal{M}$ be a von Neumann algebra, $\omega, \sigma \in \mathcal{S}_{\leq}(\mathcal{M})$, and $\mathcal{E}$ completely positive contraction. Then*

$$\mathcal{P}(\omega,\sigma) \geq \mathcal{P}(\mathcal{E}_*(\omega), \mathcal{E}_*(\sigma)) \ . \tag{3.11}$$

*Proof.* The proof in the finite-dimensional case can be found in Tomamichel09. It is a direct consequence of the definition of the generalized fidelity and equation (3.6), from which it follows that $\mathcal{F}(\omega,\sigma) \leq \mathcal{F}(\mathcal{E}(\omega), \mathcal{E}(\sigma))$. □

An important property of the purified distance is the following.

**Lemma 3.4.6.** *Let $\omega_{AB} \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$ and $(\pi, \mathcal{H}, |\xi_\omega\rangle)$ a purifications of $\omega_{AB}$ with relevant system $\mathcal{M}_{AB}$ and complementary system $\mathcal{M}_C$. For any state $\sigma_{AB} \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$ there exists a purification $(\pi, \mathcal{H}, |\xi_\sigma\rangle)$ such that* [5]

$$\mathcal{P}(\sigma_{AC}, \omega_{AC}) \leq \mathcal{P}(\sigma_{AB}, \omega_{AB}) \ , \tag{3.12}$$

*where $\sigma_{AC}$ and $\omega_{AC}$ denote the restriction of $|\xi_\sigma\rangle$ and $|\xi_\omega\rangle$ onto $\mathcal{M}_{AC}$.*

*Proof.* Let us assume that $\omega_{AB}$ and $\sigma_{AB}$ are normalized. Otherwise the same argument applies to $\hat{\omega}_{AB}$ and $\hat{\sigma}_{AB}$ defined in Lemma 3.4.2. According to the definition of the fidelity in Equation (3.4) there exists a purification $(\pi, \mathcal{H}, |\xi_\sigma\rangle)$ of $\sigma$ such that $F_{\mathcal{M}_{AB}}(\sigma_{AB}, \omega_{AB}) = F_{\mathcal{B}(\mathcal{H})}(|\xi_\sigma\rangle, |\xi_\omega\rangle)$. Using the definition of the purified distance, we obtain

$$\mathcal{P}_{\mathcal{M}_{AB}}(\sigma_{AB}, \omega_{AB}) = \mathcal{P}_{\mathcal{B}(\mathcal{H})}(|\xi_\sigma\rangle, |\xi_\omega\rangle) \geq \mathcal{P}_{\mathcal{M}_{AC}}(\sigma_{AC}, \omega_{AC}) \ , \tag{3.13}$$

where we applied the monotonicity under quantum channels (3.11) in the last inequality. □

[5] We can always assume that $\mathcal{H}$ is large enough that every state on $\mathcal{M}_{AB}$ admits a purification.

# 4. Smooth Min- and Max-Entropies on von Neumann Algebras

## 4.1. Introduction

The smooth conditional min- and max-entropies, $\mathrm{H}_{\min}^{\epsilon}(A|B)_{\omega}$ and $\mathrm{H}_{\max}^{\epsilon}(A|B)_{\omega}$, for finite-dimensional systems $A$ and $B$ were introduced in [Ren05, KRS09, TCR10]. Their importance stem mostly from their operational significance (see Section 1.3 for a discussion of the role of entropies in information theory). They are used to characterize quantum information theoretic tasks in the non-asymptotic regime and depend on a smoothing parameter $\epsilon$ which, in an operational sense, is related to a failure probability or an allowed error. Such an error is due to the probabilistic nature of the problem and is required to vanish if rates in the asymptotic limit are considered.[1] The $\epsilon$-smooth min-entropy $\mathrm{H}_{\min}^{\epsilon}(A|B)_{\omega}$ of a state $\omega_{AB}$ is defined as the maximization of the min-entropy ($\epsilon = 0$) over states which are indistinguishable from $\omega_{AB}$ up to a probability of order $\epsilon$.[2] The same applies to the $\epsilon$-smooth max-entropy $\mathrm{H}_{\max}^{\epsilon}(A|B)_{\omega}$ with the minimization of the $\epsilon = 0$ case. The smooth min- and max-entropy are connected via purification, that is, if $\omega_{ABC}$ is a pure state then $\mathrm{H}_{\min}^{\epsilon}(A|B)_{\omega} = -\mathrm{H}_{\max}^{\epsilon}(A|C)_{\omega}$. This is called the duality relation. This feature is shared with other entropic quantities, for instance the von Neumann entropy is self-dual and $\alpha$-Rényi entropies are dual for $1/\alpha + 1/\beta = 2$ (see e.g., [CCYZ12]).

The conditional min-entropy of a classical quantum state has the intuitive and useful interpretation of being the logarithm of the guessing probability [KRS09]. The max-entropy of a classical quantum state can be associated with the distance to a secure key [KRS09]. The smooth entropies have been used to characterize various problems in information theory like for instance data compression [RW04, RW05, RR12], channel coding problems [DBWR10, Ber08, RWW06, MD09, BD10c, WR12, RR11, HD11], and privacy amplification [Ren05, TSSR10]. Moreover, similar quantities are used in entanglement theory [Dat09, BD10b, BD10a, BD11, BD09]. From the one-shot results, the asymptotic limit can be obtained via the asymptotic equipartition property were the von Neumann entropy emerges [TCR09, Ren05] (c.f. Section 4.5.3).

In the following sections, we define the smooth min- and max-entropies for states $\omega_{AB}$, where the first system $A$ is given by the von Neumann algebra of all operators on a separable Hilbert space and the conditional system $B$ is modeled by an arbitrary von Neumann algebra. This setting is sufficient for most of the operational applications including the one given in Chapter 6. An extension of the smooth min-

[1] For a discussion of the information theory in the asymptotic limit see Section 1.3 and references therein.

[2] This means that using the best possible measurements the succeed probability to distinguish the two states is of order $\epsilon$.

and max-entropy to infinite-dimensional systems which is based on a more analytical approach is considered in [FAR11] (c.f. Section 4.5.2). Furthermore, we prove that most of the properties known from the finite-dimensional setting as well as the operational interpretations for smooth and non-smooth min- and max-entropies can be extended to this more general setting.

## 4.2. Definition of Min- and Max-Entropy

In the following we consider multipartite systems $\mathcal{M}_{ABC} = \mathcal{M}_A \vee \mathcal{M}_B \vee \mathcal{M}_C$ with the restriction that system $A$ is always a type I factor, that is, $\mathcal{M}_A \simeq \mathcal{B}(\mathcal{H}_A)$. Since $\mathcal{B}(\mathcal{H}_A)$ is nuclear we can unambiguously write the system as the tensor product $\mathcal{M}_{ABC} = \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{M}_{BC}$. The conditional min-entropy is defined similarly as in the case of finite-dimensional Hilbert spaces [Ren05, KRS09].

**Definition 4.2.1.** *Let $\mathcal{M}_{AB} = \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{M}_B$ with $\mathcal{M}_B$ a von Neumann algebra, and $\omega_{AB} \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$. The min-entropy of $\omega_{AB}$ conditioned on $B$ is defined as*

$$\mathrm{H}_{\min}(A|B)_\omega = -\log \inf_{\sigma_B \in \mathcal{S}(\mathcal{M}_B)} \inf\{\lambda \mid \lambda\, \tau_A \otimes \sigma_B \geq \omega_{AB}\} \,, \tag{4.1}$$

*where $\tau_A$ denotes the trace in $\mathcal{H}_A$, i.e. $\tau_A(x) = \mathrm{Tr}(x)$ for all $x \in \mathcal{B}(\mathcal{H}_A)$.*

The unconditional min-entropy is obtained for trivial side information $\mathcal{M}_B \simeq \mathbb{C}$. If the state $\omega_A$ on $\mathcal{M}_A \simeq \mathcal{B}(\mathcal{H}_A)$ can be written with the density operator $\rho_A$ via $\omega_A(a) = \mathrm{Tr}\rho_A a$, then the unconditional min-entropy is given by the quantum Rényi entropy of order $\infty$ [FAR11]

$$\mathrm{H}_{\min}(A)_\omega = -\log \|\rho_A\| \,, \tag{4.2}$$

and thus determined by the largest eigenvalue of $\rho_A$. The unconditional min-entropy is always positive and 0 if and only if $\omega$ is a pure state. Moreover, if $\mathcal{H}_A$ is a $d_A$-dimensional Hilbert space then the maximal entropy is $\log d_A$ and attained for the maximally mixed state $\rho_A = (1/d_A)\mathbb{1}_A$. This is in analogy to the von Neumann entropy and expected by a reasonable entropy measure. If we assume for the moment that $\mathcal{M}_A \simeq \mathcal{M}_B \simeq \mathcal{B}(\mathcal{H})$ with $\mathcal{H}$ a $d$-dimensional Hilbert space, then we find that $\mathrm{H}_{\min}(A|B) = -\log d$ is the minimal possible entropy and attained for the maximally entangled state

$$|\Psi\rangle = \sum_{k=1}^{d} |a_k, b_k\rangle \,, \tag{4.3}$$

where $|a_k\rangle$ and $|b_k\rangle$ are orthonormal bases of $\mathcal{H}$.[3] Hence, for $d$-dimensional systems the range of the conditional min-entropy lies between $-\log d$ and $\log d$.

The min-entropy can be rewritten in the more compact form

$$\mathrm{H}_{\min}(A|B)_\omega = -\log \inf\{\sigma_B(\mathbb{1}), \mid \tau_A \otimes \sigma_B \geq \omega_{AB},\, \sigma_B \in \mathcal{S}(\mathcal{M}_B)\} \,. \tag{4.4}$$

[3] Note that the same holds for the conditional von Neumann entropy

by combining the two optimizations. Similar to the von Neumann entropy (see e.g., [OP93]), the min-entropy can be written in terms of a relative entropy, namely, the relative max-entropy [Dat09]

$$\mathrm{D}_{\max}(\omega \,||\, \sigma) = \inf\{\mu \in \mathbb{R} : \omega \leq 2^{\mu} \cdot \sigma\} \ . \tag{4.5}$$

By means of the relative max-entropy the min-entropy simply reads

$$\mathrm{H}_{\min}(A|B)_{\omega} = -\inf_{\sigma_B} \mathrm{D}_{\max}(\omega \,||\, \tau \otimes \sigma_B) \, .$$

We define the conditional max-entropy of a state $\omega_{AB}$ on $\mathcal{M}_{AB}$ as the dual of the min-entropy [KRS09].[4]

**Definition 4.2.2.** *Let $\mathcal{M}_{AB} = \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{M}_B$ with $\mathcal{M}_B$ a von Neumann algebra, and $\omega_{AB} \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$. The max-entropy of $\omega_{AB}$ conditioned on $B$ is defined as*

$$\mathrm{H}_{\max}(A|B)_{\omega} = -\mathrm{H}_{\min}\left(A'|C\right)_{\omega} , \tag{4.6}$$

*with $\omega_{A'B'C}$ an arbitrary purification $(\pi, \mathcal{K}, |\xi\rangle)$ of $\omega_{AB}$ with $\mathcal{M}_{A'B'} = \pi(\mathcal{M}_{AB})$ the relevant system such that $\mathcal{M}_{A'} \simeq \mathcal{B}(\mathcal{H}_{A'})$ for a suitable $\mathcal{H}'_A$, and $\mathcal{M}_C = \pi(\mathcal{M}_{A'B'})'$ the complementary system.*

For the sake of simplicity, we often use a purification $(\pi, \mathcal{K}, |\xi\rangle)$ such that $\pi(\mathcal{M}_A)$ is isomorphic to $\mathcal{M}_A$ and write again $\mathcal{M}_A$ for $\pi(\mathcal{M}_A)$. The next Lemma shows that the conditional max-entropy is well defined, that is, independent of the choice of the purification.

**Lemma 4.2.3.** *Let $\mathcal{M}_{AB} = \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{M}_B$ with $\mathcal{M}_B$ a general von Neumann algebra, $\omega_{AB} \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$, and $(\pi_i, \mathcal{K}_i, |\xi_i\rangle)$, $i = 1, 2$, two purifications of $\omega_{AB}$ with $\pi_i(\mathcal{M}_A) = \mathcal{M}_{A_i}$ and complementary systems $\mathcal{M}_{C_i}$. Then it follows that*

$$\mathrm{H}_{\min}(A_1|C_1)_{\omega^1} = \mathrm{H}_{\min}(A_2|C_2)_{\omega^2} \ , \tag{4.7}$$

*where $\omega^i_{A_iC_i}$ is the restricted state corresponding to $|\xi_i\rangle$.*

*Proof.* The proof follows the same line of reasoning as the one given in [TCR10, Lemma 13] for finite-dimensional Hilbert spaces. According to Lemma 3.2.2, we know that there exists a partial isometry $V : \mathcal{K}_1 \to \mathcal{K}_2$ with $|\xi_2\rangle = V|\xi_1\rangle$ and $V\pi_1(a) = \pi_2(a)V$ for all $a \in \mathcal{M}_{AB}$. Then it follows for all $x \in \mathcal{M}_{A_2} \otimes \mathcal{M}_{C_2}$ that

$$\omega^2_{A_2C_2}(x) = \langle \xi_2 | x \xi_2 \rangle = \langle \xi_1 | V^* x V \xi_1 \rangle \tag{4.8}$$

$$= \omega^1_{A_1C_1}(V^* x V) \ , \tag{4.9}$$

where we used in the last equality that $V^*xV \in \mathcal{M}_{A_1} \otimes \mathcal{M}_{C_1}$. This follows from the fact that $(\mathcal{M}_{A_i} \otimes \mathcal{M}_{C_i})' = \pi_i(\mathcal{M}_B)$ and for all $|\phi\rangle, |\psi\rangle \in \mathcal{K}_1$ and $y \in \mathcal{M}_B$

$$\langle \phi | V^* x V \pi_1(y) \psi \rangle = \langle \phi | V^* x \pi_2(y) V \psi \rangle = \langle \phi | V^* \pi_2(y) x V \psi \rangle = \langle \phi | \pi_1(y) V^* x V \psi \rangle \ .$$

[4] The definition of the max-entropy here is different to the one used in [Ren05].

From (4.8) we obtain that $\omega^1_{A_1C_1} \leq \tau_{A_1} \otimes \sigma_{C_1}$ implies $\omega^2_{A_2C_2} \leq V(\tau_{A_1} \otimes \sigma_{C_1})V^*$, where we used the notation $V(\tau_{A_1} \otimes \sigma_{C_1})V^*(x) = \tau_{A_1} \otimes \sigma_{C_1}(V^*xV)$ adopted from the density matrix formalism. But since $V$ commutes with $\pi_2(\mathcal{M}_A)$, it is of the form $V_A \otimes V_C$ such that $V(\tau_A \otimes \sigma_{C_1})V^* = V_A\tau_{A_1}V_A^* \otimes V_B\sigma_{C_1}V_B^*$. Because of $\tilde{V}\sigma_{C_1}V^*(\mathbb{1}) \leq \sigma_{C_1}(\mathbb{1})$ and $V_A\tau_{A_1}V_A^* \leq \tau_{A_2}$, we can conclude that $\mathrm{H}_{\min}(A_1|C_1)_{\omega^1} \leq \mathrm{H}_{\min}(A_2|C_2)_{\omega^2}$. Since the argument was symmetric, we get equality. □

The unconditional max-entropy of a state $\omega_A$ on $\mathcal{M}_A \simeq \mathcal{B}(\mathcal{H}_A)$ represented by the density matrix $\rho_A$ is shown to be equal to the quantum 1/2-Rényi entropy [FAR11]

$$\mathrm{H}_{\max}(A)_\omega = 2\log \mathrm{Tr}\rho^{\frac{1}{2}}\,.$$

Hence, we obtain as for the min-entropy that the unconditional max-entropy is equal to 0 for pure states and $\log d_A$ for the maximally mixed state on a $d_A$-dimensional Hilbert space. Similar to the min- and von Neumann entropy follows that for $d$-dimensional A and B systems the minimal conditional entropy is given by $-\log d$ and attained for the maximally entangled state given in Equation (4.3).

## 4.3. Definition of Smooth Min- and Max-Entropies

The smooth entropies are obtained from the plain entropies by optimizing over a set of states which are close to the relevant state. The basic idea of smoothing is that in a single shot scenario a task can in general just be satisfied up to a small failure probability. As discussed in Section 1.3, allowing to optimize the entropies over states which cannot be distinguished up to a probability in the same order as the failure probability results usually in a tighter characterization of the task. The optimization is done over a set of states which are close in the purified distance (see Definition 3.4.3).

**Definition 4.3.1.** *Let $\mathcal{M}$ be a von Neumann algebra, $\omega \in \mathcal{S}_\leq(\mathcal{M})$, and $\epsilon \geq 0$. We define the smoothing set around $\omega$ as*

$$\mathcal{B}^\epsilon_{\mathcal{M}}(\omega) = \{\sigma \in \mathcal{S}_\leq(\mathcal{M}) : \mathcal{P}_{\mathcal{M}}(\omega, \sigma) \leq \epsilon\}\,. \tag{4.10}$$

We usually omit the indication of the von Neumann algebra in the subscript of the smoothing set whenever it is clear from the context.

**Definition 4.3.2.** *Let $\mathcal{M}_{AB} = \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{M}_B$ with $\mathcal{M}_B$ a von Neumann algebra, $\omega_{AB} \in \mathcal{S}_\leq(\mathcal{M}_{AB})$ and $\epsilon \geq 0$. The $\epsilon$-smooth min-entropy of $\omega_{AB}$ conditioned on $B$ is defined as*

$$\mathrm{H}^\epsilon_{\min}(A|B)_\omega = \sup_{\bar{\omega}_{AB} \in \mathcal{B}^\epsilon(\omega_{AB})} \mathrm{H}_{\min}(A|B)_{\bar{\omega}}\,, \tag{4.11}$$

*and the $\epsilon$-smooth max-entropy of $\omega_{AB}$ conditioned on $B$ as*

$$\mathrm{H}^\epsilon_{\max}(A|B)_\omega = \inf_{\bar{\omega}_{AB} \in \mathcal{B}^\epsilon(\omega_{AB})} \mathrm{H}_{\max}(A|B)_{\bar{\omega}}\,. \tag{4.12}$$

Note that the non-smoothed min- and max-entropy are retrieved for $\epsilon = 0$. The ball $\mathcal{B}^\epsilon_{\mathcal{M}}(\cdot)$ is chosen in such a way that the smooth conditional min-entropy is unaffected by freedoms which could potentially stem from the non-uniqueness of purifications. This can be seen as the smooth analogue of Lemma 4.2.3, and is connected to the fact that the smooth min-entropy is independent under a projective embedding of the physical system into a larger one (see Section 3.4.

**Lemma 4.3.3.** *Let $\mathcal{M}_{AB} = \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{M}_B$ with $\mathcal{M}_B$ a von Neumann algebra, $\omega_{AB} \in \mathcal{S}_\leq(\mathcal{M}_{AB})$ and $\epsilon \geq 0$. Moreover, let $(\pi_1, \mathcal{K}_1, |\xi_1\rangle)$ and $(\pi_2, \mathcal{K}_2, |\xi_2\rangle)$ be two purifications of $\omega_{AB}$ with relevant system $\mathcal{M}_{A_i} = \pi_i(\mathcal{M}_A)$ and complementary systems $\mathcal{M}_{C_i}$ such that $\mathcal{M}_{A_i} \simeq \mathcal{B}(\mathcal{H}_{A_i})$. Then it follows that*

$$\mathrm{H}^\epsilon_{\min}(A_1|C_1)_{\omega^1} = \mathrm{H}^\epsilon_{\min}(A_2|C_2)_{\omega^2} \ , \tag{4.13}$$

*where $\omega^i_{A_iC_i}$ is the restricted state corresponding to $|\xi_i\rangle$.*

*Proof.* We use ideas from [TCR10] in which the analog for the finite-dimensional case was proven. First, we observe that due to the symmetry of equation (4.13), it is sufficient to show inequality in one direction. According to Lemma 3.2.2, we know that there exists a partial isometry $V : \mathcal{K}_1 \to \mathcal{K}_2$ with $|\xi_2\rangle = V|\xi_1\rangle$ and $V\pi_1(a) = \pi_2(a)V$ for all $a \in \mathcal{M}_{AB}$. Furthermore, we know from the proof of Lemma 4.2.3 that for all $\sigma_{A_1C_1} \in \mathcal{S}_\leq(\mathcal{M}_{A_1C_1})$ the subnormalized state $V\sigma_{A_1C_1}V^*(x) = \sigma_{A_1C_1}(V^*xV)$ on $\mathcal{M}_{A_2C_2}$ satisfies $\mathrm{H}_{\min}(A_1|C_1)_\sigma \leq \mathrm{H}_{\min}(A_2|C_2)_{V\sigma V^*}$ and $V\omega^1_{A_1C_1}V^* = \omega^2_{A_2C_2}$. Hence,

$$\begin{aligned}\mathrm{H}^\epsilon_{\min}(A_1|C_1)_{\omega^1} &= \sup_{\sigma_{A_1C_1} \in \mathcal{B}^\epsilon(\omega^1_{A_1C_1})} \mathrm{H}_{\min}(A_1|C_1)_\omega \\ &\leq \sup_{\sigma_{A_1C_1} \in \mathcal{B}^\epsilon(\omega^1_{A_1C_1})} \mathrm{H}_{\min}(A_2|C_2)_{V\sigma V^*} \ ,\end{aligned}$$

and the only thing which is left to prove is that $V\sigma_{A_1C_1}V^* \in \mathcal{B}^\epsilon(\omega^2_{A_2C_2})$ for all $\sigma_{A_1C_1} \in \mathcal{B}^\epsilon(\omega^1_{A_1C_1})$. But this is equivalent to show that

$$\mathcal{F}(\omega^1_{A_1C_1}, \sigma_{A_1C_1}) \leq \mathcal{F}(V\omega^1_{A_1C_1}V^*, V\sigma_{A_1C_1}V^*) \, .$$

Let $p = VV^*$ be the projector onto the image of $V$. Since $p\mathcal{M}_{A_2C_2}p$ is a von Neumann algebra and $V\omega_{A_1C_1}V^*, V\sigma_{A_1C_1}V^*$ have support projection $p$, we can use Definition 3.4.1 to compute

$$\begin{aligned}\mathcal{F}_{\mathcal{M}_{A_2C_2}}(V\omega^1_{A_1C_1}V^*, V\sigma_{A_1C_1}V^*) &= \mathcal{F}_{p\mathcal{M}_{A_2C_2}p}(V\omega^1_{A_1C_1}V^*, V\sigma_{A_1C_1}V^*) \\ &= \sup_{p\mathcal{M}_{A_2C_2}p \curvearrowright \hat{\mathcal{N}}} \sup_{\bar\omega, \bar\sigma} F_{\mathcal{N}}(\bar\omega, \bar\sigma) \\ &\geq F_{\hat{\mathcal{M}}_{A_1C_1}}(\hat\omega^1_{A_1C_1}, \hat\sigma_{A_1C_1}) \\ &= \mathcal{F}_{\mathcal{M}_{A_1C_1}}(\omega^1_{A_1C_1}, \sigma_{A_1C_1}) \, ,\end{aligned}$$

where $\hat{\mathcal{M}}_{A_1C_1}$, $\hat\omega^1_{A_1C_1}$ and $\hat\sigma_{A_1C_1}$ are as defined in Lemma 3.4.2. Note that the inequality follows from $p\mathcal{M}_{A_2C_2}p \curvearrowright \hat{\mathcal{M}}_{A_1C_1}$ via the isometry $V \oplus 1$ and the fact that $\hat\omega^1_{A_1C_1}, \hat\sigma_{A_1C_1}$ are valid extensions of $V\omega^1_{A_1C_1}V^*, V\sigma_{A_1C_1}V^*$. □

Next we show that the duality relation also holds for the smooth min- and max-entropies.

**Proposition 4.3.4.** *Let $\mathcal{M}_{AB} = \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{M}_B$ with $\mathcal{M}_B$ a von Neumann algebra, $\omega_{AB} \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$, $(\pi, \mathcal{K}, |\xi\rangle)$ an arbitrary purification of $\omega_{AB}$ with relevant system $\pi(\mathcal{M}_A) \simeq \mathcal{M}_A$ and complementary system $\mathcal{M}_C = \pi(\mathcal{M}_{AB})'$, and $\epsilon \geq 0$. Then it follows that*

$$\mathrm{H}^{\epsilon}_{\max}(A|B)_{\omega} = -\mathrm{H}^{\epsilon}_{\min}(A|C)_{\omega} \ . \tag{4.14}$$

*Proof.* The ideas for the proof are adapted from [TCR10]. Because of Lemma 4.3.3 we can assume that $\pi$ together with $\mathcal{K}$ is a standard form of $\mathcal{M}$ such that each state in $\mathcal{M}_{AB}$ admits a purification in $\mathcal{K}$. According to the definitions of the smooth entropies, we have to show that

$$\sup_{\sigma_{AB} \in \mathcal{B}^{\epsilon}(\omega_{AB})} \mathrm{H}_{\min}(A|C)_{|\xi_\sigma\rangle} = \sup_{\eta_{AC} \in \mathcal{B}^{\epsilon}(\omega_{AC})} \mathrm{H}_{\min}(A|C)_{\eta} \ , \tag{4.15}$$

where $|\xi_\sigma\rangle \in \mathcal{K}$ is a purification of $\sigma_{AB}$. From Lemma 4.2.3, we know that the min-entropy does not depend on the particular choice of the purification $|\xi_\sigma\rangle$. We can therefore choose $|\xi_\sigma\rangle$ such that $\mathcal{F}_{\mathcal{M}_{AB}}(\omega_{AB}, \sigma_{AB}) = \mathcal{F}_{\mathcal{B}(\mathcal{H})}(|\xi\rangle, |\xi_\sigma\rangle)$ and thus,

$$\mathcal{P}_{\mathcal{M}_{AB}}(\omega_{AB}, \sigma_{AB}) = \mathcal{P}_{\mathcal{B}(\mathcal{H})}(|\xi\rangle, |\xi_\sigma\rangle) \geq \mathcal{P}_{\mathcal{M}_{AC}}(|\xi\rangle, |\xi_\sigma\rangle) \ ,$$

from which '$\leq$ ' in (4.15) follows. In order to prove inequality in the other direction, we observe that there exists a von Neumann algebra $\mathcal{N} \subset \mathcal{B}(\tilde{\mathcal{K}})$ such that $\mathcal{M}_{ABC} \curvearrowright \mathcal{N}$ and each state $\eta_{AC}$ has a purification $\xi_\eta$ in $\tilde{\mathcal{K}}$.[5] Let $p$ be the projector such that $\mathcal{M}_{ABC}$ is isomorphic to $p\mathcal{N}p$ and identify $p\tilde{\mathcal{K}}$ with $\mathcal{K}$. Hence, we can find a purification $|\xi\rangle$ of $\omega_{AB}$ in $\tilde{\mathcal{K}}$ with $p|\xi\rangle = |\xi\rangle$. Moreover, we know that for all $\eta_{AC}$ exists a $|\xi_\eta\rangle \in \tilde{\mathcal{K}}$ with $\mathcal{P}_{\mathcal{M}_{AC}}(\eta_{AC}, \omega_{AC}) = \mathcal{P}_{\mathcal{B}(\tilde{\mathcal{K}})}(|\xi\rangle, |\xi_\eta\rangle)$. It therefore follows that

$$\begin{aligned}\sup_{\eta_{AC} \in \mathcal{B}^{\epsilon}(\omega_{AC})} \mathrm{H}_{\min}(A|C)_{\eta} &= \sup_{\||\chi\rangle\| \leq 1, \mathcal{P}_{\mathcal{B}(\tilde{\mathcal{K}})}(|\xi\rangle, |\chi\rangle) \leq \epsilon} \mathrm{H}_{\min}(A|C)_{|\chi\rangle} \\ &= \sup_{\||\chi\rangle\| \leq 1, \mathcal{P}_{\mathcal{B}(\tilde{\mathcal{K}})}(|\xi\rangle, |\chi\rangle) \leq \epsilon} \mathrm{H}_{\min}(A|C)_{p|\chi\rangle} \ ,\end{aligned}$$

where the last equality is due to $\mathcal{M}_{ABC} \cong p\mathcal{N}p$, and therefore $|\chi\rangle$ and $p|\chi\rangle$ induce the same states on $\mathcal{M}_{ABC}$. Since $\mathcal{P}_{\mathcal{B}(\tilde{\mathcal{K}})}(|\xi\rangle, |\chi\rangle) \geq \mathcal{P}_{\mathcal{M}_{AB}}(|\xi\rangle, |\chi\rangle)$ and each $\eta_{AB}$ admits a purification in $\mathcal{K}$, we find '$\geq$ ' in (4.15). □

## 4.4. Smooth Min- and Max-Entropies of Classical-Quantum States

As discussed in Section 3.3, we model a classical-quantum system with classical degrees of freedom described by a countable set $X$ correlated with an arbitrary

[5] We can choose the standard form to be $\mathcal{K} = \mathcal{H}_X^{\otimes 2} \otimes \mathcal{H}_B^{\phi}$ with $\mathcal{H}_B^{\phi}$, $\mathcal{M}_B^{\phi}$ a standard form of $\mathcal{M}_B$ and $\mathcal{H}_X^{\otimes 2} = \mathcal{H}_X \otimes \mathcal{H}_X$. We then have that the complementary system is $\mathcal{M}_C = \mathcal{H}_X \otimes (\mathcal{M}_B^{\phi})'$. Hence, we can choose $\tilde{\mathcal{K}} = \mathcal{H}_X^{\otimes 4} \otimes \mathcal{H}_B^{\phi}$ and $\mathcal{N} = \mathcal{B}(\mathcal{H}_X^{\otimes 4}) \otimes \mathcal{M}_B^{\phi} \vee (\mathcal{M}_B^{\phi})'$.

system $\mathcal{M}_B$ by the von Neumann algebra $\ell^\infty(X) \otimes \mathcal{M}_B$.[6] Let us denote by $\mathcal{H}_X$ a Hilbert space spanned by a orthonormal basis $\{|x\rangle\}_{x\in X}$. We can then embed $\ell^\infty(X) \otimes \mathcal{M}_B$ into $\mathcal{B}(\mathcal{H}_X) \otimes \mathcal{M}_B$ in such a way that a state $\omega_{XB} = (\omega_B^x)$ can be identified by

$$\omega_{XB} = \sum_x e_x \otimes \omega_B^x \tag{4.16}$$

where $e_x$ is the pure state corresponding to the density matrix $|x\rangle\langle x|$ (see Section 3.3). The state $\omega_{XB}$ can therefore be seen as a state on $\mathcal{B}(\mathcal{H}_X) \otimes \mathcal{M}_B$ and Definitions 4.2.1, 4.2.2 and 4.3.2 of the non-smooth and smooth min- and max-entropies apply.

Using this embedding and Definition 4.3.2 of the smooth min- and max-entropy, we optimize the min- and max-entropy over states in $\mathcal{S}(\mathcal{B}(\mathcal{H}_X) \otimes \mathcal{M}_B)$ which are $\epsilon$-close to $\omega_{XB}$. This includes states which are not in $\mathcal{S}_\leq(\ell^\infty(X) \otimes \mathcal{M}_B)$ and are therefore not conform with the considered system. But as shown in the following, there exists always a classical quantum state which attains the optimum in the definitions of the smooth min- and max-entropy. Hence, the smoothing formalism is compatible with the embedding of a classical system $\ell(X) \otimes \mathcal{M}_B$ into the quantum system $\mathcal{B}(\mathcal{H}_X) \otimes \mathcal{M}_B$.

**Lemma 4.4.1.** *Let $\mathcal{M}_B$ be a von Neumann algebras, $X$ a countable set, and $\omega_{XB} \in \mathcal{S}_\leq(\ell^\infty(X) \otimes \mathcal{M}_B)$. Then, it holds that*

$$\begin{aligned} \mathrm{H}_{\min}^\epsilon(X|B)_\omega &= \sup_{\bar\omega_{XB}\in\mathcal{B}_{\mathrm{cq}}^\epsilon(\omega_{XB})} \mathrm{H}_{\min}(X|B)_{\bar\omega} \\ \mathrm{H}_{\max}^\epsilon(X|B)_\omega &= \inf_{\bar\omega_{XB}\in\mathcal{B}_{\mathrm{cq}}^\epsilon(\omega_{XB})} \mathrm{H}_{\max}(X|B)_{\bar\omega} \ , \end{aligned}$$

*where $\mathcal{B}_{\mathrm{cq}}^\epsilon(\omega_{XB}) := \{\sigma_{XB} \in \mathcal{S}_\leq(\ell^\infty(X) \otimes \mathcal{M}_B) |\, \mathcal{P}(\omega_{XB}, \sigma_{XB}) \leq \epsilon\}$.*

*Proof.* The proof can be carried over from the finite-dimensional case, where it was discussed in [Ren05, Remark 3.2.4] for the min-entropy, and in [RR12, Lemma 3] for the max-entropy. For the sake of completeness, we sketch the idea. Let $\mathcal{H}_X$ be the closure of the span of the orthonormal bases $\{|x\rangle\}_{x\in X}$ and let $\mathcal{E} : \ell^\infty(X) \to \mathcal{B}(\mathcal{H}_X)$ be the quantum channel which embeds $\ell^\infty(X)$ into the diagonal algebra with respect to this basis. For an arbitrary $\bar\omega_{XB} \in \mathcal{B}_{M_{|X|}\otimes\mathcal{M}_B}^\epsilon(\omega_{XB})$, it then follows from equation (3.11) that $\mathcal{E} \otimes \mathrm{id}(\bar\omega_{XB}) \in \mathcal{B}_{\mathrm{cq}}^\epsilon(\omega_{XB})$, and a straightforward calculation shows that $\mathrm{H}_{\min}(X|B)_{\bar\omega} \leq \mathrm{H}_{\min}(X|B)_{\mathcal{E}\otimes\mathrm{id}(\bar\omega)}$. This proves the part for the min-entropy.

For the max-entropy, we take a purification $\{|\xi\rangle, \pi, \mathcal{H}\}$ of $\bar\omega_{XB}$ on a Hilbert space $\mathcal{H} = \mathcal{H}_X^{\otimes 2} \otimes \mathcal{H}_B$, where $\mathcal{M}_B$ acts on $\mathcal{H}_B$ and the complementary system of $\mathcal{M}_{XB}$ is given by $\mathcal{M}_{X'C} = \mathcal{B}(\mathcal{H}_X) \otimes \pi(\mathcal{M}_B)$. By the duality between the min- and max-entropy, it is sufficient to show that $\mathrm{H}_{\min}(X|X'C)_{\bar\omega} \leq \mathrm{H}_{\min}(X|X'C)_{\mathcal{E}_{XX'}\otimes\mathrm{id}(\bar\omega)}$ for $\mathcal{E}_{XX'}$ the projection onto the subspace given by $P^{XX'} = \sum_{x\in X} |x\rangle\langle x| \otimes |x\rangle\langle x|$, while the cq-state given by the restriction of $\mathcal{E}_{XX'} \otimes \mathrm{id}(\bar\omega_{XBC})$ onto $\mathcal{M}_{XB}$ is still in $\mathcal{B}_{M_{|X|}\otimes\mathcal{M}_B}^\epsilon(\omega_{XB})$. But this follows in complete analogy to [RR12, Lemma 3]. □

[6] Note that since $\mathcal{M}_B$ is an arbitrary von Neumann algebra it can also be an abelian one describing a classical system.

In the following we indicate classical systems by capital letters $X$, $Y$ and $Z$ in contrast to quantum systems $A$, $B$ and $C$. But this notation can lead to some ambiguity. Consider the max-entropy of a classical quantum state $\omega_{XB}$ defined via its purification which can be without loss of generality chosen to be a vector state in the Hilbert space $\mathcal{H}_X \otimes \mathcal{H}_{X'} \otimes \mathcal{H}_B \otimes \mathcal{H}_{B'}$ where $\mathcal{H}_{X'}$ ($\mathcal{H}_{B'}$) is isomorphic to $\mathcal{H}_X$ ($\mathcal{H}_B$) and $\mathcal{H}_B$ is the Hilbert space of a standard form of $\mathcal{M}_B$. Denoting the purification by $\omega_{XX'BB'}$, we can write $\mathrm{H}_{\max}(X|B)_\omega = \mathrm{H}_{\min}(X|X'B')_\omega$. But by a simple calculation one can convince oneself that the state $\omega_{XX'B'}$ is in general not a classical quantum state on $\mathcal{B}(\mathcal{H}_X) \otimes \mathcal{M}_{X'B'}$ and cannot be written as a sequence $(\omega_{X'B'})_{x \in X}$. Hence, in spite of $\mathrm{H}_{\max}(X|B)_\omega$ being the entropy of a classical quantum state, $\mathrm{H}_{\min}(X|X'B')_\omega$ is not.

## 4.5. Properties of Smooth Min- and Max-Entropies

This section is aimed to list the most important properties of the smooth and non-smooth min- and max-entropies which are needed in the proceeding chapters. Note that all the properties which hold for the smooth min- and max-entropies also hold for the non-smoothed ones, by setting the smoothing parameter $\epsilon = 0$. Most of the results were first proven in the context of finite-dimensional Hilbert spaces. For a more comprehensive discussion of properties of the smooth min- and max-entropy in the finite-dimensional setting we refer to [Tom12].

### 4.5.1. Data Processing Inequality

An important property of the smooth min- and max-entropy is, that local operations on the conditional system $B$ can never decrease the uncertainty about the system $A$. This is called the data processing inequality, and is shown for the finite-dimensional case in [TCR10].

**Proposition 4.5.1.** *Let $\mathcal{M}_A \simeq \mathcal{B}(\mathcal{H}_A)$, $M_B$ and $M_C$ von Neumann algebras, $\omega_{AB} \in \mathcal{S}_\leq(\mathcal{M}_{AB})$, $\mathcal{E} : \mathcal{M}_C \to \mathcal{M}_B$ a quantum channel, and $\epsilon \geq 0$. Then, it follows that*

$$\mathrm{H}^\epsilon_{\min}(A|B)_\omega \leq \mathrm{H}^\epsilon_{\min}(A|C)_{\mathrm{id}_A \otimes \mathcal{E}_*(\omega)} \tag{4.17}$$

$$\mathrm{H}^\epsilon_{\max}(A|B)_\omega \leq \mathrm{H}^\epsilon_{\max}(A|C)_{\mathrm{id}_A \otimes \mathcal{E}_*(\omega)} \ . \tag{4.18}$$

*Proof.* The proof is based on the same ideas as the one for finite-dimensional Hilbert spaces [TCR10]. We first consider the case for the conditional min-entropy for $\epsilon = 0$. Because $\mathcal{E}$ is completely positive, we have that $\omega_{AB} \leq \tau_A \otimes \sigma_B$ implies $\mathrm{id}_A \otimes \mathcal{E}_*(\omega_{AB}) \leq \tau_A \otimes \mathcal{E}_*(\sigma_B)$. Furthermore, since $\mathcal{E}$ is unital, we find that $\mathcal{E}_*(\sigma_B) \in \mathcal{S}_\leq(\mathcal{M}_C)$ whenever $\sigma_B \in \mathcal{S}_\leq(\mathcal{M}_C)$. Together with the definition of the conditional min-entropy, the inequality follows. For $\epsilon > 0$, the inequality follows straightforwardly by using the fact that the purified distance is monotonically decreasing under quantum channels (3.11). Now we lift the property from the smooth conditional min- to the smooth conditional max-entropy via the duality. For that we take a purification $(\mathcal{H}, \pi, |\xi\rangle)$ of $\omega_{AB}$ on $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_{A'} \otimes \mathcal{H}_B$ with $\mathcal{H}_{A'}$ isomorphic to $\mathcal{H}_A$ such that $\pi(\mathcal{M}_A) = \mathcal{B}(\mathcal{H}_A)$ and $\pi(\mathcal{M}_B) \subset \mathcal{B}(\mathcal{H}_B)$. We remark that the concatenation $\hat{\mathcal{E}} = \pi \circ \mathcal{E}$ is a completely positive, unital map from $\mathcal{M}_C$ onto $\pi(\mathcal{M}_B)$. Due to

Stinespring's dilation theorem [Pau02], there exists a Hilbert space $\mathcal{H}_C = \mathcal{H}_R \oplus \mathcal{H}_B$, a representation $\pi_{\mathcal{E}}$ of $\mathcal{M}_C$ on $\mathcal{H}_C$, and an isometry $V : \mathcal{H}_B \to \mathcal{H}_C$ such that $\hat{\mathcal{E}}(a) = V^* \pi_{\mathcal{E}}(a) V$ for all $a \in \mathcal{M}_C$. Hence, for all $y \in \mathcal{M}_{AC}$

$$[\mathrm{id}_A \otimes \mathcal{E}_*(\omega_{AB})](y) = \omega_{AB}(\mathrm{id}_A \otimes \mathcal{E}(y)) = \langle \xi \,|(\mathbb{1}_{AA'} \otimes V^*)(\mathrm{id}_A \otimes \pi_{\mathcal{E}})(y)(\mathbb{1}_{AA'} \otimes V)\xi \rangle \,,$$

which implies that $(\mathcal{H}, \pi_{\mathcal{E}}, \mathbb{1}_{AA'} \otimes V|\xi\rangle)$ is a purification of $\mathrm{id}_A \otimes \mathcal{E}_*(\omega_{AB})$. If we denote $\mathcal{M}_{B'} = \pi(\mathcal{M}_B)'$, $\mathcal{M}_{C'} = \pi_{\mathcal{E}}(\mathcal{M}_C)$ and $\mathcal{M}_{V(C')} = V^* \pi_{\mathcal{E}}(\mathcal{M}_C)' V$, we obtain from $V^* \pi_{\mathcal{E}}(\mathcal{M}_C) V \subset \mathcal{M}_B$ that $\mathcal{M}_{B'} \subset \mathcal{M}_{V(C')}$. Because the map $x \to V^* x V$ from $\mathcal{M}_{C'}$ into $V(\mathcal{M}_{C'})$ is unital and completely positive, the restriction on a subalgebra is a quantum channel and $\mathbb{1} \otimes V^* V|\xi\rangle = |\xi\rangle$, we obtain via the duality

$$\begin{aligned} \mathrm{H}^{\epsilon}_{\max}(A|C)_{\mathrm{id}_A \otimes \mathcal{E}_*(\omega)} &= -\mathrm{H}^{\epsilon}_{\min}\left(A|A'C'\right)_{\mathbb{1} \otimes V|\xi\rangle} \geq \mathrm{H}^{\epsilon}_{\min}\left(A|A'V(C')\right)_{|\xi\rangle} \\ &\geq -\mathrm{H}^{\epsilon}_{\min}\left(A|A'B'\right)_{|\xi\rangle} = \mathrm{H}^{\epsilon}_{\max}(A|B)_{\omega} \,. \end{aligned}$$

□

A special case of the data processing inequality is obtained if one considers restrictions onto subsystems. In particular, for von Neumann algebras $\mathcal{M}_C \subset \mathcal{M}_B$ the inequality yields $\mathrm{H}^{\epsilon}_{\min}(A|B)_{\omega} \leq \mathrm{H}^{\epsilon}_{\min}(A|C)_{\omega}$, as well as $\mathrm{H}^{\epsilon}_{\max}(A|B)_{\omega} \leq \mathrm{H}^{\epsilon}_{\max}(A|C)_{\omega}$. Hence, we get the chain of inequalities

$$\mathrm{H}^{\epsilon}_{\min}(A)_{\omega} \geq \mathrm{H}^{\epsilon}_{\min}(A|B)_{\omega} \geq \mathrm{H}^{\epsilon}_{\min}(A|BC)_{\omega} = -\mathrm{H}^{\epsilon}_{\max}(A)_{\omega} \,,$$

for $\omega_{ABC}$ being a purification of $\omega_{AB} \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$. The same applies to the max-entropy and we find that

$$\mathrm{H}^{\epsilon}_{\max}(A)_{\omega} \geq \mathrm{H}^{\epsilon}_{\max}(A|B)_{\omega} \geq -\mathrm{H}^{\epsilon}_{\min}(A)_{\omega} \,.$$

Recall that the non-smooth unconditional min-entropy $\mathrm{H}_{\min}(A)_{\omega}$ corresponds to the quantum $\infty$-Rényi entropy, that is, if $\rho_{\omega}$ is the corresponding density matrix of $\omega$, then $\mathrm{H}_{\min}(A)_{\omega} = -\log \|\rho_{\omega}\|$. The non-smooth max-entropy is given by the quantum 1/2-Rényi entropy $\mathrm{H}_{\max}(A)_{\omega} = 2 \log \mathrm{Tr} \rho^{\frac{1}{2}}$. Hence, we can conclude that for $\epsilon > 0$ the smooth entropies are always finite. This is due to the fact that we can always find a state $\bar{\omega}$ with finite-dimensional support projection which is $\epsilon$ close in the purified distance to $\omega$, and for such a state the max-entropy is finite.[7] This is not true for $\epsilon = 0$, because density matrices $\rho$ exist for which $\mathrm{Tr} \rho^{\frac{1}{2}}$ is infinite.

### 4.5.2. Finite-Dimensional Approximation for Type I Factors

Let us consider the case where $\mathcal{M}_{AB} = \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{B}(\mathcal{H}_B)$ with $\mathcal{H}_A$ and $\mathcal{H}_B$ separable Hilbert spaces. A convenient way to transport properties from finite-dimensional to infinite-dimensional Hilbert spaces is by using finite-dimensional approximations. Such a tool was developed in [FAR11] for the min- and max-entropies. Since we consider the full algebra of bounded operators on a Hilbert space, we can work with density matrices $\rho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$.

[7] Note that the unconditional min-entropy is always finite.

**Theorem 4.5.2.** *Let $(P_k^A)_k \subset \mathcal{B}(\mathcal{H}_A)$ and $(P_k^B)_k \subset \mathcal{B}(\mathcal{H}_B)$ be two sequences of projectors which converge in the weak operator topology to the identity, and set $P_k = P_k^A \otimes P_k^B$. For any density matrix $\rho \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ holds that*

$$\mathrm{H}_{\min}(A|B)_\rho = \lim_{k\to\infty} \mathrm{H}_{\min}(A|B)_{P_k\rho P_k} \tag{4.19}$$

$$\mathrm{H}_{\max}(A|B)_\rho = \lim_{k\to\infty} \mathrm{H}_{\max}(A|B)_{P_k\rho P_k}\,. \tag{4.20}$$

For a prove of this result and further details we refer to [FAR11].

### 4.5.3. The Quantum Asymptotic Equipartition Property

As discussed in Section 1.3 the von Neumann entropy characterizes most of the quantum and classical information theoretic tasks in the asymptotic limit. We thus want that in this limit the smooth min- and max-entropy approach the von Neumann entropy. Recall that the asymptotic limit is the error free case in the limit of infinite repetition of an i.i.d. resource. Hence, we expect that the limit $n \to \infty$ followed by the limit $\epsilon \to 0$ of $\frac{1}{n}\mathrm{H}^\epsilon_{\min}(\mathrm{A}^\mathrm{n}|\mathrm{B}^\mathrm{n})_{\omega^{\otimes \mathrm{n}}}$ and $\frac{1}{n}\mathrm{H}^\epsilon_{\max}(\mathrm{A}^\mathrm{n}|\mathrm{B}^\mathrm{n})_{\omega^{\otimes \mathrm{n}}}$ is equal to $H(A|B)_\omega$. This was shown for classical and finite-dimensional systems in [Ren05, TCR09] and shows a necessary property expected from a one-shot counterpart of the von Neumann entropy. We address now the question if this can be extended to an infinite-dimensional setting and find under an affirmative answer under certain constraints. For a more general case, we find only inequality in one direction, but which nevertheless, turns out to be the relevant for applications in quantum key distribution (c.f. Section 6.3.2).

In the following we do not consider general von Neumann algebras but restrict ourselves to the case where the systems are type I factors $\mathcal{M}_{AB} = \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{B}(\mathcal{H}_B)$. This allows us to work unambiguously with density matrices. The conditional von Neumann entropy is now defined via the relative entropy [Kle31, Lin73, Lin74, HS10], given for $\rho, \sigma \in \mathcal{S}_{\leq}(\mathcal{H})$ as

$$\mathrm{H}(\rho\|\sigma) := \sum_{jk} |\langle a_j|b_k\rangle|^2 (a_j \log a_j - a_j \log b_k + b_k - a_j)\,, \tag{4.21}$$

where $\{|a_j\rangle\}_j$ is an arbitrary orthonormal eigenbasis of $\rho$ with corresponding eigenvalues $a_j$, and analogously for $\{|b_k\rangle\}_k$, $b_k$, and $\sigma$. The relative entropy is always positive, possibly $+\infty$, and equal to 0 if and only if $\rho = \sigma$ [Lin73]. For states $\rho_{AB}$ with $H(A)_\rho < +\infty$, the conditional von Neumann entropy is defined to be [Kuz11]

$$\mathrm{H}(A|B)_\rho := \mathrm{H}(A)_\rho - \mathrm{H}(\rho_{AB}\|\rho_A \otimes \rho_B). \tag{4.22}$$

Note that under the same conditions as in Theorem 4.5.2, the conditional von Neumann entropy can similarly be approximated by means of finite-dimensional truncations [Kuz11]. In particular, for any density operator $\rho_{AB} \in \mathcal{S}(H_A \otimes H_B)$ satisfying $\mathrm{H}(A)_\rho < \infty$ holds that

$$\lim_{k\to\infty} \mathrm{H}(A|B)_{P_k\rho P_k} = \mathrm{H}(A|B) \tag{4.23}$$

for any sequence of projectors of the form $P_k = P_k^A \otimes P_k^B$ converging in the weak operator topology to the identity. Using this result the ordering

$$\mathrm{H}_{\min}\left(A|B\right)_\rho \leq \mathrm{H}(A|B)_\rho \leq \mathrm{H}_{\max}\left(A|B\right)_\rho \tag{4.24}$$

follows directly from the finite-dimensional case [TCR09].

**Theorem 4.5.3.** *Let $\rho \in \mathcal{S}_\leq(\mathcal{H}_A \otimes \mathcal{H}_B)$ be such that $\mathrm{H}(A)_\rho < \infty$. For any $\epsilon > 0$, it follows that*

$$\frac{1}{n}\mathrm{H}^\epsilon_{\min}(A^n|B^n)_{\rho^{\otimes n}} \geq \mathrm{H}(A|B)_\rho - \frac{1}{\sqrt{n}} 4\log(\eta)\sqrt{\log\frac{2}{\epsilon^2}}\,, \tag{4.25}$$

*and*

$$\frac{1}{n}\mathrm{H}^\epsilon_{\max}(A^n|B^n)_{\rho^{\otimes n}} \leq \mathrm{H}(A|B)_\rho + \frac{1}{\sqrt{n}} 4\log(\eta)\sqrt{\log\frac{2}{\epsilon^2}}. \tag{4.26}$$

*for $n \geq (8/5)\log(2/\epsilon^2)$, and $\eta = 2^{-\frac{1}{2}\mathrm{H}_{\min}(A|B)_\rho} + 2^{\frac{1}{2}\mathrm{H}_{\max}(A|B)_\rho} + 1$. Here $A^n$ and $B^n$ denotes the $n$-fold copy of the $A$ and $B$ system.*

Let us fix some notation before we prove Theorem 4.5.3. In all what follows $\{P_k^A\}$ and $\{P_k^B\}$ denote sequences of projectors which converge in the weak operator topology to the identity. Note that this also implies that $(P_k^A)^{\otimes n}$ and $(P_k^B)^{\otimes n}$ converge weakly operator to the identity. For any state $\rho_{AB} \in \mathcal{S}(\mathcal{H}_{AB})$ we define the normalized sequence of states

$$\hat{\rho}^k_{AB} := \frac{1}{q_k} P_k^A \otimes P_k^B \rho_{AB} P_k^A \otimes P_k^B\,, \tag{4.27}$$

where $q_k = \mathrm{Tr}(P_k^A \otimes P_k^B \rho_{AB} P_k^A \otimes P_k^B)$. As shown in [FAR11], the approximation as given in Theorem 4.5.2 also holds for the sequence $\hat{\rho}^k_{AB}$. We need the following Lemma to prove Theorem 4.5.3.

**Lemma 4.5.4.** *Let $\rho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and $\hat{\rho}^k_{AB}$ as defined in Equation (4.27). For any fixed $1 > t > 0$, there exists a $k_0 \in \mathbb{N}$ such that*

$$\mathrm{H}^\epsilon_{\min}\left(A|B\right)_\rho \geq \mathrm{H}^{t\epsilon}_{\min}(A|B)_{\hat{\rho}^k}, \quad \forall k \geq k_0. \tag{4.28}$$

*Proof.* In the following let $t \in (0,1)$ be fixed. According to the definition of the smooth min-entropy in Equation (4.11), it is enough to show that $\mathcal{B}^{t\epsilon}(\hat{\rho}^k_{AB}) \subseteq \mathcal{B}^\epsilon(\rho_{AB})$ for all $k \geq k_0$. Note that the purified distance is compatible with trace norm convergence, i.e., $\|\rho_{AB} - \hat{\rho}^k_{AB}\|_1 \to 0$ implies that $P(\hat{\rho}^k_{AB}, \rho_{AB}) \to 0$. Hence, there exists a $k_0$ such that $P(\hat{\rho}^k_{AB}, \rho_{AB}) < (1-t)\epsilon$ for all $k \geq k_0$. For $k \geq k_0$ and $\tilde{\rho}_{AB} \in \mathcal{B}^{t\epsilon}(\hat{\rho}^k_{AB})$, we therefore find $P(\tilde{\rho}_{AB}, \rho_{AB}) \leq P(\tilde{\rho}_{AB}, \hat{\rho}^k_{AB}) + P(\hat{\rho}^k_{AB}, \rho_{AB}) < \epsilon$, such that $\tilde{\rho}_{AB} \in \mathcal{B}^\epsilon(\rho_{AB})$. □

*Proof. (Theorem 4.5.3)* Let $\hat{\rho}^k_{AB}$ be again defined as in Equation (4.27). If we fix $1 > t > 0$ and $n \in \mathbb{N}$, it follows by Lemma 4.5.4 that we can find a $k_0 \in \mathbb{N}$ such that $\mathrm{H}^\epsilon_{\min}(A^n|B^n)_{\rho^{\otimes n}} \geq \mathrm{H}^\epsilon_{\min}(A^n|B^n)_{(\hat{\rho}^k)^{\otimes n}}$ for every $k \geq k_0$. Since Equation (4.25) is

valid for the finite-dimensional case [TCR09], we can apply it to $\mathrm{H}^{\epsilon}_{\min}(A^n|B^n)_{(\hat{\rho}^k)^{\otimes n}}$ to obtain

$$\frac{1}{n}\mathrm{H}^{\epsilon}_{\min}(A^n|B^n)_{(\hat{\rho}^k)^{\otimes n}} \geq H(A|B)_{\hat{\rho}^k} - \frac{1}{\sqrt{n}} 4\log(\eta_k)\sqrt{\log\frac{2}{(t\epsilon)^2}}$$

for any $n \geq (8/5)\log(2/(t\epsilon)^2)$, and $\eta_k = 2^{-\frac{1}{2}\mathrm{H}_{\min}(A|B)_{\hat{\rho}^k}} + 2^{\frac{1}{2}\mathrm{H}_{\max}(A|B)_{\hat{\rho}^k}} + 1$. Hence, we find that

$$\frac{1}{n}\mathrm{H}^{\epsilon}_{\min}(A^n|B^n)_{\rho^{\otimes n}} \geq H(A|B)_{\hat{\rho}^k} - \frac{1}{\sqrt{n}} 4\log(\eta_k)\sqrt{\log\frac{2}{(t\epsilon)^2}} \tag{4.29}$$

for all $k \geq k_0$. Since the left hand side of Equation (4.29) is independent of $k$ we can use (4.23) and Proposition 4.5.2, to find

$$\begin{aligned}\frac{1}{n}\mathrm{H}^{\epsilon}_{\min}(A^n|B^n)_{\rho^{\otimes n}} &\geq \lim_{k\to\infty}\left\{\mathrm{H}(A|B)_{\hat{\rho}^k} - \frac{1}{\sqrt{n}} 4\log(\eta_k)\sqrt{\log\frac{2}{(t\epsilon)^2}}\right\} \\ &= \mathrm{H}(A|B)_{\rho} - \frac{1}{\sqrt{n}} 4\log(\eta)\sqrt{\log\frac{2}{(t\epsilon)^2}}\ .\end{aligned}$$

We finally take the limit $t \to 1$ in the above inequality, as well as in the condition $n \geq (8/5)\log(2/(t\epsilon)^2)$ to obtain the first part of the proposition.

For the second part we use the duality of the conditional von Neumann entropy, i.e., $\mathrm{H}(A|B)_\rho = -\mathrm{H}(A|C)_\rho$ for a purification $\rho_{ABC}$ [Kuz11]. This, together with the duality relation for smooth min- and max-entropy (4.14) yields (4.26). □

If the Hilbert space $\mathcal{H}_A$ of the first system is finite-dimensional, we obtain the whole quantum asymptotic equipartition property for the min- and max-entropy.

**Corollary 4.5.5.** *Let $\mathcal{H}_A$ be a finite-dimensional and $\mathcal{H}_B$ a separable Hilbert space. Then, for any density operator $\rho_{AB} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B)$ follows that*

$$\lim_{\epsilon\to 0}\lim_{n\to\infty}\frac{1}{n}\mathrm{H}^{\epsilon}_{\min}(A^n|B^n)_{\rho^{\otimes n}} = \mathrm{H}(A|B)_\rho \tag{4.30}$$

*and*

$$\lim_{\epsilon\to 0}\lim_{n\to\infty}\frac{1}{n}\mathrm{H}^{\epsilon}_{\max}(A^n|B^n)_{\rho^{\otimes n}} = \mathrm{H}(A|B)_\rho\ . \tag{4.31}$$

This statement follows simply from a continuity argument for the conditional von Neumann entropy.

*Proof.* Let $\epsilon > 0$ be sufficiently small, $\hat{\rho}^k_{AB}$ be defined as in Equation (4.27) and $\sigma_{AB} \in \mathcal{B}^{\epsilon}(\rho_{AB})$. Furthermore, we set $\sigma^k_{AB} = P^A_k \otimes P^B_k \sigma_{AB} P^A_k \otimes P^B_k$ and $\hat{\sigma}^k_{AB} = (1/\mathrm{Tr}\sigma^k_{AB})\sigma^k_{AB}$. By using $\mathrm{H}_{\min}(A|B)_{\sigma^k} = H_{\min}(A|B)_{\hat{\sigma}^k} + \log\mathrm{Tr}\sigma^k_{AB}$ and the relation (4.24), we find $\mathrm{H}_{\min}(A|B)_{\sigma^k} \leq \mathrm{H}(A|B)_{\hat{\sigma}^k}$. Since $\mathrm{H}(A|B)_{\hat{\sigma}^k}$ is effectively finite-dimensional, we can use Fannes' inequality [AF04] to obtain (for $k$ sufficiently large) $\mathrm{H}(A|B)_{\hat{\sigma}^k} \leq \mathrm{H}(A|B)_{\hat{\rho}^k} + 4\Delta_k \log d_A + 4H_{\mathrm{bin}}(\Delta_k)$, with $d_A = \dim(H_A)$, $\Delta_k = \|\hat{\rho}^k_{AB} - \hat{\sigma}^k_{AB}\|_1$, and $H_{\mathrm{bin}}(t) = -t\log t - (1-t)\log(1-t)$. Due to the general

relation $\|\rho-\sigma\|_1 \leq 2P(\rho,\sigma)$ (see Lemma 6 in [TCR10]), we have $\|\rho_{AB}-\sigma_{AB}\|_1 \leq 2\epsilon$ for all $\sigma_{AB} \in \mathcal{B}^\epsilon(\rho_{AB})$, which yields $\lim_{k\to\infty}\Delta_k = \|\rho_{AB}-\hat{\sigma}_{AB}\|_1 \leq 4\epsilon$, where $\hat{\sigma}_{AB} = \sigma_{AB}/\mathrm{Tr}(\sigma_{AB})$. Combined with (4.23) this leads to

$$\mathrm{H}^\epsilon_{\min}(A|B)_\rho = \sup_{\sigma_{AB}\in\mathcal{B}^\epsilon(\rho_{AB})} \lim_{k\to\infty} \mathrm{H}_{\min}(A|B)_{\sigma^k} \tag{4.32}$$

$$\leq H(A|B)_\rho + 16\epsilon\log d_A + 4H_{\mathrm{bin}}(4\epsilon) \tag{4.33}$$

Applied to an n-fold tensor product we thus obtain

$$\frac{1}{n}H^\epsilon_{\min}(\rho_{AB}^{\otimes n}|B^n) \leq H(\rho_{AB}|B) + 16\epsilon\log d_A + \frac{4}{n}H_{\mathrm{bin}}(4\epsilon)\,. \tag{4.34}$$

Equation (4.30) follows by combining (4.34) with the lower bound in (4.25), taking the limits $n\to\infty$ and $\epsilon\to 0$. Equation (4.31) follows directly by the duality of the conditional von Neumann entropy [Kuz11] together with the duality of the smooth min- and max-entropy (4.14). □

### 4.5.4. Chain Rules and Bounds for Smooth Entropies

The following properties are needed in Section 4.9 and 6.2.2. We start with a simple chain rule for the smooth min-entropy.

**Lemma 4.5.6.** *Let $\mathcal{M}_{ABC} = \mathcal{B}(\mathcal{H}_A)\otimes\mathcal{B}(\mathcal{H}_B)\otimes\mathcal{M}_C$ with $\mathcal{M}_C$ a general von Neumann algebra and $\dim\mathcal{H}_B = n$ finite, and $\omega_{ABC}\in\mathcal{S}(\mathcal{M}_{ABC})$. Then it follows that*

$$\mathrm{H}^\epsilon_{\min}(AB|C)_\omega \leq \mathrm{H}^\epsilon_{\min}(A|BC)_\omega + \log(n)\ .$$

For the sake of completeness we give a proof of the statement, although it is similar to the one in the finite-dimensional case [RR12, Lemma 5].

*Proof.* For any $\delta_1>0$, there exists $\bar{\omega}_{ABC}\in\mathcal{B}^\epsilon(\omega_{ABC})$ such that $\mathrm{H}^\epsilon_{\min}(AB|C)_\omega \leq \mathrm{H}_{\min}(AB|C)_{\bar{\omega}} + \delta_1$, and for any $\delta_2>0$, there exists $\sigma_C\in\mathcal{S}(\mathcal{M}_C)$ such that $\mathrm{H}_{\min}(AB|C)_{\bar{\omega}} \leq -D_{\max}(\omega_{ABC}\|\tau_{AB}\otimes\sigma_C)$, where $\tau_{AB}$ denotes the trace on $M_m\otimes M_n$. Now we calculate

$$\begin{aligned}
\mathrm{H}^\epsilon_{\min}(A|BC)_\omega + \log(n) &\geq \mathrm{H}_{\min}(A|BC)_{\bar{\omega}} + \log(n)\\
&\geq -D_{\max}(\bar{\omega}_{ABC}\|\tau_A\otimes\frac{\tau_B}{n}\otimes\sigma_C) + \log(n)\\
&= -D_{\max}(\bar{\omega}_{ABC}\|\tau_{AB}\otimes\sigma_C) \geq \mathrm{H}_{\min}(AB|C)_{\bar{\omega}} - \delta_2\\
&\geq \mathrm{H}^\epsilon_{\min}(AB|C)_\omega - \delta_1 - \delta_2\ ,
\end{aligned}$$

and since that holds for any $\delta_1,\delta_2>0$, the claim follows. □

Next we show that discarding classical information can only decrease the min-entropy.

**Lemma 4.5.7.** *Let $\mathcal{M}_{AXB} = \mathcal{B}(\mathcal{H}_A)\otimes\ell^\infty(X)\otimes\mathcal{M}_B$ with $\mathcal{M}_B$ a general von Neumann algebra, $X$ a set of finite cardinality $|X|$, and $\omega_{AXB}\in\mathcal{S}_\leq(\mathcal{M}_{AXB})$. Then it follows that*

$$\mathrm{H}^\epsilon_{\min}(AX|B)_\omega \geq \mathrm{H}^\epsilon_{\min}(A|B)_\omega\ . \tag{4.35}$$

*Proof.* For $\epsilon = 0$, the proof from [Ren05, Lemma 3.1.9] is also valid for von Neumann algebras. For $\epsilon > 0$, we proceed as follows. For all $\delta > 0$, there exists a cq-state $\bar{\omega}_{AB} \in \mathcal{B}^\epsilon(\omega_{XB})$ such that $\mathrm{H}^\epsilon_{\min}(A|B)_\omega \leq \mathrm{H}_{\min}(A|B)_{\bar{\omega}} + \delta$. We then take a purification $(\mathcal{H}, \pi, |\xi\rangle)$ of $\omega_{AXB}$ such that there exists also a purification $(\mathcal{H}, \pi, |\eta\rangle)$ of $\bar{\omega}_{AB}$ in $\mathcal{H}$. Now, by the definition of the purified distance (Definition 3.4.3), we can even find a purification $|\eta\rangle$ of $\bar{\omega}_{AB}$ such that $\mathcal{P}_{\mathcal{M}_{AB}}(\omega_{AB}, \bar{\omega}_{AB}) = \mathcal{P}_{\mathcal{B}(\mathcal{H})}(|\xi\rangle, |\eta\rangle)$. Hence, if we denote by $\bar{\omega}_{AXB}$ the state induced by $|\eta\rangle$, we get that $\bar{\omega}_{AXB} \in \mathcal{B}^\epsilon(\omega_{AXB})$. We can then estimate

$$\mathrm{H}^\epsilon_{\min}(A|B)_\omega \leq \mathrm{H}_{\min}(A|B)_{\bar{\omega}} + \delta \leq \mathrm{H}_{\min}(AX|B)_{\bar{\omega}} + \delta \leq \mathrm{H}^\epsilon_{\min}(AX|B)_\omega + \delta \ ,$$

where we used the result for $\epsilon = 0$. Since this holds for any $\delta > 0$, the proof is completed. □

We conclude this section with a bound for the smooth max-entropy.

**Lemma 4.5.8.** *Let $\mathcal{M}_{ABX} = \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{M}_B \otimes \ell^\infty(X)$ with $\mathcal{M}_B$ a general von Neumann algebra, $X$ a set of finite cardinality, and $\omega_{ABX} \in \mathcal{S}_\leq(\mathcal{M}_{ABX})$. Then it follows that*

$$\mathrm{H}_{\max}(A|BX)_\omega \geq \mathrm{H}_{\max}(A|B)_\omega - \log|X| \ . \tag{4.36}$$

*Proof.* We follow the proof from the finite-dimensional case [RR12, Lemma 4], and express Equation (4.36) in terms of the conditional min-entropy by means of the duality relation (Proposition 4.3.4). Let us write $\omega_{ABX} = (\omega^x_{AB})_{x \in X}$ and take a representation $\pi$ of $\mathcal{M}_{AB}$ on some Hilbert space $\mathcal{H}$ for which each $\omega^x_{AB}$ admits a purification $|\xi_x\rangle \in \mathcal{H}$. We denote the complementary system by $\mathcal{M}_R$. It then follows that $|\xi\rangle = \sum_x |\xi_x\rangle \otimes |x\rangle \otimes |x\rangle$ in $\mathcal{H} \otimes \mathbb{C}^{|X|} \otimes \mathbb{C}^{|X|}$ is a purification of $\omega_{ABX}$. Hence, Equation (4.36) turns into

$$\mathrm{H}_{\min}(A|RXX')_\omega \geq \mathrm{H}_{\min}(A|RX')_\omega - \log|X| \ , \tag{4.37}$$

with $\omega_{ABRXX'}$ the state corresponding to $|\xi\rangle$. Note that $X, X'$ do not refer to classical systems anymore, but to a finite dimensional quantum system of dimension $|X|$. If we define $\omega^{x,x'}_{ABR}$ as the functional on $\mathcal{M}_{ABR}$ given by $a \mapsto \mathrm{Tr}(a|\xi_x\rangle\langle\xi_{x'}|)$ one finds that (4.37) is equivalent to

$$\mathrm{H}_{\min}(A|RX)_\omega \geq \mathrm{H}_{\min}(A|RX)_{\tilde{\omega}} - \log|X| \ ,$$

where $\omega_{ARX} = (\omega^{x,x'}_{AR})_{xx'}$ and $\tilde{\omega}_{ARX} = (\omega^{x,x'}_{AR}\delta_{x,x'})_{xx'}$. This inequality now follows from the definition of the conditional min-entropy (Definition 4.2.1) and the fact that $\omega_{ARX} \leq |X| \cdot \tilde{\omega}_{ARX}$. In order to see that the latter property holds, note that for any positive operator $E = (E_{xx'})_{xx'} \in \mathcal{M}_{ARX}$ the matrix $M_E = \left(\omega^{x,x'}_{AR}(E_{xx'})\right)_{xx'}$ is positive, and thus,

$$\begin{aligned}\omega_{ARX}(E) = \mathrm{Tr}\left[(1)_{xx'} \cdot M_E\right] &\leq \|(1)_{xx'}\| \cdot \mathrm{Tr}\left[M_E\right] \\ &= \|(1)_{xx'}\| \cdot \tilde{\omega}_{ARX}(E) \\ &\leq |X| \cdot \tilde{\omega}_{ARX}(E) \ ,\end{aligned}$$

where $(1)_{xx'}$ denotes the matrix with all entries equal to 1. □

## 4.6. Operational Approach to Min- and Max-Entropy

The definition of good entropy measures in information theory is justified by their operational significance, thus, if they can be linked to a particular task or a particular meaning. The min-entropy $\mathrm{H}_{\min}(X)$ of a classical random variable gives the logarithm of the probability to correctly guess the outcome of a random experiment distributed according to $X$. This is extended to side information for $\mathrm{H}_{\min}(X|B)$ which is just the guessing probability of the outcome of $X$ given the side-information encoded in $B$ (see [KRS09] for the finite-dimensional case and Proposition 4.6.5 for the generalization). In the fully quantum case where the $A$ system is finite-dimensional $\mathrm{H}_{\min}(A|B)$ characterizes roughly speaking the distance to a maximally entangled state [KRS09]. The proof given here is based on a generalized Hahn-Banach theorem for positive functionals on an ordered unit vector space (Theorem 4.6.1). It is different to the one given in [FAR11] for infinite-dimensional systems which is based on the finite-dimensional approximation technique (see Section 4.5.2).

The max-entropy $\mathrm{H}_{\max}(X)_p$ of a classical random variable $X$ measures the degree of uniformity. If $X$ takes value in a finite alphabet of seize $d$ and $u_X$ denotes the uniform distribution of $X$, we find that $\mathrm{H}_{\max}(X) = \log dF(p, u_X)$. In the classical quantum case, $\mathrm{H}_{\max}(X|B)$, this generalizes to the distance to a secure state, that is, a state which is uniformly distributed on $X$ and uncorrelated to $B$ [KRS09]. This result can be derived from the interpretation of the min-entropy via the duality between min- and max-entropy. We start with some basics on ordered vector spaces.

### 4.6.1. Preliminaries on Ordered Vector Spaces

The techniques we employ here are based on the theory of ordered vector spaces and nicely developed in a work by Paulsen et al. [PT09]. Let $V$ be a vector space over $\mathbb{R}$ and $V^+ \subset V$ a pointed cone, that is, a subset closed under addition which satisfies $\lambda V^+ \subset V^+$ for all $\lambda \geq 0$ and $V^+ \cap -V^+ = \{0\}$. Such a tuple $(V, V^+)$ is called an ordered real vector space. A cone introduces a partial ordering in $V$ via $v \geq w$ if $v - w \in V^+$. We call elements in $V^+$ positive, and say that $v$ majorizes $w$ if $v \geq w$. A cone $V^+$ is called a full cone if $V^+ \cup -V^+ = V$, and in such a case we have a complete ordering. A subspace $E \subset V$ is said to majorize $V^+$ if for all $v \in V^+$ exists a $z \in E$ such that $z \geq v$.

Given an ordered real vector space $(V, V^+)$, a linear functional $f : V \to \mathbb{R}$ is called positive if $f(v) \geq 0$ for all $v \in V^+$. We denote the set of all linear bounded functionals by $V^*$ and write $g \geq 0$ if $g \in V^*$ is positive. We are interested in a Hahn Banach like extension theorem for positive functionals. It turns out that the positivity condition impose bounds on possible extensions. Let in the following $V^+$ be a full cone, $E$ a subspace of $V$ which majorizes $V^+$ and $f : E \to \mathbb{R}$ a positive linear functional. We define upper and lower bounds for any $v \in V$ via

$$u_f(v) := \inf\{f(z) \mid z \geq v,\, z \in E\} \tag{4.38}$$

$$l_f(v) := \sup\{f(z) \mid v \geq z,\, z \in E\}. \tag{4.39}$$

The following result is the content of Lemma 2.13 and Theorem 2.14 from [PT09].

**Theorem 4.6.1.** *Let $V$ be an ordered real vector space with a full cone $V^+$, $E \subset V$ a subspace which majorizes $V^+$, and $f : E \to \mathbb{R}$ a positive functional on $E$. Then there exists a positive extension $\tilde{f}$ on $V$ and any such extension satisfies*

$$u_f(v) \leq \tilde{f}(v) \leq u_f(v) \ , \ v \in V. \tag{4.40}$$

*Moreover, for any $v \in V$ there exists a positive extension of $f$ such that one of the inequalities in Eq. (4.40) turns into equality.*

Using the definition of $u_f(v)$ we obtain for any positive function $f : E \to \mathbb{R}$

$$\inf\{f(z) \mid z \geq v,\, z \in E\} = \sup\{g(v) \mid g \in V^* \ ,\ g \geq 0\,,\ g|_E \equiv f\}\,. \tag{4.41}$$

Note that this can be seen as a duality relation between the minimization over the subcone $E \cap V^+$ and the convex optimization over positive functionals $g \geq 0$ with $g|_E \equiv f$. This can now directly be used to reformulate the min-entropy.

### 4.6.2. Min-Entropy and Quantum Correlations

In the following we restrict to the case in which the A system is finite-dimensional, that is, $\mathcal{M}_{AB} = M_n \otimes \mathcal{M}_B$ with $\mathcal{M}_B$ an arbitrary von Neumann algebra. We consider the real ordered vector space given by the hermitian functionals $V = \mathcal{N}^h(\mathcal{M}_{AB})$ with cone $V^+ = \mathcal{N}^+(\mathcal{M}_{AB})$. It is then clear that $V^+$ is indeed a full cone. We define the subspace $E = \{\eta_{AB} \mid \eta_{AB} = \tau_A \otimes \eta_B\,,\ \eta_B \in \mathcal{N}^h(\mathcal{M}_B)\}$ of $V$, and note that $E$ majorizes $V^+$. On $E$ we define the linear positive functional $f_{\mathbb{1}}$ via $f_{\mathbb{1}}(\eta_{AB}) = \frac{1}{n}\eta_{AB}(\mathbb{1}) = \eta_B(\mathbb{1})$ where $\eta_{AB} = \tau_A \otimes \eta_B$. Using this notation and Equation (4.4), we can rewrite the min-entropy of a state $\omega_{AB} \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$ as

$$2^{-\mathrm{H}_{\min}(A|B)_\omega} = \inf\{f_{\mathbb{1}}(\sigma_{AB}) \mid \sigma_{AB} \geq \omega_{AB},\, \sigma_{AB} \in E\} \ = u_{f_{\mathbb{1}}}(\omega_{AB}) \ ,$$

where the last equality is simply the application of the definition (4.38). Hence, the min-entropy is the solution of an optimization problem over the subcone of positive functionals of the form $\tau_A \otimes \sigma_B$. According to Eq. (4.41), we can rewrite it as the supremum over positive extensions $g$ on $V$ of $f_{\mathbb{1}}$ such that $g|E = f_{\mathbb{1}}$. Since $V^*$ is simply $\mathcal{M}_{AB} = M_n(\mathcal{M}_B)$, the possible extensions are positive operators $M = (M_{ij}) \in \mathcal{M}_{AB}$ such that for all $\eta_{AB} = \tau_A \otimes \eta_B$

$$\eta_{AB}(M) = \sum_i \eta_B(M_{ii}) = f_{\mathbb{1}}(\eta_{AB}) = \eta_B(\mathbb{1}). \tag{4.42}$$

Hence, the condition that the restriction onto $E$ is $f_{\mathbb{1}}$ translates into $\sum_i M_{ii} = \mathbb{1}$. This leads to the following assertion.

**Lemma 4.6.2.** *Let $\mathcal{M}_{AB} = M_n \otimes \mathcal{M}_B$ with $\mathcal{M}_B$ a von Neumann algebra, and $\omega_{AB} \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$. Then*

$$\mathrm{H}_{\min}\,(A|B)_\omega = -\log \sup\{\omega_{AB}(M) \mid M = (M_{ij}) \in M_n(\mathcal{M}_B)_+,\, \sum_i M_{ii} = \mathbb{1}\}\ . \tag{4.43}$$

In order to simplify Eq. (4.43) such that we obtain the expression known for separable Hilbert spaces [KRS09, FAR11], we use the identification between positive operators in $M_n(\mathcal{M}_B)$ and completely positive maps $\mathcal{E} : M_n \to \mathcal{M}_B$. This correspondence between states on $M_n(\mathcal{M}_B)$ and completely positive maps $\mathcal{E} : \mathcal{M}_B \to M_n$ is discussed in details in [Pau02, Chapter 6].

**Lemma 4.6.3.** *There is a one-to-one correspondence between positive operators $M = (M_{ij})$ in $M_n(\mathcal{M}_B)$ and completely positive maps $\mathcal{E} : M_n \to \mathcal{M}_B$ via the relation $\mathcal{E}(|i\rangle\langle j|) = M_{ij}$. Furthermore, the map $\mathcal{E}$ corresponding to $(M_{ij})$ is unital and therefore a quantum channel, if and only if $\sum_i M_{ii} = \mathbb{1}$.*

*Proof.* Let $\mathcal{M}_B$ acting on $\mathcal{H}_B$. We show only one direction, namely, that the map $\mathcal{E}$ defined via $\mathcal{E}(|i\rangle\langle j|) = M_{ij}$ for a positive operator $(M_{ij})$ is completely positive. The opposite direction can be shown by a similar calculation. Note that it is enough to prove that $\mathcal{E}$ is positive on $M_n \otimes M_n$. Any positive operator $A \in M_n \otimes M_n$ can be decomposed as

$$A = \sum_{i,k,l,m,n} \bar{c}^i_{k,m} c^i_{l,n} |k,m\rangle\langle l,n| \ ,$$

with coefficients $c^i_{k,m}$ in $\mathbb{C}$. A small computation shows that for any state $|\Psi\rangle = \sum_k |k\rangle \otimes |\psi_k\rangle$ in $\mathbb{C} \otimes \mathcal{H}_B$ holds that $\langle \Psi \,|\mathcal{E}(A)\Psi\,\rangle = \langle \Phi \,|M\Phi\,\rangle \geq 0$, where

$$|\Phi\rangle = \sum_{i,k,m} c^i_{k,m} |\psi_k\rangle.$$

The unitality of $\mathcal{E}$ for operators satisfying $\sum_i M_{ii} = \mathbb{1}$ is clear. □

If we take an operator $(M_{ij})$, the dual of the corresponding completely positive map $\mathcal{E}$ is simply given as $\mathcal{E}_*(\omega) = \sum_{i,j} \omega(M_{ij})|j\rangle\langle i|$, where we use the identification of states and density operators in $M_n$. Using Lemma 4.6.3, we find that we can rewrite Lemma 4.6.2 in the following form [KRS09, FAR11].

**Theorem 4.6.4.** *Let $\mathcal{M}_{AB} = M_n \otimes \mathcal{M}_B$ with $\mathcal{M}_B$ a von Neumann algebra, $\omega_{AB} = (\omega^{ij}_B) \in \mathcal{S}_\leq(\mathcal{M}_{AB})$, and $|\Phi_{AA'}\rangle = \sum_{i=1}^n |\phi_i\rangle \otimes |\psi_i\rangle$, where $\{|\phi_i\rangle\}$ and $\{|\psi_i\rangle\}$ are orthonormal bases of $\mathbb{C}^n$. Then*[8]

$$\mathrm{H}_{\min}\left(A|B\right)_\omega = -\log \sup_{\mathcal{E}_*} F((\mathrm{id}_A \otimes \mathcal{E}_*)(\omega_{AB}), |\Phi_{AA'}\rangle)\,, \tag{4.44}$$

*where the supremum is taken over all quantum channels $\mathcal{E} : M_n \to \mathcal{M}_B$.*

The quantity in the logarithm of the right hand side of (4.44) is referred to as the quantum correlation in [KRS09, FAR11] and, divided by $n$, it measures how close $\omega_{AB}$ can be brought to the maximally entangled state by means of local operations on the $B$ system.

[8] The difference of a square in comparison to [KRS09, FAR11] is due to the different definition of the fidelity.

*Proof.* The theorem is obtained via the relation

$$F((\mathrm{id}_A \otimes \mathcal{E}_*)(\omega_{AB}), |\Phi_{AA'}\rangle) = \sum_{ij} \omega_B^{ij}(M_{ij}) \,, \tag{4.45}$$

where $(M_{ij})$ is the positive operator corresponding to the quantum channel $\mathcal{E}$ as given in Lemman 4.6.3. Here, we have chosen the basis for $|\Phi_{AA'}\rangle$ such that it is compatible with $\mathcal{E}_*$, that is, we set $\mathcal{E}_*(\omega) = \sum_{i,j} \omega(M_{ij})|\psi_j\rangle\langle\psi_i|$. □

**The Guessing Probability** The analogue of Proposition 4.6.2 for classical quantum systems leads to the guessing probability [KRS09]. We start with a classical quantum state $\omega_{XB} = (\omega_B^x)_{x\in X}$ on $\ell^\infty(X) \otimes \mathcal{M}_B$, where the classical part $X$ is given to Alice and the quantum part $\mathcal{M}_B$ to Bob who are space-like separated. Bob wants to guess the value of the random variable $X$ by performing the optimal measurement. The guessing probability characterizes the probability that Bob's guess is correct and can be expressed by the formula

$$p_{\mathrm{guess}}(X|B)_\omega = \sup\{ \sum_{x\in X} \omega_B^x(E_x) \;:\; E_x \in \mathcal{M}_B,\; E_x \geq 0,\; \sum_x E_x = \mathbb{1}\} \,. \tag{4.46}$$

**Proposition 4.6.5.** *Let $\mathcal{M}_{XB} = \ell^\infty(X) \otimes \mathcal{M}_B$ with $\mathcal{M}_B$ be a von Neumann algebra, and $\omega_{XB} \in \mathcal{S}(\mathcal{M}_{XB})$. Then*

$$\mathrm{H}_{\min}\left(X|B\right)_\omega = -\log p_{\mathrm{guess}}(X|B)_\omega \;, \tag{4.47}$$

*with $p_{\mathrm{guess}}(X|B)_\omega$ as defined in* (4.46).

This result is just the classical version of Proposition 4.6.2, and the prove can be adapted from it.

### 4.6.3. Max-Entropy and Decoupling Accuracy

We use the result from the previous section together with the duality between min- and max-entropy and show the link between the smooth conditional max-entropy of $\omega_{AB}$ to its distance to a state which is completely mixed on $A$ and decoupled from $B$ [KRS09, FAR11]. We measure the distance by means of the fidelity

$$\mathrm{d}_{\mathrm{dec}}(A|B)_\omega := \sup_{\sigma_B \in \mathcal{S}(\mathcal{M}_B)} F(\omega_{AB}, \tau_A \otimes \sigma_B) \tag{4.48}$$

and call it the decoupling accuracy of $\omega_{AB}$ with respect to $B$ [KRS09]. Note that the measure scales with the dimension of the $A$ system since $\tau_A$ is the trace in $M_n$ and therefore not normalized. Hence, for the normalized state $\omega_{AB} = \tau_A/n \otimes \sigma_B$ the decoupling accuracy is $n$.

**Theorem 4.6.6.** *Let $\mathcal{M}_{AB} = M_n \otimes \mathcal{M}_B$ with $\mathcal{M}_B$ a von Neumann algebra. For any state $\omega_{AB} = (\omega_B^{ij}) \in \mathcal{S}_\leq(\mathcal{M}_{AB})$, it follows that*

$$\mathrm{H}_{\max}\left(A|B\right)_\omega = \log \mathrm{d}_{\mathrm{dec}}(A|B)_\omega \;. \tag{4.49}$$

The proof is a simple adaption from the ones given in [KRS09, FAR11] and based on the operational interpretation of the min-entropy.

*Proof.* Recall that each state in $\mathcal{M}_{AB}$ can be purified in the standard form, that is, in $M_n \otimes M_n \otimes \mathcal{M}_B^\phi$, where $\mathcal{M}_B^\phi$ is a standard form of $\mathcal{M}_B$. We denote the purifying system by $\mathcal{M}_{A'B'}$ since it consists of a copy of the A-system $\mathcal{M}_{A'} = M_n$ and the commutant $\mathcal{M}_{B'} = (\mathcal{M}_B^\phi)'$ of the system $B$. Thus, $\mathcal{M}_{ABA'B'} \subset \mathcal{B}(\mathcal{K})$ with $\mathcal{K} = \mathbb{C}^{2n} \otimes \mathcal{H}_\phi$. Let now $\xi_\omega \in \mathcal{K}$ be a purification of $\omega_{AB}$ and $|\Phi_{AA'}\rangle$ a non-normalized maximally entangled state on $\mathcal{M}_{AA'}$ as in Theorem 4.6.4, thus a purification of $\tau_A$. Then with $\eta_\sigma \in \mathcal{H}_\phi$ a purification of $\sigma \in \mathcal{S}(\mathcal{M}_B)$, we find that

$$\begin{aligned} F(\omega_{AB}, \tau_A \otimes \sigma_B) &= \sup_{U \in \mathcal{M}_{A'B'}} |\langle \xi_\omega | U(\Phi_{AA'} \otimes \eta_\sigma) \rangle|^2 \\ &= \sup_{U \in \mathcal{M}_{A'B'}} F_{\mathcal{B}(\mathcal{K})}(U\xi_\omega, \Phi_{AA'} \otimes \eta_\sigma) \\ &\leq \sup_{U \in \mathcal{M}_{A'B'}} F_{\mathcal{M}_{AA'}}(U\xi_\omega, \Phi_{AA'} \otimes \eta_\sigma) \ , \end{aligned}$$

where the supremum is taken over unitaries $U$ in $\mathcal{M}_{A'B'}$. According to Stinespring's dilation theorem [Pau02], applying a unitary followed by a restriction of the state is a quantum operation, such that the state on $\mathcal{M}_{AA'}$ described by $U\xi_\omega$ can be obtained by applying a quantum operation $\mathcal{E}_U : \mathcal{N}(\mathcal{M}_{A'B'}) \to \mathcal{N}(M_{A'})$ on $\omega_{AA'B'}$. Hence, together with Theorem 4.6.4 we obtain that

$$\begin{aligned} F(\omega_{AB}, \tau_A \otimes \sigma_B) &\leq \sup_U F_{\mathcal{M}_{AA'}}((\mathrm{id}_A \otimes \mathcal{E}_U)(\omega_{AA'B'}, \Phi_{AA'}) \\ &\leq 2^{-\mathrm{H}_{\min}(A|A'B')_\omega} = 2^{\mathrm{H}_{\max}(A|B)_\omega} \ . \end{aligned}$$

Taking the supremum over all $\sigma_B \in \mathcal{S}(\mathcal{M}_B)$ we find the inequality in one direction. In order to show the other direction, we note that according to Theorem 4.6.4, there exists for all $\delta > 0$ a quantum operation $\mathcal{E} : \mathcal{N}(\mathcal{M}_{A'B'}) \to \mathcal{N}(M_{A'})$ such that

$$2^{\mathrm{H}_{\max}(A|B)_\omega} \leq F((\mathrm{id}_A \otimes \mathcal{E})(\omega_{AA'B'}), |\Phi_{AA'}\rangle) + \delta \ . \tag{4.50}$$

Let now $|\xi_{\omega^\mathcal{E}}\rangle$ be a purification of $(\mathrm{id}_{AB} \otimes \mathcal{E})(\omega_{ABA'B'})$, which can always be found on the extended system $\mathcal{M}_{AA'CBB'}$, where $\mathcal{M}_C = M_{n^2}$. With an arbitrary $|\theta\rangle \in \mathbb{C}^{n^2} \otimes \mathcal{H}_\phi$, we obtain

$$\begin{aligned} F((\mathrm{id}_A \otimes \mathcal{E})(\omega_{AA'B'}), |\Phi_{AA'}\rangle) &= \sup_{U \in \mathcal{M}_{DBB'}} |\langle \xi_{\omega^\mathcal{E}} | U(\Phi_{AA'} \otimes \theta) \rangle|^2 \\ &\leq \sup_{U \in \mathcal{M}_{DBB'}} F_{\mathcal{M}_{AB}}(|\xi_{\omega^\mathcal{E}}\rangle, |\Phi_{AA'}\rangle \otimes |U\theta\rangle) \ . \end{aligned}$$

Since the reduced state of $|\xi_{\omega^\mathcal{E}}\rangle$ on $\mathcal{M}_{AB}$ is $\omega_{AB}$, and there exists for all $\sigma_B \in \mathcal{S}(\mathcal{M}_B)$ a purification of the form $|U\theta\rangle$ with $U$ unitary in $\mathcal{M}_{DBB'}$, we conclude that

$$2^{\mathrm{H}_{\max}(A|B)_\omega} \leq \sup_{\sigma_B \in \mathcal{S}(\mathcal{M}_B)} F(\omega_{AB}, \tau_A \otimes \sigma_B) + \delta \ . \tag{4.51}$$

Because this holds for any $\delta > 0$, we found the inequality in the other direction. □

Let us consider the special case where we have a classical-quantum system $\mathcal{M}_{XB}$ given by the discrete alphabet $X$ and the von Neumann algebra $\mathcal{M}_B$ (see Section 3.3). It then follows from Equation (4.49) that it can be written as

$$\mathrm{H}_{\max}(X|B)_\omega = 2\log\sup\Big\{\sum_x \sqrt{F(\omega_B^x,\sigma_B)}\;\Big|\;\sigma_B\in\mathcal{S}(\mathcal{M}_B)\Big\}. \tag{4.52}$$

This form will be useful to generalize the max-entropy to continuous alphabets in Section 5.2.

## 4.7. Entropic Uncertainty Relation for Smooth Min- and Max-Entropies

Entropic uncertainty relations quantify the inherent statistical ignorance of measurement outcomes of two non-commuting observables. The first rigorous proof of such an uncertainty relation goes back to Maassen and Uffink in 1988 [MU88] and was formulated for dual pairs of Rényi entropies including the case of the von Neumann entropy in the limit $\alpha\to 1$. For a review about entropic uncertainty relations and further reading see the nice surveys [WW10, BBR11] and references therein. Let us assume that we have a resource described by the quantum state $\omega_A$ and we can perform two different measurements modeled by POVM's $\{E_x\}_{x\in X}$ and $\{F_y\}_{y\in Y}$ with discrete sets $X$ and $Y$. Let us denote the classical system describing the outcome of the measurements also by $X$ and $Y$. The distribution of the random variables $\omega_X$ and $\omega_Y$ satisfy the inequality

$$\mathrm{H}_\alpha(X)_\omega + \mathrm{H}_\beta(Y)_\omega \geq -\log c\,, \tag{4.53}$$

where $(1/\alpha)+(1/\beta)=2$ and

$$c=\sup_{x,y}\|\sqrt{E_x}\sqrt{F_y}\|^2. \tag{4.54}$$

The constant $c$ determines the complementary of the measurements. In the case where a measurement operator $E_x$ commutes with one $F_y$ we obtain $c=0$ and the inequality becomes trivial. For a $d$-dimensional system measured by two maximally complementary rank-one measurements the constant is $c=\frac{1}{d}$.

Recently, it was realized that a similar relation holds when access to correlated quantum systems $B$ is given [BCC+10, RB09]. In fact, it revealed a subtle interplay between uncertainty and entanglement and reads for the von Neumann entropy as [BCC+10]

$$\mathrm{H}(X|B)_\omega + \mathrm{H}(Y|B)_\omega \geq -\log c + \mathrm{H}(A|B)_\omega \tag{4.55}$$

where H(X|B) (resp. H(Y|B)) is the conditional von Neumann entropy of the outcome distribution $X$ (resp. $Y$) given the quantum system $B$ (the measurements act only on system A). This can be turned into a tripartite version via a simple purification argument and reads

$$\mathrm{H(X|B)}_\omega + \mathrm{H(Y|C)}_\omega \geq -\log \mathrm{c} \tag{4.56}$$

where $\omega_{ABC}$ is an arbitrary tripartite state and again $\{E_x\}_{x\in X}$ and $\{F_y\}_{y\in Y}$ are POVM's on A.

Such entropic uncertainty relations with quantum side information were lately also proven for other entropies [TR11, CYGG, CYZ11], among them the smooth min- and max-entropies and the $\alpha$-Rényi entropies. We generalize this in the following to a setting were states on arbitrary von Neumann algebras can be measured. This is for instance relevant in the case of position and momentum operators which will be discussed in Section 5.3 and used to prove security of the continuous-variable quantum key distribution protocol considered in Section 6.3.

**Theorem 4.7.1.** *Let $\mathcal{M}_{ABC}$ be a tripartite system described by arbitrary von Neumann algebras $\mathcal{M}_A$, $\mathcal{M}_B$ and $\mathcal{M}_C$, $\omega_{ABC} \in \mathcal{S}_\leq(\mathcal{M}_{ABC})$, $\{E_A^x\}_{x\in X}$ and $\{F_A^y\}_{y\in Y}$ POVM's on $\mathcal{M}_A$ with discrete outcomes $X$ and $Y$, and $\epsilon \geq 0$. Then*

$$\mathrm{H}_{\min}^{\epsilon}(X|B)_\omega + \mathrm{H}_{\max}^{\epsilon}(Y|C)_\omega \geq -\log \max_{x,y} \left\| \sqrt{E_A^x} \cdot \sqrt{F_A^y} \right\|^2 , \tag{4.57}$$

*where $\omega_{XB} = (\omega_B^x)$ with $\omega_B^x(\cdot) = \omega_{AB}(E_A^x \cdot)$, and $\omega_{YC} = (\omega_C^y)$ with $\omega_C^y(\cdot) = \omega_{AC}(F_A^y \cdot)$ are cq-states on $\mathcal{M}_B$ and $\mathcal{M}_C$, respectively.*

The proof is different to the one in [TR11] and uses the form of the min-entropy derived in Section 4.6.2.

*Proof.* We first prove the inequality for $\epsilon = 0$. Without loss of generality, we can assume that $\mathcal{M}_{ABC}$ is already in standard form acting on a Hilbert space by $\mathcal{H}$. Let $|\xi\rangle \in \mathcal{H}$ be a purification of $\omega_{ABC}$ and denote by $\mathcal{M}_D = \mathcal{M}'_{ABC}$ the complementary system. The first step is the application of the duality relation to the max-entropy. For that, we note that $|F_y^{\frac{1}{2}}\xi\rangle$ is a purification of $\omega_C^y$ such that $\sum_y |y, y, F_y^{\frac{1}{2}}\xi\rangle$ is a purification of $\omega_{YC}$ on $\mathcal{H}_Y \otimes \mathcal{H}'_Y \otimes \mathcal{H}$ with complementary system $M_{Y'ABD}$. Here we used the notation $\mathcal{H}_Y \simeq \mathcal{H}'_Y \simeq \mathbb{C}^{|Y|}$ and $\mathcal{M}_{Y'} = M_{|Y'|}$ for the operators acting on $\mathcal{H}_{Y'}$. Let us denote the state induced by $|y, F_y^{\frac{1}{2}}\xi\rangle\langle y', F_{y'}^{\frac{1}{2}}\xi|$ on $M_{Y'ABCD}$ by $\omega_{Y'ABCD}^{y,y'}$ and set $\omega_{YY'ABCD} = (\omega_{ABCD}^{y,y'})_{y,y'}$. By the definition of the max-entropy, we have that $\mathrm{H}_{\max}(Y|C)_\omega = -\mathrm{H}_{\min}(Y|Y'ABD)_\omega$ and can rewrite the inequality (4.57) as

$$\mathrm{H}_{\min}(X|B)_\omega \geq \mathrm{H}_{\min}\left(Y|Y'ABD\right)_\omega - \log c ,$$

where $c$ is defined in equation (4.54). Using Proposition 4.6.5 and 4.6.2, the inequality above yields

$$\begin{aligned} &p_{guess}(X|B)_\omega \\ &\leq c \sup\Big\{ \sum_{y,y'} \omega_{Y'ABD}^{y,y'}(M_{y,y'}) \;\Big|\; (M_{y,y'}) \in M_{|Y|}(\mathcal{M}_{Y'ABD})_+, \sum_y M_{yy} = \mathbb{1} \Big\} \end{aligned} \tag{4.58}$$

Starting with the guessing probability and using $\sum_y F_y = \mathbb{1}$, we can compute

$$\begin{aligned} p_{guess}(X|B)_\omega &= \sup_{\{N_x\}} \sum_x \omega_B^x(N_x) = \sup_{\{N_x\}} \sum_x \omega_{ABCD}(E_x^{\frac{1}{2}} N_x E_x^{\frac{1}{2}}) \\ &= \sup_{\{N_X\}} \sum_{y,y',x} \omega_{ABCD}(F_y E_x^{\frac{1}{2}} N_x E_x^{\frac{1}{2}} F_{y'}) \\ &= \sup_{\{N_X\}} \sum_{y,y'} \omega_{Y'ABCD}^{y,y'}(\sum_x |y\rangle\langle y'| \otimes F_y^{\frac{1}{2}} E_x^{\frac{1}{2}} N_x E_x^{\frac{1}{2}} F_{y'}^{\frac{1}{2}}) \\ &= \sup_{\{N_X\}} \sum_{y,y'} \omega_{Y'ABCD}^{y,y'}(M_{y,y'}(N_x)), \end{aligned}$$

where the supremum is taking over $\{N_x\} \subset (\mathcal{M}_B)_+$ with $\sum_x N_x \leq \mathbb{1}$ and the operator $M_{y,y'}(\{N_x\}) \in \mathcal{M}_{Y'ABD}$ introduced in the last equality is defined as

$$M_{y,y'}(\{N_x\}) = \sum_x |y\rangle\langle y'| \otimes F_y^{\frac{1}{2}} E_x^{\frac{1}{2}} N_x E_x^{\frac{1}{2}} F_{y'}^{\frac{1}{2}}.$$

In order to proof the inequality in (4.58), the positivity of $(M_{y,y'}(\{N_x\}))_{y,y'}$ in $M_{|Y|}(\mathcal{M}_{Y'ABD})$ and that $\sum_y M_{y,y'}(\{N_x\}) \leq c\mathbb{1}$ has to be shown. The positivity is obvious from the rewriting $M_{y,y'}(\{N_x\}) = \sum_x (R_y^x)^* R_y^x$ with $R_y^x = \langle y| \otimes N_x^{\frac{1}{2}} E_x^{\frac{1}{2}} F_y^{\frac{1}{2}}$. The latter is obtained by the estimation

$$\begin{aligned} \sum_y M_{y,y'}(\{N_x\}) &= \sum_{x,y} |y\rangle\langle y| \otimes F_y^{\frac{1}{2}} E_x F_y^{\frac{1}{2}} N_x \\ &\leq \max_{x,y} \|F_y^{\frac{1}{2}} E_x F_y^{\frac{1}{2}}\| \sum_{x,y} |y\rangle\langle y| \otimes N_x \\ &\leq \max_{x,y} \|F_y^{\frac{1}{2}} E_x F_y^{\frac{1}{2}}\| \ , \end{aligned}$$

where we used that $N_x$ commutes with $E_x$ and $F_y$ and that $\sum N_x \leq \mathbb{1}$. This completes the proof for $\epsilon = 0$.

Let us know assume that $\epsilon > 0$. We define the isometries $U_F : \mathcal{H} \to \mathcal{H} \otimes \mathcal{H}_{YY'}$ and $U_E = \mathcal{H} \to \mathcal{H} \otimes \mathcal{H}_{XX'}$ for $\mathcal{H}_Y \simeq \mathcal{H}_{Y'} \simeq \mathbb{C}^{|Y|}$ and $\mathcal{H}_X \simeq \mathcal{H}_{X'} \simeq \mathbb{C}^{|X|}$ by

$$U_F = \sum_{y \in Y} |y, y\rangle \otimes F_y^{\frac{1}{2}} \quad \text{and} \quad U_E = \sum_{x \in X} |x, x\rangle \otimes E_x^{\frac{1}{2}} \ .$$

As shown in Lemma 4.4.1, there exists a state $\tilde{\omega}_{YC} \in \mathcal{B}^\epsilon_{\mathrm{cq}}(\omega_{YC})$ for which $\mathrm{H}^\epsilon_{\max}(Y|C)_\omega = \mathrm{H}_{\max}(Y|C)_{\tilde{\omega}}$. Let us take a purification $\tilde{\omega}_{YY'ABCD}$ of it such that (cf. Lemma 3.4.6)

$$\mathcal{P}(\omega_{YY'ABCD}, \tilde{\omega}_{YY'ABCD}) = \mathcal{P}(\omega_{YC}, \tilde{\omega}_{YC}) \leq \epsilon. \tag{4.59}$$

We can now apply the uncertainty relation to the state $\tilde{\omega}_{ABC}$ given by $a \mapsto \tilde{\omega}_{YY'ABCD}(U_F a U_F^*)$ for $a \in \mathcal{M}_{ABC}$. The state $\tilde{\omega}_{XB}$ is then simply given by $b \mapsto \tilde{\omega}_{YY'ABCD}(U_F U_E^* b U_E U_F^*)$ for $b \in \mathcal{M}_{XB}$. Since $\mathcal{E}(b) = U_F U_E^* b U_E U_F^*$ is a completely positive contraction and $\tilde{\omega}_{XB} = \mathcal{E}_*(\tilde{\omega}_{YY'ABCD})$ as well as $\omega_{XB} = \mathcal{E}_*(\omega_{YY'ABCD})$, we can apply Lemma 3.4.5 and find from Equation (4.59) that $\mathcal{P}(\omega_{XB}, \tilde{\omega}_{XB}) \leq \epsilon$. Finally, we use that the smooth min-entropy is obtained as the supremum over $\epsilon$-close states and the desired inequality follows. □

## 4.8. Privacy Amplification against Quantum Adversaries

Let us consider the situation where we have a classical random variable $X$ which might be correlated with another system $E$ not further specified at the moment.[9] The goal of privacy amplification is to process the variable $X$ in such a way that the new generated random variable $K$ is (almost) uniformly distributed and (almost) uncorrelated to the system $E$. This is of importance for many cryptographic tasks like for instance quantum key distribution. The case without side-information $E$ was first analyzed in [BBR88, ILL89] and then extend to classical side-information in [BBCM95, RW05]. The security in the case where the $E$ system is modeled by a finite-dimensional quantum system was discussed in [KMR05, RK05, Ren05, TSSR10]. The generalization to finite-dimensional separable Hilbert spaces can be obtained by approximation techniques from [FAR11] as presented in [Fur09].

The striking property is that the post-processing, independently whether the side-information is quantum or classical, consists always of applying a hash function to a smaller alphabet drawn at random from a special family satisfying certain properties. The size of the alphabet of the new random variable is determined by the security parameter which quantifies how uniform and uncorrelated the final random variable should be and the initial state. This size can be optimally characterized by the smooth min-entropy of the inital state [ILL89, Ren05, TSSR10].

We consider in the following the case where the side-information $E$ is modeled by a von Neumann algebra $\mathcal{M}_E$. This generalizes the result of privacy amplification to the most general situation. Let us assume that the initial state is the classical quantum state $\omega_{XE}$. The ideal state which one aims for is

$$\frac{1}{|K|}\tau_K \otimes \omega_E \ ,$$

where $\tau_K = (1, \ldots, 1) \in \ell^1(K)$. In general, one can only hope to obtain an "almost" ideal state, why we introduce a security parameter quantifying the closeness to the ideal state. We use the following composable security definition [RK05].

**Definition 4.8.1.** *Let $\mathcal{M}_E$ be a von Neumann algebra, $K$ a countable finite set, $\omega_{KE} \in \otimes\mathcal{S}_{\leq}(\ell^\infty(K) \otimes \mathcal{M}_E)$ a classical quantum state and $\varepsilon \geq 0$. We call $\omega_{KE}$ an $\epsilon$-secure key with respect to $E$ if*

$$\|\omega_{KE} - \frac{1}{|K|}\tau_K \otimes \omega_E\|_{\ell^1_K(\mathcal{N}(\mathcal{M}_E))} \leq \epsilon \, ,$$

*where $\omega_E$ is the reduced of $\omega_{KE}$ on $\mathcal{M}_E$.*

Henceforth, we omit the subscript $\ell^1_X(\mathcal{N}(\mathcal{M}_E))$ for the norm. The idea of how to achieve an $\epsilon$-secure key from the initial state $\omega_{XE}$ is to randomly combine several indices $x$ into a single one, and thereby reducing the alphabet from $X$ to $K$ with $|K| < |X|$. This can be accomplished by drawing the functions at random from a family of two-universal hash functions which ensure that the collision of two values in $X$ is small enough.

[9] We use here the letter $E$ in perspective of cryptography in which an eavesdropper is usually called Eve.

**Definition 4.8.2.** *Let $X, K$ be sets of finite cardinality such that $|K| \leq |X|$. A family of $\{X, K\}$-hash functions is a set $\{\mathcal{F}, \mathbb{P}_{\mathcal{F}}\}_{X,K}$, where every element $f \in \mathcal{F}$ is a function $f : X \to K$, called hash function, and $\mathbb{P}_{\mathcal{F}}$ is a probability measure on the set $\mathcal{F}$. A family of $\{X, K\}$-hash functions is called two-universal if for all $x, y \in X$ with $x \neq y$*

$$\mathbb{P}_{\mathcal{F}}\left(f(x) = f(y)\right) \leq \frac{1}{|K|} \ . \tag{4.60}$$

The existence of two-universal hash families in the case $|K| \leq |X|$ was shown in [CW79, WC81]. We denote the operator corresponding to a function $f : X \to K$ which maps classical-quantum states on $\mathcal{M}_{XE}$ to classical-quantum states on $\mathcal{M}_{KE}$ by $T_f$. Formally, it maps $\ell^1(X) \otimes \mathcal{N}(\mathcal{M}_E)$ to $\ell^1(K) \otimes \mathcal{N}(\mathcal{M}_E)$ and is given by

$$T_f(\omega_{XE}) = \Big( \sum_{x \in X : f(x) = i} \omega_E^x \Big)_{i \in K} , \tag{4.61}$$

for $i \in K$ and $\omega_{XE} = (\omega_E^x)_{x \in X}$. We are now ready to state the main theorem of this section.

**Theorem 4.8.3.** *Let $\mathcal{M}_E$ be a von Neumann algebra, $X$ and $K$ two sets of finite cardinality with $|K| \leq |X|$, $\{\mathcal{F}, \mathbb{P}_{\mathcal{F}}\}_{X,K}$ a family of two-universal $\{X, K\}$-hash functions, and $\omega_{XE} = (\omega_E^x)_{x \in X}$ a classical-quantum state in $\mathcal{S}_{\leq}(\ell^\infty(X) \otimes \mathcal{M}_E)$. It then follows that*

$$\Big\langle \big\| T_f(\omega_{XE}) - \frac{1}{|K|} \tau_K \otimes \omega_E \big\| \Big\rangle_{\mathcal{F}} \leq \sqrt{|K| \cdot 2^{-\mathrm{H}_{\min}(X|E)_\omega}} \ , \tag{4.62}$$

*where $\langle \cdot \rangle_{\mathcal{F}}$ denotes the expectation value over the functions $f$ with respect to $\mathbb{P}_{\mathcal{F}}$ and $\omega_E = \sum_x \omega_E^x \in \mathcal{S}_{\leq}(\mathcal{M}_E)$ is the reduced state of $\omega_{XE}$ on $\mathcal{M}_E$.*

The proof is different from the finite dimensional ones in [Ren05, TSSR10] and is close to the arguments used in the classical case [BBR88, ILL89, BBCM95]. It uses the non-commutative Radon-Nikodym derivative as introduced in Section 2.2.3.

*Proof.* Because the alphabet $X$ is finite, so is the value of $\mathrm{H}_{\min}(X|E)_\omega$ and we can assume that there exists a $\sigma_E \in \mathcal{S}(\mathcal{M}_E)$ such that $\omega_E^x \leq \lambda \cdot \sigma_E$ for all $x \in X$ and suitable $\lambda > 0$. Let $(\mathcal{H}, \pi, \mathcal{P}, J)$ be a standard form of $\mathcal{M}$ on $\mathcal{H}$ with cone $\mathcal{P}$ and modular conjugation $J$ (see Section 2.2.2). As usual we identify $\pi(\mathcal{M})$ with $\mathcal{M}$. There exist now vector representatives $\xi_x$, $\xi_\omega$ and $\xi_\sigma$ in $\mathcal{P}$ for $\omega_E^x$ ($x \in X$), $\omega_E = \sum_x \omega_E^x$ and $\sigma_E$. Moreover, since $\sigma$ majorizes $\omega_E^x$ there are non-commutative Radon-Nikodym derivatives $D_x \in \mathcal{M}'$ such that $|\xi_x\rangle = D_x|\xi_\sigma\rangle$ ($x \in X$) (see Section 2.2.3). The same holds for $\omega_E$, that is, there is an operator $D \in \mathcal{M}'$ with $D|\xi_\sigma\rangle = |\xi_\omega\rangle$ which additionally satisfies (see Equation (2.5))

$$\sum_{x \in X} D_x^* D_x |\xi_\sigma\rangle = D^* D |\xi_\sigma\rangle \, . \tag{4.63}$$

According to the definition of the norm on $\ell^1(\mathcal{N}(\mathcal{M}_E))$ (see Equation (3.2)) and the definition of $T_F$ (see Equation (4.61)), the left hand side of Equation (4.62)

corresponds to the expectation value of

$$\sum_{i\in K} \sup_{a_i\in\mathcal{M}_E,\|a_i\|=1} \Big| \sum_{x\in X:f(x)=i} \omega_E^x(a_i) - \frac{1}{|K|}\omega_E(a_i)\Big| . \tag{4.64}$$

Using the notation above, we can rewrite the terms in the absolute value by

$$\begin{aligned}
&\sum_{x\in X:f(x)=i} \omega_E^x(a_i) - \frac{1}{|K|}\omega_E(a_i) \\
&= \sum_{x\in X:f(x)=i} \langle \xi_\sigma \,| D_x^* D_x \, a_i \xi_\sigma \,\rangle - \frac{1}{|K|} \langle \xi_\sigma \,| D^* D \, a_i \xi_\sigma \,\rangle \\
&= \langle \Big( \sum_{x\in X:f(x)=i} D_x^* D_x - \frac{1}{|K|} D^* D \Big) \xi_\sigma \,| a_i \xi_\sigma \,\rangle \,,
\end{aligned}$$

where in the last step, we employed that $a_i \in \mathcal{M}$ and $D_x$, $D$ are elements of $\mathcal{M}'$ and thus commute with $a_i$. We now insert this expression into (4.64), take the expectation value over the family $\mathcal{F}$ and employ that for any vectors $\varphi_{i,f}, \psi_{i,f} \in \mathcal{H}$ the inequality

$$\Big\langle \sum_{i\in K} |\, \langle \varphi_{i,f} \,| \psi_{i,f} \,\rangle| \Big\rangle_{\mathcal{F}} \leq \sqrt{\Big\langle \sum_{i\in K} \langle \varphi_{i,f} \,| \varphi_{i,f} \,\rangle \Big\rangle_{\mathcal{F}}} \sqrt{\Big\langle \sum_{i\in K} \langle \psi_{i,f} \,| \psi_{i,f} \,\rangle \Big\rangle_{\mathcal{F}}} .$$

holds, which follows by applying two times the Cauchy-Schwarz inequality. This then yields

$$\begin{aligned}
&\Big\langle \| T_f(\omega_{XE}) - \frac{1}{|K|} \tau_K \otimes \omega_E \| \Big\rangle_{\mathcal{F}}^2 \\
&\leq |K| \Big\langle \sum_{i\in K} \langle \xi_\sigma \,| \Big( \sum_{x\in X:f(x)=i} D_x^* D_x - \frac{1}{|K|} D^* D \Big)^2 \xi_\sigma \,\rangle \Big\rangle_{\mathcal{F}} ,
\end{aligned}$$

where we used that

$$\sum_{i\in K} \sup_{a_i\in\mathcal{M}_E,\|a_i\|=1} \langle \xi_\sigma \,| a_i^* a_i \xi_\sigma \,\rangle \leq \sum_{i\in K} \sup_{a_i\in\mathcal{M}_E,\|a_i\|=1} \|a_i\|^2 \leq |K| \,.$$

Using the relation given in Equation (4.63), we can compute

$$\begin{aligned}
&\Big\langle \sum_{i\in K} \langle \xi_\sigma \,| \Big( \sum_{x\in X:f(x)=i} D_x^* D_x - \frac{1}{|K|} D^* D \Big)^2 \xi_\sigma \,\rangle \Big\rangle_{\mathcal{F}} \\
&= \Big\langle \sum_{i\in K} \langle \xi_\sigma \,| \Big( \sum_{x\in X:f(x)=i} D_x^* D_x \Big)^2 \xi_\sigma \,\rangle \Big\rangle_{\mathcal{F}} - \frac{1}{|K|} \langle \xi_\tau \,| D^* D D^* D \xi_\sigma \,\rangle \,,
\end{aligned} \tag{4.65}$$

where we applied the identity

$$\Big\langle \sum_{i\in K} \sum_{x\in X:f(x)=i} \Big\rangle_{\mathcal{F}} \equiv \sum_{x\in X} \,.$$

We focus now on the first term in line (4.65). Note first that we can write the quadratic term by

$$\begin{aligned}\Big(\sum_{x\in X:f(x)=i} D_x^* D_x\Big)^2 &= \sum_{x\in X:f(x)=i}\sum_{y\in X:f(y)=i} D_x^* D_x D_y^* D_y \\ &= \sum_{x\in X}\sum_{y\in X}(1-\delta_{x,y})\,\delta_{f(x)=i}\,\delta_{f(y)=i}\,D_x^* D_x D_y^* D_y \\ &\quad + \sum_{x\in X:f(x)=i} D_x^* D_x D_x^* D_x\ .\end{aligned}$$

Next we have to take the expectation value over the family of two-universal hash functions. For that, we first note that by the definition of two-universal (see Definition 4.8.2) the relation

$$\Big\langle \sum_{i\in K}(1-\delta_{x,y})\,\delta_{f(x)=i}\,\delta_{f(y)=i}\Big\rangle_{\mathcal{F}} \leq \frac{1}{|K|}\,,$$

holds. Moreover, we use the property that the modular conjugation $J$ leaves the cone $\mathcal{P}$ invariant, i.e., $|\psi\rangle = J|\psi\rangle$ for all $\psi\in\mathcal{P}$, and that $J\mathcal{M}J\subset\mathcal{M}'$ to conclude that

$$\begin{aligned}\langle\xi_\sigma\,|D_x^* D_x D_y^* D_y \xi_\sigma\,\rangle &= \langle\xi_\sigma\,|JD_x^* JD_x D_y^* D_y\xi_\sigma\,\rangle = \langle\xi_\sigma\,|JD_xJD_y^*JD_x^*JD_y\xi_\sigma\,\rangle \\ &= \langle\xi_\sigma\,|D_y^*JD_xJJD_x^*JD_y\xi_\sigma\,\rangle \geq 0\,.\end{aligned}$$

Hence, we get the following bound for the quadratic term in (4.65),

$$\begin{aligned}\Big\langle \sum_{i\in K}\langle\xi_\sigma\,|\Big(\sum_{x\in X:f(x)=i} D_x^* D_x\Big)^2\xi_\sigma\,\rangle\Big\rangle_{\mathcal{F}} &\leq \sum_{x\in X}\langle\xi_\sigma\,|D_x^* D_x D_x^* D_x\xi_\sigma\,\rangle \\ &\quad + \frac{1}{|K|}\,\langle\xi_\sigma\,|D^*DD^*D\xi_\sigma\,\rangle\,,\end{aligned}$$

where we again used (4.63). Inserting this into (4.65), we see that the second term is canceled, and thus we are left with the bound

$$\Big\langle \|T_f(\omega_{XE}) - \frac{1}{|K|}\tau_K\otimes\omega_E\|\Big\rangle_{\mathcal{F}}^2 \leq |K|\sum_{x\in X}\langle\xi_\sigma\,|D_x^* D_x D_x^* D_x\xi_\sigma\,\rangle\ .$$

The expression on the right hand side can be estimated further, since we know that due to the Lemma **??** and the definition of Radon-Nikodym derivatives $\langle\xi_\sigma\,|\sum_{x\in X} D_x^* D_x\xi_\sigma\,\rangle = \omega_E(\mathbb{1}) \leq 1$. Hence, we find

$$\begin{aligned}\sum_{x\in X}\langle\xi_\sigma\,|D_x^* D_x D_x^* D_x\xi_\sigma\,\rangle &\leq \max_{x\in X}\|D_x^* D_x\|\,\langle\xi_\sigma\,|\sum_{x\in X} D_x^* D_x\xi_\sigma\,\rangle \\ &\leq 2^{\mathrm{D}_{\max}(\omega_{XE}||\tau_X\otimes\sigma_E)}\ ,\end{aligned}$$

where the last step follows from Equation (2.4). This yields the final bound

$$\Big\langle \|T_f(\omega_{XE}) - \frac{1}{|K|}\tau_K\otimes\omega_E\|\Big\rangle_{\mathcal{F}} \leq \sqrt{|K|\cdot 2^{\mathrm{D}_{\max}(\omega_{XE}||\tau_X\otimes\sigma_E)}}\,.$$

Finally, since our considerations are valid for all suitable $\sigma_E \in \mathcal{S}(\mathcal{M}_E)$, the assertion follows easily by taking the infimum over this set and inserting the definition of the min-entropy of classical quantum states. □

The result in Theorem 4.8.3 can be generalized to the smooth min-entropy.

**Corollary 4.8.4.** *For the same conditions as in Theorem 4.8.3 and $\epsilon \geq 0$, it holds that*

$$\left\langle \|T_f(\omega_{XE}) - \frac{1}{|K|}\tau_K \otimes \omega_E\| \right\rangle_{\mathcal{F}} \leq \sqrt{|K| \cdot 2^{-\mathrm{H}_{\min}^{\epsilon}(X|E)_\omega}} + 4\epsilon \ ,$$

*where $< \cdot >_{\mathcal{F}}$ denotes the expectation value over the family of two-universal hash functions and $\omega_E = \sum_x \omega_E^x \in \mathcal{S}(\mathcal{M}_E)$.*

*Proof.* The idea of the proof is the same as in [Ren05, TSSR10], but we repeat the argument for completeness. Using the definition of the smooth conditional min-entropy (Defintion 4.3.2), we know that for any $\delta > 0$ we can find $\bar{\omega}_{XE} \in \mathcal{B}^{\epsilon}(\omega_{XE})$ such that

$$\mathrm{H}_{\min}(X|E)_{\bar{\omega}} \geq \mathrm{H}_{\min}^{\epsilon}(X|E)_\omega - \delta \ .$$

By Lemma 3.4.4, $\bar{\omega}_{XE} \in \mathcal{B}^{\epsilon}(\omega_{XE})$ implies $\|\bar{\omega}_{XE} - \omega_{XE}\| \leq 2\epsilon$, and moreover, by the monotonicity of the norm under (quantum) channels, it follows that

$$\|T_f(\bar{\omega}_{XE}) - T_f(\omega_{XE})\| \leq 2\epsilon \ .$$

Using the triangle inequality and Theorem 4.8.3, we can conclude that

$$\begin{aligned}
\left\langle \|T_f(\omega_{XE}) - \frac{1}{|K|}\tau_K \otimes \omega_E\| \right\rangle_{\mathcal{F}} &\leq \left\langle \|(T_f(\bar{\omega}_{XE}) - \frac{1}{|K|}\tau_K \otimes \bar{\omega}_E\| \right\rangle_{\mathcal{F}} \\
&\quad + \left\langle \|T_f(\bar{\omega}_{XE}) - T_f(\omega_{XE})\| \right\rangle_{\mathcal{F}} + \|\bar{\omega}_E - \omega_E\| \\
&\leq \sqrt{|K| \cdot 2^{-\mathrm{H}_{\min}(X|E)_{\bar{\omega}}}} + 4\epsilon \\
&\leq \sqrt{|K| \cdot 2^{-\mathrm{H}_{\min}^{\epsilon}(X|E)_\omega + \delta}} + 4\epsilon \ .
\end{aligned}$$

Because this holds for any $\delta > 0$, the claim follows. □

The procedure in a privacy amplification step goes now as follows. Let us assume that that the initial state $\omega_{XE} \in \ell^1(X) \otimes \mathcal{S}(\mathcal{M}_E)$ is and that we want to generate an $\epsilon$-secure key. Then, we choose $K = \{0,1\}^{\ell}$ with

$$\ell = \sup_{0 \leq \epsilon' \leq \epsilon/4} \left\lfloor \mathrm{H}_{\min}^{\epsilon'}(X|E)_\omega - 2\log\frac{1}{\epsilon - 4\epsilon'} \right\rfloor , \tag{4.66}$$

and apply a hash function chosen from a two-universal family of $\{X, K\}$-hash functions according to the distribution $\mathbb{P}_{\mathcal{F}}$. A straightforward calculation shows that by Corollary 4.8.4, we get an $\epsilon$-secure key with respect to $\mathcal{M}_E$ of $\ell$ bits. This is optimal up to terms of order $O(\log 1/\epsilon)$. Let us first consider the ideal case.

**Proposition 4.8.5.** *Let $\mathcal{M}_E$ be a von Neumann algebra, $X, K$ sets of finite cardinality with $|K| \leq |X|$, and $f : X \mapsto K$. If a classical quantum state $\omega_{XE} = (\omega_E^x)_{x\in X}$ in $\mathcal{S}(\ell^\infty(X) \otimes \mathcal{M}_E)$ satisfies $T_f(\omega_{XE}) = \frac{1}{|K|}\tau_K \otimes \sigma_E$ for some $\sigma_E \in \mathcal{S}(\mathcal{M}_E)$, then*

$$\log |K| \leq \mathrm{H}_{\min}(X|E)_\omega \ .$$

*Proof.* The idea of the proof is exactly the same as in [TSSR10], but we repeat the argument for completeness. By the definition of the guessing probability (4.46), it is easily seen that the probability for the adversary to guess $K$ can not be smaller than the probability to guess $X$, that is,

$$p_{\text{guess}}(X|E)_\omega \leq p_{\text{guess}}(K|E)_\omega \, .$$

Furthermore, $p_{\text{guess}}(K|E) = 2^{-\log |K|}$ and by the operational interpretation of the min-entropy of classical quantum states as the guessing probability, Proposition 4.6.5, we conclude that

$$\mathrm{H}_{\min}(X|E)_\omega = -\log p_{\text{guess}}(X|E)_\omega \geq -\log p_{\text{guess}}(K|E)_\omega = \log |K| \ .$$

□

Hence, for any given classical quantum state $\omega_{XE}$, it is impossible to extract more than $\mathrm{H}_{\min}(X|E)_\omega$ bits of perfect key. We generalize this to the case of an $\epsilon$-perfect key (see also [Tom12])

**Corollary 4.8.6.** *Let $\mathcal{M}_E$ be a von Neumann algebra, $X, K$ sets of finite cardinality with $|K| \leq |X|$, and $f : X \mapsto K$. If a classical quantum state $\omega_{XE} = (\omega_E^x)_{x\in X}$ in $\mathcal{S}(\ell^\infty(X) \otimes \mathcal{M}_E)$ satisfies $\|T_f(\omega_{XE}) - \frac{1}{|K|}\tau_K \otimes \sigma_E\| \leq \epsilon$ for some $\sigma_E \in \mathcal{S}(\mathcal{M}_E)$, then*

$$\log |K| \leq \mathrm{H}_{\min}^{\sqrt{\epsilon}}(X|E)_\omega \ .$$

*Proof.* Let us denote $T_f(\omega_{XE})$ by $\omega_{f(X)E}$ and write for arbitrary states $\eta_1 \approx_\epsilon \eta_2$ if the purified distance between them satisfies $\mathcal{P}(\eta_1, \eta_2) \leq \epsilon$. According to Lemma 3.4.4, $\|\omega_{f(X)E} - \frac{1}{|K|}\tau_K \otimes \sigma_E\| \leq \epsilon$ then implies that

$$\omega_{f(X)E} \approx_{\sqrt{\epsilon}} \frac{1}{|K|}\tau_K \otimes \sigma_E \ .$$

Furthermore, by the definition of the smooth min-entropy, Definition 4.3.2, there exists for any $\delta > 0$ a classical-quantum state $\bar{\omega}_{KE} \in \mathcal{B}^{\sqrt{\epsilon}}(\omega_{f(X)E})$ with

$$\mathrm{H}_{\min}(K|E)_{\bar{\omega}} \geq \mathrm{H}_{\min}^{\sqrt{\epsilon}}(K|E)_\omega - \delta \ .$$

We define $\tilde{T}_f : \mathcal{N}(M_{|X|}) \to \ell^1(K)$ as the concatenation of the measurement in the diagonal basis $|x\rangle\langle x|$, $x \in X$, and applying the function $f$ on $x$. If we show that there exists a preimage $\bar{\omega}_{XE}$ of $\bar{\omega}_{KE}$ under $\tilde{T}_f$ which satisfies $\bar{\omega}_{XE} \approx_{\sqrt{\epsilon}} \omega_{XE}$, we obtain

$$\mathrm{H}_{\min}^{\sqrt{\epsilon}}(X|E)_\omega \geq \mathrm{H}_{\min}(X|E)_{\bar{\omega}} \geq \mathrm{H}_{\min}(K|E)_{\bar{\omega}} \geq \mathrm{H}_{\min}^{\sqrt{\epsilon}}(K|E)_\omega - \delta \geq \log |K| - \delta \ ,$$

where the second inequality is due to Proposition 4.8.5. Because this holds for any $\delta > 0$, the claim follows. Hence, it remains to prove the existence of such a state $\bar{\omega}_{XE}$. $\tilde{T}_f$ is a quantum channel, thus completely positive and unital, and it has a Stinespring dilation [Pau02], $V_X : \mathbb{C}^{|X|} \to \mathbb{C}^{|K|} \otimes \mathbb{C}^{|X|}$, which is given by $V_X = \sum_x |f(x)\rangle_K \otimes |x\rangle\langle x|_{X''}$. Here, the ancilla of the dilation is denoted by $X''$. Applied on a state $\sigma_{EX} \in \mathcal{S}(M_{|X|} \otimes \mathcal{M}_E)$, this means that $\tilde{T}_f(\sigma_{XE})$ is the restriction of the state $V_X^* \sigma_{XB} V_X(a) = \sigma_{XB}\big((V_X^* \otimes \mathbb{1}_E)x(V_X \otimes \mathbb{1})\big)$ onto system $K$ and $E$, where $a \in \mathcal{M}_X \otimes \mathcal{M}_E$. Now let $\omega_{XX'EE'}$ be a purification $(\pi, \mathcal{H}, |\xi_\omega\rangle)$ of the cq-state $\omega_{XE}$, where $\mathcal{H} = \mathbb{C}^{|X|} \otimes \mathbb{C}^{|X|} \otimes \mathcal{H}_{EE'}$. Then it follows that $|\xi_\omega^V\rangle = V_X \otimes \mathbb{1}_X \otimes \mathbb{1}_{EE'} |\xi_\omega\rangle$ is a purification of $\omega_{KE}$ in $\mathcal{H}' = \mathbb{C}^{|K|} \otimes \mathcal{H}$, since the restriction of $\omega_{KX''X'EE'} = V_X^* \omega_{XX'EE'} V_X$ onto system K and E is $\omega_{KE}$. Now we take $\bar{\omega}_{KE} \approx_{\sqrt{\epsilon}} \omega_{KE}$ as defined above and note that this implies $F(\omega_{KE}, \bar{\omega}_{KE}) \geq 1 - \epsilon$. We can chose the representation $\pi$ and the Hilbert space $\mathcal{H}_{EE'}$ in such a way that $\bar{\omega}_{KE}$ has a purification $|\xi_{\bar{\omega}}\rangle$ in $\mathcal{H}'$ (see Section 2.2.2). Then we obtain by the definition of the fidelity

$$F(\omega_{KE}, \bar{\omega}_{KE}) = \sup_{U \in \pi(\mathcal{M}_{KE})', \|U\| \leq 1} F_{\mathcal{B}(\mathcal{H}')}(|\xi_\omega^V\rangle, U|\xi_{\bar{\omega}}\rangle) \ .$$

Let $p = V_X^* V_X$ be the projector onto the image of $V_X$ and observe that for all $U \in \pi(\mathcal{M}_{KE})'$

$$F(p|\xi_\omega^V\rangle, U|\xi_{\bar{\omega}}\rangle) = F(|\xi_\omega^V\rangle, pU|\xi_{\bar{\omega}}\rangle) \ .$$

We can therefore conclude that the optimum is attained for a purification $|\xi_{\bar{\omega}}^{op}\rangle$ in $p\mathcal{H}'$. Because $V : \mathcal{H} \to p\mathcal{H}'$ is unitary, and the fidelity is invariant under unitary transformation, we obtain

$$\begin{aligned} 1 - \epsilon \leq F(\omega_{KE}, \bar{\omega}_{KE}) &= F_{\mathcal{B}(p\mathcal{H}')}(|\xi_\omega^V\rangle, |\xi_{\bar{\omega}}^{op}\rangle) \\ &= F_{\mathcal{B}(\mathcal{H})}((V_X^* \otimes \mathbb{1})|\xi_\omega\rangle, (V_X^* \otimes \mathbb{1})|\xi_{\bar{\omega}}^{op}\rangle) \\ &\leq F(\omega_{XE}, \bar{\omega}_{XE}) \, . \end{aligned}$$

where $\bar{\omega}_{XE}$ is the restriction onto $\mathcal{M}_{XE}$ of the state corresponding to $(V_X^* \otimes \mathbb{1})|\xi_{\bar{\omega}}^{op}\rangle$. Note that the last equality is due to the monotonicity of the fidelity (3.6). By construction $\tilde{T}_f$ maps $\bar{\omega}_{XE}$ to $\bar{\omega}_{KE}$ and therefore we have found the desired state. □

## 4.9. Classical Data Compression with Quantum Side Information

The coding question of how much a classical random variable can be compressed is one of the most fundamental tasks in classical information theory, and the answer goes back to the pioneering work of Shannon [Sha48] (see Section 1.3). We consider here the situation in which a classical random variable $X$ in Alice's lab is correlated with the system $B$ in Bob's lab, and ask how many bits Alice needs to send to Bob, such that he can recover $X$. In the asymptotic limit of an i.i.d. source the problem is given by the so-called classical Slepian Wolf theorem [SW71] if the $B$ system is classical and generalized by Devetak and Winter for the quantum case [DW03]. In

both cases the optimal achievable rate is given by the conditional Shannon entropy $H(X|B)$ where $B$ can be either classical or quantum. The optimal characterization for the one-shot case was recently given in [RR12] and linked to the conditional smooth max-entropy.

All theses results assume explicitly that the quantum system can be modeled on a finite-dimensional Hilbert space. We show that these result carry over to the case when that Bob's observable algebra is given by a general von Neumann algebra. This is of particular interest as this allows for instance to restrict Bob's measurement by symmetry constraints rather then just considering all possible observables on a Hilbert space. The discussion as well as the proof follow similar reasoning as in [RR12].

Let $\omega_{XB} \in \mathcal{S}(\ell^\infty_{|X|} \otimes \mathcal{M}_B)$ be the classical-quantum state shared between Alice and Bob. By $X$ we denote the classical random variable and by the von Neumann algebra $\mathcal{M}_B$ the quantum system at Bob's site. A one-way classical communication protocol to transmit the random variable $X$ from Alice to Bob then consists of a classical encoding map $\mathcal{E} : \ell^1(X) \to \ell^1(C)$ on Alice's side, and a decoding map $\mathcal{D} : \ell^1(C) \otimes \mathcal{N}(\mathcal{M}_B) \to \ell^1(X)$ on Bob's side, where the classical alphabet $C$ specifies the number of bits, $\log|C|$, that are transmitted. The decoding map can be written as $\mathcal{D} = \{\mathcal{D}^c\}_{c\in C}$, where the quantum channel $\mathcal{D}^c$ onto the classical outcome $X$ can be described by a POVM $\{D^c_x\}_{x\in X}$. In particular, this means that if Bob receives the value $c \in C$ from Alice he performs the measurement $\{D^c_x\}$, and declares the measurement outcome to be his guess of the value hold by Alice. In the following every such protocol is specified by the triple $(\mathcal{E}, \mathcal{D}, C)$.

**Definition 4.9.1.** *Let $\mathcal{M}_B$ be a von Neumann algebra, $X$ a set of finite cardinality $|X|$, and $\omega_{XB} \in \mathcal{S}(\ell^\infty_{|X|} \otimes \mathcal{M}_B)$. Then, the error probability of a protocol $(\mathcal{E}, \mathcal{D}, C)$ for $\omega_{XB}$ is given by*

$$p_{\mathrm{err}}(\omega_{XB}; \mathcal{E}, \mathcal{D}) = 1 - \sum_x \omega^x_B(D^{\mathcal{E}(x)}_x) \ , \tag{4.67}$$

*and a protocol is called $\epsilon$-reliable if $p_{\mathrm{err}}(\omega_{XB}; \mathcal{E}, \mathcal{D}) \leq \epsilon$.*

The main result of this section is the following quantification of the achievable error probability, as it was shown for the finite-dimensional case in [RR12].

**Theorem 4.9.2.** *Let $\mathcal{M}_B$ be a von Neumann algebra, $X$ a set of finite cardinality $|X|$, and $\omega_{XB} \in \mathcal{S}(\ell^\infty_{|X|} \otimes \mathcal{M}_B)$. Then there exist for any alphabet $C$ with $|C| \leq |X|$, an encoding map $\mathcal{E}$ and a decoding map $\mathcal{D}$, such that the protocol $(\mathcal{E}, \mathcal{D}, C)$ satisfies*

$$p_{\mathrm{err}}(\omega_{XB}; \mathcal{E}, \mathcal{D}) \leq \sqrt{\frac{1}{|C|} \cdot 2^{\mathrm{H}_{\max}(X|B)_\omega + 3}} \ . \tag{4.68}$$

The protocol for which the bound is achieved, is in complete analogy to the finite-dimensional version [RR12]. We start by sketching the idea. For the encoding we employ the property of a family of two-universal hash functions $\mathcal{F}$ (Definition 4.8.2). In particular, we show that the averaged error probability over a family of two-universal hash functions $\mathcal{F}$ is bounded as in Equation (4.68). From this we can then

conclude that there exists a function $f \in \mathcal{F}$ suitable as an encoding map. Now assume that Alice holds the value $x$ and sends the message $c = f(x)$ to Bob. Bob then knows that $x \in f^{-1}(c)$, and applies as the decoding map a measurement which is appropriate to distinguish between the states $\omega_B^x$ for $x \in f^{-1}(c)$. For that, he uses a POVM $\{D^c_{x';f}\}_{x' \in X}$ with $D^c_{x';f} = 0$ if $x' \notin f^{-1}(c)$, which we choose as an adapted 'pretty good measurement' [HW94] to distinguish the ensemble $\{\omega_B^x\}_{x \in f^{-1}(c)}$.

The proof is based on the two following technical results. The first is an operator inequality proven in [HN03].

**Lemma 4.9.3.** *[HN03, Lemma 2] Let $\mathcal{M}$ be a von Neumann algebra, $S, T \in \mathcal{M}_+$, and $S \leq \mathbb{1}$. If $(S+T)$ is invertible in $\mathcal{M}$,[10] then it holds that*

$$\mathbb{1} - (S+T)^{-\frac{1}{2}} S (S+T)^{-\frac{1}{2}} \leq 2(\mathbb{1} - S) + 4T. \tag{4.69}$$

The next lemma was first proven in the finite-dimensional setting [ACMT+07], and then generalized to von Neumann algebras [Oga10].

**Lemma 4.9.4.** *Let $\mathcal{M}$ be a von Neumann algebra, $\phi, \eta \in \mathcal{S}_{\leq}(\mathcal{M})$, $s_+$ the support projection onto the positive part of $\phi - \eta$, and $s_- = \mathbb{1} - s_+$. Then*

$$\phi(s_-) + \eta(s_+) \leq \mathcal{F}(\phi, \eta)^{\frac{1}{2}} \ . \tag{4.70}$$

*Proof.* The statement follows directly from [Oga10, Corollary 1.1]. In order to see this we note that the relative modular operator $\Delta_{\eta,\phi}$ in a standard form $\{\mathcal{M}, \mathcal{H}, \mathcal{P}, J\}$ of $\mathcal{M}$ satisfies $\Delta_{\eta,\phi}|\xi_\phi\rangle = |\xi_\eta\rangle$ for $|\xi_\phi\rangle, |\xi_\eta\rangle \in \mathcal{P}$ purifications of $\phi$ and $\eta$, respectively. Hence, by the definition of the generalized fidelity

$$\|\Delta_{\eta,\phi}^{1/2} \xi_\phi\| = \langle \xi_\phi \, | \Delta_{\eta,\phi} \xi_\phi \rangle = \langle \xi_\phi \, | \xi_\eta \rangle \leq \mathcal{F}(\phi, \eta)^{\frac{1}{2}} \ .$$

Furthermore, we observe that

$$\begin{aligned} \phi(\mathbb{1}) + \eta(\mathbb{1}) - |\phi - \eta|(\mathbb{1}) &= \phi(\mathbb{1}) + \eta(\mathbb{1}) - (\phi - \eta)(s_+) + (\phi - \eta)(\mathbb{1} - s_+) \\ &= 2(\phi(s_-) + \eta(s_+)) \ . \end{aligned}$$

□

We are now ready to prove the main result of this section.

*Proof. (Theorem 4.9.2)* The proof follows the same arguments as in the finite-dimensional case [RR12]. Let $\{\mathcal{F}, \mathbb{P}_\mathcal{F}\}_{X,C}$ be a family of two-universal hash functions from the alphabet $X$ onto $C$ (Definition 4.8.2). We define $\Pi_x$ to be the support projection onto the positive part of $\omega_B^x - 2^{-m-1}\omega_B$, where $\omega_B = \sum_x \omega_B^x$. Note that $\Pi_x \in \mathcal{M}_B$ for all $x \in X$.

Since the Hilbert space $\mathcal{H}_B$ on which $\mathcal{M}_B$ acts is in general infinite-dimensional, we have to introduce some regularizing terms, parameterized in $\epsilon$, in order to apply

[10] In the finite-dimensional case this requirement can be neglected by taking the inverse on the support of $S + T$.

Lemma 4.9.3.[11] For any $f \in \mathcal{F}$ and $c \in C$, we define for $\epsilon > 0$ and $x \in f^{-1}(c)$ the two families of operators

$$S^c_{x;f}(\epsilon) := \frac{\Pi_x + \epsilon \mathbb{1}}{1 + \epsilon |f^{-1}(c)|}$$

and

$$T^c_{x;f}(\epsilon) := \Big( \sum_{x' \in X} \Pi_{x'} \delta_{x'c} + \epsilon |f^{-1}(c)| \mathbb{1} \Big) - S^c_{x;f}(\epsilon) \, .$$

It is straightforward to see that $S^c_{x;f}(\epsilon) + T^c_{x;f}(\epsilon)$ is invertible for any $\epsilon > 0$ and $x \in f^{-1}(c)$. By the help of these operators, we now define an $\epsilon$-family of decoding measurements $\{D^c_{x;f}(\epsilon)\}_{x \in X}$ conditioned on the fact that the encoding map is $f \in \mathcal{F}$ and the obtained message is $c$ via

$$D^c_{x;f}(\epsilon) = \big(S^c_{x;f}(\epsilon) + T^c_{x;f}(\epsilon)\big)^{-\frac{1}{2}} S^c_{x;f}(\epsilon) \big(S^c_{x;f}(\epsilon) + T^c_{x;f}(\epsilon)\big)^{-\frac{1}{2}} \, ,$$

if $x \in f^{-1}(c)$ and $D^c_{x;f}(\epsilon) = 0$ else. For any $\epsilon > 0$ it is true that $D^c_{x;f}(\epsilon)$ is a positive operator in $\mathcal{M}_B$ and $\sum_x D^c_{x;f}(\epsilon) \leq \mathbb{1}$. Hence, $\{D^c_{x;f}(\epsilon)\}_{x \in X}$ defines a valid but possibly incomplete measurement. On the other side, one can check that by setting $S = S^c_{x;f}(\epsilon)$ and $T = T^c_{x;f}(\epsilon)$ the conditions in Lemma 4.9.3 are satisfied, from which we obtain that

$$\mathbb{1} - D^c_{x;f}(\epsilon) \leq 2(\mathbb{1} - S^c_{x;f}(\epsilon)) + 4 T^c_{x;f}(\epsilon) \, . \tag{4.71}$$

Now, the idea is to define the particular measurements $D^c_{x';f}$ of the decoding map as the limit of $D^c_{x;f}(\epsilon)$ for $\epsilon \to 0$. For that, we consider the sequence $\{D^c_{x;f}(1/n)\}_{n=1}^{\infty}$ in $\mathcal{M}_B$ and observe that it is bounded due to the fact that the elements are measurement operators. In particular, the sequence lies in the unit sphere of $\mathcal{B}(\mathcal{H}_B)$. We can therefore apply the Banach-Alaoglu theorem [RS78, Theorem VI.26], which says that there exists a $\sigma$-weakly converging subsequence $\Lambda \subset \mathbb{N}$ of $\{D^c_{x;f}(1/n)\}_{n=1}^{\infty}$. The limit of this subsequence is now used to define the appropriate measurements at the decoder

$$D^c_{x;f} = \sigma - \lim_{\Lambda \ni n \to \infty} D^c_{x;f}(1/n) \, .$$

Since $\mathcal{M}_B$ is $\sigma$-weakly closed, we know that $D^c_{x;f} \in \mathcal{M}_B$, and hence defines a possible measurement in $\mathcal{M}_B$. Because positivity is preserved under taking the $\sigma$-weak limit, we obtain from Equation (4.71) that

$$\mathbb{1} - D^c_{x;f} \leq 2(\mathbb{1} - \Pi_x) + 4 \sum_{x' \notin x} \Pi_{x'} \delta_{x'c} \, , \tag{4.72}$$

for all $x \in X$. The right hand side of the inequality is obtained by taking the $\sigma$-weak limit of $S^c_{x;f}(\epsilon)$ and $T^c_{x;f}(\epsilon)$. If we denote the decoding map corresponding to the measurements $\{D^c_{x;f}\}_{x \in X}$ by $\mathcal{D}^c_f$, we can bound the expectation value of the error

[11] This is in contrast to the finite-dimensional case, where Lemma 4.9.3 is applied directly.

via

$$\begin{aligned}\Big\langle p_{\mathrm{err}}(\omega_{XB}, f, \mathcal{D}_f^c)\Big\rangle_{\mathcal{F}} &= \Big\langle \sum_x \omega_B^x (\mathbb{1} - D_{x;f}^{f(x)})\Big\rangle_{\mathcal{F}} \\ &\leq \sum_x \omega_B^x \Big(2(\mathbb{1} - \Pi_x) + \frac{4}{|C|}\sum_{x'} \Pi_{x'}\Big) \\ &= 2\Big[\sum_x \omega_B^x(\mathbb{1} - \Pi_x) + \frac{2}{|C|}\sum_x \omega_B(\Pi_x)\Big] \\ &= 2\Big[\omega_{XB}\Big((\mathbb{1} - \Pi_x)_{x\in X}\Big) + \frac{2}{|C|}\tau_X \otimes \omega_B\Big((\Pi_x)_{x\in X}\Big)\Big] \ .\end{aligned}$$

The first inequality is obtained via the inequality (4.72) and the defining property (4.60) of a family of two-universal hash functions. Finally, we apply Lemma 4.9.4 with $\phi = \omega_{XB}$ and $\eta = 2/|C|\tau_X \otimes \omega_B$ to obtain

$$\Big\langle p_{\mathrm{err}}(\omega_{XB}, f, \mathcal{D}_f^c)\Big\rangle_{\mathcal{F}} \leq 2F\big(\omega_{XB}, \frac{2}{|C|}\tau_X \otimes \omega_B\big)^{1/2} \leq \sqrt{\frac{1}{|C|}\cdot 2^{\mathrm{H}_{\max}(X|B)_\omega + 3}} \ ,$$

where the last inequality is due to the operational interpretation of the max-entropy as shown in Theorem 4.6.6. This shows the existence of a suitable $f \in \mathcal{F}$ for which the bound is achieved, and thus completes the proof. □

This theorem can be extended to the smooth max-entropy.

**Corollary 4.9.5.** *Let $\mathcal{M}_B$ be a von Neumann algebra, $X$ a set of finite cardinality $|X|$, $\omega_{XB} \in \mathcal{S}(\ell^\infty_{|X|} \otimes \mathcal{M}_B)$, and $\epsilon \geq 0$. Then there exist for any alphabet $C$ with $|C| \leq |X|$, an encoding map $\mathcal{E}$ and a decoding map $\mathcal{D}$, such that the protocol $(\mathcal{E}, \mathcal{D}, C)$ satisfies*

$$p_{\mathrm{err}}(\omega_{XB}; \mathcal{E}, \mathcal{D}) \leq \sqrt{\frac{1}{|C|}\cdot 2^{\mathrm{H}^\epsilon_{\max}(X|B)_\omega + 3}} + 2\epsilon \ . \tag{4.73}$$

*Proof.* The idea of the proof is exactly the same as in [RR12], but we repeat the argument for completeness. In the following we fix the alphabet $C$. Let $\mathbb{P}^\omega_{(\mathcal{E},\mathcal{D})}(x, x')$ be the joint probability distribution of the value $x$ hold by Alice and the guess of Bob $x'$, if they use the protocol $(\mathcal{E}, \mathcal{D})$, and the source is given by $\omega_{XB}$. A straightforward computation shows that

$$p_{\mathrm{err}}(\omega_{XB}, \mathcal{E}, \mathcal{D}) = \frac{1}{2}\|(\omega_B^x(\mathbb{1})\delta_{xx'})_{x,x'} - (\mathbb{P}^\omega_{(\mathcal{E},\mathcal{D})}(x, x'))_{x,x'}\|_{\ell^1(X\times X)} \ .$$

For any $\delta > 0$, we can find a classical-quantum state $\bar\omega_{XB} \in \mathcal{B}^\epsilon(\omega_{XB})$ such that $\mathrm{H}^\epsilon_{\max}(X|B)_\omega \geq \mathrm{H}_{\max}(X|B)_{\bar\omega} - \delta$. If $(\bar{\mathcal{E}}, \bar{\mathcal{D}})$ is a protocol for which Theorem 4.9.2 applies for the state $\bar\omega_{XB}$, we can use the triangle inequality to estimate

$$\begin{aligned}p_{\mathrm{err}}(\omega_{XB}, \bar{\mathcal{E}}, \bar{\mathcal{D}}) &\leq p_{err}(\omega_{XB}, \bar{\mathcal{E}}, \bar{\mathcal{D}}) + \frac{1}{2}\|(\omega_B^x(\mathbb{1}))_x - (\bar\omega_B^x(\mathbb{1}))_x\|_{\ell^1(X)} \\ &\quad + \frac{1}{2}\|\mathbb{P}^{\bar\omega}_{(\bar{\mathcal{E}},\bar{\mathcal{D}})}(x, x'))_{x,x'} - \mathbb{P}^{\bar\omega}_{(\bar{\mathcal{E}},\bar{\mathcal{D}})}(x, x'))_{x,x'}\|_{\ell^1(X\times X)} \\ &\leq \sqrt{\frac{1}{|C|}\cdot 2^{\mathrm{H}^\epsilon_{\max}(X|B)_\omega + \delta + 3}} + \|\bar\omega_{XB} - \omega_{XB}\| \ ,\end{aligned}$$

where we used in the last inequality that the trace distance can only decrease if one applies a quantum channel. Using Lemma 3.4.4 we can finally bound $\|\bar{\omega}_{XB}-\omega_{XB}\| \leq 2\epsilon$, from which the result then follows. □

Let us assume that the state shared between Alice and Bob is given by $\omega_{XB} \in \mathcal{S}(\ell^\infty(X)\otimes\mathcal{M}_B)$ and that they aim to transmit the Alice's information to Bob with success probability higher than $1-\epsilon$. Then, Corollary 4.9.5 means that theoretically, there is a decoding and encoding strategy such that the number of bits Alice has to send is given by

$$\ell = \inf_{0\leq\epsilon'\leq\epsilon/2} \left\lceil \mathrm{H}_{\max}^{\epsilon'}(X|B)_\omega + 2\log\frac{1}{\epsilon-2\epsilon'} + 6 \right\rceil . \tag{4.74}$$

This length is optimal up to a term of order $O(\log 1/\epsilon)$.

**Lemma 4.9.6.** *Let $\mathcal{M}_B$ be a von Neumann algebra, $X$ a set of finite cardinality $|X|$, $\omega_{XB} \in \mathcal{S}(\ell^\infty_{|X|}\otimes\mathcal{M}_B)$, and $(\mathcal{E},\mathcal{D},C)$ be protocol with $p_{\mathrm{err}}(\omega_{XB},\bar{\mathcal{E}},\bar{\mathcal{D}}) \leq \epsilon$ for some $\epsilon > 0$. Then*

$$\log|C| \geq \mathrm{H}_{\max}^{\sqrt{2\epsilon}}(X|B)_\omega \ . \tag{4.75}$$

*Proof.* The idea of the proof is exactly the same as in [RR12], but we repeat the argument for completeness. Because of $p_{\mathrm{err}}(\omega_{XB},\bar{\mathcal{E}},\bar{\mathcal{D}}) \leq \epsilon$, we know that $\mathbb{P}^\omega_{(\mathcal{E},\mathcal{D})}(x,x')$, as defined in the proof of Corollary 4.9.5, satisfies $\|\mathbb{P}^\omega_{(\mathcal{E},\mathcal{D})} - \mathbb{P}_{\mathrm{id}}\|_{\ell^1(X\times X)} \leq \epsilon$, where $\mathbb{P}_{\mathrm{id}}(x,x') = \omega_B^x(\mathbb{1})\delta_{xx'}$. Bounding the purified distance by the $\ell^1$-norm (Lemma 3.4.4) and using that $\mathrm{H}_{\max}(X|X')_{\mathbb{P}_{\mathrm{id}}} = 0$ we obtain

$$\mathrm{H}_{\max}^{\sqrt{2\epsilon}}(X|BC)_\omega \leq \mathrm{H}_{\max}^{\sqrt{2\epsilon}}\left(X|X'\right)_\omega \leq \mathrm{H}_{\max}\left(X|X'\right)_{\mathbb{P}_{\mathrm{id}}} = 0 \ ,$$

where the data processing inequality (4.18) is applied in the first inequality. For any $\delta > 0$ we can find a classical-quantum state $\bar{\omega}_{XBC} \in \mathcal{B}^{\sqrt{2\epsilon}}(\omega_{XBC})$ such that $\mathrm{H}_{\max}^{\sqrt{2\epsilon}}(X|BC)_\omega \geq \mathrm{H}_{\max}(X|BC)_{\bar{\omega}} - \delta$. Hence, with Lemma 4.5.8

$$\log|C| \geq \mathrm{H}_{\max}(X|B)_{\bar{\omega}} - \delta \geq \mathrm{H}_{\max}^{\sqrt{2\epsilon}}(X|B)_\omega - \delta \ ,$$

where the last inequality is due to $\mathcal{P}(\omega_{XB},\bar{\omega}_{XB}) \leq \sqrt{2\epsilon}$. Because this holds for all $\delta > 0$, we found the desired result. □

# 5. Uncertainty Relation for Position and Momentum Operators

## 5.1. Introduction

The idea of the uncertainty principle goes back to an exposition by Heisenberg in 1927 [Hei25]. The first rigorous formulation for position and momentum operators $Q$ and $P$ was stated in terms of the standard deviations of their distributions, $\sigma_Q = \sqrt{\langle Q^2 - \langle Q\rangle^2\rangle}$ and $\sigma_P = \sqrt{\langle P^2 - \langle P\rangle^2\rangle}$, and reads [Ken27, Hei27]

$$\sigma_Q \sigma_P \geq \frac{1}{2}\,. \tag{5.1}$$

The units are chosen such that $\hbar = 1$. But the formulation of the uncertainty principle by means of the standard deviation has some serious drawbacks (see for instance [Deu83, BBR11]), which are removed by using entropies as measures of uncertainty. The first entropic uncertainty relation in terms of the differential Shannon entropy [Sha48] was derived by Hirschman in [HJ57] and later improved in [Bec75, BBM75] for pure states. If $H(Q)$ and $H(P)$ denote the differential Shannon entropy of the position and the momentum distribution, the inequality is given by

$$H(Q) + H(P) \geq \log c\,, \tag{5.2}$$

for $c = 2\pi$ for mixed states and $c = e\pi$ for pure states. The uncertainty relation for mixed states can be further strengthened to [FL11]

$$H(Q) + H(P) \geq \log 2\pi + H(\rho)\,, \tag{5.3}$$

where $H(\rho)$ denotes the von Neumann entropy of the measured state.

In [BB06] an entropic uncertainty relation for dual pairs of Rényi entropies $(1/\alpha + 1/\beta)$ is presented. For the unconditional min- and max-entropy, that is, $\alpha = \infty$ and $\beta = 1/2$, it is given by

$$\mathrm{H}_{\min}(Q) + \mathrm{H}_{\max}(P) \geq \log 2\pi\,. \tag{5.4}$$

We introduce in Section 5.2 the concept of a conditional differential min- and max-entropy and show that the same inequality holds for arbitrary side-information (see Theorem 5.3.3).

The idea is to start first with the experimentally relevant setting of a finite measurement accuracy (c.f. [BBR11]). We introduce a finite spacing of the real line which quantifies the precision of the used measurement devices. This leads to a discretized outcome distribution for which the uncertainty relation derived in Section 4.7 applies. The measurement overlap can be computed using Fourier theory [LP64]. By an approximation statement for the differential min- and max-entropies derived in Section 5.2.2, the continuous version is then obtained by letting the measurement precision go to infinity.

## 5.2. Min- and Max-Entropy for Continuous Variables

### 5.2.1. Definition of Differential Min- and Max-Entropy

Before we define the differential min- and max-entropies, we discuss the mathematical framework needed to describe classical quantum states for continuous distributions. We again use the framework of von Neumann algebras as the basic mathematical object to describe such systems. In the following, $X$ stands for a measure space given by a triple $(X, \Sigma, \mu)$, where $\Sigma$ is a $\sigma$-algebra of subsets of $X$ and $\mu$ a measure. In the following, we always assume that $X$ is locally compact and $\mu$ is a Radon measure. For a survey about measure theory see for instance [RS78]. Every abelian von Neumann algebra can be associated to $L^\infty(X)$ for a suitable measure space $X$ (see for instance [Tak01, Chapter 3.1]). Here, we denote by $\mathcal{L}^\infty(X)$ the algebra of the measurable functions $f : X \to \mathbb{C}$ together with point wise multiplication which are bounded with respect to the norm

$$\|f\|_{\mathcal{L}^\infty(X)} = \mathrm{essup}_x |f(x)| \; . \tag{5.5}$$

$L^\infty(X)$ is then obtained as the quotient $\mathcal{L}^\infty(X)/\sim$ where $f \sim g$ if $\|f-g\|_{\mathcal{L}^\infty(X)} = 0$. We are interested in the combination of a classical and a quantum system. This is modeled by the tensor product $L^\infty(X) \otimes \mathcal{M}_B$, $X$ is a measure space and $\mathcal{M}_B$ a von Neumann algebra describing the quantum system. It is now useful to think about operators on $L^\infty(X) \otimes \mathcal{M}_B$ as functions $E : X \to \mathcal{M}_B$. Here, $E \in L^\infty(X, \mathcal{M}_B)$ is just a measurable function which takes values in the von Neumann algebra $\mathcal{M}_B$ with bounded supremum norm

$$\|E\|_{L^\infty(X,\mathcal{M}_B)} := \mathrm{essup_x}\|\mathrm{E(x)}\|; , \tag{5.6}$$

where $\|\cdot\|$ is the norm on $\mathcal{M}_B$. Note that most of the measure theory can be generalized to functions which take values in a Banach space. In [Tak01, Chapter 4.7] it is shown that $L^\infty(X, \mathcal{M}_B)$ is isomorphic to $L^\infty(X) \otimes \mathcal{M}_B$. The normal functionals on it are given by $L^1(X) \otimes \mathcal{N}(\mathcal{M}_B) \simeq L^1(X, \mathcal{N}(\mathcal{M}_B))$, where the latter denote the equivalence classes[1] of measurable functions $\eta : X \to \mathcal{N}(\mathcal{M}_B)$ equipped with the norm

$$\|\eta\|_{L^1(X,\mathcal{N}(\mathcal{M}_B))} := \int_X \|\eta^{(x)}\| \mathrm{d}\mu(x) \; . \tag{5.7}$$

It is convenient to write the arguments for functions which take value in $\mathcal{N}(\mathcal{M}_B)$ as $x \mapsto \eta^{(x)}$. We use the abbreviation $\mathcal{M}_{XB}$ for classical-quantum systems $L^\infty(X) \otimes \mathcal{M}_B$. Since the norms defined in Equation (5.6) and (5.7) are the canonical norms on $\mathcal{M}_{XB}$ and $\mathcal{S}(\mathcal{M}_{XB})$, we omit the subscribed whenever it is clear from the context.

Note that abelian algebras on separable Hilbert spaces are generated by selfadjoint operators [Tak01, Chapter 3.1]. The case of a discrete classical variable as discussed in Section 3.3 corresponds to an operator with a point spectrum. If there are continuous parts of the spectrum the classical alphabet is continuous. Let us for instance take the position operator $Q$ on the Hilbert space $\mathcal{H} = L^2(\mathbb{R})$. The spectrum of $Q$

[1] As in the case of $L^\infty(X)$ we obtain $L^1(X)$ by identifying functions which are similar almost every where, that is, up to a set of measure 0.

is $\mathbb{R}$ and using the functional calculus it can be written with respect to a projective POVM $\mu_Q$ as

$$Q = \int_{\mathbb{R}} x \mathrm{d}\mu_{\mathrm{Q}}(\mathrm{x}). \tag{5.8}$$

We are now ready to define the differential conditional min- and max-entropies. They are obtained by straightforward generalizations of their operational interpretations given in Equation 4.47 and 4.52.

**Definition 5.2.1.** *Let $\mathcal{M}_{XB} = L^\infty(X) \otimes \mathcal{M}_B$ with $\mathcal{M}_B$ a von Neumann algebra and $(X, \Sigma, \mu)$ a locally compact measure space $X$ with Radon measure $\mu$, and $\omega_{XB} \in \mathcal{S}_\leq(\mathcal{M}_{XB})$. The* conditional min-entropy *of $X$ given $B$ is defined as*

$$\mathrm{H}_{\min}(X|B)_\omega = -\log \sup \left\{ \int_X \omega_B^{(x)}(E_B(x)) \mathrm{d}\mu(\mathrm{x}) : \mathrm{E} \in \mathrm{L}^\infty(\mathrm{X}, \mathcal{M}_{\mathrm{B}})_+ \right\} . \tag{5.9}$$

*Furthermore, the* conditional max-entropy *of $X$ given $B$ is defined as*

$$\mathrm{H}_{\max}(X|B)_\omega = 2 \log \sup \left\{ \int_X \sqrt{F(\omega_B^{(x)}, \sigma_B)} \mathrm{d}\mu(\mathrm{x}) : \sigma_{\mathrm{B}} \in \mathcal{S}(\mathcal{M}_{\mathrm{B}}) \right\} . \tag{5.10}$$

Note that the conditional min-entropy is well defined since $x \mapsto \omega^{(x)}(E(x))$ is measurable [Tak01, Chapter 4.7] and since the state is positive the integral can be bounded by

$$\int \omega_B^{(x)}(E_B(x)) \mathrm{d}\mu(\mathrm{x}) \leq \|\mathrm{E}\| \int_{\mathrm{X}} \|\omega_{\mathrm{B}}^{(\mathrm{x})}\| \mathrm{d}\mu(\mathrm{x}) = \|\mathrm{E}\| \cdot \|\omega_{\mathrm{XB}}\| .$$

Since $F(\omega_B^{(x)}, \sigma_B) \leq \|\omega_B^{(x)}\|$, we find that $x \mapsto \sqrt{F(\omega_B^{(x)}, \sigma_B)}$ is measurable and[2]

$$\int_X \sqrt{F(\omega_B^{(x)}, \sigma_B)} \mathrm{d}\mu(\mathrm{x}) \leq \int_{\mathrm{X}} \|\omega_{\mathrm{B}}^{(\mathrm{x})}\| \mathrm{d}\mu(\mathrm{x}) .$$

Note that in the case where $\mu$ is a singular point measure, we retrieve the min- and max-entropy of a classical quantum state as given in Equation 4.47 and 4.52. In the case of trivial side information, i.e., $\mathcal{M}_B = \mathbb{C}$ and $\omega(x) \in \mathcal{L}^1(X)$, we find that $H_{\min}(X)_\omega = -\log \|\omega(x)\|_{\mathcal{L}^\infty(X)}$ and $H_{\max}(X)_\omega = 2 \log \int \sqrt{\omega(x)} \mathrm{d}\mu(\mathrm{x}) = \log \|\omega(\mathrm{x})\|_{\mathcal{L}^{1/2}(\mathrm{X})}$. These correspond to the differential Rényi entropy of order $\infty$ and $1/2$.

Smooth versions of the above entropies are given by a variation over close states. Note that the definitions of distance measures in Section 3.4 are introduced for general von Neumann algebras why they also hold for continuous variables. The only difference is that the embedding of the classical system to the quantum system is different such that the smoothing set has to be adjusted.

**Definition 5.2.2.** *Let $\mathcal{M}_{XB} = \mathcal{L}^\infty(X) \otimes \mathcal{M}_B$ with $\mathcal{M}_B$ a von Neumann algebra and $X$ a measure space, $\omega_{XB} \in \mathcal{S}_\leq(\mathcal{M}_{XB})$ and $\varepsilon \geq 0$. Furthermore, we define the*

[2] Note that this is simply the data processing inequality.

*smoothing set* $\mathcal{B}^{\varepsilon}_{cq}(\omega_{XB}) := \{\sigma_{XB} \in \mathcal{S}_{\leq}(\mathcal{M}_{XB}) \,|\, \mathcal{P}(\omega_{XB}, \sigma_{XB}) \leq \varepsilon\}$. *The smooth differential conditional min-entropy of* $X$ *given* $B$ *is defined as*

$$H^{\varepsilon}_{\min}(X|B)_{\omega} = \sup_{\bar{\omega} \in \mathcal{B}^{\varepsilon}_{cq}(\omega_{XB})} H_{\min}(X|B)_{\bar{\omega}} \ ,$$

*and the smooth differential conditional max-entropy of* $X$ *given* $B$ *as*

$$H^{\varepsilon}_{\max}(X|B)_{\omega} = \inf_{\bar{\omega} \in \mathcal{B}^{\varepsilon}_{cq}(\omega_{XB})} H_{\max}(X|B)_{\bar{\omega}} \ .$$

The smooth differential min- and max-entropies satisfy the data processing inequality (c.f. Proposition 4.5.1)

**Proposition 5.2.3.** *Let* $\mathcal{M}_{XBC} = \mathcal{L}^{\infty}(X) \otimes \mathcal{M}_{BC}$ *with* $X$ *a measure space and* $\mathcal{M}_{BC} = \mathcal{M}_B \vee \mathcal{M}_C$ *a composite system of two commuting von Neumann algebras. For all states* $\omega_{XBC} \in \mathcal{S}_{\leq}(\mathcal{M}_{XBC})$ *follows that*

$$\begin{aligned} H^{\varepsilon}_{\min}(X|BC)_{\omega} &\leq H^{\varepsilon}_{\min}(X|B)_{\omega} \\ H^{\varepsilon}_{\max}(X|BC)_{\omega} &\leq H^{\varepsilon}_{\max}(X|B)_{\omega} \, . \end{aligned}$$

*Proof.* We consider first the case $\epsilon = 0$. The inequality for the min-entropy is obtained by using that any $E \in \mathrm{POVM}(\mathrm{X}, \mathcal{M}_{\mathrm{B}})$ lies also in $\mathrm{POVM}(\mathrm{X}, \mathcal{M}_{\mathrm{BC}})$ and $\omega^x_B(E_x) = \omega^x_{BC}(E_x)$. For the max-entropy one exploits the fact that the fidelity can only increase when restricting to a subsystem, that is, $F(\omega_{BC}, \sigma_{BC}) \leq F(\omega_B, \sigma_B)$. Let us turn to the case of $\epsilon > 0$. Using that $\mathcal{P}(\omega_{XBC}, \bar{\omega}_{XBC}) \geq \mathcal{P}(\omega_{XB}, \bar{\omega}_{XB})$ [], we find the inequality for the smooth min-entropy directly from the $\epsilon = 0$ case. It is little more involved for the max-entropy as we have to take the infimum over the smoothing set. Note that for all $\delta > 0$, there exists a $\bar{\omega}_{XB} \in \mathcal{B}^{\varepsilon}_{cq}(\omega_{XB})$ such that $H^{\varepsilon}_{\max}(X|B)_{\omega} + \delta \geq H_{\max}(X|B)_{\bar{\omega}} \geq H_{\max}(X|BC)_{\bar{\omega}}$ where the last equation holds for any norm preserving positive extension $\bar{\omega}_{XBC}$ of $\bar{\omega}_{XB}$. It is therefore enough to show that for all $\bar{\omega}_{XB} \in \mathcal{B}^{\varepsilon}_{cq}(\omega_{XB})$ exists an extension $\bar{\omega}_{XBC}$ in $\mathcal{B}^{\varepsilon}_{cq}(\omega_{XBC})$. Without loss of generality we can assume that the states are normalized. We go to the standard representation of $\mathcal{M}_{XBC}$ on the Hilbert space $\mathcal{H}$, which we also denote by $\mathcal{M}_{XBC}$. Let $\xi_{\omega} \in \mathcal{H}$ be the vector representation of $\omega_{XBC}$ in the positive cone and $\xi_{\bar{\omega}} \in \mathcal{H}$ an arbitrary vector representation of $\omega_{XB}$. Then there exists a unitary $U \in \mathcal{M}'_{XB}$ such that $F(\omega_{XB}, \bar{\omega}_{XB}) = |\langle \xi_{\omega} | U \xi_{\bar{\omega}} \rangle|^2$. If we define $\bar{\omega}_{XBC}$ to be the state corresponding to $U\xi_{\bar{\omega}}$ we find that

$$\begin{aligned} F(\omega_{XBC}, \bar{\omega}_{XBC}) = \sup_{V \in \mathcal{M}'_{XBC}} |\langle \xi_{\omega} | VU \xi_{\bar{\omega}} \rangle|^2 &\leq \sup_{V \in \mathcal{M}'_{XB}} |\langle \xi_{\omega} | VU \xi_{\bar{\omega}} \rangle|^2 \\ &= F(\omega_{XB}, \bar{\omega}_{XB}), \end{aligned}$$

where the suprema are taken such that $\|V\| \leq 1$. But this implies by definition of the purified distance (Defintion 3.4.3) that $\bar{\omega}_{XBC} \in \mathcal{B}^{\varepsilon}_{cq}(\omega_{XBC})$. □

### 5.2.2. Approximation of Differential Min- and Max-Entropy

In the following $(X, \Sigma, \mu)$ is always a measure space where $X$ is locally compact and $\mu$ a complete Radon measure.[3] First, we introduce the concept of a partition.

[3] A complete measure space is a space in which every subset of a set of measure zero is measurable. Every measure space admits a completion.

**Definition 5.2.4.** *Let $(X, \Sigma, \mu)$ be a measure space. We call a collection of measurable subsets $\{I_k\}_{k\in\Lambda}$ such that $\Lambda$ is countable, $X = \bigcup_{k\in\Lambda} I_k$ and $\mu(I_k \cap I_l) = 0$ for all $k \neq l \in \Lambda$ a (discrete) partition of $X$. Given two partitions $\mathcal{P}_1 = \{I_k\}$ and $\mathcal{P}_2 = \{J_k\}$, we say that $\mathcal{P}_1$ is finer than $\mathcal{P}_2$ if for any $I_k$ exists a $J_l$ such that $I_k \subset J_l$ and denote it by $\mathcal{P}_1 \geq \mathcal{P}_2$.[4] The fineness of the partition $\mathcal{P}$ is defined as $\lambda(\mathcal{P}) = \sup_k \mu(I_k)$.*

We address in the following the question under what conditions the conditional min- and max-entropies of a classical quantum state $\omega \in L^1(X, \mathcal{N}^+(\mathcal{M}_B))$ can be approximated. Let $\mathcal{P} = \{I_k\}_{k\in\Lambda}$ be a partition of $X$. For a state $\omega_{XB} \in L^1(X, \mathcal{N}^+(\mathcal{M}_B))$ given by the map $x \mapsto \omega(x)$, we define the discretized classical quantum state $(\omega_k^{\mathcal{P}})_{k\in\Lambda}$ via

$$\omega_k^{\mathcal{P}} = \int_{I_k} \omega \, \mathrm{d}\mu \, . \tag{5.11}$$

and denote the min- and max-entropy of it by $\mathrm{H}_{\min}(X(\mathcal{P})|B)_\omega$ and $\mathrm{H}_{\max}(X(\mathcal{P})|B)_\omega$. In the following, we omit the indication $\mathcal{P}$ in $\omega_k^{\mathcal{P}}$ and simply write $\omega_k$ if it is clear from the context. We are interested whether the entropies $\mathrm{H}_{\min}(X(\mathcal{P})|B)_\omega$ and $\mathrm{H}_{\max}(X(\mathcal{P})|B)_\omega$ converge to the the corresponding entropies of $\omega_{XB}$, if the fineness goes to zero. In this limit, the entropies have to be regularized by a term which is logarithmic in the order of the fineness of the partition. We find that in the case of the max-entropy under specific assumption on the measure space $X$ the approximation holds (see Theorem 5.2.11). For the min-entropy a further condition on the state $\omega_{XB}$ has to be assumed (see Corollary 5.2.14). For $X = \mathbb{R}^n$ the result can be combined to the following main statement.

**Theorem 5.2.5.** *Let $\mathcal{M}_B$ be a von Neumann algebra, $X = \mathbb{R}^n$, $\mu$ the Lebesgue measure, $\omega \in L^1(X, \mathcal{M}_B)$ essentially bounded and $\mathcal{P}_n = \{I_k^n\}_{k\in\Lambda_n}$ a monotone sequence of partitions $\mathcal{P}_1 \leq \mathcal{P}_2 \leq ...$ into intervals with equal length $\delta_n$ such that $\delta_n \to 0$. If $H_{\max}(X(\mathcal{P}_n)|B)_\omega$ is finite for any $n$, then it follows that*

$$\lim_{n\to\infty} \Big( H_{\max}(X(\mathcal{P}_n)|B)_\omega + \log \delta_n \Big) = H_{\max}(X|B)_\omega. \tag{5.12}$$

*If for any $\epsilon > 0$ a compact subset $K \subset X$ with finite measure exists such that $\int_{X\setminus K} \|\omega\| \mathrm{d}\mu \leq \epsilon$, then it follows that*

$$\lim_{n\to\infty} \Big( H_{\min}(X(\{I_k^n\})|B)_\omega + \log \delta_n \Big) = H_{\min}(X|B)_\omega. \tag{5.13}$$

The proof of the statement is given separately for the min- and max-entropy in the following two paragraphs. The results are derived for a general measure space $X$.

**Approximation of the Max-Entropy.** Let $\omega \in L^1(X, \mathcal{M})$ be a state. If we assume that the fineness is constant, i.e., $\lambda(I_k) = \lambda$ for all $k$, the regularized max-entropy of

[4] It is easy to see that $\geq$ defines a partial order on the set of all partitions.

$(\omega_k)_{k\in\Lambda}$ is given by

$$H_{\max}(X(\{I_k\})|B)_\omega + \log\lambda = 2\log\sup_\sigma \sum_k \sqrt{\lambda}F(\omega_k,\sigma)^{\frac{1}{2}}$$
$$= 2\log\sup_\sigma \sum_k \sqrt{\mu(I_k)}F(\omega_k,\sigma)^{\frac{1}{2}}.$$

Hence, the goal is to show that for any sequence of partitions $\mathcal{P}_n = \{I_k^n\}$ with $\mathcal{P}_1 \leq \mathcal{P}_2 \leq \mathcal{P}_3 \leq ...$ and $\lambda(\mathcal{P}_n) \to 0$ $(n \to \infty)$, it holds that

$$\lim_{n\to\infty}\sup_\sigma \sum_k \sqrt{\mu(I_k^n)}F\Big(\int_{I_k^n}\omega\,\mathrm{d}\mu,\,\sigma\Big)^{\frac{1}{2}} = \sup_\sigma \int \mathrm{F}\big(\omega(\mathrm{x}),\sigma\big)^{\frac{1}{2}}\mathrm{d}\mu(\mathrm{x}). \tag{5.14}$$

We first show that this holds for compact $X$ and then extended it to locally compact spaces. Let us neglect the supremum over $\sigma$ in (5.14) at the moment. We show at the end that limit and supremum can be interchanged. We start with the observation of a simple property of the fidelity.

**Lemma 5.2.6.** *Let $\mathcal{M}$ be a von Neumann algebra and $\omega_1,\omega_2,\sigma \in \mathcal{N}^+(\mathcal{M})$. It holds that*

$$F(\omega_1+\omega_2,\sigma)^{\frac{1}{2}} \leq F(\omega_1,\sigma)^{\frac{1}{2}} + F(\omega_2,\sigma)^{\frac{1}{2}}. \tag{5.15}$$

*Proof.* Take a Hilbert space $\mathcal{H}$ such that vector representatives of $\omega_i$ and $\sigma$ exists. If $|\xi_1\rangle$ and $|\xi_2\rangle$ are particular vector states of $\omega_1$ and $\omega_2$, we have that $|\phi\rangle = |1,\xi_1\rangle + |2,\xi_2\rangle$ on $\mathbb{C}^2\otimes\mathcal{H}$ is a vector state representation of $\omega_1+\omega_2$. Hence, we obtain

$$F(\omega_1+\omega_2,\sigma)^{\frac{1}{2}} = \sup_{\eta_\sigma}\langle\phi|\eta_\sigma\rangle \leq \sup_{\eta_\sigma}\langle 1,\xi_1|\eta_\sigma\rangle + \sup_{\eta_\sigma}\langle 2,\xi_2|\eta_\sigma\rangle = F(\omega_1,\sigma)^{\frac{1}{2}} + F(\omega_2,\sigma)^{\frac{1}{2}},$$

where the supremum is taken over all possible vector state representatives of $\sigma$ on $\mathbb{C}^2\otimes\mathcal{H}$. □

We proceed with a technical statement which is the basic ingredient in the following main statements [Kiu].

**Lemma 5.2.7.** *Let $(X,d_X)$ be a metric space, $(Y,\|\cdot\|)$ a normed space, $\mu$ a finite Borel measure on $X$, $g: X\to Y$ norm-bounded uniformly continuous, and $f: Y\to\mathbb{R}_+$ uniformly continuous on $g(X)$ such that there exists a monotonically increasing function $p:\mathbb{R}_+\to\mathbb{R}_+$ with $f(y)\leq p(\|y\|)$ for any $y\in Y$. Then, for any $\epsilon>0$ there exists a $\delta>0$ such that for any discrete partition $\{I_k\}$ with $\sup_{x,y\in I_k} d_X(x,y)\leq\delta$ for any $k$, it holds that*

$$\Big|\sum_k \mu(I_k) f\big(\frac{1}{\mu(I_k)}\int_{I_k} g\,\mathrm{d}\mu\big) - \int f\circ g\,\mathrm{d}\mu\Big| \leq \epsilon. \tag{5.16}$$

*Proof.* Observe first that the sum is finite. Since $\mu(X)$ is finite, this follows from $f(g(x)) \leq p(\|g(x)\|)$ as well as $\|\frac{1}{\mu(I_k)}\int_{I_k} g\,\mathrm{d}\mu\| \leq \sup_x\|g(x)\|$ together with the monotonicity of $p$ and boundedness of $g$. Taking an arbitrary $x_k\in I_k$, we can bound the left hand side of Equation (5.16) by

$$\sum_k \mu(I_k)\Big(\big|f\big(\frac{1}{\mu(I_k)}\int_{I_k} g\,\mathrm{d}\mu\big) - f(g(x_k))\big| + \frac{1}{\mu(I_k)}\int\big|f\circ g - f(g(x_k))\big|\,\mathrm{d}\mu\Big). \tag{5.17}$$

Because $f$ is uniformly continuous on $g(X)$, we can choose a $\delta_1 \geq 0$, such that for any $y_1, y_2 \in g(X)$ with $|y_1 - y_2| \leq \delta_1$, it holds that $|f(y_1) - f(y_2)| \leq \epsilon/(2\mu(X))$. Since $g$ is uniform continuous, we can find a $\delta > 0$ such that $\|g(x_1) - g(x_2)\| \leq \delta_1$ whenever $d_X(x_1, x_2) \leq \delta$. Given that the partition $\{I_k\}$ satisfies $\sup_{x,y \in I_k} d_X(x, y) \leq \delta$, we therefore conclude that

$$\Big\| \frac{1}{\mu(I_k)} \int_{I_k} g(x) \, \mathrm{d}\mu(x) - g(x_k) \Big\| \leq \frac{1}{\mu(I_k)} \int_{I_k} \big\| g(x) - g(x_k) \big\| \, \mathrm{d}\mu(x) \leq \delta_1$$

such that the first term in the sum in Equation (5.17) can be bounded by $\epsilon/(2\mu(X))$ for any $k$. The same holds for the second term in the sum by which we obtain the desired result. □

By Lusin's Theorem [Lus12] the above statement can be extended to essentially bounded functions on compact spaces.

**Theorem 5.2.8.** *Let $\mathcal{M}$ be a von Neumann algebra, $(X, d)$ a compact metric space with complete and finite Radon measure $\mu$. For any $\sigma \in \mathcal{M}$, $\omega \in \mathcal{L}^1(X, \mathcal{N}^+(\mathcal{M}))$ essentially bounded and $\epsilon > 0$, there exists a $\delta > 0$ such that for any partition $\{I_k\}$ with $\sup_{x,y \in I_k} d(x, y) \leq \delta$ for all $k$ follows that*

$$\Big| \sum_k \sqrt{\mu(I_k)} F\big( \int_{I_k} \omega \, \mathrm{d}\mu, \, \sigma \big)^{\frac{1}{2}} - \int F(\omega(x), \sigma)^{\frac{1}{2}} \, dmu(x) \Big| \leq \epsilon \, . \tag{5.18}$$

*Proof.* According to Lusin's Theorem [Lus12], there exists for any $\tilde{\epsilon} > 0$ a compact subset $K \subset X$ such that $\omega$ is continuous on $K$ and $\mu(X \setminus K) \leq \tilde{\epsilon}$. The strategy is now to apply Lemma 5.2.7 onto the support of $K$ and find bounds for the remaining parts. We first note that the possibly infinite sum in Equation (5.18) is well defined. This is due to $F(\eta, \sigma)^{1/2} \leq \|\eta\|^{1/2}$ together with the condition that $\omega$ is essentially bounded, which leads to an upper bound of the sum given by $\mu(X)\|\omega\|_\infty$. For a partition $\{I_k\}$, let us define $I_k^K = I_k \cap K$ and $I_k^0 = I_k \cap (X \setminus K)$, such that $\sum_k \mu(I_k^K) = \mu(K)$ and $\sum_k \mu(I_k^0) = \mu(X \setminus K) \leq \tilde{\epsilon}$. Using Lemma 5.2.6, we can bound

$$F\big( \int_{I_k} \omega \, dmu \, , \sigma \big)^{\frac{1}{2}} = F\big( \int_{I_k^K} + \int_{I_k^0} \omega \, \mathrm{d}\mu \, , \sigma \big)^{\frac{1}{2}} \leq \mathrm{F}\big( \int_{\mathrm{I_k^K}} \omega \, \mathrm{d}\mu \, , \sigma \big)^{\frac{1}{2}} + \mathrm{F}\big( \int_{\mathrm{I_k^0}} \omega \, \mathrm{d}\mu \, , \sigma \big)^{\frac{1}{2}} .$$

Hence, the sum in Equation (5.18) can be estimated by

$$\begin{aligned}
\sum_k \sqrt{\mu(I_k)} F\big( \int_{I_k} \omega \, \mathrm{d}\mu \, , \sigma \big)^{\frac{1}{2}} \leq & \sum_k \sqrt{\mu(I_k)} F\big( \int_{I_k^K} \omega \, \mathrm{d}\mu \, , \sigma \big)^{\frac{1}{2}} \\
& + \sum_k \sqrt{\mu(I_k)} F\big( \int_{I_k^0} \omega \, \mathrm{d}\mu \, , \sigma \big)^{\frac{1}{2}} \\
\leq & \sum_k \sqrt{\mu(I_k^K)} F\big( \int_{I_k^K} \omega \, \mathrm{d}\mu \, , \sigma \big)^{\frac{1}{2}} \\
& + \sum_k \sqrt{\mu(I_k^0)} F\big( \int_{I_k^K} \omega \, \mathrm{d}\mu \, , \sigma \big)^{\frac{1}{2}} \\
& + \sum_k \sqrt{\mu(I_k)} F\big( \int_{I_k^0} \omega \, \mathrm{d}\mu \, , \sigma \big)^{\frac{1}{2}} .
\end{aligned}$$

The first sum can now be treated using Lemma 5.2.7 because $\omega$ is continuous on the compact set $K$ and $\eta \to F(\eta, \sigma)$ is continuous and upper bounded by $p(\eta) = \|\eta\|^{1/2}$. The second sum can be bounded by the Cauchy-Schwarz inequality

$$\begin{aligned}\sum_k \sqrt{\mu(I_k^0)} F\Big(\int_{I_k^K} \omega \, \mathrm{d}\mu \, , \sigma\Big)^{\frac{1}{2}} &\leq \sum_k \sqrt{\mu(I_k^0)} \int_{I_k^K} \|\omega\| \, \mathrm{d}\mu \\ &\leq \Big(\sum_k \mu(I_k^0)\Big)^{\frac{1}{2}} \Big(\sum_k \int_{I_k^K} \|\omega\| \, \mathrm{d}\mu\Big)^{\frac{1}{2}} \\ &\leq \tilde{\epsilon}^{\frac{1}{2}} \|\omega\|_1^{\frac{1}{2}}.\end{aligned}$$

The third sum can also be estimated with the Cauchy-Schwarz inequality

$$\begin{aligned}\sum_k \sqrt{\mu(I_k)} F\big(\int_{I_k^0} \omega \, \mathrm{d}\mu \, , \sigma\big)^{\frac{1}{2}} &\leq \sum_k \sqrt{\mu(I_k)} \Big(\int_{I_k^0} \|\omega(x)\| \, \mathrm{d}\mu(x)\Big)^{\frac{1}{2}} \\ &\leq \Big(\sum_k \mu(I_k)\Big)^{\frac{1}{2}} \Big(\sum_k \int_{I_k^0} \|\,\omega(x)\| \, \mathrm{d}\mu(x)\Big)^{\frac{1}{2}} \\ &\leq \mu(X)^{\frac{1}{2}} \tilde{\epsilon}^{\frac{1}{2}} \|\omega\|_\infty^{\frac{1}{2}} \, .\end{aligned}$$

Hence, for a given $\epsilon > 0$, we first choose a $\tilde{\epsilon}$ such that

$$\tilde{\epsilon} \leq \epsilon^2 / (3\|\omega|_1^{1/2} + 2(\mu(X)\|\omega|_\infty)^{1/2})^2$$

and $\tilde{\epsilon} \leq \epsilon/(3\|\omega\|_\infty)$ holds. Then we choose $K$ according to Lusin's theorem such that $\mu(X \setminus K) \leq \tilde{\epsilon}$. Using that $|a - b| \leq |a - b_1| + |b_2|$ whenever $b \leq b_1 + b_2$, we can use the estimations above to bound

$$\begin{aligned}&\Big|\sum_k \sqrt{\mu(I_k)} F\big(\int_{I_k} \omega \, \mathrm{d}\mu \, , \sigma\big)^{\frac{1}{2}} - \int F(\omega(x), \sigma)^{\frac{1}{2}} \, \mathrm{d}\mu\Big| \\ &\leq \Big|\sum_k \sqrt{\mu(I_k^K)} F\big(\int_{I_k^K} \omega \, \mathrm{d}\mu \, , \sigma\big)^{\frac{1}{2}} - \int_k F(\omega(x), \sigma)^{\frac{1}{2}} \, \mathrm{d}\mu\Big| + \frac{2\epsilon}{3}.\end{aligned}$$

Choosing now $\delta$ such that Lemma 5.2.7 is satisfied with $\epsilon/3$ for the restriction of $\omega$ onto $K$ completes the proof. □

Let us summarize the findings so far. In the case that $X$ is a compact space, $\mu$ a finite measure on $X$, and $\mathcal{P}_1 \leq \mathcal{P}_2 \leq ...$ a sequence of discrete partitions, $P_n = \{I_k^n\}$, such that there exists a zero sequence $\delta_n$ with $\sup_{x,y \in I_k^n} d(x, y) \leq \delta_n$ for all $k$, we have that

$$\lim_{n\to\infty} \sum_k \sqrt{\mu(I_k^n)} F\big(\int_{I_k^n} \omega \, \mathrm{d}\mu \, , \sigma\big)^{\frac{1}{2}} = \int \mathrm{F}(\omega(\mathrm{x}), \sigma)^{\frac{1}{2}} \mathrm{d}\mu \tag{5.19}$$

for any essentially bounded $\omega(x)$ and any $\sigma \in \mathcal{S}(\mathcal{M})$. We use the abbreviation

$$\gamma(n, \sigma|\omega) := \sum_k \sqrt{\mu(I_k^n)} F\big(\int_{I_k^n} \omega \mathrm{d}\mu \, , \sigma\big)^{\frac{1}{2}} \tag{5.20}$$

for any sequence of partitions satisfying the condition above. The limit in Equation (5.19) can be replaced by an infimum. In order to see this, we employ the concavity of the fidelity. Let $m \leq n$ and observe that due to $\mathcal{P}_m \leq \mathcal{P}_n$, we can find for any $l$ sets $I^n_{k_l}$ such that $I^m_l = \bigcup_{k_l} I^n_{k_l}$ and $\bigcup_{l,k} I^n_{k_l} = X$ (almost). Hence,

$$\gamma(m, \sigma|\omega) = \sum_l \mu(I^m_l) F\Big( \sum_k \big(\frac{\mu(I^n_{k_l})}{\mu(I^m_l)}\big) \frac{1}{I^n_{k_l}} \int_{I^n_{k_l}} \omega \, \mathrm{d}\mu \, , \sigma \Big)^{\frac{1}{2}} \tag{5.21}$$

$$\geq \sum_{l,k} \mu(I_{k_l}) F\big(\frac{1}{\mu(I^n_{k_l})} \int_{I^n_{k_l}} \omega \, \mathrm{d}\mu \, , \sigma\big)^{\frac{1}{2}} \tag{5.22}$$

$$= \gamma(n, \sigma|\omega) \ , \tag{5.23}$$

for all $m \leq n$. Thus, $\gamma(n, \sigma|\omega)$ is monotonously decreasing in $n$.

We can now generalize Theorem 5.2.8 to non-compact measure spaces. Let us start with some definitions.

**Definition 5.2.9.** *Let $(X, \Sigma, \mu)$ be a locally compact measure space with complete Radon measure $\mu$ and $\mathcal{P} = \{I_k\}_{k\in\Lambda}$ a partition of $X$. We call $\mathcal{P}$ an essentially compact partition of $X$ if for any subset $\Delta \subset \Lambda$ of finite cardinality $\bigcup_{k\in\Delta} I_k$ is compact. Furthermore, we call $\mathcal{P}$ an essentially finite-measure partition of $X$ if for any subset $\Delta \subset \Lambda$ of finite cardinality $\mu(\bigcup_{k\in\Delta} I_k)$ is finite.*

As an example, $\mathbb{R}^n$ admits a sequence of essentially compact and finite-measure partitions so that Theorem 5.2.5 is a special case of the following statement.

**Corollary 5.2.10.** *Let $(X, d)$ be a metric space with complete Radon measure $\mu$ such that it admits a sequence of essentially compact and finite-measure partitions $\mathcal{P}_n = \{I^n_k\}_{k\in\Lambda_n}$, with $\mathcal{P}_1 \leq \mathcal{P}_2 \leq ...$ and*

$$\delta_n := \sup_k \sup_{x,y\in I^n_k} d(x, y)$$

*is a zero sequence. Moreover, let $\omega \in L^1(X, \mathcal{N}^+(\mathcal{M}))$ be essentially bounded and assume that there exists a $n_0 \in \mathbb{N}$ with $\gamma(n_0, \sigma|\omega)$ finite. Then, for any $\sigma \in \mathcal{S}(\mathcal{M})$ and $\epsilon > 0$ there exists a $N_0 \geq n_0$ such that*

$$\Big| \sum_k \sqrt{\mu(I^n_k)} F\big( \int_{I^n_k} \omega \, \mathrm{d}\mu, \, \sigma\big)^{\frac{1}{2}} - \int \mathrm{F}(\omega(\mathrm{x}), \sigma)^{\frac{1}{2}} \mathrm{d}\mu(\mathrm{x}) \Big| \leq \epsilon \ . \tag{5.24}$$

*for any $n \geq N_0$.*

*Proof.* Let us assume that $n_0 = 1$. Otherwise, we just consider the statement for $\mathcal{P}_{n_0} \leq \mathcal{P}_{n_0+1} \leq ....$ Let us fix $\epsilon > 0$. Since $\gamma(1, \sigma|\omega)$ is finite, there exists a subset $\Delta_1 \subset \Lambda_1$ of finite cardinality with

$$\sum_{k\in\Lambda_1\setminus\Delta_1} \sqrt{\mu(I^1_k)} F\big( \int_{I^1_k} \omega \, \mathrm{d}\mu, \, \sigma\big)^{\frac{1}{2}} \leq \epsilon/3 \ .$$

Because the partition $\mathcal{P}_1$ is essentially compact and finite-measure, we have

$$J = \bigcup_{k\in\Delta_1} I^1_k \tag{5.25}$$

is compact and of finite measure. Because of $\mathcal{P}_1 \leq \mathcal{P}_n$, there exists for every $n$ a subset $\Delta_n \subset \Lambda_n$ such that $J = \bigcup_{k\in\Delta_n} I_k^n$. Using the same argument as in (5.21), we find for every $n$

$$\sum_{k\in\Lambda_n\setminus\Delta_n} \sqrt{\mu(I_k^n)}F\big(\int_{I_k^n} \omega\,\mathrm{d}\mu,\,\sigma\big)^{\frac{1}{2}} \leq \sum_{\mathrm{k}\in\Lambda_1\setminus\Delta_1} \sqrt{\mu(\mathrm{I}_\mathrm{k}^1)}\mathrm{F}\big(\int_{\mathrm{I}_\mathrm{k}^1} \omega\,\mathrm{d}\mu,\,\sigma\big)^{\frac{1}{2}} \leq \frac{\epsilon}{3}\,.$$

This means that independently of $n$, we have that the sum over the set $J$ is $\epsilon/3$ close to the total sum. From the monotonicity argument in (5.21), we can also conclude that

$$\int_{X\setminus J} F(\omega(x),\sigma)^{\frac{1}{2}}\mathrm{d}\mu(\mathrm{x}) \leq \frac{\epsilon}{3}.$$

Since $J$ is compact and of finite measure, we can now apply Theorem 5.2.8 and find a $\delta$ such that for every $n$ with $\delta_n \leq \delta$

$$\Big|\sum_{k\in\Delta_n} \sqrt{\mu(I_k^n)}F\big(\int_{I_k^n} \omega\,\mathrm{d}\mu,\,\sigma\big)^{\frac{1}{2}} - \int_{\mathrm{J}} \mathrm{F}(\omega(\mathrm{x}),\sigma)^{\frac{1}{2}}\mathrm{d}\mu(\mathrm{x})\Big| \leq \frac{\epsilon}{3}\,.$$

Choosing $N_0$ such that $\delta_n \leq \delta$ for all $n \geq N_0$, and combining the different estimates proves the claim. □

The following statement proves the part for the max-entropy in Theorem 5.2.5.

**Theorem 5.2.11.** *Let $\mathcal{M}$ be a von Neumann algebra, $(X,d)$ a locally compact metric space, $\mu$ a complete Radon measure on $X$ and $\omega \in \mathcal{L}^1(X,\mathcal{N}^+(\mathcal{M}))$ $\mu$-essentially bounded. For any sequence of discrete partitions $P_n = \{I_k^n\}$ of $X$ satisfying the same conditions as in Corollary 5.2.10, it follows that*

$$\lim_{n\to\infty}\sup_{\sigma\in\mathcal{S}(\mathcal{M})}\sum_k \sqrt{\mu(I_k^n)}F\Big(\int_{I_k^n}\omega\mathrm{d}\mu,\sigma\Big)^{\frac{1}{2}} = \sup_{\sigma\in\mathcal{S}(\mathcal{M})}\int \mathrm{F}\big(\omega(\mathrm{x}),\sigma\big)^{\frac{1}{2}}\mathrm{d}\mu(\mathrm{x}). \quad (5.26)$$

*Furthermore, if $\lambda_n = \inf\{\mu(I_k^n)\,|\,\mu(I_k^n)\neq 0\}$ is such that $\lambda_n > 0$ for all $n$, we get that*

$$\lim_{n\to\infty}\Big(H_{\max}(X(\{I_k^n\})|B)_\omega + \log\lambda_n\Big) \leq H_{\max}(X|B)_\omega, \quad (5.27)$$

*and equality holds if $\mu(I_k^n) = \lambda_n$ for all $n$ and $k$. Here, we denoted $\mathcal{M} = \mathcal{M}_B$.*

Note that the inequality in the opposite direction of (5.27)

$$H_{\max}(X|B)_\omega \leq H_{\max}(X(\{I_k^n\})|B)_\omega + \log\lambda_n$$

follows directly from the monotonicity of $\gamma(n,\sigma|\omega)$ shown in (5.21). The proof of the theorem is based on Sion's minimax theorem [Sio58].

*Proof.* According to the discussion before, we have to show

$$\inf_n\sup_\sigma \gamma(n,\sigma|\omega) = \sup_\sigma\inf_n \gamma(n,\sigma|\omega). \quad (5.28)$$

The proof is a simple application of Sion's minimax theorem [Sio58]. It says that if $\mathcal{X}$ is a compact convex subset of a topological space, $\mathcal{Y}$ a convex subset of a

linear topological space, and $f : \mathcal{X} \times \mathcal{Y} \to \mathbb{R}$ a function such that (1) $f(x, \cdot)$ is upper semi-continuous (u.s.c.) and quasi-concave for every $x$ and (2) $f(\cdot, y)$ is lower semi-continuous (l.s.c.) and quasi-convex for every $y$, then $\min_x \sup_y f(x, y) = \sup_y \min_x f(x, y)$. We are applying it to the function $f(\lambda, \sigma) := \gamma(\lceil \frac{1}{\lambda} \rceil, \sigma|\omega)$ where $\lceil \lambda \rceil$ denotes the ceiling function, and $f(0, \sigma) := \lim_{n\to\infty} \gamma(n, \sigma|\omega)$. We have that $\mathcal{X} = [0, 1]$ is compact and convex and $\mathcal{Y} = \mathcal{S}_{\leq}(\mathcal{M})$ is convex. Moreover, since the fidelity is concave and continuous, condition (1) is satisfied. Note that $f(\sigma, \cdot)$ meets condition (2) because $\gamma(n, \sigma|\omega)$ is monotonically decreasing in $n$ and we take it at $\lceil \frac{1}{\lambda} \rceil$. Hence, we can apply Sion's minimax theorem and obtain Equality (5.28). The second statement follows now directly by the definition of the max-entropy. □

**Approximation of the Min-Entropy.** Let us assume for the moment that the partition $\mathcal{P} = \{I_k\}$ of $X$ is such that $\mu(I_k) = \delta$ for all $k$. The min-entropy of a state $\omega \in L^1(X, \mathcal{M})$ with respect to the partition $\mathcal{P}$ is then given by

$$\begin{aligned} &H_{\min}(X(\{I_k\})|B)_\omega + \log \delta \\ &= -\log \sup \Big\{ \sum_k \omega^k(\frac{1}{\delta} E_k) \,|\, E_k \in \mathcal{M}_+, \sum_k E_k \leq \mathbb{1} \Big\} \\ &= -\log \sup \Big\{ \int \omega^x(E(x)) \mathrm{d}\mu(x) \,|\, E \geq 0 \text{ is } \{I_k\}\text{-simple}\,, \int E \,\mathrm{d}\mu \leq \mathbb{1} \Big\}\,, \end{aligned}$$

where the $\{I_k\}$-simple functions are the ones which can be written as $\sum_k E_k \mathbf{1}_{I_k}$, with $\mathbf{1}_I$ the indicator function on $I$. Hence, it follows directly that

$$H_{\min}(X(\{I_k\})|B)_\omega + \log \delta \geq H_{\min}(X|B)_\omega\,. \tag{5.29}$$

For the following it is convenient to introduce the notation

$$M(\omega) := \sup \Big\{ \int \omega^x(E(x)) \,|\, E \in \mathcal{L}^\infty(X, \mathcal{M})\,, \int E \,\mathrm{d}\mu \leq \mathbb{1} \Big\}. \tag{5.30}$$

**Lemma 5.2.12.** *Let $(X, d)$ be a metric space, $\mu$ a finite measure on $X$ and $\omega \in L^1(X, \mathcal{M})$ uniformly continuous. Then, for any $\epsilon > 0$ there exists a $\delta > 0$ such that for any partition $\{I_k\}_{k\in\Lambda}$ with $\sup_k \sup_{x,y\in I_k} d(x, y) \leq \delta$, there exists a positive $\{I_k\}$-simple function $F$ with*

$$\int \omega^x(F(x)) \,\mathrm{d}\mu(x) \geq M(\omega) - \epsilon. \tag{5.31}$$

*Proof.* According to the definition of $M(\omega)$, there exists $E \in L^\infty(X, \mathcal{M})$ such that

$$\int \omega^x(E(x)) \,\mathrm{d}\mu(x) \geq M(\omega) - \frac{\epsilon}{2}\,. \tag{5.32}$$

Due to the uniform continuity of $\omega$, we can find a $\delta > 0$ such that for any $x, y \in X$ with $d(x, y) \leq \delta$ holds that $\|\omega^x - \omega^y\| \leq \epsilon/(2\mu(X)\|E\|_\infty)$. Let $\{I_k\}$ be a partition of $X$ such that $\sup_{x,y\in I_k} d(x, y) \leq \delta$. We define the $\{I_k\}$-simple function $\eta = \sum \eta_k \mathbf{1}_{I_k}$ with values in $\mathcal{N}^+(\mathcal{M})$, where $\eta_k = 1/\mu(I_k) \int_{I_k} \omega^x \,\mathrm{d}\mu(x)$. We can estimate

$$\begin{aligned} M(\omega) &\leq \int \omega^x(E(x)) \,\mathrm{d}\mu(x) + \frac{\epsilon}{2} &(5.33)\\ &= \int (\omega^x - \eta^x)(E(x)) \,\mathrm{d}\mu(x) + \int \eta^x(E(x)) \,\mathrm{d}\mu(x) + \frac{\epsilon}{2}. &(5.34) \end{aligned}$$

The second term can be rewritten as

$$\begin{aligned}\int \eta^x(E(x))\,\mathrm{d}\mu(x) &= \sum_k \int \eta_k(E(x))\mathbf{1}_{I_k}(x)\mathrm{d}\mu(x)\\ &= \sum_k \mu(I_k)\eta_k\Big(\frac{1}{\mu(I_k)}\int E(x)\mathbf{1}_{I_k}(x)\mathrm{d}\mu(x)\Big)\\ &= \sum_k \int \omega^y(E_k)\mathbf{1}_{I_k}(y)\mathrm{d}\mu\\ &= \int \omega^y(\sum_k E_k\mathbf{1}_{I_k}(y))\mathrm{d}\mu\\ &= \int \omega^y(F(y))\mathrm{d}\mu\end{aligned}$$

where $E_k = 1/\mu(I_k)\int_{I_k} E\mathrm{d}\mu$ and $F = \sum_k E_k 1_{I_k}$ is a $\{I_k\}$-simple function. The first term in (5.34) can now be bounded by

$$\int (\omega^x - \eta^x)(E(x))\,\mathrm{d}\mu(x) \leq \|E\|_\infty \int \|\omega^x - \eta^x\|\mathrm{d}\mu \leq \frac{\epsilon}{2\mu(X)}\int \mathrm{d}\mu = \frac{\epsilon}{2}\,,$$

where we used that for almost every $x_0 \in X$

$$\begin{aligned}\|\omega^{x_0} - \eta^{x_0}\| &= \|\omega^{x_0} - \frac{1}{\mu(I_k)}\int_{I_k}\omega^x\,\mathrm{d}\mu(x)\|\\ &\leq \frac{1}{\mu(I_k)}\int_{I_k}\|\omega^{x_0} - \omega^x\|\\ &\leq \frac{\epsilon}{2\mu(X)\|E\|_\infty}\,.\end{aligned}$$

Here we have chosen $I_k$ such that $x_0 \in I_k$. Putting all these steps together, we obtain the desired result. □

Using Lusin's Theorem [Lus12] this can be extended to essentially bounded functions.

**Theorem 5.2.13.** *Let $\mathcal{M}$ be a von Neumann algebra, $(X,d)$ a compact metric space, $\mu$ a finite complete Radon measure on $X$ and $\omega \in L^1(X,\mathcal{N}^+(\mathcal{M}))$ $\mu$-essentially bounded. For any sequence of discrete partitions $P_n = \{I_k^n\}$ of $X$ with $\mathcal{P}_1 \leq \mathcal{P}_2 \leq ...$ such that $\delta_n := \sup_k \sup_{x,y\in I_k^n} d(x,y)$ is a zero sequence, it holds that*

$$M(\omega) = \lim_{n\to\infty}\sup\Big\{\sum_k \frac{1}{\mu(I_k^n)}\int_{I_k^n}\omega^x(E_k)\,|\,E_k \geq 0, \sum_k E_k \leq \mathbb{1}\Big\}\,. \tag{5.35}$$

*Furthermore, if $\lambda_n = \inf\{\mu(I_k^n)\,|\,\mu(I_k^n)\neq 0\}$ is such that $\lambda_n > 0$ for all $n$, we get*

$$\lim_{n\to\infty}\Big(H_{\min}(X(\{I_k^n\})|B)_\omega + \log\lambda_n\Big) \leq H_{\min}(X|B)_\omega, \tag{5.36}$$

*and equality holds if $\mu(I_k^n) = \lambda_n$ for all $n$ and $k$. Here, we denoted $\mathcal{M} = \mathcal{M}_B$.*

*Proof.* We show that for any $\epsilon > 0$ there exists a $n_0$, such that for any $n \geq n_0$ exists a $\mathcal{P}_n$-simple function $F$ such that (5.31) holds. Let us fix an arbitrary $\epsilon > 0$ and choose $E \in \mathcal{L}^\infty(X, \mathcal{M})$ such that

$$\int \omega^x(E(x))\,\mathrm{d}\mu(x) \geq M(\omega) - \frac{\epsilon}{3}\,.$$

Next, we use Lusin's theorem and take a compact subset $K$ of $X$ such that $\mu(X\backslash K) \leq \epsilon/(3\|E\|_\infty\|\omega\|_\infty)$ and $\omega$ is continuous on $K$. We can then bound

$$\begin{aligned} M(\omega) &\leq \int \omega^x(E(x))\,\mathrm{d}\mu(x) + \frac{\epsilon}{3} \\ &= \int_K \omega^x(E(x))\,\mathrm{d}\mu(x) + \int_{X\backslash K} \omega^x(E(x))\,\mathrm{d}\mu(x) + \frac{\epsilon}{3} \\ &\leq \int_K \omega^x(E(x))\,\mathrm{d}\mu(x) + \|E\|_\infty\|\omega\|_\infty \int_{X\backslash K} \mathrm{d}\mu + \frac{\epsilon}{3} \\ &\leq \int_K \omega^x(E(x))\,\mathrm{d}\mu(x) + 2\frac{\epsilon}{3}. \end{aligned}$$

Applying Lemma 5.2.12 to $\omega$ restricted to $K$ such that Equation (5.31) is satisfied with $\epsilon/3$ completes the proof of the first part. The second part involving the min-entropy follows straightforwardly by definition. □

This can now be generalized to non-compact metric spaces as follows.

**Corollary 5.2.14.** *Let $\mathcal{M}$ be a von Neumann algebra, $(X, d)$ a locally compact metric space, $\mu$ a complete Radon measure and $\{\mathcal{P}_n\}_n$ as in Theorem 5.2.13. If $\omega \in \mathcal{L}^1(X, \mathcal{N}^+(\mathcal{M}))$ is $\mu$-essentially bounded and for any $\epsilon > 0$ there exists a compact subset $C \in X$ of finite measure such that $\int_{X\backslash C} \|\omega\|\mathrm{d}\mu \leq \epsilon$, then*

$$M(\omega) = \lim_{n\to\infty} \sup\Big\{ \sum_k \frac{1}{\mu(I_k^n)} \int_{I_k^n} \omega^x(E_k) \,|\, E_k \geq 0, \sum_k E_k \leq \mathbb{1} \Big\}. \tag{5.37}$$

*Furthermore, if $\lambda_n = \inf\{\mu(I_k^n) \,|\, \mu(I_k^n) \neq 0\}$ is such that $\lambda_n > 0$ for all $n$, we get*

$$\lim_{n\to\infty} \Big( H_{\min}(X(\{I_k^n\})|B)_\omega + \log\lambda_n \Big) \leq H_{\min}(X|B)_\omega, \tag{5.38}$$

*and equality holds if $\mu(I_k^n) = \lambda_n$ for all $n$ and $k$. Here, we set $\mathcal{M} = \mathcal{M}_B$.*

*Proof.* The proof is a straightforward application of Theorem 5.2.13. We have to show that for any $\epsilon > 0$ there exists a $n_0$, such that for any $n \geq n_0$ there is a $\mathcal{P}_n$-simple function $F$ such that (5.31) holds. Let us fix $\epsilon > 0$ and choose $C$ with $\int_{X\backslash C} \|\omega\|\mathrm{d}\mu \leq \epsilon/2$. We can apply the result from 5.2.13 to $(C, d)$ implying the existence of a $n_0$ such that for any $n \geq n_0$ is a $\mathcal{P}_n$ simple function such that (5.31) holds with $\epsilon/2$. Putting these steps together yields the desired result. □

### 5.2.3. Interpretation of Min- and Max-entropies of Continuous Outcomes

Let us take a connected subset $X \subset \mathbb{R}$ and define $\mathcal{P}_\delta$ as the partition of $X$ into intervals of equal length $\delta$. In the following we consider a state $\omega \in L^(X, \mathcal{M}_B)$ for which

$$\lim_{\delta \to 0} \left( \mathrm{H}_{\min}\left(X(\mathcal{P}_\delta)|B\right)_\omega + \log \delta \right) = \mathrm{H}_{\min}\left(X|B\right)_\omega \,. \tag{5.39}$$

The min-entropy for discrete outcomes can be interpreted as the guessing probability 4.46

$$p_{\mathrm{guess}}(X(\mathcal{P}_n)|B)_\omega = 2^{-\mathrm{H}_{\min}(X(\mathcal{P}_\delta)|B)_\omega}. \tag{5.40}$$

If we denote $p_c(X|B)_\omega = 2^{-\mathrm{H}_{\min}(X|B)_\omega}$, Equation (5.39) can be rewritten as

$$p_c(X|B)_\omega = \lim_{\delta \to 0} \frac{p_{\mathrm{guess}}(X(\mathcal{P}_\delta)|B)_\omega}{\delta} \,. \tag{5.41}$$

Because of $\lim_{\delta\to 0} p_{\mathrm{guess}}(X(\mathcal{P}_\delta)|B)_\omega = 0$, we obtain that $p_c(X|B)_\omega$ is just the derivative of $p_{\mathrm{guess}}(X(\mathcal{P}_\delta)|B)_\omega$ at $\delta = 0$. Hence, we have that for small spacing $\delta$, the guessing probability

$$p_{\mathrm{guess}}(X(\mathcal{P}_n)|B)_\omega = p_c(X|B)_\omega \delta - \Theta(\delta^2) \,, \tag{5.42}$$

where the higher order correction is always negative. Hence, the guessing probability corresponding to a spacing $\delta$ is always upper bounded by $p_c(X|B)_\omega \delta$.

In order to discuss the meaning of the conditional max-entropy for continuous outcomes we consider an interval $X \subset \mathbb{R}$ with $\mu(X) = |X| < \infty$ and a state $\omega$ in $L^1(X, \mathcal{M}_B)$ with

$$\lim_{\delta \to 0} \left( \mathrm{H}_{\max}\left(X(\mathcal{P}_\delta)|B\right)_\omega + \log \delta \right) = \mathrm{H}_{\max}\left(X|B\right)_\omega \,. \tag{5.43}$$

The max-entropy with respect to a partition $\mathcal{P}_\delta$ of $X$ into intervals of constant lengths $\delta$ can be written as

$$\mathrm{H}_{\max}\left(X(\delta)|B\right)_\omega = \sup_{\sigma_B} \log \left( \frac{|X|}{\delta} F(\omega_{X(\delta)B}, \tau_{X(\delta)} \otimes \sigma_B) \right) , \tag{5.44}$$

where $X(\delta)$ is the random variable obtained by partitioning according to $\mathcal{P}_\delta$ and $\tau_{X(\delta)} = 1/|X(\delta)| \mathrm{id}_{X(\delta)}$ the tracial state on $X(\delta)$. If we define the closeness of $\omega_{XB}$ to the uncorrelated uniform distribution on $X$ as

$$\mathrm{r}_{\mathrm{key}}(X(\delta)|B)_\omega = \sup_{\sigma_B} F(\omega_{X(\delta)B}, \tau_{X(\delta)} \otimes \sigma_B) \tag{5.45}$$

we can write the max-entropy as $H_{\max}(X(\delta)|B)_\omega = \log \frac{|X|}{\delta} \mathrm{r}_{\mathrm{key}}(X|B)_\omega$. Using now Equation (5.43), we can infer that

$$\lim_{\delta \to \infty} \mathrm{r}_{\mathrm{key}}(X(\delta)|B)_\omega = \frac{1}{|X|} r_c(X|B)_\omega \tag{5.46}$$

where $r_c(X|B)_\omega = 2^{H_{\max}(X|B)_\omega}$. Hence, we get that for small $\delta \approx 0$

$$r_c(X|B)_\omega \cdot |X| \approx \mathrm{r}_{\mathrm{key}}(X(\delta)|B)_\omega \tag{5.47}$$

implying that $r_c(X|B)_\omega \cdot |X|$ is a lower bound for $\mathrm{r}_{\mathrm{key}}(X(\delta)|B)_\omega$ for any $\delta$.

## 5.3. Position and Momentum Uncertainty Relations with Quantum Side Information

By position and momentum operators, we denote a pair of selfadjoint operators $Q$ and $P$ acting on a Hilbert space $\mathcal{H} \simeq L^2(\mathbb{R})$ satisfying the cannonical commutation relation $[P, Q] = i$. They can uniquely be represented on $\mathcal{H}$ as the multiplication and differential operator acting on smooth functions as $Q\psi(x) = x\psi(x)$ and $P\psi(x) = (1/i)\frac{d}{dx}\psi(x)$. The spectrum for both operators is equal to $\mathbb{R}$ and there exist projective operator valued measures denoted by $\mu_Q$ and $\mu_P$ such that

$$Q = \int_{\mathbb{R}} x \, \mathrm{d}\mu_Q(x) \qquad P = \int_{\mathbb{R}} x \, \mathrm{d}\mu_P(x). \tag{5.48}$$

The integrals converge weakly and for any $\psi \in \mathcal{H}$ induces $\langle\psi|\mathrm{d}\mu_Q(x)\psi\rangle$ and $\langle\psi|\mathrm{d}\mu_P(x)\psi\rangle$ a Borel measure on $\mathbb{R}$.

We are interested in the uncertainty of the outcome distributions of position and momentum measurements quantified by the uncertainty relation with quantum side information derived in Theorem 4.7.1. We consider first the case of a finite measurement precision. This corresponds to a partition of the real line, where the fineness of the partition characterizes the resolution of the measurement apparatus used in the experiment. Even though a measurement with infinite precision does not exist in real world, it is theoretically interesting to consider the limit when the fineness goes zero. It also brings a practical advantage because the computation of entropies for continuous outcome distributions are often easier than for the discretized probability distributions. This is especially true for the important class of Gaussian states.

### 5.3.1. Measurements with Finite Spacing

For convenience, we use the notation $\mathcal{M}_A = \mathcal{B}(\mathcal{H})$ ($\mathcal{H} \simeq L^2(\mathbb{R})$) for the system on which the position and momentum measurements are performed. The von Neumann algebras used to model the side-information are denoted by $\mathcal{M}_B$ and $\mathcal{M}_C$. The projections which correspond to a position and momentum measurement in the interval $I$ are

$$Q[I] := \int_I \mathrm{d}\mu_Q \text{ and } P[I] = \int_I \mathrm{d}\mu_P \, . \tag{5.49}$$

Let $\mathcal{P}_\delta = \{I_k\}_{k\in\mathbb{N}}$ be a partition of the real line (see Definition 5.2.4) into intervals $I_k$ with equal length $\delta$. Given a state $\omega_{ABC} \in \mathcal{S}(\mathcal{M}_{ABC})$, the post-measurement state obtained by measuring $Q$ with the finite spacing $\mathcal{P}_\delta$ is given by

$$\omega^\delta_{QBC} = (\omega^{Q,n}_{BC})_{n\in\mathbb{N}} \, , \tag{5.50}$$

where $\omega^{Q,n}_{BQ}$ is the state on $\mathcal{M}_{BC}$ defined by $a \mapsto \omega_{ABC}(Q[I_n]a)$. Analogously, we denote the post-measurement state obtained by measuring the momentum operator $P$ with spacing $\mathcal{P}_\delta$ by

$$\omega^\delta_{PBC} = (\omega^{P,n}_{BC})_{n\in\mathbb{N}} \, , \tag{5.51}$$

where $\omega^{P,n}_{BQ}$ is the state on $\mathcal{M}_{BC}$ defined by $a \mapsto \omega_{ABC}(P[I_n]a)$.

In order to allow for full generality, we introduce different spacings $\delta q$ and $\delta p$ for the two observables $Q$ and $P$ and denote the partitions by $\mathcal{P}_{\delta q} = \{I_k\}_{k\in\Lambda_Q}$ and $\mathcal{P}_{\delta p} = \{J_k\}_{k\in\Lambda_P}$ with $\Lambda_{P/Q} \simeq \mathbb{N}$. The complementarity of the measurements in the uncertainty relation in Theorem 4.7.1 is quantified by

$$\begin{aligned} c = \sup_{k,l} \|\sqrt{Q[I_k]}\sqrt{P[I_l]}\|^2 &= \sup_{k,l} \|\sqrt{Q[I_k]}P[I_l]\sqrt{Q[I_k]}\| \\ &= \sup_{k,l} \|Q[I_k]P[J_l]Q[I_k]\| \,, \end{aligned}$$

where we used $\|A\|^2 = \|A^*A\|$ and that the operators are projectors. Since the translation in position $\exp(-iaP)$ and momentum $\exp(-itQ)$ are unitary operators it is clear that $\|Q[I_k]P[J_l]Q[I_k]\|$ does not depend on $k, l$. Hence, we can neglect the supremum and conclude that it only depends on the lengths $\delta p$ and $\delta q$. The same argument holds for the dilation such that the value of $c$ is determined by the product of the lengths of the intervals $\delta q \delta p$. It then follows that for any two intervals $I_k \in \mathcal{P}_{\delta q}$ and $J_l \in \mathcal{P}_{\delta p}$ (see e.g. [LP64] or also [KW10] and references therein)

$$c = c(\delta q, \delta p) := \|Q[I_k]P[J_l]Q[I_k]\| = \frac{1}{2\pi}\delta q \delta p \cdot S_0^{(1)}\left(1, \frac{\delta q \delta p}{4}\right)^2 \tag{5.52}$$

where $S_0^{(1)}(\cdot, x)$ is the 0th radial prolate spheroidal wave function of the first kind. Hence, if we apply Theorem 4.7.1, we obtain the following uncertainty relation.

**Theorem 5.3.1.** *Let $Q$ and $P$ be position and momentum operators, that is, they act on $\mathcal{H} = L^2(\mathbb{R})$ and satisfy $[P, Q] = i$. Furthermore, let $\mathcal{M}_B, \mathcal{M}_C$ be von Neumann algebras and $\omega_{ABC} \in \mathcal{S}(\mathcal{M}_{ABC})$, where we denote $\mathcal{M}_{ABC} = \mathcal{B}(\mathcal{H}) \otimes \mathcal{M}_{BC}$. For any $\epsilon \geq 0$ and $\delta q, \delta p > 0$, it follows that*

$$\mathrm{H}_{\min}^{\epsilon}(Q|B)_{\omega^{\delta q}} + \mathrm{H}_{\max}^{\epsilon}(P|C)_{\omega^{\delta p}} \geq -\log c(\delta q, \delta p), \tag{5.53}$$

*where $\omega_{QBC}^{\delta q}$ and $\omega_{PBC}^{\delta p}$ are the post-measurement states as defined in Equation (5.50) and (5.51).*

The complementarity term $-\log c(\delta q, \delta p)$ is plotted in Figure 5.1 for $\delta q = \delta p$. Note that the result can be generalized to $\mathcal{H} = L^2(\mathbb{R}^n) = L^2(\mathbb{R})^{\otimes n}$, where $n$ pairs of position and momentum operators $Q_i$ and $P_i$ for $i = 1, 2, ..., n$ are considered. The case $n = 3$ describes for instance the observables corresponding to the position and momentum of one particle in a three dimensional space time. But the position and momentum operators model for instance also the quadrature variables of the electromagnetic field. That is, the system corresponding to n pairs of position and momentum operators describes the electromagnetic degrees of freedom of $n$ modes of a light field. This will be used in Section 6.3. In the case of a general $n$, the constant in the uncertainty relation changes to

$$c = \|\bigotimes_{i=1}^{n} Q_i[I_k]P_i[J_l]Q_i[I_k]\| = \prod_{i=1}^{n} \|Q_i[I_k]P_i[J_l]Q_i[I_k]\| = c(\delta q, \delta p)^n \,. \tag{5.54}$$

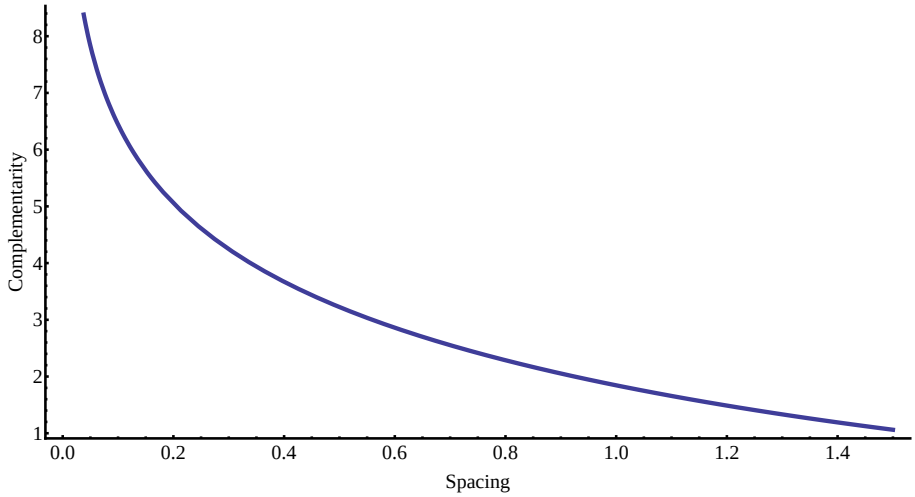


Figure 5.1.: The constant $-\log c(\delta, \delta)$ measuring the complementary of the position and the momentum observable in Equation (5.53) for equal spacing $\delta$. Note that the units are such that the width of the vacuum is $\delta = 1$ for which we obtain $-\log c \approx 1.85$.

Note that we can neglect the supremum over the intervals since the operator norm of $Q_i[I_k]P_i[J_l]Q_i[I_k]$ only depends on the product of their lengths. If we denote $\mathcal{M}_{A^n} = \mathcal{B}(\mathcal{H}) = \mathcal{B}(L^2(\mathbb{R}))^{\otimes n}$, the uncertainty relation for a state $\omega_{A^nBC} \in \mathcal{S}(\mathcal{M}_{A^nBC})$ where each $Q_i$ and $P_i$ is measured with the same spacing $\delta q$ and $\delta p$ is given by

$$\mathrm{H}^{\epsilon}_{\min}\left(Q^n|B\right)_{\omega^{\delta q}} + \mathrm{H}^{\epsilon}_{\max}\left(P^n|C\right)_{\omega^{\delta p}} \geq -n \log c(\delta q, \delta p). \tag{5.55}$$

Note that the post-measurement state $\omega^{\delta q}_{Q^nBC} = (\omega^{\delta q,k}_{BC})_{k\in\mathbb{N}^n}$ is defined via $a \mapsto \omega_{A^nBC}(\bigotimes_{i=1}^n Q_i[I_{k_i}]a)$. The same holds for $\omega^{\delta p}_{P^nBC}$ with the momentum operator $P$ instead of the position operator.

Let us address the question if the uncertainty in Equation (5.53) is tight. In the case where $\epsilon \neq 0$, one can hardly expect that this is true. This is because of the definitions of the smooth min- and max-entropy as optimizations over states close in the purified distance. Let us therefore restrict to the case $\epsilon = 0$. According to the data processing inequality given in Proposition 4.5.1, the uncertainty relation (5.53) also holds without side information. For convenience, we exchange the min- and max-entropy and arrive at

$$\mathrm{H}_{\min}(P)_{\omega^{\delta p}} + \mathrm{H}_{\max}(Q)_{\omega^{\delta q}} \geq -\log c(\delta q, \delta p)\,. \tag{5.56}$$

The above inequality is saturated by measuring a pure state for which the support in constraint on one interval $I_k$ of the $Q$ measurement. The idea is that the min-entropy only sees the largest eigenvalue and the size of the support essentially does not affect its value. In contrast the max-entropy is sensitive on how large the support

is. It is therefore intuitively clear that in order to make the max-entropy small the distribution should be (more) peaked for the $Q$ measurement.

**Lemma 5.3.2.** *For every spacing $\delta q$ and $\delta p$ there exists a state such that equality holds in (5.56). Thus, the uncertainty relation in (5.53) is tight for $\epsilon = 0$.*

*Proof.* Without any restriction, we assume that the partitions for the $Q$ and $P$ measurement include the intervals $I = [-\delta q/2, \delta q/2]$ and $J = [-\delta p/2, \delta p/2]$. Let us take a pure state $\psi \in L^2(\mathbb{R})$ with support restricted to $I$. Therefore the measurement distribution for the $Q$ measurement is equal to 1 for one output and zero else. Thus, we can conclude that $H_{\max}(Q) = 0$. Note that the probability distribution of the continuous momentum measurement is given by $|\mathcal{F}(\psi(q))|^2$, where $\mathcal{F}$ denotes the Fourier transform. Therefore, we find for the min-entropy that

$$\begin{aligned} 2^{-\mathrm{H}_{\min}(\mathrm{P})} &= \int \mathbf{1}_{[-\delta p/2, \delta p/2]}(p) |\mathcal{F}(\psi)|^2 dp \\ &= \frac{1}{2\pi} \int \mathbf{1}_I(r) \mathbf{1}_J(p) \mathbf{1}_I(q) \bar{\psi}(r) \psi(q) e^{-i(q-r)p} dr dp dq \\ &= \langle \psi | Q[I] P[J] Q[I] | \psi \rangle \,, \end{aligned}$$

where $\mathbf{1}_I$ denotes the indicator function of $I$. But using Equation (5.52) and that $Q[I]P[J]Q[I]$ is selfadjoint, we can write the overlap

$$c(\delta q, \delta p) = \| Q[I] P[J] Q[I] \| = \sup_{\phi \in L^2(\mathbb{R})} \langle \phi | Q[I] P[J] Q[I] | \phi \rangle \,. \tag{5.57}$$

Since the supremum can be restricted to functions with support $I$, we find that $\mathrm{H}_{\min}(\mathrm{P}) = -\log \mathrm{c}(\delta \mathrm{p}, \delta \mathrm{p})$ which proves the claim. We note that $\psi \in {}^2(\mathbb{R})$ for which equality in (5.56) is attained (or equivalently maximizes the right hand side of (5.57)) is the normalized projection of the radial prolate spheroidal wave function of the first kind onto the interval $I$ (see for instance [KW10]). □

### 5.3.2. Measurements with Continuous Outcomes

We generalize the uncertainty relation in Theorem 5.3.1 to continuous measurement outcomes by means of the approximation results for the differential min- and max-entropy presented in Theorem 5.2.5. We use the same notation as in the previous section. For a state $\omega_{ABC}$, we denote the post-measurement state of a continuous outcome measurement of the position operator $Q$ by $\omega_{QBC}$. The state is an element of $\mathcal{S}(L^\infty(\mathbb{R}) \otimes \mathcal{M}_{BC})$ and defined by the action

$$f \otimes a \mapsto \omega_{ABC}\Big( \int_{\mathbb{R}} f(x) \, \mathrm{d}\mu_Q(x) \otimes a \Big) \tag{5.58}$$

for $f \in L^\infty(\mathbb{R})$ and $a \in \mathcal{M}_{BC}$. As discussed in Section 5.2.1, we can identify the state $\omega_{QBC}$ with an element in $L^1\big(\mathbb{R}, \mathcal{N}^+(\mathcal{M}_{BC})\big)$, that is, a measurable function $\omega^Q_{BC}(x)$ which takes values in $\mathcal{N}^+(\mathcal{M}_{BC})$ and satisfies $\int_{\mathbb{R}} \|\omega^Q_{BC}(x)\| \, \mathrm{d}\mu(x) < \infty$. The same of course holds for the post-measurement state obtained by a continuous momentum measurement. In this case, we denote the state as $\omega_{PBC}$ and the associated function as $\omega^P_{BC}$.

**Theorem 5.3.3.** *Let $Q$ and $P$ be position and momentum operators and $\mathcal{M}_B, \mathcal{M}_C$ be von Neumann algebras and set $\mathcal{M}_{ABC} = \mathcal{B}(\mathcal{H}) \otimes \mathcal{M}_{BC}$. Furthermore, let $\omega_{ABC} \in \mathcal{S}(\mathcal{M}_{ABC})$ with continuous post-measurement states $\omega_{QBC}$ and $\omega_{PBC}$ in $L^1\big(\mathbb{R}, \mathcal{N}^+(\mathcal{M}_{BC})\big)$ such that*

- *$\omega_{QBC}$ and $\omega_{PBC}$ are essentially bounded,*
- *there is a $\delta p > 0$ such that the discretized max-entropy $\mathrm{H}_{\max}\left(P(\delta p)|C\right)_{\omega^{\delta p}}$ is bounded,*[5]
- *and for any $\epsilon > 0$ there exists a compact subset $K \subset \mathbb{R}$ with*

$$\int_{\mathbb{R}\setminus K} \|\omega_B^Q(x)\| \, \mathrm{d}\mu(x) \leq \epsilon \, .$$

*Then, it follows that*

$$\mathrm{H}_{\min}\left(Q|B\right)_\omega + \mathrm{H}_{\max}\left(P|C\right)_\omega \geq \log 2\pi. \tag{5.59}$$

The conditions of the theorem are for instance satisfied if the post-measurement states $\omega_B^Q(x)$ and $\omega_C^P(x)$ admit a continuous representative in $\mathcal{L}^1\big(\mathbb{R}, \mathcal{N}^+(\mathcal{M}_{BC})\big)$.

*Proof.* The proof is a combination of the approximation theorem for differential min- and max-entropies (Theorem 5.2.5) and the uncertainty relation for finite spacing (5.53). Let us assume that $\delta q = \delta p = \delta$. Then the uncertainty relation (5.53) for $\epsilon = 0$ together with the definition of $c(\delta q, \delta p)$ in Equation (5.52) yields

$$\mathrm{H}_{\min}\left(Q(\delta)|B\right)_{\omega^\delta} + \log\delta + \mathrm{H}_{\max}\left(P(\delta)|C\right)_{\omega^\delta} + \log\delta \geq \log \frac{2\pi}{S_0^{(1)}\big(1, \delta^2/4\big)^2} \, , \tag{5.60}$$

where $Q(\delta)$ and $P(\delta)$ indicate that the outcome distribution of a position and momentum measurement with a spacing $\delta$ are considered. Since the condition of Theorem 5.2.5 are satisfied for the post-measurement states, we obtain using $S_0^{(1)}\big(1, \delta^2/4\big) \to 1$ $(\delta \to 0)$ the desired inequality in the limit $\delta \to 0$. □

The uncertainty relation is tight and saturated in the case without side-information. The states which saturate the inequality are pure Gaussian state with a minimal uncertainty product of their variances $\sigma_X \sigma_P = 1/2$ [BB06]. A simple computation shows that for a Gaussian distribution

$$f(x) = \frac{e^{-\frac{1}{2\sigma^2}}}{\sqrt{2\pi} \cdot \sigma}$$

the min- and max-entropies are $\mathrm{H}_{\min}(X) = \log(\sqrt{2\pi}\sigma)$ and $\mathrm{H}_{\max}(X) = \log(2\sqrt{2\pi}\sigma)$. Hence, in the case of $\sigma_X \sigma_P = 1/2$, we obtain equality in (5.59).

[5] Here, the system $P(\delta p)$ refers to the discrete alphabet induced by the spacing $\delta p$.

# 6. Finite-Key Analysis for Continuous-Variable Quantum Key Distribution

## 6.1. Introduction

In a continuous-variable protocol, the information is encoded in the field quadratures of a light state which are measured by homodyne or heterodyne detection. The quantum system of a stationary field mode is modeled by the infinite-dimensional Hilbert space $\mathcal{H} \simeq L^2(\mathbb{R})$ and can be thought as generated by the observables of the amplitude and phase quadrature given by operators $Q$ and $P$ which obey the canonical commutation relation. These operators are unbounded and the spectrum is the real line, and thus, continuous (see Section 5). The information in a continuous-variable protocols is usually encoded by Gaussian states which have the advantage that they can be efficiently prepared in an experiment. Prepare and measure protocols based on a finite number of possible displacements (relative to the vacuum state) are called discrete modulation protocols and were first proposed in [Ral99, Rei00, Hil00]. Later on a Gaussian modulation was proposed in [CLA01] which can be realized as an entanglement based protocol using a two-mode squeezed state (c.f. Section 6.3.1). For a review about the possible implementations see for instance the recent review in [WPGP$^+$12] and references therein.

Results concerning the security of such protocols are often based on results explicitly derived for quantum systems modeled on a finite-dimensional Hilbert space and assumed to hold also for continuous-variable systems. This includes for instance the asymptotic key rate formula derived by Devetak and Winter in [DW05] for i.i.d. quantum sources as well as the general finite-key formula by Renner [Ren05]. Both are information theoretic statements and characterize the optimal extractable key rate using one-way classical post-processing. The key length formula in [Ren05] are derived via the characterization of privacy amplification by the smooth min-entropy (c.f. Section 4.8) and the Devetak-Winter rate [DW05] can be retrieved via the asymptotic equipartition property [Ren05, TCR09]. Using the results from Chapter 4, these results will be rigorously generalized to the finite-dimensional case in Section 6.2.2.

Another subtle problem is to prove security of a continuous-variable protocol against coherent attacks in the finite-key regime (see Section 1.4 for the basic notions). Techniques like the exponential de-Finetti theorem [Ren07] or the post-selection technique [CKR09] which allow to lift the security from collective to coherent attacks do not apply directly to infinite-dimensional quantum systems [CKMR07]. In [RC09], the de-Finetti theorem is combined with a truncation of the Hilbert space dimension such that it can be applied under certain constraints to continuous-variable

protocols. But an estimation of the required measurements in one run necessary to obtain a non-vanishing key rate turned out to be extremely high and hardly feasible in practice. The estimation was based on conditions derived in [Ped08], where they also show that it is not clear that the technique is robust in the experimental parameters. Even the bounds on the finite-key rate obtained for qubit protocols which are based on [Ren07] are quite pessimistic [SLS10]. This has been improved by [CKR09], but so far, no generalization to infinite-dimensions are proven. Alternative approaches based on entanglement distillation has been analyzed in [GP01, vAIC05] but without a quantitative analysis.

We circumvent this problem and use the idea from [TR11, TLGR12] and employ the uncertainty relation with quantum side-information for the smooth min- and max-entropy (see Section 4.7). It allows to bound the information of an eavesdropper about the measurement outcomes of Alice by the knowledge about the strength of the correlations between the outcomes between Alice and Bob. But the correlations are directly accessible to Alice and Bob and can be probed on a random sample of the data. The uncertainty relation for phase and amplitude measurements $Q$ and $P$ as derived in Theorem 5.3.1 depends on the binning $\delta_q$ and $\delta_p$ of the measurement outcomes. In order for the uncertainty relation to be strong enough the binning has to be chosen relatively which on the order side requires a highly squeezed Gaussian state to still generate strong enough correlations. Nevertheless, we find in Section 6.3.2 a non-vanishing key rate for an experimentally achievable squeezing strength (c.f. [EHD$^+$11b, EHD$^+$11a]) for a two-mode squeezed state protocol similar to [CLA01].

We further compute the finite-key rate secure against collective Gaussian attacks in Section 6.3.4 by using the asymptotic equipartition property from Section 4.5.3. A similar finite-key analysis has been discussed in [LGG10] for a protocol based on heterodyne detection. We use state estimation to determine the information a possible eavesdropper could have about the measurement data and the extremality of Gaussian attacks [GPC06, NGA06]. Comparison with the finite-key rate computed against coherent attacks, we find a gap which is due to the non-tightness of the uncertainty relation.

## 6.2. Security Definition and Finite-Key Rate for a Generic Protocol

In a quantum key distribution (QKD) protocol two parties, Alice and Bob, communicate via quantum and classical channels in order to establish a secret key. In the following, we assume that the classical channels are always authenticated such that Alice and Bob know that the message is sent by the other party and not by an adversary trying to learn about the key. We also assume that Alice and Bob are honest and only an outside adversary, from now on called Eve, is malicious.

We consider an entanglement based protocol in which an entangled state is first distributed between Alice and Bob and then measured. A part of the data is used to estimate the knowledge of a possible eavesdropper about it. This procedure is referred to as parameter estimation (PE) and involves classical communication between Alice and Bob. In case that the information of the eavesdropper is small enough, a secret

key is extracted from the remaining data by means of classical post-processing.

For the following discussion, we divide the protocol which we denote by $\mathcal{P}$ into two subparts. The first part $\mathcal{P}_1$ consists of the part where quantum mechanics plays the key role. It includes the distribution of the quantum state, the performed measurements and the parameter estimation step. Output of this part is a so-called raw key $X_A$ and $X_B$ on Alice's and Bob's side or a flag Ⓢ, which tells them to abort the entire protocol. If the protocol did not abort, they pursue with the second part $\mathcal{P}_2$, the classical post-processing, in which they first apply an error correction protocol followed by privacy amplification to extract the final key denoted by $S_A$ and $S_B$ on Alice's and Bob's side. In the following subsections, we define the security criterion and explain how to compute the extractable length of a finite-key.

### 6.2.1. Composable Security Definition

The current standard for security proofs of cryptographic primitives asks for composable security, which demands that the concatenation of two secure protocols remain secure. This is especially important for a quantum key distribution protocol which only produces a key, which then serves as a resource for other tasks, like for instance one-time pad. In quantum key distribution, we also assume that Alice and Bob are honest players and that security has only be proven against an outside adversary. In that case, composable security is thus weaker than for instance in oblivious transfer or secure function evaluation where even the parties can be malicious. In this latter situation one refers to the term universally composable security (see, e.g., [Can01, Unr10] and references therein).

The following security definitions are based on the discussion of composable security in quantum key distribution presented in [MQR09] (c.f. [RK05, BOHL$^+$05]). The idea is to define the security according to the possibility to distinguish the given "real" protocol with an "ideal" protocol. As described above, a general quantum key distribution protocol $\mathcal{P}$ outputs either two binary strings $s_A$ and $s_B$ on Alice's and Bob's side (the key) or a flag Ⓢ which stands for abort. The protocol is a statistical process and only the probability distribution of the keys denoted by $\omega_{S_AS_B}$ can be characterized. Hence, the outputs of the protocol ar described by random variables $S_A$ and $S_B$. For simplicity, we use the symbols $S_A$ and $S_B$ to indicate both the random variable and the alphabet. During the run of the protocol a malicious third party Eve may wiretap the quantum channel, such that the key distribution is correlated with her system denoted by $E$. Hence, the overall output is described by a classical quantum state

$$\omega_{S_AS_BE} = \sum_{s_A,s_B} p(s_A,s_B)|s_a,s_B\rangle\langle s_a,s_B| \otimes \omega_E^{s_A,s_B} \ , \tag{6.1}$$

where $p(s_A,s_B)$ denotes the distribution of the keys and $\omega_E^{s_A,s_B} \in \mathcal{S}(\mathcal{M}_E)$ a state of Eve's system modeled on a von Neumann algebra $\mathcal{M}_E$. Furthermore, we denote by $p_{\text{ab}}$ the probability that the protocol aborts, and thus, outputs Ⓢ and $p_{\text{pass}} = (1-p_{\text{ab}})$. An ideal secure key is uniformly distributed on $S_A$ and maximally classically correlated to $S_B$, while uncorrelated to $E$. This is captured in the following definition.

**Definition 6.2.1.** *A protocol $\mathcal{P}$ which outputs a state $\omega_{S_AS_BE}$ is called*

- $\epsilon_c$-correct *if* $\mathrm{Prob}_\omega[S_A \neq S_B] \leq \epsilon_c$, *and correct if this holds for* $\epsilon_c = 0$.
- $\epsilon_s$-secret *if* [1]

$$\inf_{\sigma_E}(1 - p_{\mathrm{ab}})\frac{1}{2}\|\omega_{S_A E} - \mathrm{u}_{S_A} \otimes \sigma_E\| \leq \epsilon_s \tag{6.2}$$

*and secret if this holds for* $\epsilon_s = 0$. *Here,* $\mathrm{u}_{S_A}$ *denotes the uniform distribution on* $S_A$ *and the infimum is take over all* $\sigma_E \in \mathcal{S}(\mathcal{M}_E)$.

*A protocol* $\mathcal{P}$ *is finally called secure or ideal if it is correct and secret, and* $\epsilon_{\mathrm{sec}}$*-secure if it is* $\epsilon_{\mathrm{sec}}$*-indistinguishable from an ideal protocol.*

The term $\epsilon$-indistinguishable means that there is no device (or protocol) interacting with the protocol $\mathcal{P}$ or its ideal version $\mathcal{P}^{\mathrm{ideal}}$, which can differ between them with success probability higher than $\epsilon$. It is easy to see that a protocol which is $\epsilon_c$-correct and $\epsilon_s$-secret is $\epsilon_{\mathrm{sec}}$-secure for $\epsilon_c + \epsilon_s \leq \epsilon_{\mathrm{sec}}$. The fact that the given definition is composable secure is shown in [MQR09], and simply relies on the indistinguishability property. Therefore, it is also essential to use the norm distance in the secrecy definition (6.2), which quantifies the possibility to distinguish between two quantum states. It has also the advantage that any further processing of the state by a classical or quantum channel can only decrease the distance. This is in contrast to security definitions which are based on a small mutual information which does not satisfy the requirement of composable security [KRBM07].

Finally, we want to stress that since the protocol is probabilistic, the security can only be guaranteed up to a failure probability. Hence, there is always a small possibility that information leaked. Note also the success is conditioned on the event that the protocol passes and therefore only the product of $(1-p_{\mathrm{ab}})$ with the distance to uniform in (6.2) can be controlled. But this is sufficient because a protocol which aborts with almost one is secure in a statistical sense up to a failure probability. Since $p_{\mathrm{ab}}$ cannot be determined in the experiment, the computed key length must be independent of it.

### 6.2.2. Finite-Key Analysis for a Generic Protocol

Let us start at the beginning of the second part of the protocol and assume that Alice and Bob have already generated the raw keys $X_A$ and $X_B$ and the parameter test has been passed. They proceed then with an error correction protocol in which Alice broadcasts $\mathrm{leak}_{\mathrm{EC}}$ bits. Based on this information Bob changes his bit string to match it with $X_A$. In order to check that the strings are $\epsilon_c$-correct Alice and Bob do the following correctness test: Alice draws a random function from a family of two-universal hash functions onto an alphabet of size $\log(1/\epsilon_c)$ and applies it to her string $X_A$. She then sends the result and the description of the function to Bob who aborts the protocol if the result does not coincide with the valued he obtains when applying the function on his string.

[1] The norm is the canonical norm on the state space given in the case of classical quantum states in Equation (3.2). If the quantum system is described by a Hilbert space $\mathcal{M}_E = \mathcal{B}(\mathcal{H}_E)$, we can use density matrices and the norm is the usual trace norm.

Let us denote by $\omega_{X_A E}$ the state between Alice and Eve conditioned on the event that the parameter estimation test is passed.[2] Furthermore, we denote the random variable corresponding to the classical communication during the error correction protocol by $M$. Recall that the number of bits $\log|M|$ is assumed to be $\mathrm{leak_{EC}} + \log(1/\epsilon_c)$. According to the privacy amplification result Corollary 4.8.4, we know that if Alice applies a hash function drawn at random from a family of two-universal hash functions (see Definition 4.8.2), which maps $X_A$ onto an alphabet $S_A$ of size $\ell = |S_A|$, we know that

$$\frac{1}{2}\|\omega_{S_A E} - \mathrm{u}_{S_A} \otimes \omega_E\| \leq \sqrt{2^{\ell - \mathrm{H}^{\epsilon}_{\min}(X_A|EM)_\omega - 2}} + 2\epsilon. \tag{6.3}$$

In order to obtain an $\epsilon_s$-secret key (see Equation (6.2)), we have to ensure that the left hand side of (6.3) is smaller than $\epsilon_s/p_{\mathrm{pass}}$. Hence, we can conclude that an $\epsilon_s$-secret key can be extracted if $\ell$ is smaller than

$$\mathrm{H}^{\epsilon}_{\min}(\mathrm{X_A}|\mathrm{EM})_\omega - 2\log\frac{\mathrm{p_{pass}}}{\epsilon_1} + 2. \tag{6.4}$$

where $\epsilon \leq (\epsilon_s - \epsilon_1)/(2p_{\mathrm{pass}})$. Using the properties of the smooth min-entropy from Lemma 4.5.6 and 4.5.7, we can further simplify

$$\mathrm{H}^{\epsilon}_{\min}(\mathrm{X_A}|\mathrm{EM})_\omega \geq \mathrm{H}^{\epsilon}_{\min}(\mathrm{X_A M}|\mathrm{E})_\omega - \log|\mathrm{M}| \geq \mathrm{H}^{\epsilon}_{\min}(\mathrm{X_A}|\mathrm{E})_\omega - \log|\mathrm{M}|. \tag{6.5}$$

Moreover, by using that $-\log p_{\mathrm{pass}} \geq 0$, we obtain the following claim.

**Theorem 6.2.2.** *Let $\omega_{X_A E}$ the state between Alice and Eve conditioned on the event that the test in parameter estimation has been passed. If one uses an error correction scheme broadcasting $\mathrm{leak_{EC}}$ bits of classical information and passes the correctness test via two-universal hash functions onto an alphabet of size $\log(1/\epsilon_c)$, then, we can extract an $\epsilon_c$-correct and $\epsilon_s$-secret key of length*

$$\mathrm{H}^{\epsilon}_{\min}(\mathrm{X_A}|\mathrm{E})_\omega - 2\log\frac{1}{\epsilon_1} - \log\frac{1}{\epsilon_{\mathrm{c}}} - \mathrm{leak_{EC}} + 2, \tag{6.6}$$

*where $\epsilon \leq (\epsilon_s - \epsilon_1)/(2p_{\mathrm{pass}})$.*

This theorem reduces the finite-key analysis to finding a bound on the smooth min-entropy. Since the state $\omega_{X_A E}$ between Alice and Eve is not known, it has to be estimated with the data obtained in the parameter estimation step. Hence, the goal is to find a lower bound on the smooth min-entropy for all states which are compatible with the observed data. This estimation can be done under different assumption. A common one is to restrict the power of Eve to for instance collective attacks.

The error correction term $\mathrm{leak_{EC}}$ can be estimated in different ways. If we use the result from Section 4.9, we now that a one-way communication protocol exists which is $\epsilon_c$ correct and leaks $\mathrm{leak_{EC}} = \mathrm{H}^{\epsilon_c/2}_{\max}(\mathrm{X_A}|\mathrm{X_B})_\omega$ bits. As shown in Lemma 4.9.6 such

[2] Of course, this state is never known to Alice nor Bob at no stage of the protocol. But we can assume that it exists.

an error correction scheme is essentially optimal. Combined with Equation (6.6), this gives the key length

$$\mathrm{H}^{\epsilon}_{\min}(\mathrm{X_A}|\mathrm{E})_{\omega} - 2\log\frac{1}{\epsilon_1} - \mathrm{H}^{\epsilon_c/2}_{\max}(\mathrm{X_A}|\mathrm{X_B})_{\omega} + 2.$$

Note that form this formula, we also obtain the Devetak-Winter rate [DW05] in the case of collective attacks by using the asymptotic equipartition property of the smooth min- and max-entropy discussed in Section 4.5.3 (see also [Ren05, TCR09, FAR11]). In particular, we can then assume that we have tensor product structure $\omega^{\otimes n}_{X_A X_B E}$, where now $\omega_{X_A X_B E}$ denotes the state after a single use of the quantum channel, such that by Corollary 4.5.5 the optimal achievable asymptotic rate is

$$r = H(X_A|E)_{\omega} - H(X_A|X_B)_{\omega} = I(X_A : X_B)_{\omega} - I(X_A : E)_{\omega}\,, \tag{6.7}$$

where $I(A : B) = H(A) - H(A|B)$ denotes the mutual information. Note that the same argument can also be done in the case where Bob have not yet measured his quantum register, which leads to an upper bound on the asymptotic key rate given by $I(X_A : B)_{\omega} - I(X_A : E)_{\omega}$.

## 6.3. Application to a Two-Mode Squeezed State Protocol

### 6.3.1. Description of the Source and the Measurements

We always assume that the labs of Alice and Bob are closed and secure and that they can trust their source and measurement devices. The source is located in Alice's lab and produces a two-mode squeezed vacuum state [BvL05, WPGP+12]. Experimentally, such a state can be generated by mixing two squeezed vacuum states over a balanced beam splitter. Alice then sends one mode to Bob over a quantum channel whereupon both measure certain quadratures of the field by means of homodyne detection. The important property of a two-mode squeezed state is that the outcome of certain quadrature measurements on Alice's and Bob's side are strongly correlated. In the following, we denote the conjugate pair of quadrature variables for Alice's and Bob's mode which exhibit the maximal amount of correlation by $Q_A, Q_B$ and $P_A, P_B$, and call them phase and amplitude measurements. Mathematically, the observables $Q_A$ and $P_A$ ($Q_B$ and $P_B$) correspond to the usual position and momentum operator obeying the canonical commutation relation $[Q_A, P_A] = i$ ($[Q_B, P_B] = i$) (see Section 5). For simplicity, we chose the units such that $\hbar = 1$. For illustration, we plotted in Figure the probability distributions of the measurement outcomes of Alice and Bob for the different choices of measurements for a two-mode squeezed state.

Mathematically, the spectrum of the phase and amplitude measurements is the real line. But in order to apply the privacy amplification result from Section 4.8 and therefore Theorem 6.2.2, it will be necessary to map the continuous outcome set to a discrete (and finite) alphabet. This is also reasonable from a experimental point of view since the resolution of a measurement device is always limited to a certain accuracy. We use a uniform binning into intervals of length $\delta$ for the range $[-\alpha + \delta, \alpha - \delta]$ for a $\alpha > 0$. The value of $\alpha$ will be chosen such that the

probability that Alice measures a quadrature larger than $\alpha$ is of order $\epsilon_s$. In the following, we assume that $\delta$ is chosen such that $M = \alpha/\delta$ is a natural number and enumerate the intervals by $I_{-M} = (-\infty, -\alpha + \delta]$, $I_{-M+1} = (\alpha - \delta, -\alpha + 2\delta]$, ...,$I_M = (\alpha - 2\delta, \alpha - \delta]$, $I_M = (\alpha - \delta, \infty)$. The outcome range is then denoted by $\mathcal{X} = \{-M, -M + 1, ..., M - 1, M\} \subset \mathbb{Z}$ and satisfies by definition $|\mathcal{X}| = 2\alpha/\delta$. The length $\delta$ has to be larger than the trusted measurement precision of the devices of Alice and Bob used to measure the quadratures. The integrated projection valued measure over the interval $I \subset \mathbb{R}$ of the phase and amplitude operators of Alice (Bob) are denoted by $Q_A(I)$ and $P_A(I)$ ($Q_B(I)$ and $P_B(I)$).

In the following section we describe the protocols for the case of coherent and collective attacks. The way how the key is generated is similar in both cases and uses the correlation in the phase an amplitude measurements. But the protocol differs in the parameter estimation procedure. In the case of coherent attacks only the quality of the correlations is tested while in the collective case state estimation is used.

### 6.3.2. Coherent Attacks

**The Protocol and a Formula for the Finite-Key Length.** Alice and Bob perform independently and uniformly at random either phase or amplitude measurement. This is repeated $2N$ times and leads to a set of $2N$ measurement outcomes. Once all the measurements are completed they broadcast publicly their choice of measurements, that is, phase or amplitude. They sift their data by discarding all measurement results in which they have measured different quadratures. Since the probability that they have chosen the same quadrature is 1/2 they end up with roughly $N$ correlated data points. Let us assume for simplicity that they are exactly $N$ measurement results left. They group their measurement outcomes according to the binning introduced in the section before and end up with $N$ data points in $\mathcal{X}$. For the following discussion, we assume that the protocol parameters $\alpha$ and $\delta$ are fixed such that $|\mathcal{X}| = 2\alpha/\delta$.

They choose a random sample of $k < N$ data points denoted by $X_A^{\mathrm{PE}}, X_B^{\mathrm{PE}} \subset \mathcal{X}^k$, which are used for parameter estimation. The remaining $n = N - k$ data points are denoted by $X_A, X_B \in \mathcal{X}^n$ and serve as the raw key from which the final key is extracted by classical post-processing as explained in Section 6.2.2. In the parameter estimation step Alice and Bob check check, how strong their outcomes are correlated. Let us define the average distance between two strings $X, Y \in \mathcal{X}^k$ as

$$d(X, Y) = \frac{1}{k} \sum_{i=1}^{k} |X_i - Y_i| \,, \tag{6.8}$$

where $X = (X_1, ..., X_k)$ and $Y = (Y_1, ..., Y_k)$. By definition, as smaller $d(X_A^{\mathrm{PE}}, x_B^{\mathrm{PE}})$ as higher is the correlation between the strings $X_A^{\mathrm{PE}}$ and $X_B^{\mathrm{PE}}$. They proceed with the following test.

***Parameter Estimation Test.*** *They broadcast the values of $X_A^{\mathrm{PE}}, X_B^{\mathrm{PE}}$ and check that $d(X_A^{\mathrm{PE}}, x_B^{\mathrm{PE}}) \leq d_0$. If not they abort the protocol.*

If this test is passed, they pursue with error correction and privacy amplification as discussed in Section 6.2.

In all what follows we trust the source which is located in Alice's lab. Hence, Eve cannot interact with Alice's mode during the whole protocol. Furthermore, we assume that $N$ uses of the source produces a state $\omega^S_{A^N B^N}$ which has tensor product structure $\omega^S_{A^N B^N} = (\omega^S_{AB})^{\otimes N}$ and that the probability that Alice measures a quadrature with absolute value smaller $\alpha$ is larger than $p_\alpha$. More formally, this means that

$$\omega^S_A\Big(Q_A([-\alpha,\alpha])\Big) \geq p_\alpha \text{ and } \omega^S_A\Big(P_A([-\alpha,\alpha])\Big) \geq p_\alpha \,. \tag{6.9}$$

We call such a source which ejects a tensor product state an i.i.d. (idependent and identical distributed) source. We are now interested to bound the probability that a quadrature value which is used for the raw key is outside of the range $[-\alpha,\alpha]$. But this is simply given by

$$g(p_\alpha, n) = 1 - p_\alpha^n. \tag{6.10}$$

As we show in the next section, the secure key length which can be extracted is computed as follows.

**Theorem 6.3.1.** *Let the source be i.i.d. and $p_\alpha$ such that the inequality in (6.10) is satisfied. We assum that an error correction scheme broadcasting* $\mathrm{leak}_{\mathrm{EC}}$ *bits of classical information is used and the correctness test via two-universal hash functions onto an alphabet of size* $\log(1/\epsilon_c)$ *is passed. Moreover, let $\gamma$ denote the function*

$$\gamma(t) = (t + \sqrt{1+t^2})\Big(\frac{t}{\sqrt{1+t^2}-1}\Big)^t \,. \tag{6.11}$$

*If the protocol passes the parameter estimation test for $d_0$, then one can extract an $\epsilon_c$-correct and $\epsilon_s$-secret key of length*

$$n[\log\frac{1}{c(\delta)} - \log\gamma(d_0+\mu)] - \mathrm{leak}_{\mathrm{EC}} - 2\log\frac{1}{\epsilon_1} - \log\frac{1}{\epsilon_c} + 2, \tag{6.12}$$

*where $c(\delta)$ is the overlap of Alice's measurement defined in Equation 6.22 and*

$$\mu = |\mathcal{X}|\sqrt{\frac{N(k+1)}{nk^2}\ln\frac{1}{\epsilon_s - \epsilon_1 - 2\sqrt{2g(p_\alpha,n)}}} \,. \tag{6.13}$$

Note that the condition $\epsilon_s - \epsilon_1 - 2\sqrt{2g(p_\alpha,n)} \geq 0$ has to be satisfied in (6.13). This can be reformulated by adding $\epsilon_1 + 2\sqrt{2g(p_\alpha,n)}$ to the security parameter $\epsilon_s$. In particular, we then obtain that the key is $(\epsilon+\epsilon_1+2\sqrt{2g(p_\alpha,n)})$-secret if we chose

$$\mu = |\mathcal{X}|\sqrt{\frac{N(k+1)}{nk^2}\ln\frac{1}{\epsilon}} \,.$$

This simply means that we assume that the security of the protocol fails whenever Alice measures a quadrature measurement higher than $\alpha$. This is only a technical problem necessary for the statistical estimations in the security analysis. More concretely, in order to be able to obtain statistical large deviation bounds the alphabet has to be finite.

The computation of the key rate is always based on certain assumption. In the case of Theorem 6.3.1 the assumptions are the following.

- Both Alice and Bob chose their measurements independently and uniformly in each run.
- The source is trusted and i.i.d. satisfying inequality (6.10).
- The measurements of Alice are modeled by projections onto the intervals of length $\delta$ of the spectrum of the one mode phase and amplitude operators $Q_A$ and $P_A$. This includes implicitly the fact that the measurement between different runs commute.

Note that no assumptions about Bob's measurement is used in the derivation of (6.6). Hence, we do not have to trust the phase reference signal (local oscillator) which is used for homodyne detection.

In practical implementations, the leakage term $\text{leak}_{\text{EC}}$ is the number of bits which have been communicated in the error correction phase. Theoretically, we assume that it is close to the asymptotic optimum which is given by the conditional von Neumann entropy $H(X_A|X_B)$ [SW71]. The conditional entropy can be written in terms of the mutual information as

$$H(X_A|X_B) = H(X_A) - I(X_A : X_B). \tag{6.14}$$

In order to account for the inefficiency of the error correction protocol and the fact that we are not in the asymptotic limit, we set[3]

$$\text{leak}_{\text{EC}} = H(X_A) - \beta I(X_A : X_B) \tag{6.15}$$

where $0 < \beta \leq 1$. Recently, new codes designed for the case of Gaussian modulation were developed which allow for high efficiencies like in the qubit case ($\beta \approx 0.95$ [JKJL11]).

Let us discuss now the dependence of the finite-key rate in Equation (6.6) on the various parameters of the protocol. For practical purposes, the value $d_0$ is simply chosen to be equal to $d(X_A^{\text{PE}}, X_B^{\text{PE}})$ which is optimal. The term $\mu$ comes from the statistical analysis and reflects the uncertainty which arise if one wants to infer properties of the raw key by analyzing the random sample $X_A^{\text{PE}}, X_B^{\text{PE}}$. As therefore expected it goes to zero if $N$ goes to infinity. If we consider the functional behavior $\mu$ in dependence of the fraction of data used for parameter estimation $k/N$, we see that it has a symmetric U-shape and takes its minimum for $k/N = 0.5$. Furthermore, $\mu$ crucially depends on $\alpha$ and $\delta$ via $|\mathcal{X}| = 2\alpha/\delta$ as well as $p_\alpha$. This is a technical problem which comes from technicalities in large deviation theory. Nevertheless, we are not aware of how to relax this dependence. For the range of $\alpha$ we have to consider, the influence of $\alpha$ on $d(X_A^{\text{PE}}, X_B^{\text{PE}})$ and $\text{leak}_{\text{EC}}$ are negligible for the two mode state considered below.

Let us assume for now that no eavesdropper is presence and discuss the dependence of the finite-key length on the binning parameter $\delta$. The numerical analysis shows that the range of $\delta$ for which a non-vanishing key rate can be expected is $\delta \leq 0.02$. The variation of $\delta$ effects directly the overlap of the quadrature measurements $c(\delta)$

[3] In practice, it turns out that the inefficiency scales with the mutual information and not with the conditional entropy

(see Equation (5.52) or (6.22)). For small $\delta$ it can be well approximated by $c(\delta) \approx \delta^2/(2\pi)$. Intuitively, it is clear that the average distance $d(X_A^{\mathrm{PE}}, X_B^{\mathrm{PE}})$ decreases if the binning $\delta$ gets smaller. Indeed, one can show that for a two mode squeezed state the distance goes inverse proportional in $\delta$ for small $\delta$. Moreover, for large arguments the function $\gamma(t)$ can be approximated by $\gamma(t) \approx 2et$. Hence, we have that[4] $\gamma(d(X_A^{\mathrm{PE}}, X_B^{\mathrm{PE}}) + \mu) \propto 1/\delta$.

Let us now approximate the leakage term $\mathrm{leak}_{\mathrm{EC}}$ given in (6.15). We denote the continuous outcome distribution of one quadrature measurements by $\tilde{X}_A^1$ and $\tilde{X}_B^1$. Since for small $\delta$, the von Neumann entropy satisfies $H(X^1) \approx h(\tilde{X}^1) - \log\delta$ with $h(\tilde{X})$ the differential entropy [CT91], we have under the assumption that the outcomes in each run are independent and identically distributed that

$$\begin{aligned}\mathrm{leak}_{\mathrm{EC}} &\approx n\big(h(\tilde{X}_A^1) - \beta(h(\tilde{X}_A^1) + h(\tilde{X}_B^1) - h(\tilde{X}_A^1\tilde{X}_B^1)\big) - n\log\delta \\ &\equiv n h_\beta(\tilde{X}_A^1|\tilde{X}_B^1) - n\log\delta\end{aligned}$$

From this it follows that for small $\delta$ and in the asymptotic limit, the leading term in the key rate is

$$r \approx \log\frac{2\pi}{\delta^2} - \log\gamma\big(d(X_A^{\mathrm{PE}}, X_B^{\mathrm{PE}})\big) - h_\beta(\tilde{X}_A^1|\tilde{X}_B^1) + \log\delta \tag{6.16}$$

$$= -\log\frac{\gamma\big(d(X_A^{\mathrm{PE}}, X_B^{\mathrm{PE}})\big)\cdot 2^{h_\beta(\tilde{X}_A^1|\tilde{X}_B^1)}\cdot\delta}{2\pi}\,. \tag{6.17}$$

Hence, the condition for a positive key rate reads

$$\frac{\gamma(d(X_A^{\mathrm{PE}}, X_B^{\mathrm{PE}}))}{\delta} \leq \frac{2\pi}{2^{h_\beta(\tilde{X}_A^1|\tilde{X}_B^1)}}. \tag{6.18}$$

Both sides of inequality (6.18) do not scale in delta anymore and the difference corresponds to the asymptotic key rate (which might vanish) for $\delta \to 0$.

**Plots of the Finite-Key Rate.** For the following plots, we use a symmetric model. This allows us to characterize the two-mode state between Alice and Bob with four parameters: squeezing $\lambda_{\mathrm{sq}}$, antisqueezing $\lambda_{\mathrm{asq}}$, transmission losses $\mu_{\mathrm{loss}}$ and excess noise $\mu_{\mathrm{en}}$. The squeezing and anti-squeezing is given in dB and describes the one-mode vacuum squeezer used in the experiment. The corresponding covariance matrix of the one mode state before the beam splitter is then given by

$$\begin{pmatrix} 10^{-\frac{\lambda_{sq}}{10}} & 0 \\ 0 & 10^{\frac{\lambda_{asq}}{10}} \end{pmatrix} \tag{6.19}$$

The two modes are then mixed over a $50:50$ beam splitter by which the two-mode squeezed vaccuum state is obtained. We assume that the losses due to transmission and coupling are similar for Bob's and Alice's mode and simply modeled by replacing a certain amount $\mu_{\mathrm{loss}}$ of the signal by vacuum. Additionally, we assume excess noise $\mu_{\mathrm{en}}$ which corresponds to classical noise added in the data acquisition procedure.

[4] Note that also $\mu$ is inverse proportional in $\delta$ since $|\mathcal{X}| \propto 1/\delta$

Both effects are gaussian noise sources and are expressed as action on the covariance matrix by

$$\Gamma \to (1 - \mu_{\text{loss}})\Gamma + (\mu_{\text{loss}} + \mu_{\text{en}})\Gamma_{\text{vac}} \,, \tag{6.20}$$

where $\Gamma_{\text{vac}}$ denotes the covariance matrix of the vacuum state which is simply the identity matrix in our units. In the following plots the excess noise is always set to $\mu_{\text{en}} = 0.01$.[5]

All the plots are calculated for security parameters $\epsilon_s = \epsilon_c = 10^-6$, and $\epsilon_1 = \epsilon_s/2$. This means that for realistic parameters $N \approx 10^8$, $\ell/N \approx 10^-1$ the security per bit is $\epsilon_s/\ell \approx 10^-13$ [TLGR12]. We consider a high efficiency error correction scheme with a leakage term given as in Equation (6.15) for $\beta = 0.95$. This can be achieved using newly developed codes suitable for Gaussian modulation [JKJL11]. The key rate is finally computed by optimizing over the remaining free parameter $\delta$, $\alpha$ and $k/N$.

In Figure 6.1 the key rate $\ell/N$ is plotted for a fixed ratio $\lambda_{\text{asq}}/\lambda_{sq} = 1.45$ between antisqueezing and squeezing and a fixed number of sifted measurement results $N = 10^9$. We see that in order to obtain a non-vanishing key rate without additional losses ($\mu_{\text{loss}} = 0$) a minimum squeezing/antisqueezing of $\lambda_{\text{sq}} \approx 8.9$ dB and $\lambda_{\text{asq}} \approx 12.9$ dB. These squeezing strengths are experimentally challenging but possible [EHD$^+$11b, EHD$^+$11a].

In Figure 6.2, the key rate $\ell/N$ for a fixed squeezing and antisqueezing of $\lambda_{\text{sq}} =$ 11dB and $\lambda_{asq} =$ 16dB depending on $N$ are plotted for losses 2%, 4% and 6%. Losses of 6% are maximally tolerated, and above this threshold the key rate vanishes even in the asymptotic limit. Experimentally, squeezing strengths of this order are possible [EHD$^+$11a] but the small tolerated noise threshold of 6% limits the distance between Alice and Bob to a few meters. The reason why the key rate decreases so rapidly by adding noise is because of the application of the uncertainty relation. For a $\delta \approx 0.02$, the squeezing has to be strong in order to not lose the correlation between Alice's and Bob's measurement. But since noise is added vacuum and it broadens the phase space distribution, it severely destroys the correlations. The comparison with the asymptotic optimal case and the case of collective attacks is discussed at the end of Section 6.3.4.

### 6.3.3. Security Proof against Coherent Attacks

We start from the formula for the secure key length for a generic protocol given in Theorem 6.2.2, such that the goal is to find a bound on the min-entropy $\text{H}^{\epsilon}_{\text{min}}(X_A|E)$. This is achieved by applying a variant of the uncertainty relation discussed in Section 4.7 for the discretized measurements of the quadrature variables $Q_A$ and $P_A$. We use the notation introduced in Section 6.3.1 and assume for the following that $\alpha$ and $\delta$ are fixed.

For the security analysis of a quantum key distribution protocol, we have to estimate the quantum state on which the measurements for the raw key are performed

[5] In the experiment presented in [EHD$^+$11a], the dark noise of the detectors is 20 dB below the signal strength, leading to a value of $\mu_{\text{en}} = 0.01$.

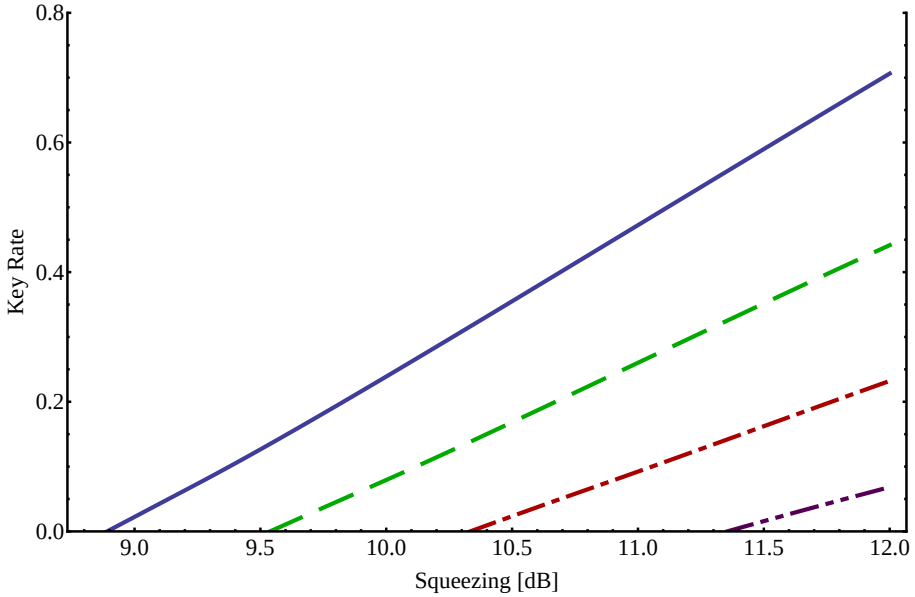


Figure 6.1.: The key rate $\ell/N$ is plotted depending on the squeezing $\lambda_{\text{sq}}$ with fixed ratio between antisqueezing and squeezing of $\lambda_{\text{asq}}/\lambda_{sq} = 1.45$ for symmetric losses of $\mu_{\text{loss}}$ of 0% (solid line), 2% (dashed line), 4% (dash-dotted line) and 6% (dash-dotted-dotted line). The excess noise $\mu_{\text{en}}$ is assumed to be 1%, the error correction efficiency $\beta = 0.95$ and the security parameters $\epsilon_s = \epsilon_c = \epsilon_{pe} = 10^{-6}$.

conditioned on the event that the parameter estimation test is passed. In our case the test consists of the check $d(X_A^{\text{PE}}, X_B^{\text{PE}}) \leq d_0$. In order to make this precise, we assume that first all the quantum systems are distributed. In our protocol, we can discard the subsystems on which Alice and Bob will measure different quadratures and are left with a quantum state on $N$ subsystems denoted by $\omega_{A^N B^N E}$.[6] Since the parameter estimation test commutes with the measurement performed for key generation, we can define the quantum state conditioned on the event that the test is passed. This means that there exists a measurement operator $\Pi^{\text{pass}}$ acting only non-trivially on the $k$ subsystems used for parameter estimation which implements the test. We denote by $\omega_{A^n B^n E}$ the state conditioned on the event that the test is passed and by $p_{\text{pass}} = 1 - p_{\text{ab}}$ the probability that the test is passed.[7] Recall that $n = N - k$ denoted the number of signals left after parameter estimation.

**Application of the Uncertainty Relation.** The goal is to apply the uncertainty relation with quantum side information for the measurements applied by Alice during the protocol (see Theorem 5.3.1). But since the measurements corresponding to the projections onto the intervals $I_{-M} = (-\infty, -\alpha + \delta]$ and $I_M = (\alpha - \delta, \infty)$ (see

[6] Note that at the moment we do not assume anything about the state except that it exists.

[7] We cannot estimate the value of $p_{\text{pass}}$ based on the information obtained in the protocol, so we bound it from above by 1.

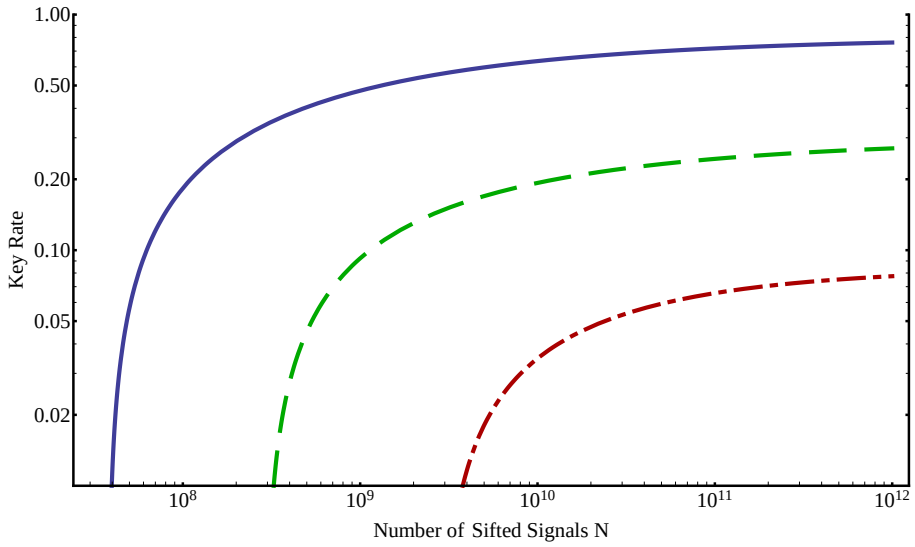


Figure 6.2.: The key rate $\ell/N$ against coherent attacks for fixed squeezing/antisqueezing of 11dB/16dB and symmetric losses of 0% (solid line), 4% (dashed line) and 6% (dash-dotted line). The excess noise $\mu_{\text{en}}$ is 1%, the error correction efficiency $\beta = 0.95$ and the security parameters $\epsilon_s = \epsilon_c = \epsilon_{pe} = 10^{-6}$.

Section 6.3.1 for notation) satisfy

$$\|Q_A^{\frac{1}{2}}(I_M)P_A^{\frac{1}{2}}(I_M)\|^2 \approx 1 \,, \tag{6.21}$$

the uncertainty relation given in Equation (4.57) is trivial. This is clear, because if the product of the lengths of the intervals of two projectors are of order of the minimal uncertainty $\hbar$, then there exists a state with a phase-space distribution sharply peaked in the square spanned by the intervals. But for such a state the entropies of both quadrature measurements are approximately 0 why also the constant in the uncertainty relation has to vanish.

In order to circumvent this problem we use the additional assumption that the source is i.i.d. and that the condition 6.10 holds. Let us introduce another partition of $\mathbb{R}$ into intervals $\{\tilde{I}_k\}_{k\in\mathbb{Z}}$ of equal length $\delta$ enumerated in a way such that $\tilde{I}_k = I_k$ for $k \in \mathcal{X}\backslash\{-M, M\}$. Since the intervals are all of length $\delta$, the overlap appearing in the uncertainty relation is according to Equation (5.52) given by

$$c(\delta) = \max_{i,j} \|Q_A^{\frac{1}{2}}(\tilde{I}_i)P_A^{\frac{1}{2}}(\tilde{I}_j)\|^2 = \frac{\delta^2}{2\pi} \cdot S_0^{(1)}(1, \frac{\delta^2}{4})^2 \,, \tag{6.22}$$

where $S_n^{(1)}(\cdot, u)$ denotes the radial prolate spheroidal wave function of the first kind. Hence, we obtain a non-trivial bound for sufficiently small $\delta$. It also follows that for a sequence of $n$ measurements the overlap is simply $c(\delta)^n$, if on each tensor factor the product $Q_A^{1/2}(\tilde{I}_i)P_A^{1/2}(\tilde{I}_j)$ appears.

In the protocol Alice chooses independently and uniformly at random for each subsystem between phase and amplitude measurement. This can be modeled by introducing a random variable $Z^n = (Z_1, ..., Z_n)$ independent and identically distributed according to the uniform distribution, where $Z_i$ takes value 0 or 1 depending on whether Alice's measures phase or amplitude in the ith run. Let us denote $\mathcal{Z}^n = [0,1]^n$, the uniform distribution over $\mathcal{Z}^n$ by $u$ and by $\{|z^n\rangle\langle z^n|\}_{z^n \in \mathcal{Z}^n}$ an orthonormal basis of a Hilbert space. The random measurement choice of Alice can now be modeled by introducing the state

$$\omega_{A^n B^n E Z^n} = \sum_{z^n \in \{0,1\}^n} \mathrm{u}(z^n) \omega_{A^n B^n E} \otimes |z^n\rangle\langle z^n| \,, \tag{6.23}$$

and the POVM $\{\Pi_{l^n}(z^n) \otimes |z^n\rangle\langle z^n|\}_{z^n \in \mathcal{Z}^n, l^n \in \mathcal{X}^n}$, where

$$\Pi_{l^n}(z^n) = \bigotimes_i \Pi_{l_i^n}(z_i^n) \tag{6.24}$$

with $\Pi_{l_i^n}(0) = Q_A(I_{l_i^n})$ and $\Pi_{l_i^n}(1) = P_A(I_{l_i^n})$. Hence, $z_i^n$ determines whether phase or quadrature is measured. In the following, we let $\bar{z}^n$ be the maximally complementary string of $z^n$, i.e, $\bar{z}_i^n = 1$ if $z_i^n = 0$ and vice versa. Let us denote the post-measurement state obtained by measuring the state $\omega_{A^n B^n E Z^n}$ by the POVM $\{\Pi_{l^n}(z^n) \otimes |z^n\rangle\langle z^n|\}$ by $\omega^n_{X_A B^n E Z^n}$. Here, $X_A$ takes values in $\mathcal{X}^k$ and denotes the random variable which describes the distribution of the raw keys in the actual protocol. Note that all parties are assumed to hold a copy of the variable $Z$ since the measurement choices have been revealed in the sifting phase. Additionally, we introduce a similar POVM for the projections onto the spectrum of Alice's phase and amplitude measurements onto the intervals $\{\tilde{I}_i\}_{i \in \mathbb{Z}}$ and denote them by

$$\tilde{\Pi}_A^{l^n}(z^n) = \bigotimes_i \tilde{\Pi}_A^{l_i}(z_i) \,, \tag{6.25}$$

where $\tilde{\Pi}_A^i(0) = Q_A(\tilde{I}_i)$ and $\tilde{\Pi}_A^i(1) = P_A(\tilde{I}_i)$ for $i \in \mathbb{Z}$. The corresponding post-measurement state is denoted by $\tilde{\omega}^n_{X_A B^n E Z^n}$. Note that here the distribution over $X_A$ can take values in $\mathbb{Z}^n$.

In a first step, we prove now that $\omega^n_{X_A B^n E Z^n}$ is close to $\tilde{\omega}^n_{X_A B^n E Z^n}$ whenever $p_\alpha$ as defined in (6.10) is small. This enables us to finally apply the uncertainty relation to $\tilde{\omega}^n_{X_A B^n E Z^n}$. We assume that the source is i.i.d. and that (6.10) holds. Let us now define $\Lambda = \mathbb{Z} \backslash \mathcal{X}$ and for every $z^n \in [0,1]^n$ the projector

$$\Pi_A^\Lambda(z^n) = \sum_{l^n \in \Lambda} \tilde{\Pi}_A^{l^n}(z^n) \tag{6.26}$$

which corresponds to the event where at least one of the quadrature measurements exceeds $\alpha$. Since

$$\omega_{A^n} = \frac{1}{p_{\text{pass}}} \mathrm{Tr}_{A^k B^N}\left(\Pi_k^{\text{pass}} \omega_{A^N B^N}\right) \leq \frac{1}{p_{\text{pass}}} \omega_A^{\otimes n} \,,$$

we obtain by substituting the definition from Equation (6.10)

$$\mathrm{Tr}\left[\omega_{A^n} \Pi_A^\Lambda(z^n)\right] \leq \frac{1 - p_\alpha^n}{p_{\text{pass}}} = \frac{2g(p_\alpha, n)}{p_{\text{pass}}} \,, \tag{6.27}$$

for every $z^n \in \mathcal{Z}^n$. Let $\omega^{z^n}_{X_A B^n E}$ be the normalized state conditioned on the event $Z^n = z^n$, which can be written as

$$\omega^{z^n}_{X_A BE} = \sum_{l^n \in \mathcal{X}^n} |l^n\rangle\langle l^n| \otimes \omega^{l^n, z^n}_{BE} \ .$$

If we use the similar notation for the state $\tilde{\omega}^n_{X_A B^n E Z^n}$, we obtain that the fidelity between $\omega^{z^n}_{X_A BE}$ and $\tilde{\omega}^{z^n}_{X_A BE}$ (see Definition 3.4)

$$\begin{aligned} F(\omega^{z^n}_{X_A BE}, \tilde{\omega}^{z^n}_{X_A BE})^{\frac{1}{2}} &= \sum_{l^n \in \mathcal{X}^n} F(\omega^{l^n, z^n}_{BE}, \tilde{\omega}^{l^n, z^n}_{BE})^{\frac{1}{2}} \\ &\geq \sum_{l^n \in \mathcal{X}^n} F(\tilde{\omega}^{l^n, z^n}_{BE}, \tilde{\omega}^{l^n, z^n}_{BE})^{\frac{1}{2}} \\ &= 1 - \mathrm{Tr}\Big[\omega_{A^n} \Pi^{\Lambda}_A(z^n)\Big] \ , \end{aligned}$$

The inequality is due to the fact that whenever $|l^n_i| \leq M - 1$ for all $i$ we have that $\omega^{l^n, z^n}_{BE} = \tilde{\omega}^{l^n, z^n}_{BE}$, and otherwise, we can write $\omega^{l^n, z^n}_{BE} = \tilde{\omega}^{l^n, z^n}_{BE} + \sigma^{l^n, z^n}_{BE}$ for a non-normalized state $\sigma^{l^n, z^n}_{BE}$. By using Equation (6.27) and that the fidelity between $\omega^n_{X_A B^n E Z^n}$ and $\tilde{\omega}^n_{X_A B^n E Z^n}$ is just the average over $z^n \in \mathcal{Z}^n$, we arrive at

$$F(\omega_{X_A B^n E Z^n}, \tilde{\omega}_{X_A B^n E Z^n}) \geq \big(1 - 2\frac{g(p_\alpha, n)}{p_{\text{pass}}}\big)^2 \geq 1 - 2\frac{g(p_\alpha, n)}{p_{\text{pass}}} \ ,$$

and by the definition of the purified distance (3.9)

$$\mathcal{P}(\omega^n_{X_A B^n E Z^n}, \tilde{\omega}^n_{X_A B^n E Z^n}) \leq \sqrt{2\frac{g(p_\alpha, n)}{p_{\text{pass}}}} \ . \tag{6.28}$$

The bound in (6.28) can now be used to bound the smooth min- and max-entropy by

$$H^{\epsilon+\tilde{\epsilon}}_{\min}(X_A|EZ^n)_\omega \geq H^{\epsilon}_{\min}(X_A|EZ^n)_{\tilde{\omega}} \tag{6.29}$$

$$-H^{\epsilon+\tilde{\epsilon}'}_{\max}(X_A|B^n Z^n)_{\tilde{\omega}} \geq -H^{\epsilon}_{\max}(X_A|B^n Z^n)_\omega \ , \tag{6.30}$$

where $\epsilon' = \sqrt{2g(p_\alpha, n)/p_{\text{pass}}}$. We simply used the definition of the smooth min- and max-entropies (Definition 4.3.2) and applied the triangle inequality as well as the monotonicity of the purified distance (3.11).

In a next step, we apply a version of the uncertainty relation shown in Theorem 4.7.1 to the state $\tilde{\omega}_{X_A Z^n B^n E}$.

**Corollary 6.3.2.** *Let $\tilde{\omega}_{AZ^n B^n E}$, $\tilde{\Pi}_{k^n}(z^n) \otimes |z^n\rangle\langle z^n|$ and $\tilde{\omega}_{X_A Z^n B^n E}$ as defined above. Then, it follows that*

$$\mathrm{H}^{\epsilon}_{\min}\left(X_A|EZ^n\right)_{\tilde{\omega}} \geq -n \log c(\delta) - \mathrm{H}^{\epsilon}_{\max}\left(X_A|B^n Z^n\right)_{\tilde{\omega}} \ . \tag{6.31}$$

A proof can be found in [Tom12, Corollary 7.6] for the finite-dimensional case, which can be straightforwardly extended to thee infinite-dimensional case. We give here only a proof for the $\epsilon = 0$ case which illustrates the idea.

*Proof.* Let us simplify notation and write $A$, $B$ and $\mathcal{Z}$ instead of $A^n$, $B^n$ and $\mathcal{Z}^n$. We then have that

$$\omega_{X_A ZBE} = \sum_{z\in\mathcal{Z}} u(z) \otimes |z\rangle\langle z| \otimes \omega^z_{X_A BE} \tag{6.32}$$

for $\omega^z_{X_A BE} = \sum_x |x\rangle\langle x| \otimes \omega_{ABE}(\Pi_x(z) \cdot \Pi_x(z))$. It is now easy to see that the uncertainty relation for $\epsilon = 0$ given in Theorem 4.7.1 can be applied for every $z$ individually to and simply gives

$$\mathrm{H}_{\min}\left(X_A|E\right)_{\omega^z} \geq -n \log c(\delta) - \mathrm{H}_{\max}\left(X_A|B\right)_{\omega^{\bar{z}}} \ . \tag{6.33}$$

Hence, by using [Tom12, Proposition 4.6], we obtain

$$\begin{aligned}
\mathrm{H}_{\min}\left(X_A|E\mathcal{Z}^n\right)_{\omega} &= -\log\Big(\sum_z u(z) 2^{-\mathrm{H}_{\min}(X_A|E)_{\omega^z}}\Big) && (6.34)\\
&\geq -\log\Big(2^{n\log c(\delta)} \sum_z u(z) 2^{-\mathrm{H}_{\max}(X_A|B)_{\omega^{\bar{z}}}}\Big) && (6.35)\\
&= -n\log c(\delta) - \mathrm{H}_{\max}\left(X_A|B\mathcal{Z}^n\right)_{\bar{\omega}} \ , && (6.36)
\end{aligned}$$

where

$$\bar{\omega}_{X_A ZBE} = \sum_{z\in\mathcal{Z}} u(\bar{z}) \otimes |z\rangle\langle z| \otimes \omega^{x,z}_{X_A BE}. \tag{6.37}$$

Since $u(\bar{z}) = u(z)$, we obtain the uncertainty relation for $\epsilon = 0$. The technically more involved proof for the $\epsilon > 0$ case can be obtained in the same way as shown in [Tom12, Corollary 7.6]. □

If we combine Corollary 6.3.2 with Equation (6.29) and (6.30) we arrive at

$$H^{\epsilon+2\epsilon'}_{\min}(X_A|EZ^n)_\omega \geq -n\log c(\delta) - H^{\epsilon}_{\max}(X_A|B^n Z^n)_\omega \ .$$

with $\epsilon' = \sqrt{2g(p_\alpha, n)/p_{\text{pass}}}$. Applying the data processing inequality from Proposition 4.5.1 with the quantum channel corresponding to Bob's measurement, we finally obtain

$$H^{\epsilon+2\epsilon'}_{\min}(X_A|EZ^n)_\omega \geq -n\log c(\delta) - H^{\epsilon}_{\max}(X_A|X_B)_\omega \ . \tag{6.38}$$

**Statistical Bound on the Smooth Max-Entropy.** We are left to bound the smooth max-entropy $H^{\epsilon'}_{\max}(X_A|X_B)_\omega$ using the information from the parameter estimation test. The following arguments are similar to the one in [TLGR12]. In a first step, we estimate the probability that the average distance of the strings $X_A$ and $X_B$ deviates from the one of the random sample $X^{\text{PE}}_A$ and $X^{\text{PE}}_B$. This can be done by using standard tools from random sampling without replacement. In the following we denote by $X^{\text{tot}}_A, X^{\text{tot}}_B \in \mathcal{X}^N$ the sequence of all measurement outcomes after sifting from which $X^{\text{PE}}_A, X^{\text{PE}}_B \in \mathcal{X}^k$ are drawn at random.

**Lemma 6.3.3.** *Let $X^{\text{tot}}_A, X^{\text{tot}}_B \in \mathcal{X}^N$ the $N$ data points of Alice and Bob after sifting and $X^{\text{PE}}_A, X^{\text{PE}}_B \in \mathcal{X}^k$ a random sample of it. Then, it follows that*

$$\text{Prob}[d(X_A, X_B) \geq d(X^{\text{PE}}_A, X^{\text{PE}}_B) + \mu | \text{“pass”}] \leq \frac{1}{p_{\text{pass}}} e^{-2\mu^2 \frac{nk^2}{|\mathcal{X}|^2 N(k+1)}} \ . \tag{6.39}$$

*Proof.* Since the probability that the protocol passes is $p_{\text{pass}}$, we find that

$$\begin{aligned}&\text{Prob}[d(X_A, X_B) \geq d(X_A^{\text{PE}}, X_B^{\text{PE}}) + \mu | \text{“pass”}] \\ &\leq \frac{1}{p_{\text{pass}}} \text{Prob}[d(X_A, X_B) \geq d(X_A^{\text{PE}}, X_B^{\text{PE}}) + \mu] \,.\end{aligned}$$

Deriving a bound on $\text{Prob}[d(X_A, X_B) \geq d(X_A^{\text{PE}}, X_B^{\text{PE}}) + \mu]$ is a standard problem from random sampling without replacement. We have that $X_A^{\text{PE}}, X_B^{\text{PE}} \in \mathcal{X}^k$ is a random sample of all measurements $X_A^{\text{tot}}, X_B^{\text{tot}} \in \mathcal{X}^N$. The quantity of interest is $|x_A^i - x_B^i|$, where $x_A^i \in X_A^{\text{tot}}$ and $x_B^i \in X_B^{\text{tot}}$. For this we denote the population mean by $d_{\text{tot}} = d(X_A^{\text{tot}}, X_B^{\text{tot}})$, the sample mean by $d_{\text{PE}} = d(X_A^{\text{PE}}, X_B^{\text{PE}})$, and for the raw key $d_{\text{key}} = d(X_A, X_B)$. Note that these are related via

$$N d_{\text{tot}} = k d_{\text{PE}} + n d_{\text{key}} \,. \tag{6.40}$$

We consider the runs of the protocol as a probabilistic process and treat $d_{\text{tot}}$ as a random variable. As shown in [Ser74], we can bound now

$$\text{Prob}[d_{\text{key}} \geq a + \mu | d_{\text{tot}} = a] \leq e^{-2n\mu^2 \frac{N}{|\mathcal{X}|^2(k+1)}} \,,$$

which is independent of $a$. Here, we used that the maximal value of $|x_A^i - x_B^i|$ is given by $|\mathcal{X}|$.[8] Using Eq. (6.40), we can compute

$$\begin{aligned}\text{Prob}[d_{\text{key}} \geq d_{\text{PE}} + \mu] &= \text{Prob}[d_{\text{key}} \geq d_{\text{tot}} + \frac{k}{N}\mu] \\ &= \sum_a \text{Prob}[d_{\text{tot}} = a] \cdot \text{Prob}[d_{\text{key}} \geq a + \frac{k}{N}\mu | d_{\text{tot}} = a] \\ &\leq e^{-2\mu^2 \frac{nk^2}{|\mathcal{X}|^2 N(k+1)}} \,.\end{aligned}$$

□

In a second step, we give now a bound on the conditional smooth min-entropy which only depends on the average distance between $X_A$ and $X_B$.

**Lemma 6.3.4.** *Let $\mathcal{X}$ be a finite alphabet, $\mathbb{P}(x, x')$ a probability distribution on $\mathcal{X}^n \times \mathcal{X}^n$ for some $n \in \mathbb{N}$, $d_0 > 0$ and $\epsilon > 0$. If $\mathbb{P}$ satisfies $\text{Prob}_{\mathbb{P}}[d(x, x') \geq d_0] \leq \epsilon^2$, then*

$$\text{H}_{\max}^{\epsilon}\left(X|X'\right)_{\mathbb{P}} \leq n \log \gamma(d_0) \,,$$

*where*

$$\gamma(t) = (t + \sqrt{1+t^2}) \Big( \frac{t}{\sqrt{1+t^2} - 1} \Big)^t \,.$$

*Proof.* The idea is to first cut off the part such that $d(x, x') \geq d_0$ by using the smoothing parameter and then bound the max-entropy. So, let us define the probability distribution

$$\mathbb{Q}(x, x') = \begin{cases} \frac{\mathbb{P}(x,x')}{\text{Prob}_{\mathbb{P}}[d(x,x') \leq d_0]}, & \text{if } d(x, x') \leq d_0 \\ 0, & \text{else} \end{cases}$$

[8] Here, it is necessary that the alphabet is finite.

and note that $F(\mathbb{P},\mathbb{Q}) = \mathrm{Prob}_{\mathbb{P}}[d(x,x') \leq d_0]$. Hence, it follows that $\mathcal{P}(\mathbb{P},\mathbb{Q}) = \sqrt{\mathrm{Prob}_{\mathbb{P}}[d(x,x') \geq d_0]} \leq \epsilon$. Using the definition of the smooth max-entropy (4.12) and that the 0-Rényi-entropy is bigger than the max-entropy [TSSR10], we obtain

$$\mathrm{H}^{\epsilon}_{\max}\left(X|X'\right)_{\mathbb{P}} \leq \mathrm{H}_{\max}\left(X|X'\right)_{\mathbb{Q}} \leq H_0(X|X')_{\mathbb{Q}} \ .$$

The conditional 0-Rényi entropy of the distribution $\mathbb{Q}$ is then given by [Ren05, Remark 3.1.4]

$$\begin{aligned} H_0(X|X')_{\mathbb{Q}} &= \max_{x'} \log |\{x \in \mathcal{X}^n \ ; \ \mathbb{Q}(x,x') \neq 0\}| \\ &\leq \log |\{x \in \mathbb{Z}^n \ ; \ \sum_{i=1}^n |x_i| \leq nd_0\}| \ . \end{aligned}$$

For any $\lambda > 0$, we can estimate

$$\begin{aligned} |\{x \in \mathbb{Z}^n \ ; \ \sum_{i=1}^n |x_i| \leq nd_0\}| &\leq \sum_{x\in\mathbb{Z}^n} \exp[\lambda(nd_0 - \sum_{i=1}^n |x_i|)] \\ &= e^{\lambda n d_0}\Big(\sum_{z\in\mathbb{Z}} e^{-\lambda|z|}\Big)^n \\ &= \Big(e^{\lambda d_0}\frac{1+e^{-\lambda}}{1-e^{-\lambda}}\Big)^n \ . \end{aligned}$$

By optimizing over $\lambda > 0$, one finds that $|\{x \in \mathbb{Z}^n \ ; \ \sum_{i=1}^n |x_i| \leq nd_0\}| \leq \gamma(d_0)^n$. This completes the proof. □

Let us now combine Lemma 6.3.3 and 6.3.4 by setting

$$(\epsilon')^2 = \frac{1}{p_{\mathrm{pass}}} e^{-2\mu^2 \frac{nk^2}{|\mathcal{X}|^2 N(k+1)}} \ , \tag{6.41}$$

from which then follows that

$$H^{\epsilon'}_{\max}(X_A|X_B)_{\omega^{\mathrm{pass}}} \leq n \log \gamma(d_0+\mu) \tag{6.42}$$

for

$$\mu = |\mathcal{X}| \sqrt{\frac{N(k+1)}{nk^2} \ln \frac{1}{\sqrt{p_{\mathrm{pass}}}\epsilon'}} \ .$$

Combining this with the uncertainty relation given in Equation (6.38) and bounding $p_{\mathrm{pass}} \leq 1$, we obtain the lower bound for the extractable finite-key length presented in Theorem 6.3.1.

### 6.3.4. Collective Attacks and Comparison with Coherent Attacks

In the case of collective attacks, we can assume that the state between Alice, Bob and Eve has tensor product structure. That is after $\tilde{N}$ use of the quantum channel the state between these three parties can be written by $\omega_{ABE}^{\otimes\tilde{N}}$. Alice and Bob can do state estimation to guess $\omega_{AB}$. From this the information of Eve can be bounded

by assuming that she holds an arbitrary purification of $\omega_{AB}$. This is then used to compute a bound on the smooth min-entropy $\mathrm{H}_{\min}^{\epsilon}(X_A|E^n)_{\omega^{\otimes n}}$ which gives then a bound on the extractable finite-key length via Theorem 6.2.2. The following treatment focuses on the information theoretic part and the finite statistics in the state estimation is mostly neglected.

**The Protocol and a Formula for the Finite-Key Length.** The protocol only differs from the case of coherent attacks in the parameter estimation phase. For the key generation Alice and Bob choose randomly and independently between phase $Q_A, Q_B$ and amplitude measurements $P_A, P_B$. With a pre-determined probability, they perform at random additional measurements necessary for state estimation. We do not specify such measurements at the moment and refer to the end of this section for a discussion. After $\tilde{N}$ measurements are performed Alice and Bob announce their measurement choices. As in the case of coherent attacks, they use the measurement in which both have measured phase or amplitude to form the raw key with the same partition as introduced in Section 6.3.1. We assume that in the following $\delta$ and $\alpha$ are fixed and that the use the measurement results from $n$ instances to form the raw key denoted by $X_A, X_B \in \mathcal{X}^n$.

The remaining data is used for state estimation. This includes the measurements explicitly done for state estimation as well as the ones which were not used for the raw key. We assume that the state estimation scheme determines a confident set $\mathcal{C}_{\epsilon_{pe}} \subset \mathbb{R}^{4\times 4}$, which ensures that whenever the protocol does not abort the covariance matrix $\Gamma$ of the two mode state $\omega_{AB}$ lies in $\mathcal{C}_{\epsilon_{pe}}$ with probability at least $1-\epsilon_{pe}$.[9] In the following, we denote the two-mode Gaussian state corresponding to a covariance matrix $\Gamma$ by $\omega_{AB}^{\Gamma}$. As proven in the next section, the described protocol leads to the following bound on the extractable finite-key length.

**Theorem 6.3.5.** *Let us assume that an error correction scheme broadcasting* $\mathrm{leak}_{\mathrm{EC}}$ *bits of classical information is used and the correctness test via two-universal hash functions onto an alphabet of size* $\log(1/\epsilon_c)$ *is passed. Moreover, we are given a confidence set* $\mathcal{C}_{\epsilon_{pe}}$*. By assuming only collective attacks, one can extract an* $\epsilon_c$*-correct and* $(\epsilon_s+\epsilon_{pe})$*-secret key of length*

$$n \cdot \inf_{\Gamma\in\mathcal{C}_{\epsilon_{pe}}} H(X_A|E)_{\omega^{\Gamma}} - \sqrt{n}\cdot\Delta - \mathrm{leak}_{\mathrm{EC}} - 2\log\frac{1}{\epsilon_1} - \log\frac{1}{\epsilon_c} + 2 \tag{6.43}$$

*where*

$$\Delta = 4\log(2^{\frac{1}{2}H_{\max}(X_A)_{\omega}+1}+1)\sqrt{\log\frac{8}{(\epsilon_s-\epsilon_1)^2}}\,. \tag{6.44}$$

*Here* $\omega_{X_AE}^{\Gamma}$ *is obtained from* $\omega_{AB}^{\Gamma}$ *by applying the POVM corresponding to Alice's measurement to an arbitrary purification* $\omega_{ABE}^{\Gamma}$*. Note that* $\omega_{X_AE}^{\Gamma}$ *depends on* $\delta$ *and* $\alpha$ *via the POVM of Alice.*

[9] We assume that Alice and Bob chose their coordinates such that the first moments of the state vanish. For the analysis presented here it is then enough to estimate the second moments of the state independent whether the state is actually a Gaussian state or not.

Given Equation (6.43), the difficulty is now to obtain reliable confident sets $\mathcal{C}_{\epsilon_{pe}}$. Note also that Theorem 6.3.5 holds for any continuous-variable protocol. The dependence on the state is implicitly via the computation of the von Neumann entropy $H(X_A|E)$ and the leakage term $\text{leak}_{\text{EC}}$. Moreover, also the binning of the measurements used to obtain the raw key $X_A \in \mathcal{X}^n$ can be changed arbitrarily. The only crucial assumption is that the measurements form a complete POVM, that is, summing up to the identity. This is necessary to replace the infimum over all states with a covariance matrix in $\mathcal{C}_{\epsilon_{pe}}$ by the infimum over the Gaussian representatives. This is usually called the optimality of Gaussian attacks [GPC06, NGA06]. The technical statement suitable for our security analysis is also proven in Appendix A.1. Unfortunately, this result is not compatible with post-selection [SRLL02], which is one of the tools to beat the 50% (3dB) loss limit.

Another way to overcome the 50% loss limit is to use a reverse reconciliation scheme [] in which the key is generated from Bob's data (which is assumed to be more noisy) and in the error correction scheme Alice corrects her data. This applies directly to our formula by changing the dependence on $X_A$ by $X_B$ in formula (6.43). The idea of reverse reconciliation is that since the source is located in Alice's lab Bob's data is more noisy, which makes it more difficult for Eve to guess Bob's measurement outcomes. The advantage then is clear from the asymptotic key rate in terms of the mutual information (6.7), in which an exchange from $X_A$ to $X_B$ only decreases Eve's mutual information about the raw key.

**Plot of the Finite-Key Rate Secure against Gaussian Collective Attacks** For the state estimation procedure and therefore the computation of the confident set $\mathcal{C}_{\epsilon_{pe}}$, we assume that Eve is restricted to collective Gaussian attacks. Under the assumption of a Gaussian state Alice and Bob then reconstruct their state using homodyne measurement of the quadratures $Q_A$, $Q_B$, $P_A$ and $P_B$ by assuming that they correspond to the coordinates leading to maximal correlations. The covariance matrix can then be estimated using likelyhood estimators. For the details as well as the explicit formulas we refer to [LGG10]. If we assume that the actual distributed Gaussian state has covariance matrix $\Gamma$, the confident set $\mathcal{C}_{\epsilon_{pe}}$ is given by [EHD+11a]

$$\mathcal{C}_{\epsilon_{pe}} = \{\tilde{\Gamma} \mid \Gamma_{ij} - \frac{f(\epsilon_{pe})}{\sqrt{N'}}\Gamma_{ij} \leq \tilde{\Gamma} \leq \Gamma_{ij} + \frac{f(\epsilon_{pe})}{\sqrt{N'}}\Gamma_{ij}\} \tag{6.45}$$

where $f(\epsilon_{pe})$ is a function depending on $\epsilon_{pe}$ and $N'$ is the number of measurements used for the reconstruction per variance.

We consider the same error model as used in the case of coherent attacks (see end of Section 6.3.2). That means, we assume symmetric losses $\mu_{\text{loss}}$ and a constant excess noise of $\mu_{\text{en}} = 0.01$.[10] Furthermore, the squeezing and antisqueezing strengths $\lambda_{\text{sq}}$ and $\lambda_{\text{asq}}$ are given for the one mode states before entangling over the balanced beam splitter. In parctice, the value of $\alpha$ has to be chosen such that the hashing

[10] It would also be interesting to discuss the effect of reverse reconciliation and consider an asymmetric situation in which the losses on Bob's side are relatively higher. But here we just focus on the comparison with the case of coherent attacks in which a symmetric model is assumed because of the small tolerated noise.

with two-universal functions is still possible. For simplicity, we take $\alpha \to \infty$ which is the theoretical optimum.

The value of $\delta$ affects the key rate via the computation of the conditional von Neumann entropy $H(X_A|E)$. Because we consider measurements with a finite spacing $\delta$, the post-measurement states conditioned on the event that for instance Alice measured $x \in \mathcal{X}$ is not a Gaussian state anymore. This makes the computation of $H(X_A|E)$ little more involved as in the case of continuous measurements (see e.g. [LBGP$^+$07]). But as shown in Appendix A.2 it can be estimated by

$$H(X_A|E)_\omega \geq H(E)_{\omega(0)} + H(X_A)_\omega - H(AB)_\omega \ ,$$

where $\omega_E(0)$ denotes the post-measurement state on Eve's side conditioned on the event that Alice measures a (continuous) quadrature $x = 0$. Since $\omega_E(0)$ and $\omega_{AB}$ are Gaussian states the von Neumann entropy can be computed (see, e.g., [SIDS04]).

If nothing else mentioned, the following plots are computed for the same parameters as in the case if coherent attacks, that is, the error correction efficiency is taken to be $\beta = 0.95$ (see Equation 6.15) and security parameters $\epsilon_s = \epsilon_c = \epsilon_{pe} = 10^{-6}$ and $\epsilon_1 = \epsilon_s/2$. In Figure 6.3, we plotted the finite-key rate for squeezing and antisqueezing $\lambda_{\text{sq}} = 11\text{dB}$ and $\lambda_{\text{sq}} = 16\text{dB}$. We see that without losses a positive key rate is obtained slightly above $N = 10^6$ sifted signals. The highest tolerated loss in this symmetric model is $\mu_{\text{loss}} = 0.25$.

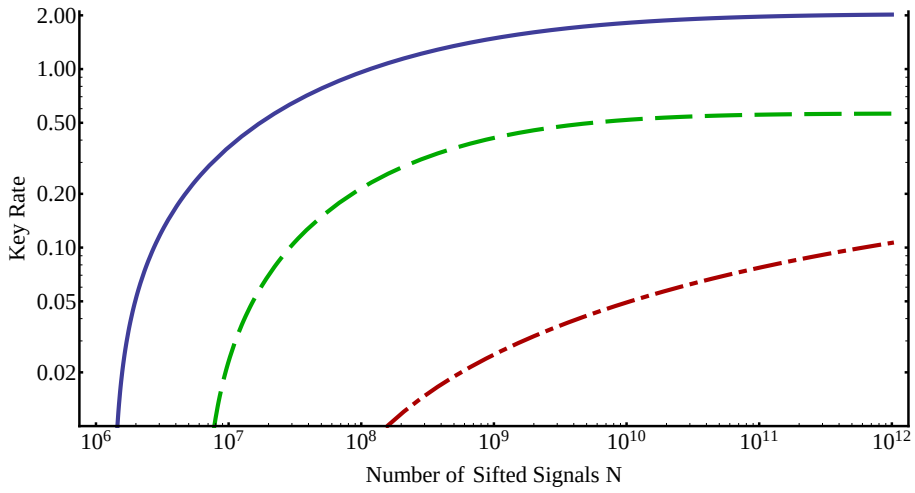


Figure 6.3.: The key rate $\ell/N$ against collective Gaussian attacks is plotted in dependence of the number of sifted Signals $N$. The squeezing/antisqueezing is 11dB/16dB and the different graphs belong to symmetric losses of 0% (solid line), 15% (dashed line), 25% (dash-dotted line). The excess noise $\mu_{\text{en}}$ is 1%, the error correction efficiency $\beta = 0.95$ and the security parameters $\epsilon_s = \epsilon_c = \epsilon_{pe} = 10^{-6}$.

We see that the key rate computed against Gaussian collective attacks is significantly higher than the one for coherent attacks. It is known that under the

assumption that we also trust Bob's measurements (and that they are modeled by projection onto the spectrum on the phase and amplitude operator), the asymptotic rate

$$I(X_A : X_B)_\omega - \beta I(X_A : E)_\omega, \tag{6.46}$$

can be proven to be secure [RC09]. This is exactly the asymptotic limit for the formula computed in the case of collective attacks. Hence, we know that the finite-key rate computed in Section 6.3.2 do not converge to the asymptotic limit.[11] In fact a closer look at the security proof given in Section 6.3.3 shows that the bound on the smooth max-entropy is essentially tight but the uncertainty relation is not. One can show that the difference is independent of the squeezing and roughly given by 1.5 bits. In Figure 6.4, we plotted the key rate for squeezing and antisqueezing of $\lambda_{\text{sq}} = 11\text{dB}$ and $\lambda_{\text{sq}} = 16\text{dB}$ in dependence on symmetric losses for coherent and collective Gaussian attacks and compare it with the asymptotic optimal rate.

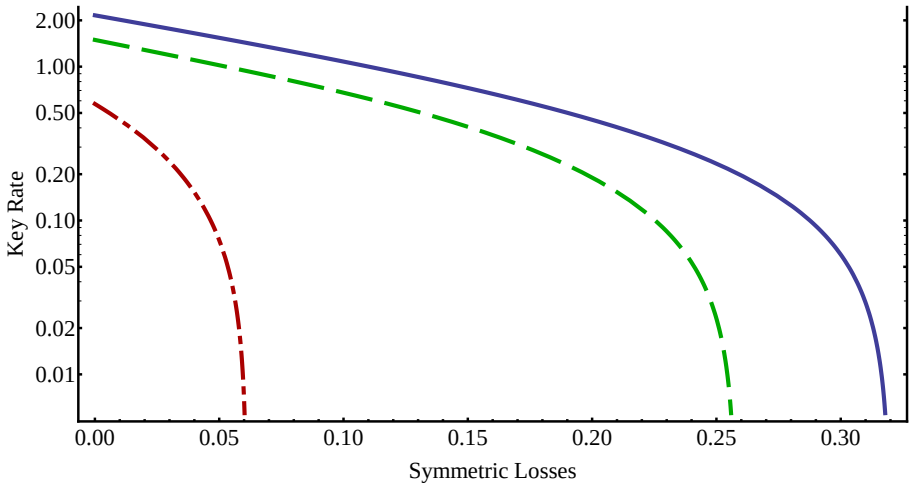


Figure 6.4.: The Key rate is plotted depending on the losses $\mu_{\text{loss}}$ for security against coherent attacks (dot-dashed line) and collective Gaussian attacks at $N = 10^9$ (dashed line), as well as the asymptotic rate 6.46 for optimal error correction $\beta = 1$ (solid line). The squeezing/antisqueezing is 11dB/16dB and for the finite-key rate we set the number of sifted signals $N = 10^9$ and the security parameters $\epsilon_s = \epsilon_c = 10^-6$.

### 6.3.5. Security Proof against Collective Attacks

Let us fix the parameters $\alpha$ and $\delta$ which determine the measurements. We start again with Theorem 6.2.2 and have to bound the smooth min-entropy. According to the definition of the confidence set $\mathcal{C}_{\epsilon_{pe}}$, we know that up to an error of $\epsilon_{pe}$ the state

[11] Note that in contrast, the security proof based on [RC09] is not suitable for a finite-key analysis because the number of signals $N$ must be of orders ($N \gtrsim 10^{14}$) which are so far not possible in practice.

$\omega_{AB}$ has a covariance matrix $\Gamma \in \mathcal{C}_{\epsilon_{pe}}$. The error $\epsilon_{pe}$ can be added to the security parameter of the protocol. Let now $\omega_{AB}$ be a state with covariance matrix $\Gamma \in \mathcal{C}_{\epsilon_{pe}}$. We then take an arbitrary purification $\omega_{ABE}$ and give Eve the entire complementary system $E$. Note that $\mathcal{H}_E$ can chosen to be isomorphic to $\mathcal{H}_{AB}$. This provides her with the best possible situation. We then denote by $\omega_{X_A BE}$ the normalized post-measurement state after Alice applied the POVM $\{\frac{1}{2}Q_A(I_i) + \frac{1}{2}P_A(I_i)\}_{i\in\mathcal{X}}$. Recall that $Q_A(I_i)$ ($P_A(I_i)$) denotes the projector onto the interval $I_i$ of the spectrum of the operator $Q_A$ ($P_A$).

We show now that for any state $\omega_{AB}$ with a covariance matrix $\Gamma \in \mathcal{C}_{\epsilon_{pe}}$ there exists a lower bound on $\mathrm{H}^{\epsilon}_{\min}(X_A^n|E^n)_{\omega^{\otimes n}}$ which only depends on the covariance matrix $\Gamma$ of $\omega_{AB}$. In order to bound the smooth min-entropy of the $n$-fold tensor product $\omega_{X_AE}^{\otimes n}$, we use the asymptotic equipartition property from Theorem 4.5.3. This leads to

$$\mathrm{H}^{\epsilon}_{\min}(X_A^n|E^n)_{\omega^{\otimes n}} \geq nH(X_A|E)_\omega - \sqrt{n}\, 4\log(\eta)\sqrt{\log\frac{2}{\epsilon^2}}\,, \tag{6.47}$$

where $\eta = 2^{-\frac{1}{2}\mathrm{H}_{\min}(X_A|E)_\omega} + 2^{\frac{1}{2}\mathrm{H}_{\max}(X_A|E)_\omega} + 1$. The value of $\eta$ can now be simplified by using that for an arbitrary purification $\omega_{X_AEC}$ of $\omega_{X_AE}$, we have according to the definition of the max-entropy (4.6)

$$-H_{\min}(X_A|E)_\omega = H_{\max}(X_A|C)_\omega \leq H_{\max}(X_A)_\omega$$

where the last inequality is due to the data processing inequality (4.18). Furthermore, we can also use the data processing inequality (4.18) to bound the max-entropy $H_{\max}(X_A|E)_\omega \leq H_{\max}(X_A)_\omega$. Using this two estimations, we obtain

$$2^{-\frac{1}{2}H_{\min}(X_A|E)_\omega} + 2^{\frac{1}{2}H_{\max}(X_A|E)_\omega} \leq 2^{\frac{1}{2}H_{\max}(X_A)_\omega + 1}\,.$$

Hence, we finally arrive at

$$H^{\epsilon}_{\min}(X_A|E)_{\omega^{\otimes n}} \geq n\cdot H(X_A|E)_\omega - \sqrt{n}\cdot\Delta \tag{6.48}$$

with

$$\Delta = 4\log(2^{\frac{1}{2}H_{\max}(X_A)_\omega + 1} + 1)\sqrt{\log\frac{2}{\epsilon^2}}\,. \tag{6.49}$$

In a last step, we use that the infimum of the von Neumann entropy $H(X_A|E)_\omega$ over all states $\omega_{AB}$ with the same covariance matrix $\Gamma$ is attained for the Gaussian state $\omega^{\Gamma}_{AB}$. This is usually referred to as the fact that Gaussian attacks are optimal within all possible ones [GPC06, NGA06]. In Appendix A.1, we give a proof by means of a general extremality theorem for Gaussian states [RWW06]. Hence, since these bounds hold for any $\Gamma \in \mathcal{C}_{\epsilon_{pe}}$, we obtain for any possible state $\omega_{AB}$ with covariance in $\mathcal{C}_{\epsilon_{pe}}$ that

$$H^{\epsilon}_{\min}(X_A^n|E)_{\omega^{\otimes n}} \geq n\cdot \inf_{\Gamma\in\mathcal{C}_{\epsilon_{pe}}} H(X_A|E)_{\omega^\Gamma} - \sqrt{n}\cdot\Delta. \tag{6.50}$$

Using this result to bound the smooth min-entropy in Theorem 6.2.2 yields Equation (6.43).

# 7. Device-Independent Quantum Key Distribution and Extremal Correlations

## 7.1. Introduction

The goal in device-independent quantum key distribution is to prove security without any assumption about the source and the measurement devices (see Section 1.4). One employs the principle that correlations can be generated by a quantum mechanical system which allow no local hidden variable model. This was realized and formalized by Bell in 1964 [Bel64]. We focus here on the question of independence of correlations often also referred to as monogamy of correlations [BKP06]. This means that independent of the actual realization of the quantum system, the measurement outcomes of the honest parties are uncorrelated to any measurement of a possible adversary (see Definition 7.6). Hence, an adversary can only guess the outcomes of the measurements. Motivated by this property, we call such correlations secure.[1]

In Section 7.3, we show that such secure correlations are in one-to-one correspondence with extremal points in the set of all possible quantum correlations. The proof, which is given here for quantum mechanics, can be generalized to any general probabilistic theory. One direction of this result, namely that extremality implies security, was shown for non-signal theories in [BLM$^+$05]. Hence, our result implies also the converse. How extremality of a correlation can be used to prove device-independent security of a two-party quantum key distribution protocol is shown in [BHK05] for the case of individual attacks and an eavesdropper which is only constraint by the non-signaling principle.

In Section 7.3.1, we discuss the rather peculiar situation in which the correlation determines the quantum representation, that is, the state and the observables uniquely. This property together with extremality implies that all possible measurements of the honest parties are statistically independent of any measurement an eavesdropper can perform (see Theorem 7.3.8).

While the general part holds for any number of parties, measurements and outcomes, we study in Section 7.4 methods to find extremal points for particular situations. In the case of two binary measurements at each site, the situation can be reduced to the study of irreducible representations of the universal C*-algebra of two projections [Ped68] and tensor products thereof (see Section 7.4.1). This is then applied to the case of 2 parties in Section 7.4.2, where a method to certify extremality is discussed, by which a parametrized family of extremal correlations are obtained.

[1] Note that here "security" refers to a property of a correlation table and should not be confused with the definition of a secure key given in the previous chapter.

In Section 7.4.3, we discuss the case of two parties and an arbitrary number of binary measurements, which was essentially solved by Tsirelson [Tsi85]. We review his results and apply it to particular questions like extremality of correlations or uniqueness of quantum representations.

## 7.2. Basic Setup and Definitions

We consider a correlation experiment with $N$ different parties which are space-like separated. Each party can measure $M$ different observables where each has $K$ different outcomes. This situation can be described by a correlation table which gives the probabilities for every outcome conditioned on every possible choices of measurements of the parties. Let us denote the measurement choices or also called settings of the $N$ parties by $\underline{s} = (s_1, \ldots, s_N)$, with $s_i \in \{1, \ldots, M\}$. For each setting $s_i$, we assume that the $K$ outcomes are similarly labeled by $\{1, 2, ..., K\}$ such that the every measurement setting $\underline{s}$ produces an output string $\underline{x} = (x_1, \ldots, x_N)$ where $x_i \in \{1, \ldots, K\}$. Hence, the experiment is fully characterized by $M^N$ conditional probability distributions denoted $\mathbb{P}(\underline{x}|\underline{s})$ satisfying

$$\sum_{i=1}^{N} \sum_{x_i=1}^{K} \mathbb{P}(\underline{x}|\underline{s}) = 1 \;\; \forall \underline{s} \in \{1, ..., M\}^n \,. \tag{7.1}$$

Such a set of conditional probability distributions $\mathbb{P}$ is called a correlation table. Moreover, we refer to such an experiment determined by $N$ parties, $M$ measurements and $K$ outcomes each as the $(N, M, K)$ case. For convenience, we always restrict to the symmetric case in which all parties have the same number of measurements $(M)$, and each measurement has the same number of outcomes $(K)$. Because the proofs of the following general results do not depend particularly on these numbers, they also hold if they are different for each party and measurement. In the following, we think of $\mathbb{P}$ as vectors in $\mathbb{R}^d$ with $d = (MK)^N$.

The assumed physical theory restricts the possible correlation tables by additional conditions other than the normalization (7.1). Let us consider the example of non-signaling theories in which no instantaneous interaction/communication is possible. Since we assume that the parties (and in particular the space-time points in which they chose and perform their measurements) are space-like separated, the outcome of party $i$ must not depend on the measurement settings $s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_N$ of the other parties. The constraints for the correlation tables then reads

$$\mathbb{P}(x_{k_1}, x_{k_2}, \ldots, x_{k_l}|s_1, s_2, \ldots, s_N) = \mathbb{P}(x_{k_1}, x_{k_2}, \ldots, x_{k_l}|s_{k_1}, s_{k_2}, \ldots, s_{k_l}) \tag{7.2}$$

for any $(x_{k_1}, x_{k_2}, \ldots, x_{k_l})$. Since these are finitely many linear constraints in $\mathbb{P}(\underline{x}|\underline{s})$, the set of all non-signaling correlation tables form a polytope. We denote them by $\mathcal{P}(N, M, K)$ or short $\mathcal{P}$ if the number of parties, measurements and outcomes are clear from the context.

The set of correlation tables which are convex combinations of deterministic events are called classical correlations and denoted by $\mathcal{C}(N, M, K)$. These are the correlations which allow a local hidden variable (LHV) model [Bel64]. Since the set is defined as the convex hull of a finite number of extreme points (the deterministic

events) it follows that also $\mathcal{C}$ is a polytope. A polytope is uniquely determined by either its extreme points or the faces. A face corresponds to a supporting hyperplane of the polytope. The inequalities which determine the face of the classical polytope $\mathcal{C}$ are called (proper) Bell inequalities [Bel64].[2] The most prominent Bell inequality is the Clauser-Horn-Shimony-Holt (CHSH) inequality which holds in the (2,2,2) case [CHSH69]. Up to relabeling it is the only proper Bell inequality in the (2,2,2) case as proven in [Fin82]. For more parties as well as larger numbers of measurements and outcomes the problem to determine all the Bell inequalities is very difficult. For more details about finding Bell inequalities as well as recent results see [Proa].

Let us turn now to the set of correlation tables which can be realized within quantum mechanics. We start with a definition (c.f. [Tsi93]).

**Definition 7.2.1.** *A quantum representation of a correlation table $\mathbb{P}$ consists of a Hilbert space $\mathcal{H}$ together with a set of positive operator valued measures $\{F_i(x_i|s_i)\}_{x_i=1}^{K}$ for $i \in \{1,\dots,N\}$ and $s_i \in \{1,\dots,M\}$, and a positive normalized linear functional $\omega : \mathcal{B}(\mathcal{H}) \to \mathbb{C}$ such that*

$$[F_i(x|s), F_j(x|s)] = 0 \tag{7.3}$$

*for all $i \neq j$ and*

$$\mathbb{P}(\underline{x}|\underline{s}) = \omega\big(F(\underline{x}|\underline{s})\big) \ , \tag{7.4}$$

*where $F(\underline{x}|\underline{s}) = \prod_i F_i(x_i|s_i)$. The set of all correlation tables $\mathbb{P}$ which admit a quantum representation is denoted by $\mathcal{Q}(N,M,K)$.*

In the following, we use the shorthand notation $(\mathcal{H}, \{F(\underline{x}|\underline{s})\}, \omega)$ for a quantum representation as given in Definition 7.2.1. The Hilbert space dimension of a quantum representation can be infinite and is not constraint. Note that we consider here the $C^*$-algebra state space of $\mathcal{B}(\mathcal{H})$ to generat $\mathcal{Q}$ and not only allow normal states which can be written as a density matrix according to Equation (2.3). This is important for the state space to be weakly* compact which implies compactness of $\mathcal{Q}$.

**Lemma 7.2.2.** *The set of quantum correlations $\mathcal{Q}$ defined above is a convex and compact set for every $(N,M,K)$.*

*Proof.* The set $\mathcal{Q}$ is a subset of the finite-dimensional vector space $\mathbb{R}^d$ with $d = (MK)^N$. Due to the normalization property given in Equation (7.1) it also follows that $\mathcal{Q}$ is bounded. We first show the convexity of $\mathcal{Q}$. Let $\mathbb{P}_1$ and $\mathbb{P}_2$ be correlation tables in $\mathcal{Q}$. We show that for any $0 \leq p \leq 1$ the correlation table $\mathbb{P} = p\mathbb{P}_1 + (1-p)\mathbb{P}_2$ admits a quantum representation. Since $\mathbb{P}_1, \mathbb{P}_2 \in \mathcal{Q}$, there exist quantum representations $(\mathcal{H}_l, \{F^{(l)}(\underline{x}|\underline{s})\}, \omega^{(l)})$ such that

$$\mathbb{P}_l(\underline{x}|\underline{s}) = \omega^{(l)}\big(F^{(l)}(\underline{x}|\underline{s})\big) \, .$$

Let us consider the direct sum of the Hilbert spaces $\mathcal{H} = \mathcal{H}_1 \oplus \mathcal{H}_2$ and define the operators $F_i(x_i|s_i) = F_i^{(1)}(x_i|s_i) \oplus F_i^{(2)}(x_i|s_i)$ and the state $\omega = p\omega_1 \oplus (1-p)\omega_2$. It is easy to verify that the operators $F_i(x_i|s_i)$ together with the state $\omega$ define a valid quantum representation of $\mathbb{P} \in \mathcal{Q}$.

[2] Sometimes any inequality which constraints classical correlation tables is called Bell inequality and not just the one which correspond to faces.

In order to show compactness, it is enough to show that $\mathcal{Q}$ is closed in $\mathbb{R}^d$. For that we consider a converging sequence $\{\mathbb{P}_k\}$ of correlation tables in $\mathcal{Q}$ with quantum representations $(\mathcal{H}_k, \{F^{(k)}(\underline{x}|\underline{s})\}, \omega^{(k)})$. Let $\mathbb{P}$ be the limit of the sequence $\mathbb{P}_k$. We then define the Hilbert space $\mathcal{H} = \bigoplus_k \mathcal{H}_k$ and the operators $F_i(x_i|s_i) = \bigoplus_k F_i^{(k)}(x_i|s_i)$. Let now $\omega_\alpha$ be the sequence of states which is zero on all subspaces $\mathcal{H}_k$ except for $k = \alpha$ and on $\mathcal{H}_\alpha$ equal to $\omega^{(\alpha)}$. Since $\|\omega_\alpha\| = 1$ for all $\alpha$, we have that the sequence is bounded. Because the state space of a $C^*$-algebra is weakly* compact (see e.g., [BR79, Theorem 2.3.15]), there exists according to the Banach Alaouglo Theorem a weakly* converging subsequence. If $\omega$ is the limit of the subsequence, then it follows that the operators $\{F_i(x_i|s_i)\}$ together with the state $\omega$ is a quantum representation of $\mathbb{P}$, and hence, $\mathbb{P} \in \mathcal{Q}$. □

Note that we use the algebraic approach and model different parties by commuting operators rather than require tensor product structure. The question whether the two approaches lead to the same set of correlation tables is referred to as Tsirelson's problem [Prob, SW08]. It is clear that correlation tables which can be obtained by assuming tensor product structure are contained in $\mathcal{Q}$. Tsirelson showed that in the case of finite-dimensional Hilbert spaces the set of correlation tables which can be obtained by modeling different parties with tensor product structure are similar to the one which can be obtained with commuting operators [Prob]. In the case of infinite-dimensional systems this is still an open question and only recently connected to Conne's embedding problem which remains an outstanding question in operator theory [JNP$^+$11].

In contrast to $\mathcal{C}$, the set $\mathcal{Q}$ is not a polytope. In particular, it is the convex span of a continuum of extremal points. For an example see [Mas03] in which the set of correlation tables for the $(2, 2, 2)$ case was completely determined by means of a set of non-linear inequalities. The convex and compact structure of $\mathcal{Q}$ allows us to use supporting hyperplanes to characterize it. A supporting hyperplane is given by a linear functional $f : \mathbb{R}^d \to \mathbb{R}$ such that there exists a real number $q_f > 0$ with[3]

$$f(v) \leq q_f \ \forall x \in \mathcal{Q} \ \text{ and } \ \exists\, v \in \mathcal{Q} : \ f(v) = q_f \,. \tag{7.5}$$

The fact that there exists always a $v$ such that $f(v) = q_f$ follows by the compactness of $\mathcal{Q}$. These supporting functionals are the analogues of the Bell inequalities for $\mathcal{Q}$ and called Tsirelson inequalities in the following.[4] Conversely, every linear functional $f$ with $q_f = \sup_{v \in \mathcal{Q}} f(v) =$ defines a supporting hyperplane of $\mathcal{Q}$. If we denote by $\mathcal{Q}^*$ the set of supporting affine functionals $(f, q_f)$, then the bipolar theorem connects the $\mathcal{Q}$ via $(\mathcal{Q}^*)^* = \mathcal{Q}$ [CT07]. The problem to find the maximal quantum value $q_f$ for a given functional $f$ is in general difficult. It can for instance be written as a hierarchy of semi-definite programs (SDP) [DLTW08, NPA08]. But the sizes of the SDP's in the hierarchies grow exponentially and the speed of convergence of the hierarchy for low orders is not clear.

The different convex sets $\mathcal{C}$, $\mathcal{Q}$ and $\mathcal{P}$ defined above satisfy $\mathcal{C} \subset \mathcal{Q} \subset \mathcal{P}$, where the inclusions are proper. For instance, in the $(2, 2, 2)$ case we have that the maximum

[3] Note that in general $d = (MK)^N$, but it is often convenient to use linear constraints as in (7.1) and (7.2) to reduce the dimensions to the actual degrees of freedom.

[4] Tsirelson was the first who proved that the maximal quantum violation of the CHSH inequality is given by $2\sqrt{2}$ [Tsi80]

value of the CHSH inequality [CHSH69] is 2 for classical correlations in $\mathcal{C}$, $2\sqrt{2}$ for quantum correlations in $\mathcal{Q}$ [Tsi85] and 4 for a non-signaling correlation in $\mathcal{P}$ [PR94].

### 7.2.1. Standard Form of a Correlation Table

According to the GNS-construction (see Theorem 2.1.2) it is clear that we can always find a quantum representation for which the state is a pure and cyclic state. Naimark's dilation theorem, which is a consequence from Stinespring's dilation theorem [Pau02], implies that we can always dilate the Hilbert space to obtain projective measurements. A quantum representation for which both holds is called a standard representation.

**Definition 7.2.3.** *Let $(\mathcal{H}, \{F(\underline{x}|\underline{s})\}, \omega)$ be a quantum representation of $\mathbb{P}$. We denote the von Neumann algebra generated by the operators $\{F(\underline{x}|\underline{s})\}$ by $\mathcal{A}(F)$.[5] The quantum representation is called cyclic, if $\omega = |\Omega\rangle\langle\Omega|$ is a vector state and $\mathcal{A}(F)|\Omega\rangle$ is dense in $\mathcal{H}$. A quantum representation is called sharp, if every $F(\underline{x}|\underline{s})$ is a projection. The quantum representation is called a standard form of $\mathbb{P}$ if it is cyclic and sharp.*

For completeness, we show how to construct explicitly a sharp and cyclic quantum representation.

**Theorem 7.2.4.** *For every $\mathbb{P} \in \mathcal{Q}$ exists a standard form, that is, a sharp and cyclic quantum representation.*

*Proof.* The proof is by construction. Let $F(\underline{x}|\underline{s})$ and $\omega$ be an arbitrary quantum representation of $\mathbb{P}$ on $\mathcal{H}$. We start by turning the measurement operators $F_i(x|s)$ into projective ones, by applying a version of the Naimark dilation successively to each observable $F_i(\cdot, s)$. It suffices to do this for one of the observables, provided we verify that in this construction not only the required commutativity conditions are preserved, but also the projection valuedness of any of the other measurements. So in order to turn the observable $F_i(\cdot, s)$ in to a projective measurement, we define the Hilbert space $\widehat{\mathcal{H}} = \bigoplus_{x=1}^{K} \mathcal{H}_x$, where each of the $\mathcal{H}_x$ is a copy of the given Hilbert space $\mathcal{H}$. We denote by $P_x$ the projection onto the summand with label $x$, and introduce the isometry

$$V : \mathcal{H} \to \widehat{\mathcal{H}} \qquad V\phi = \bigoplus_x \sqrt{F_i(x,s)}\phi\,.$$

Then we set $\widehat{F}_i(x,s) = P_x$ such that $V^*\widehat{F}_i(x,s)V = F_i(x,s)$, where $V^*$ is the adjoint operator of $V$. For other observables at the same site, e.g., $F_i(\cdot, r)$ with $r \neq s$, we set

$$\widehat{F}_i(x,r) = \begin{cases} VF_i(1,r)V^* + (\mathbb{1} - VV^*) & \text{for } x = 1 \\ VF_i(x,r)V^* & \text{for } x > 1 \end{cases}$$

Because $V$ is an isometry, we again have that $V^*\widehat{F}_i(x,r)V = F_i(x,r)$ for all $x$. Moreover, $\widehat{F}_i(x,r)^2 = VF_i(x,r)^2V^*$ for $x > 1$ and $\widehat{F}_i(1,r)^2 = VF_i(1,r)^2V^* + (\mathbb{1} - VV^*)$,

[5] Concretely, the von Neumann algebra $\mathcal{A}(F)$ is defined as the $\sigma$-weak closure of the set of all linear combinations of products of $F_i(x,s)$

so that a projective measurement remains projective. For observables at all other sites $j \neq i$, we take $\widehat{F}_j(x,r) = \bigoplus_{x'} F_j(x,r)$, i.e., as the original observable acting similar on each of the summands. Once again, this preserves projective valuedness, and not only satisfies $V^*\widehat{F}_j(x,r)V = F_j(x,r)$, but even the stronger relation $\widehat{F}_j(x,r)V = VF_j(x,r)$. With this relation it is easy to see that the $\widehat{F}_j(x,r)$ for different $j$ (including $j = i$) commute, so that we can form the product $\widehat{F}(\underline{x}|\underline{s})$ unambiguously and find $V^*\widehat{F}(\underline{x}|\underline{s})V = F(\underline{x}|\underline{s})$. Hence if we define the state $\hat{\omega}$ via $\hat{\omega}(a) = \omega(V^*aV)$, we obtain a quantum representation of the same point $\mathbb{P} \in \mathcal{Q}$, with $\widehat{F}_i(\cdot, s)$ projective measurements. In order to turn $\hat{\omega}$ into a pure and cyclic state, we apply the Gelfand-Naimark-Segal (GNS) construction (Theorem 2.1.2) of the algebra $\mathcal{A}(\hat{F})$ with respect to the state $\hat{\omega}$. We finally end up with a sharp and cyclic representation of $\mathbb{P}$. □

## 7.3. Secure Correlations and Extremality

Let us consider the $(N, M, K)$ case and assume that the $N$ parties use the experiment to distribute shared and private randomness among them. In the following, we assume that the $N$ parties are honest. With privacy, we mean that no (additional) malicious party (Eve) should have any information about their measurement outcomes. We always assume that the adversary is limited by the law of quantum mechanics and has no access to the labs of the honest parties. The goal is to characterize the property of a correlation table $\mathbb{P} \in \mathcal{Q}$, which guarantees privacy to them. Since we are interested in a theoretical characterization of correlation tables, we assume for simplicity that the correlation tables are known exactly to the $N$ honest parties (but also to Eve). Thus, we neglect any statistical uncertainty which comes along in the estimation of the correlation tables by a finite sample.

In order to be able to extract shared randomness from the outcomes of the correlation experiment, we have to require that the correlations of the measurement outcomes of the different parties are strong enough. Moreover, in order to generate randomness the outcome distribution of each individual measurement $s_i$ should be close to the uniform distribution. But since this is apparent by the knowledge of the correlation table, and furthermore, classical error correction and randomness extraction schemes can be applied to enhance correlation and randomness, we neglect this conditions and put emphasis on the security against wiretapping.

Since the honest parties only know the correlation table $\mathbb{P}$ the property has to hold for any quantum representation of $\mathbb{P}$. Let us assume that $\{F(\underline{x}|\underline{s})\}$ and $\omega$ is a quantum representation of $\mathbb{P}$ on $\mathcal{H}$. Because we model space-like separated parties by commuting operators, we admit Eve to perform every measurement which corresponds to a positive operator $E$ commuting with all $F(\underline{x}|\underline{s})$, that is, $E \in \mathcal{A}(F)'$ with $\mathcal{A}(F)'$ the commutant of $\mathcal{A}(F)$ (see Section 2.1.2 for definitions). For instance, if there exists a POVM $\{E(\underline{x}, \underline{s})\}$ in $\mathcal{A}(F)'$ such that

$$\omega\big(F(\underline{x}|\underline{s})E(\underline{y}, \underline{t})\big) = \mathbb{P}(\underline{x}|\underline{s})\delta_{\underline{xy}}\delta_{\underline{st}} \ ,$$

we have to assume that Eve has complete information about the measurement outcomes of the honest parties.[6]. Hence, in order to ensure privacy, we have to require

[6]This does not mean that she has complete information in a practical situation but we have always

that for any quantum representation all possible measurements of Eve have to be uncorrelated with the outcome distribution of the honest parties. This motivates the following definition.

**Definition 7.3.1.** *A correlation table $\mathbb{P} \in \mathcal{Q}$ is called secure if for any quantum representation $(\mathcal{H}, \{F(\underline{x}|\underline{s})\}, \omega)$ of $\mathbb{P}$ and any operator $E$ commuting with all $F_i(x_i|s_i)$*

$$\omega\big(EF(\underline{x}|\underline{s})\big) = \omega(E)\,\mathbb{P}(\underline{x}|\underline{s})\,. \tag{7.6}$$

Note that this definition also includes correlation tables which are trivially insecure, that is, correlation tables for which Eve can correctly guess the outcome of every setting $\underline{s}$ without additional information. These are the deterministic events in which each choice of measurements $\underline{s}$ assigns a unique outcome $\underline{x}$. These correlation tables are the only extremal points of $\mathcal{C}$.[7] Hence, our security definition only captures the additional advantage (beside a guess without additional knowledge), which comes from correlations due to the interaction of the eavesdropper with the quantum system shared by the honest parties. Since the guessing probability of an eavesdropper of the setting $\underline{s}$ without additional knowledge is simply given by the highest frequency of the probability distribution $\max_{\underline{x}} \mathbb{P}(\underline{x}|\underline{s})$ and can be characterized by the min-entropy (see Definition 4.46), it can be estimated by knowing $\mathbb{P}$ (see [ILL89] for details on classical randomness extraction).

The following statement gives a geometric characterization of all secure correlation tables.

**Theorem 7.3.2.** *A correlation table $\mathbb{P} \in \mathcal{Q}$ is secure if and only if it is extremal in $\mathcal{Q}$.*

*Proof.* Suppose, $\mathbb{P}$ is secure, but not extremal. Then there exists a direct sum representation and a convex decomposition with $\mathbb{P} = \lambda\mathbb{P}_1 + (1-\lambda)\mathbb{P}_2$, $0 \leq \lambda \leq 1$. Now use Equation (7.6) with $E$ being the projector onto the first (second) summand to get $\mathbb{P} = \mathbb{P}_1$ ($\mathbb{P} = \mathbb{P}_2$). This shows that the convex combination is indeed trivial and $\mathbb{P}$ is extremal. Conversely, suppose $\mathbb{P}$ is extremal. Take any commuting $0 < E < \mathbb{1}$ and set $\lambda = \mathrm{Tr}(\rho E)$. Define $\mathbb{P}_1 = (1/\lambda)\mathrm{Tr}(\rho EF(\underline{x}|\underline{s}))$ and $\mathbb{P}_2 = (1/(1-\lambda))\mathrm{Tr}(\rho(\mathbb{1}-E)F(\underline{x}|\underline{s}))$ such that $\mathbb{P} = \lambda\mathbb{P}_1 + (1-\lambda)\mathbb{P}_2$. As $\mathbb{P}$ is extremal, it holds that $\mathbb{P} = \mathbb{P}_1$, which is just equation (7.6), so $\mathbb{P}$ is secure. □

Theorem 7.3.2 simplifies the unhandy definition of secure correlation tables with a clear geometric meaning and reduces the problem of finding secure correlation tables to finding extremal points in $\mathcal{Q}$. Nevertheless, to find extremal points or even to check that a point is extremal are generally hard tasks. Numerical algorithms fail to be efficient even for small $N$, $M$ and $K$. We discuss methods to find extremal points in Section 7.4. An example of extremal points are the correlation tables which maximally violate the CHSH inequalities with a value of $2\sqrt{2}$ [Tsi85].

to consider the worst case scenario.

[7] Note that these points are also extremal for $\mathcal{Q}$ and $\mathcal{P}$.

### 7.3.1. Algebraically Unique Correlation Tables

Let us introduce the universal $C^*$-algebra to the $(N, M, K)$ case. Roughly speaking, it is the $C^*$-algebra given by the direct sum of every possible observable configuration $F(\underline{x}|\underline{s})$ satisfying the requirements in Definition 7.2.1.

**Definition 7.3.3.** *The universal $C^*$-algebra $\mathcal{U}(N, M, K)$ to the $(N, M, K)$ case is the $C^*$-algebra generated by positive elements $\tilde{F}_i(x|s)$ and the identity $\mathbb{1}$ satisfying $[\tilde{F}_i(x|s), \tilde{F}_j(x|s)] = 0$ for all $i \neq j$ and $\sum_x \tilde{F}_i(x|s) = \mathbb{1}$ for all $s$ with the property that for any possible set of positive operators $\{F_i(x|s)\}$ on $\mathcal{H}$ satisfying the condition in Definition 7.2.1, there exists a representation $\pi : \mathcal{U}(N, M, K) \to \mathcal{B}(\mathcal{H})$ such that $F_i(x|s) = \pi\big(\tilde{F}_i(x|s)\big)$.*

In the following we fix $N$, $M$, $K$ and simply write $\mathcal{U}$ instead of $\mathcal{U}(N, M, K)$. A quantum representation of $\mathbb{P}$ fixes a state $\omega$ on $\mathcal{U}$ such that $\mathbb{P}((\underline{x}|\underline{s})) = \omega(F(\underline{x}|\underline{s}))$. Of course, their might be different states which lead to the same $\mathbb{P}$. Nevertheless, we obtain a direct relation between quantum representations and the state space $\mathcal{S}(\mathcal{U})$. Note that the state space $\mathcal{S}(\mathcal{U})$ is a weakly*-compact and convex set which is therefore generated by its extremal points which correspond to the pure states (see e.g., [BR79, Theorem 2.3.15]). We define the map $\gamma$ from $\mathcal{S}(\mathcal{U})$ to $\mathcal{Q}$ via $\gamma : \omega \mapsto \omega(\tilde{F}(\underline{x}|\underline{s}))$. It is clear that the function is affine, that is,

$$\gamma\Big(\sum_{k=1}^{n} p_k \omega_k\Big) = \sum_{k=1}^{n} p_k \gamma(\omega_k)$$

for any probability distribution $p_k$ and $\omega_k \in \mathcal{S}(\mathcal{U})$. The pre-image $\gamma^{-1}(\mathbb{P})$ of a correlation table $\mathbb{P}$ determines the set of all quantum representations of $\mathbb{P}$ (up to unitary equivalence).

**Lemma 7.3.4.** *For every $\mathbb{P} \in \mathcal{Q}$ is the pre-image $\gamma^{-1}(\mathbb{P})$ convex and weakly* compact. Furthermore, if $\mathbb{P}$ is extremal in $\mathcal{Q}$ then the extremal points of $\gamma^{-1}(\mathbb{P})$ are also extremal points of $\mathcal{S}(\mathcal{U})$.*

*Proof.* The convexity follows directly from the fact that $\gamma$ is affine. Since $\mathcal{S}(\mathcal{U})$ is weakly* compact it is enough to show that $\gamma^{-1}(\mathbb{P})$ is sequentially closed. Let us take an arbitrary weakly* converging sequence $\omega_k$ in $\gamma^{-1}(\mathbb{P})$. Since $\omega_k(\tilde{F}(\underline{x}|\underline{s})) = \mathbb{P}(\underline{x}|\underline{s})$, the same holds for the limit. Hence, $\gamma^{-1}(\mathbb{P})$ is weakly* closed. Let us now assume that $\mathbb{P}$ is extremal. If $\omega$ is not extremal in $\mathcal{S}(\mathcal{U})$ then there exists a non trivial convex combination $\omega = p\omega_1 + (1-p)\omega_2$ where at least one of the points is not in $\gamma^{-1}(\mathbb{P})$. But this means that $\mathbb{P} = p\mathbb{P}_1 + (1-P)\mathbb{P}_2$ where $\mathbb{P}_1 \neq \mathbb{P}$ which contradicts the extremality of $\mathbb{P}$. □

One can easily see that for instance extremal points in $\mathcal{S}(\mathcal{U})$ are not necessarily mapped to extremal points of $\mathcal{Q}$ and that the pre-image of an extremal $\mathbb{P}$ can be a face of $\mathcal{S}(\mathcal{U})$.

A special case is given if the correlation table determines the quantum representation completely. This means that solely by knowing $\mathbb{P}$, we have full knowledge about the measurements and the state.

**Definition 7.3.5.** *A correlation table $\mathbb{P} \in \mathcal{Q}$ is called algebraically unique if it admits a unique correlation table up to unitary equivalence, i.e., $\gamma^{-1}(\mathbb{P})$ contains only one point.*

Note that a algebraically unique correlation table $\mathbb{P}$ is not necessary an extremal point of $\mathcal{Q}$, but has to lie on the boundary $\partial\mathcal{Q}$. In order to see this we consider the negative implication which would say that a non-extremal point can never be algebraically unique. But this for instance happens if a d-dimensional face ($d \geq 2$) of $\mathcal{S}(\mathcal{U})$ is faithfully mapped onto $\mathcal{Q}$. But, if we assume that an algebraically unique correlation table is also extremal in $\mathcal{Q}$, we can conclude that the pre-image $\gamma^{-1}(\mathbb{P})$ is an extremal point of $\mathcal{S}(\mathcal{U})$. This implies the following statement.

**Corollary 7.3.6.** *Suppose that $(\mathcal{H}, \{F(\underline{x}|\underline{s})\}, \omega)$ is a standard form of an algebraically unique and extremal correlation table $\mathbb{P}$. Then each $F(\underline{x}|\underline{s})$ is a projection. Moreover, the representation is irreducible, so that every operator on the representation space can be approximated weakly by a polynomial in the $F(\underline{x}|\underline{s})$. At each site the operators $F_i(x|s)$ generate a factor.*

*Proof.* The projection valuedness of the measurement operators follows because we know that their exists a sharp quantum representation and all are unitary equivalent. Since $\gamma^{-1}(\mathbb{P})$ is a pure state, Proposition 2.1.3 implies that the GNS construction yields an irreducible representation. Since the GNS construction is cyclic and $\mathbb{P}$ is algebraically unique we the claim follows. Recall that we call a von Neumann algebra a factor if the commutant is trivial. But the fact that for an irreducible representation the commutant consists only of multiples of the identity is for instance proven in [BR79, Proposition 2.3.8]. □

The above corollary suggests that an algebraically unique and extremal correlation table satisfies an even stronger security condition as the one in Definition 7.3.1. Namely, that for any representation and all possible measurements of Eve and all measurments in $\mathcal{A}(F)$ the outcome distributions factorize. We call this algebraically secure.

**Definition 7.3.7.** *A correlation table $\mathbb{P} \in \mathcal{Q}$ is called algebraically secure if for any quantum representation $(\mathcal{H}, \{F(\underline{x}|\underline{s})\}, \omega)$ and any operator $E$ commuting with all $F_i(x|s)$, and any $\tilde{F} \in \mathcal{A}(F)$*

$$\omega\Big(E\tilde{F}\Big) = \omega(E)\,\omega(\tilde{F})\,. \tag{7.7}$$

Note that obviously an algebraically secure correlation table is secure and therefore also extremal according to Theorem 7.3.2. We find the following equivalence relation.

**Theorem 7.3.8.** *A correlation table is algebraically secure if and only if it is extremal and algebraically unique.*

*Proof.* Assume first that $\mathbb{P}$ is algebraically secure. Since $\mathbb{P}$ is extremal according to Theorem 7.3.2 it remains to show algebraic uniqueness of the quantum representation. Let $(\mathcal{H}, \{F(\underline{x}|\underline{s})\}, \omega)$ and $(\mathcal{H}', \{F'(\underline{x}|\underline{s})\}, \omega')$ be two standard forms of $\mathbb{P}$. Condition (7.7) implies that for all corresponding operators $\tilde{F} \in \mathcal{A}(F)$ and $\tilde{F}' \in \mathcal{A}(F')$,

$\omega(\tilde{F}) = \omega(\rho'\tilde{F}')$. Otherwise, we can take the direct sum representation of the two standard forms and $E$ as the projector on the first or second summand to find a contradiction to condition (7.7). Let us denote the cyclic vector states corresponding to $\omega$ and $\omega'$ by $|\Omega\rangle$ and $|\Omega\rangle'$. Define then the unitary operator $U$ via $U\tilde{F}|\Omega\rangle = \tilde{F}'|\Omega'\rangle$ which transforms one representation into the other. Because $|\Omega\rangle$ and $|\Omega'\rangle$ are cyclic $U$ can be extended to a unitary from $\mathcal{H}$ to $\mathcal{H}'$. Hence, the standard forms are unitary equivalent. Since this holds for any two standard forms this implies that the correlation table is algebraically unique. This proves the first direction.

Let us assume that $\mathbb{P}$ is extremal and algebraically unique and $(\mathcal{H}, \{F(\underline{x}|\underline{s})\}, \omega)$ is a standard form of $\mathbb{P}$. Let $0 \leq E \leq \mathbb{1}$ be an arbitrary operator commuting with all $F_i(x|s)$. Since $\mathbb{P}$ is extremal it is also secure. But this implies that the state on $\mathcal{H}$ defined via $a \mapsto \frac{1}{\omega(E)}\omega(\sqrt{E}a\sqrt{E})$ together with the operators $F_i(x|s)$ is a valid quantum representation of $\mathbb{P}$. Since $\mathbb{P}$ is algebraically unique the representation have to be unitarily equivalent to $(\mathcal{H}, \{F(\underline{x}|\underline{s})\}, \omega)$, which implies $E = \mathbb{1}$. Hence, we find that the condition in Equation (7.7) is satisfied for $E$. Since this holds for any $0 \leq E \leq \mathbb{1}$, we can conclude that $\mathbb{P}$ is algebraically secure. □

Even though the property of algebraically uniqueness seems to be quite demanding, we see in the following chapter that it is not a rare property for an extremal point. For example, the correlation table maximizing the CHSH inequality is algebraically secure [Tsi85]. Furthermore, as shown in Section 7.4.3, every extremal correlation table in the $(2, 2, 2)$ case is algebraically secure.

## 7.4. Extremal Correlation Tables

In the previous section, we showed that extremality of a correlation table provides security in the sense that the outcome distributions are independent of any measurement of an eavesdropper. Here, we discuss methods to find or certify extremal correlation tables. This is generally difficult and numerical algorithms are not efficient (c.f. [DLTW08, NPA08]). Nevertheless, for particular $N$, $M$ and $K$ the problem can be simplified essentially. We start in Section 7.4.1 with a discussion of the $(N, 2, 2)$ case, in which we show that all the extremal points admit a quantum representation on a Hilbert space corresponding to $N$ qubits. This is then used in Section 7.4.2 to construct a certification scheme for extremality for the $(2, 2, 2)$ case. We conclude with a discussion of the case of full correlations in the $(2, M, 2)$-case which is based on results by Tsirelson [Tsi85].

### 7.4.1. The (N,2,2) Case and the C*-Algebra of Two Projections

Let us consider the situation in which we have $N$ parties with each two possible binary measurements. In the following, we can restrict our attention to projective measurement since each correlation table admits a sharp representation. Since we consider binary measurements, they are completely determined by one projector. Hence, the algebraic structure generated by the two possible measurements at each side are determined by two projectors each standing for one measurement. Hence, the important object is the universal C*-algebra generated by two projections for which the representation is well understood [Ped68, Rae89].

**The C*-algebra of Two Projections.** The universal C*-algebra $C^*(p,q)$ of two projections $p$ and $q$ is defined by the property that for any Hilbert space $\mathcal{H}$ and any two projections $P$ and $Q$ in $\mathcal{H}$ there exists a representation $\pi : C^*(p,q) \to \mathcal{B}(\mathcal{H})$ such that $P = \pi(p)$ and $Q = \pi(q)$ (c.f. Definition 7.3.3). As shown in [Ped68, Rae89], $C^*(p,q)$ is isomorphic to the matrix valued functions $f : [0,\pi] \to M_2$[8] with the property that $f(0)$ and $f(\pi)$ are diagonal. The generators $p$ and $q$ are represented by the functions

$$p(\theta) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad q(\theta) = \frac{1}{2}\begin{pmatrix} (1+\cos\theta) & \sin\theta \\ \sin\theta & (1-\cos\theta) \end{pmatrix}. \tag{7.8}$$

Note that $p(\theta)$ is the projection onto the subspace spanned by the vector $(1,0)$ and $q(\theta)$ onto $(\cos\frac{\theta}{2}, \sin\frac{\theta}{2})$. Hence, $\theta/2$ is the angle between the projections $p(\theta)$ and $q(\theta)$. Using the Pauli matrices the projections can be written as $p(\theta) = \frac{1}{2}(\mathbb{1} + \sigma_3)$ and $q(\theta) = \frac{1}{2}(\mathbb{1} + \sin(\theta)\sigma_1 + \cos(\theta)\sigma_3)$.

The pure states of $C^*(p,q)$ are given by the functionals

$$\omega(f) = \int_0^1 \langle\psi|f(\theta)\psi\rangle\, \delta(\theta - \theta_0)\, \mathrm{d}\theta\,.$$

for $\psi \in \mathbb{C}^2$ and $\theta_0 \in [0,\pi]$. The GNS construction of pure states leads to irreducible representations and they are given for $\theta_0 \in (0,\pi)$ by $\pi_{\theta_0} : C^*(p,q) \to \mathcal{B}(\mathbb{C}^2)$ where the generators $p$ and $q$ are mapped onto $p(\theta_0)$ and $q(\theta_0)$. Hence, the representation space is $\mathcal{H} = \mathbb{C}^2$ and $\theta_0/2$ describes the angle between the projections. In the case $\theta_0 = 0, \pi$ the projectors commute and we obtain two 1-dimensional representations of $C^*(p,q)$.

**Characterization of the (N,2,2) Case** Let us come back to the case where we have $N$ parties and therefore $N$ commuting pairs of projections. Since the algebra $C^*(q,p)$ is nuclear we obtain the following characterization of the $(N,2,2)$ case.

**Theorem 7.4.1.** *The universal C*-algebra which describes the $(N,2,2)$ case is given by $\mathcal{U}(2,2,2) = C^*(p,q)^{\otimes N}$. Furthermore, every extremal point admits a quantum representation on $\mathcal{H} = (\mathbb{C}^2)^{\otimes N}$ determined by angles $(\theta_1, ..., \theta_N)$ and a real state $|\psi\rangle \in \mathcal{H}$ such that $F_i(0|0)$ and $F_i(0|1)$ are given by $\frac{1}{2}(\mathbb{1}+\sigma_3)$ and $\frac{1}{2}(\mathbb{1}+\sin(\theta_i)\sigma_1+\cos(\theta_i)\sigma_3)$ on the ith tensor factor and act like the identiy on the others.*[9]

*Proof.* We use first the we can always find a sharp representation which allows us to consider the universal C*-algebra of $N$ pair of commuting projections. Because $C^*(q,p)$ is the tensor product of a finite-dimensional and an abelian C*-algebra, we have that it is nuclear which means that for every C*-algebra $\mathcal{A}$ the C*-tensor product $C^*(q,p) \otimes \mathcal{A}$ is unique [Tak01, Mur90]. Hence, we have that the universal C*-algebra generated by $N$ commuting pairs of projections is given by $C^*(q,p)^{\otimes N}$. Lemma 7.3.4 implies that for every extremal point $\mathbb{P}$ in $\mathcal{Q}$ an extremal point in $\mathcal{S}(\mathcal{U}(N,2,2))$ exists which generates $\mathbb{P}$. Hence, it is enough to consider the extremal points of $C^*(q,p)^{\otimes N}$ which correspond to the pure states, and thus, to irreducible representations. But

[8] With $M_2$ we denote the $2 \times 2$ matrices with complex entries.

[9] Note that the other measurements are simply given by $F_i(1|s) = \mathbb{1} - F_i(0|s)$.

as discussed above they are given by fixing $N$ angles $(\theta_1, ..., \theta_N)$ and a vector state $|\psi\rangle \in \mathcal{H}$. It remains to show that the state $|\psi\rangle$ can be chosen in $\mathbb{R}^n$. This is essentially because all the obserbales $F_i(x|s)$ are real. In particular, for fixed angles $(\theta_1, ..., \theta_N)$ the representation induced by $|\psi\rangle$ generates the same correlation table as the one induced by the complex conjugate $|\bar{\psi}\rangle$. Hence, so does the convex combination $1/2(|\psi\rangle\langle\psi| + |\bar{\psi}\rangle\langle\bar{\psi}|)$. But if one decomposes $|\psi\rangle$ into real and imaginary parts $|\psi\rangle = |\phi\rangle + i|\eta\rangle$ for $\psi, \eta$ real, we find that $1/2(|\psi\rangle\langle\psi| + |\bar{\psi}\rangle\langle\bar{\psi}|) = 1/2(|\phi\rangle\langle\phi| + |\eta\rangle\langle\eta|)$ is real. □

Since every point of a $d$-dimensional convex set can be written as the convex combination of at most $d+1$ extremal points, we find that every point $\mathbb{P} \in \mathcal{Q}$ allows a representation given by the direct sum of at most $4^N + 1$ irreducible representations. In the following we denote the correlation table which corresponds to angles $\underline{\theta} = (\theta_1, ..., \theta_N)$ and a real state $|\psi\rangle$ by $\mathbb{P}_{(\underline{\theta},\psi)}$. Furthermore, we denote the measurement operators corresponding to $\underline{\theta}$ by $F^{(\underline{\theta})}(\underline{x}|\underline{s})$.

**Maximal Violation of Tsirelson Inequalities.** The characterization of the quantum representations in the $(N, 2, 2)$ case given in Theorem 7.4.1 can now be use to find maximal violations of Tsirelson inequalities, from which extremality can be concluded under certain conditions. Let $\mathcal{Q} \subset \mathbb{R}^d$ and $f : \mathbb{R}^d \to \mathbb{R}$ be a linear functional. In order to obtain a supporting hyperplane on $\mathcal{Q}$ (see Equation (7.5)) we have to determine $q_f = \max_{\mathbb{P}\in\mathcal{Q}} f(\mathbb{P})$. Since the maximum is always attained for an extremal point in $\mathcal{Q}$, it is sufficient to maximize over all irreducible representations parameterized by angles $\underline{\theta} \in [0, \pi]^N$ and real vectors $\psi \in \mathbb{R}^{2^N}$ such that

$$q_f = \sup_{\underline{\theta},\psi} f\big(\mathbb{P}_{\underline{\theta},\psi}\big). \tag{7.9}$$

Let us assume that $f(\mathbb{P}) = \sum_{\underline{x},\underline{s}} f(\underline{x}|\underline{s})\mathbb{P}(\underline{x}|\underline{s})$. For a set of measurements $\{F(\underline{x}|\underline{s})\}$, we then define the Tsirelson operator corresponding to $f$ by

$$T_f(F) := \sum_{\underline{x},\underline{s}} f(\underline{x}|\underline{s})\, F(\underline{x}|\underline{s})\,. \tag{7.10}$$

This then allows us to write

$$f(\mathbb{P}_{\underline{\theta},\psi}) = \langle\psi|T_f(F^{(\theta)})\psi\rangle. \tag{7.11}$$

Optimizing the righthand side of the above equation over all $\theta_i \in [0, \pi]$ and $\psi \in \mathbb{R}^{2^N}$ yields $q_f$ and therefore a supporting hyperplane. If there is exactly one set of parameters $\theta_1, ..., \theta_N$ and a unique state $\psi$ for which the maximum is attained, the corresponding probability distribution $\mathbb{P}$ is algebraically secure. In the case where more than one possible choice of $\theta_1, ..., \theta_N, \psi$ leads to a maximal violation, we can determine the convex span of the corresponding probability distributions. This corresponds to the face given by the intersection of $\mathcal{Q}$ and the hyperplane $\{\mathbb{P} \mid \sum_{\underline{x},\underline{s}} c(\underline{x}|\underline{s})\mathbb{P}(\underline{x}|\underline{s}) = Q_c\}$. Extremal points of that face are extremal points of $\mathcal{Q}$, and thus, secure probability distributions.

### 7.4.2. Certification of Extramility in the (2,2,2) Case

The goal is to use the characterization of extremal correlations in the $(2,2,2)$ case given in Theorem 7.4.1 to certify extremality of a correlation table. Since every extremal correlation table admits an irreducible representation, it suffices to consider correlation tables $\mathbb{P}_{(\underline{\theta},\psi)}$ for $\underline{\theta} \in [0,1]^2$ and $\psi \in \mathbb{R}^4$. The goal is to construct for a given $\mathbb{P}_{(\underline{\theta},\psi)}$ a Tsirelsen inequality which is saturated by $\mathbb{P}_{(\underline{\theta},\psi)}$. If there exists such an inequality which is not trivial, and no other probability distribution in $\mathcal{Q}$ saturates it (or alternatively that just one quantum representation of $\mathbb{P}$ exists), extremality of $\mathbb{P}$ is certified.

We call the two parties Alice and Bob and write $\underline{\theta} = (\theta_A, \theta_B)$. The Hilbert space is given by $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ where $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^2$. Since we consider binary observables given by projectors, we can equivalently work with selfadjoint operators with eigenvalues $\pm 1$ denoted by $A_1, A_2 \in \mathcal{B}(\mathcal{H}_A)$ $(B_1, B_2 \in \mathcal{B}(\mathcal{H}_B))$ on Alice's (Bob's) side. Note, that the condition to have selfadjoint operators with eigenvalues $\pm 1$ simply means that $A_i^2 = \mathbb{1}$ and $\mathrm{Tr} A_i = 0$. We further set $A_0 = \mathbb{1}_A$, $B_0 = \mathbb{1}_B$, $A = (A_0, A_1, A_2)$ and $B = (B_0, B_1, B_2)$. We denote the tuple of observables $A$ and $B$ which correspond to the representation $(\theta_A, \theta_B)$ by $A(\theta_A) = \big(A_0(\theta_A), A_1(\theta_A), A_2(\theta_A)\big)$ and $B(\theta_B) = \big(B_0(\theta_A), B_1(\theta_A), B_2(\theta_A)\big)$. Note that $A_0(\theta_A) = B_0(\theta_A) = \mathbb{1}$ are independent of the particular choice of the angles.

The problem of finding a Tsirelson inequality for $\mathbb{P}_{(\underline{\theta},\psi)}$ can be formulated in the following way.
*Find a positive operator*

$$T(A,B) = \sum_k P_k(A,B)^* P_k(A,B)\,, \tag{7.12}$$

*with $P_k(A,B)$ polynomials in $A_i \otimes B_j$, $i,j = 0,1,2$, such that*

***(i)*** *$P_k(A,B)\psi = 0$ for all $k$*

***(ii)*** *For all possible observables $A_i$ and $B_j$ satisfying $A_i^2 = \mathbb{1}$, $B_j^2 = \mathbb{1}$, $\mathrm{Tr} A_i = 0$ and $\mathrm{Tr} B_j = 0$ follows that $T(A,B)$ is linear in $A_i \otimes B_j$, i.e., $T(A,B) = \sum_{i,j} t_{ij} A_i \otimes B_j$ with $t_{ij} \in \mathbb{R}$.*

The ansatz for $T(A,B)$ ensures that the operator is positive (and thus also self-adjoint) for any observables $A_i$ and $B_j$. Condition (ii) implies that for any observables $A_i, B_j$ and state $\omega$ leading to the correlation table $\mathbb{P}$, the expression $\omega\big(T(A,B)\big)$ defines a linear functional of $\mathbb{P}$ denoted by $f_T(\mathbb{P})$. This means that $T(A,B)$ is the Tsirelson operator to the linear functional $f_T$. Condition (i) together with the ansatz of $T$ in Equation (7.12) ensures that $f_T$ defines a supporting hyperplane at $\mathbb{P}_{(\underline{\theta},\psi)}$, that is, $f_T(\mathbb{P}_{(\underline{\theta},\psi)}) = 0$ and $f_T(\mathbb{P}) \geq 0$ for any $\mathbb{P} \in \mathcal{Q}$. The approach to construct manifest positive operators with an ansatz like in Equation (7.12) is closely related to the ideas in [DLTW08].

The problem above induces a natural hierarchy by the degree of the polynomials $P_k(A,B)$ used in the ansatz of the operator $T$. In general, it is not clear which degree is sufficient to construct for a given $\mathbb{P}_{(\underline{\theta},\psi)}$ a Tsirelson inequality (if even non trivial ones exist). The idea is to start with the lowest order and sort out angles $\underline{\theta}$

and states $\psi$ for which this is possible. Note for instance that the lowest order is sufficient to find the CHSH inequality which corresponds to the Tsirleson operator

$$I_{\text{CHSH}} = A_1 \otimes (B_1 + B_2) + A_2 \otimes (B_1 - B_2)\,. \tag{7.13}$$

In particular, it is easy to check that []

$$\begin{aligned} 2\sqrt{2}\mathbb{1} - I_{\text{CHSH}} = \frac{1}{2}\Big((A-B)^*(A-B) + (A-B)(A-B)^*\Big) \\ + \frac{1}{4}\sum_{j=1}^{2}\Big([\mathbb{1} - (A_j \otimes \mathbb{1})^2] + [\mathbb{1} - (\mathbb{1} \otimes B_j)^2]\Big) \end{aligned}$$

where $A = 1/2(A_1 + iA_2) \otimes \mathbb{1}$ and $B = 1/(2\sqrt{2})\mathbb{1} \otimes (B_1 + B_2 + i(B_1 - B_2))$. Since $A_i^2 = \mathbb{1}$ and $B_i^2 = \mathbb{1}$, we see that it can be written as in Equation (7.12) with polynomials $P_k$ which have only degree 1. In the following, we give an analytical solution for the lowest non trivial order of the hierarchy.

**Lowest Order Certificate** We want to construct a Tsirelson operator

$$T = \sum_{i=1}^{2} P_i(A_k, B_l)^\dagger P_i(A_k, B_l) \tag{7.14}$$

with

$$P_i = \sum_{j=1}^{2}(\alpha_{ij} A_j \otimes \mathbb{1} - \beta_{ij}\mathbb{1} \otimes B_j) \tag{7.15}$$

where $\alpha$ and $\beta$ are matrices in $M_2$, such that the conditions (i) and (ii) from above are satisfied for at least one quantum representation $\underline{\theta}$ and $\psi$. For given angles $\theta_A$ and $\theta_B$ the concrete form of the observables (see Theorem 7.4.1) is given by $A_i(\theta_A) = \sum_j t(\theta_A)_{ij} X_j$ and $B_i(\theta_B) = \sum_j t(\theta_B)_{ij} X_j$ with $X_1 = \sigma_1$, $X_2 = \sigma_3$ and

$$t(\theta) = \begin{pmatrix} 0 & 1 \\ \sin\theta & \cos\theta \end{pmatrix}.$$

Note that the case $\theta_A = 0, \pi$ ($\theta_B = 0, \pi$) corresponds to the case where the measurements on Alice's (Bob's) side commute, which lead to correlation tables $\mathbb{P}$ which can be generated by a LHV model.[10] Hence, we restrict our attention to representations with $\theta_A, \theta_B \neq 0, \pi$. Recall also that it is suffices to consider only real states $\psi$ since all observables are real.

We start by analyzing condition (i). Using the particular form of the observables $A_i(\theta_A)$ and $B_j(\theta_B)$ expressed through $t(\theta)$, we find that $P_i\psi = 0$, $i = 1, 2$, results in

$$[X_i \otimes \mathbb{1}]\psi = \sum_j \eta_{ij}[\mathbb{1} \otimes X_j]\psi \;\; (i = 1, 2) \tag{7.16}$$

[10] From the form $I^2_{\text{CHSH}} = 4 - [A_1, A_2] \otimes [B_1, B_2]$ one directly sees that if one of the pairs of observables commute the maximal CHSH inequality violation is 2. Hence, there exists an LHV model realizing the correlation table.

where $\eta = t(\theta_A)^{-1}\alpha^{-1}\beta t(\theta_B)$. We assumed here that $\alpha$ is invertible. However, this is not a restriction since otherwise the state $\psi$ has to be of product form.

In the following it is convenient to use the isomorphism between $\mathcal{H}$ and the Hilbert space $M_2$ of $2 \times 2$ matrices with the Hilbert-Schmidt inner product. States $\phi = (\phi_1, \phi_2, \phi_3, \phi_4)$ in $\mathcal{H}$ are identified with matrices

$$\hat{\phi} = \begin{pmatrix} \phi_1 & \phi_2 \\ \phi_3 & \phi_4 \end{pmatrix}$$

and $[A \otimes \mathbb{1}]\phi$ (respectively, $[\mathbb{1} \otimes B]\phi$) can be written as the matrix multiplication $A\hat{\phi}$ (respectively, $\hat{\phi}B^T$). Moreover, we have that $\phi$ is a purification of the density matrix $\rho = (\hat{\phi}^*\hat{\phi})^T$ on $\mathbb{C}^2$. Equation (7.16) is then equivalent to

$$X_i\hat{\psi} = \sum_{j=1}^{2} \eta_{ij}\hat{\psi}X_j. \tag{7.17}$$

The following assertion characterizes condition (i).

**Lemma 7.4.2.** *A real vector $\psi \in \mathcal{H}$ admits an $\eta \in M_2$ such that the relation (7.16) holds if and only if $\hat{\psi}^T\hat{\psi}$ is a multiple of $\mathbb{1}$. Then, it holds that*

$$\eta_{ij} = \frac{1}{2}\mathrm{Tr}(\hat{\psi}^{-1}X_i\hat{\psi}X_j) \tag{7.18}$$

*for $i, j = 1, 2$.*

*Proof.* We first note that $\hat{\psi}$ must be invertible. This is due to the fact that otherwise the reduced state of $\psi$ given by $(\hat{\psi}^*\hat{\psi})^T$ has determinant 0 and is therefore a pure state. We then multiply equation (7.17) with $X_k\hat{\psi}^{-1}$ from the left to find $\sum_j \eta_{ij}X_kX_j = X_k\hat{\psi}^{-1}X_i\hat{\psi}$. Recalling that $\mathrm{Tr}(X_kX_j) = 2\delta_{kj}$, we can take the trace and obtain (7.18).

We turn now to the first part of the statement. Multiplication from the right of (7.17) with $\hat{\psi}^{-1}$ shows that $X_i = \sum_j \eta_{ij}\hat{\psi}X_j\hat{\psi}^{-1}$. Thus, we obtain that

$$\mathrm{Tr}(X_iX_k) = \sum_{j,l} \eta_{ij}\eta_{kl}\mathrm{Tr}(X_jX_l),$$

from which follows that $\eta\eta^T = \mathbb{1}$. On the other hand one can check that the set $G$ of all $\hat{\psi}$ for which there exists a $\eta$ such that (7.16) holds and $\det(\hat{\psi}) = 1$, describes a group together with the usual matrix multiplication. Moreover, the map $\hat{\psi} \mapsto \eta(\hat{\psi})$ induced by (7.18) is a group homomorphism such that $\eta(\hat{\psi}^T) = \eta^{-1}$. From this we can then conclude that $\hat{\psi}^T\hat{\psi} \propto \mathbb{1}$ is the necessary and sufficient condition to solve (7.16). □

Lemma 7.4.2 says that condition (i) is only satisfied if $\frac{1}{\det\hat{\psi}}\hat{\psi}$ is an orthogonal matrix. Hence, the possible states $\psi$ for which condition (i) can be satisfied are parameterized by

$$\phi_x^{\pm} = \frac{1}{\sqrt{2}}(\cos x, \mp\sin x, \sin x, \pm\cos x) \tag{7.19}$$

where $x \in [0, \pi)$. The state $\psi$ determines the corresponding $\eta$ uniquely through equation (7.18).

Since the reduced state of $\psi$ is equal to $(\hat{\psi}^* \hat{\psi})^T$, it follows directly that $\phi_x^{\pm}$ is maximally entangled. From this follows also that the expectation values of all local observables $A_l$ and $B_j$ vanish, that is, $\langle \phi_x^{\pm} | A_j \phi_x^{\pm} \rangle = \langle \phi_x^{\pm} | B_j \phi_x^{\pm} \rangle = 0$ for $j = 1, 2$.

We turn now to condition (ii) and compute the expectation value of $T$ with respect to $\phi \in \mathcal{H}$,

$$\begin{aligned} \langle T \rangle_\phi = \mathrm{Tr}(\alpha^* \alpha + \beta^* \beta) - \sum_{j,k} (\alpha^* \beta + (\beta^* \alpha)^T)_{jk} \langle A_j \otimes B_k \rangle_\phi \\ + \sum_{j \neq k} ((\alpha^* \alpha)_{jk} \langle A_j A_k \rangle_\phi + (\beta^* \beta)_{jk} \langle B_j B_k \rangle_\phi), \end{aligned}$$

where $\langle \cdot \rangle_\phi = \langle \phi | \cdot \phi \rangle$ denotes the expectation value with respect to $\phi$. Thus, condition (ii) requires that the matrices $\alpha^* \alpha$ and $\beta^* \beta$ are diagonal. In this case the Tsirelson inequality reads

$$\sum_{j,k} (\alpha^* \beta + (\beta^* \alpha)^T)_{jk} \langle A_j \otimes B_k \rangle \leq \mathrm{Tr}(\alpha^* \alpha + \beta^* \beta). \tag{7.20}$$

The coefficients $c_{ij}$ in condition (ii) are therefore $c_{jk} = (\alpha^* \beta + (\beta^* \alpha)^T)_{jk}$ for $j, k = 1, 2$, $c_{00} = -\mathrm{Tr}(\alpha^* \alpha + \beta^* \beta)$, and the others 0.

Since the expectation value of $T$ is invariant under scaling and simultaneous unitary transformation of $\alpha$ and $\beta$, we can without loss of generality assume that $\alpha = \mathrm{diag}(1, \lambda)$ with $\lambda > 0$. This can always be achieved by the polar decomposition. Using now that $\eta = t(\theta_A)^{-1} \alpha^{-1} \beta t(\theta_B)$ we can write $\beta = \alpha \gamma$ with $\gamma = t(\theta_A) \eta t(\theta_B)^{-1}$. The condition that $\beta^* \beta$ is diagonal is then equivalent to

$$\lambda^2 = -\frac{\overline{\gamma_{11}} \gamma_{12}}{\overline{\gamma_{21}} \gamma_{22}} > 0, \tag{7.21}$$

which completely characterizes condition (ii).

The following statement summarizes the results from the discussions of the two conditions.

**Theorem 7.4.3.** *The conditions (i) and (ii) are satisfied for maximally entangled states $\phi_x^{\pm} = \frac{1}{\sqrt{2}}(\cos x, \mp \sin x, \sin x, \pm \cos x)$ ($x \in [0, \pi)$) and angles $(\theta_A, \theta_B)$ for which the inequality*

$$(\lambda_x^{\pm})^2 := -\frac{\sin(2x) \sin(2x \pm \theta_B)}{\sin(2x - \theta_A) \sin(2x - \theta_A \pm \theta_B)} > 0. \tag{7.22}$$

*holds. Moreover, the corresponding Tsirelson inequality is given by (7.20) with coefficients determined by*

$$\alpha^* \beta + (\beta^* \alpha)^T = \frac{2}{\sin \theta_B} \begin{pmatrix} \pm \sin(2x \pm \theta_B) & \mp \sin(2x) \\ \pm (\lambda_x^{\pm})^2 \sin(2x - \theta_A \pm \theta_B) & \mp (\lambda_x^{\pm})^2 \sin(2x - \theta_A) \end{pmatrix} \tag{7.23}$$

*and*

$$\mathrm{Tr}(\alpha^* \alpha + \beta^* \beta) = -\frac{2 \sin \theta_A \sin(4x - \theta_A \pm \theta_B)}{\sin(2x - \theta_A) \sin(2x - \theta_A \pm \theta_B)}. \tag{7.24}$$

*Proof.* Because of Lemma 7.4.2, we can constrain to representations $(\psi, \theta_A, \theta_B)$ with $\psi = \phi_x^{\pm}$. For these states we can compute $\eta$ via equation (7.18), and insert it into $\gamma = t(\theta_A)\eta t(\theta_B)^{-1}$ to find that

$$\gamma_x^{\pm} = \frac{1}{\sin\theta_B} \begin{pmatrix} \pm\sin(2x \pm \theta_B) & \mp\sin(2x) \\ \pm\sin(2x - \theta_A \pm \theta_B) & \mp\sin(2x - \theta_A) \end{pmatrix} \tag{7.25}$$

Condition (7.21) can then be computed to be given by (7.22). Provided that the inequality (7.22) is satisfied, the method applies and we can compute $\alpha = \mathrm{diag}(1, \lambda)$ and $\beta = \alpha\gamma$ and obtain the Tsirelson inequality from (7.20). Expressed in $\lambda_x^{\pm}$, one finds the coefficients given in the statement. □

As argued before, among the possible $\mathbb{P}$ for which the method applies are also the probability distributions which lead to maximal violation of a CHSH inequality (7.13). The corresponding values of $x$ and $\theta_A, \theta_B$ in Theorem 7.4.3 are $\theta_A = \theta_B = \pi/2$ and $\psi = \phi_x^{\pm}$ with $x = \pi/8 + n\pi/4$ $(n = 0, 1, 2, 3)$.

### 7.4.3. The (2,M,2) Case and Clifford Algebras

Let us consider the case of 2 parties Alice and Bob with each $M$ binary measurements. In the following we restrict our consideration on full correlations. We therefore assume that each measurement is described by an observable $A_i$ for Alice and $B_i$ for Bob with outcomes $\pm 1$. Hence, in the notation before this reads as $A_i = F_1(1|i) - F_1(2|i)$ and $B_i = F_2(1|i) - F_2(2|i)$.

**Definition 7.4.4.** *We call the expectation values of the correlation of the observables $A_i, B_i$ between Alice an Bob given by*

$$C_{ij} := \langle A_i B_j \rangle \tag{7.26}$$

*the correlation matrix. Moreover, it is called a quantum correlation matrix if there exists selfadjoint observables $A_i, B_i$ $(i = 1, ..., M)$ on a Hilbert space $\mathcal{H}$ satisfying $A_i^2 = B_i^2 = \mathbb{1}$ for every $i$ and $[A_i, B_j] = 0$ for every $i, j$, and a state $\omega$ such that $C_{ij} = \omega(A_i B_j)$. The set of all quantum correlation matrices $C$ is denoted by $\mathcal{Q}_{\mathrm{cor}}$.*[11]

Note that the restriction to self-adjoint operators $A_i, B_i$ obeying $A_i^2 = B_i^2 = \mathbb{1}$ does not impose any limitation on the quantum representations since always a sharp representation exists and we can choose the binary outcomes by $\pm 1$. In [Tsi85], this was already proven by Tsirelson. It is easy to see that the probability distributions $\mathbb{P}(\underline{x}|\underline{s})$ can be reconstructed by the correlation matrix $C_{ij}$ together with the knowledge of the expectation values of the local observables $\langle A_i \rangle$ and $\langle B_j \rangle$ (see e.g., [Tsi93]). Tsirelson characterized the quantum correlation matrices completely in [Tsi85].

**Theorem 7.4.5.** ***(Tsirelson '85)*** *For every correlation matrix $C \in \mathcal{Q}_{\mathrm{cor}}$ exist vectors $x_1, ..., x_M$ and $y_1, ..., y_M$ in an Euclidean vector space such that*

$$C_{ij} = \langle x_i | y_j \rangle \ \ \forall i, j \tag{7.27}$$

[11] In [Tsi93] the correlation tables $\mathbb{P}$ are called behaviors and $C_{ij}$ the correlation matrix.

*and* $\|x_i\| \leq 1$, $\|y_j\| \leq 1$. *We call such a collection of vectors a c-system of* $C$, *and the dimension of the linear hull of the vectors* $\{x_1, ..., x_M, y_1, ..., y_M\}$ *its rank. If* $C$ *is extremal in* $\mathcal{Q}_{\text{cor}}$ *then all c-system are isometric to each other and the linear span of* $\{x_1, ..., x_M\}$ *is equal to the one of* $\{y_1, ..., y_M\}$.

Possible cyclic quantum representations are given by representations of the Clifford algebra. In the following, we give a short overview of the construction presented in [Tsi85]. This reduces the problem to check if a quantum correlation is extremal to check whether the rank of the c-system is even. The Clifford algebra $C(n)$ of order n is generated by Hermitian elements $X_1, ..., X_n$ satisfying the relations $\{X_i, X_j\} = 2\mathbb{1}\delta_{ij}$ (see, e.g., [Sim96] for a discussion of the properties of Clifford algebras). For a vector $x \in \mathbb{R}^n$ let us define

$$X(x) := \sum_{i=1}^{n} x_i X_i. \tag{7.28}$$

Since $X^2(x) = \|x\|\mathbb{1}$, the Clifford algebra exhibits an explicit invariance under isometries.

The representation theory of Clifford algebras is well understood [Sim96]. For even n there exists exactly one irreducible representation of $C(n)$, and its generated algebra is isomorphic to the full matrix algebra $M_{2^{\frac{n}{2}}}$. In the case of an odd n there are two unitary inequivalent representations, and the generated algebra of each of them is isomorphic to the full matrix algebras $M_{2^{\frac{n-1}{2}}}(\mathbb{C})$. In particular, starting with the unique representation $\pi_n$ of $C(n)$ for $n$ even, the two irreducible representations of $C(n+1)$ can be constructed from $\pi_n$. Let $\hat{X}_i := \pi_n(X_i)$ be the representatives of the generators $X_i$. Then, the two inequivalent irreducible representations of $C(n+1)$ can be constructed by $\hat{X}_1, ..., \hat{X}_n$, and

$$\hat{X}_{n+1} = \begin{cases} \pm\hat{X}_1...\hat{X}_n, & n = 0 \ mod\ 4; \\ \pm i\hat{X}_1...\hat{X}_n, & n = 2 \ mod\ 4. \end{cases} \tag{7.29}$$

Let us denote the representation of $C(n+1)$ corresponding to the plus sign in (7.29) as $\pi^+_{n+1}$, respectively, their representatives as $\hat{X}^+_i$, and similar for the one belonging to the minus sign as $\pi^-_{n+1}$ and $\hat{X}^-_1$. Due to the uniqueness of the representation $\pi_n$ up to unitary equivalence, it is straightforward to see the relation between the two representations $\pi^+_{n+1}$ and $\pi^-_{n+1}$. In terms of the representatives they are linked by $\hat{X}^+_i = -\hat{X}^-_i$ for $n = 0$ module 4, and by complex conjugation $\hat{X}^+_i = \bar{\hat{X}}^-_i$ for $n = 2$ modulo 4.

Given a c-system $x_1, ..., x_M$ and $y_1, ..., y_M$ with rank $n$ the cyclic quantum representations of the corresponding correlation matrix $C_{ij}$ can now be constructed through the Clifford algebra $C(n)$. If the rank $n$ is even, then we have according to the discussion before a unique cyclic quantum representation which corresponds to the tensor product of the unique representations of $C(n)$, that is $\pi_n \otimes \pi_n$. More explicitly, the observables are given by $A_i = \hat{X}(x_i) \otimes \mathbb{1}$ and $B_j = \mathbb{1} \otimes \hat{X}(y_j)$, and the quantum state by the unique eigenvector of $\frac{1}{n}(\hat{X}_1 \otimes \hat{X}_1 + ... + \hat{X}_n \otimes \hat{X}_n)$ to the eigenvalue 1 [Tsi85].

If the rank $n = 1$ modulo 4, then the two cyclic quantum representation are given by $\pi^+_n \otimes \pi^+_n$ and $\pi^-_n \otimes \pi^-_n$. The observables and the state are constructed in the same

manner as for even $n$. The other combinations $\pi_n^+ \otimes \pi_n^-$ and $\pi_n^- \otimes \pi_n^+$ are not possible because the operator $\frac{1}{n}(\hat{X}_1 \otimes \hat{X}_1 + ... + \hat{X}_n \otimes \hat{X}_n)$ does not has an eigenvalue $+1$. Finally, if the rank is $n = 3$ modulo 4, then the two cyclic quantum representation are given by $\pi_n^+ \otimes \pi_n^-$ and $\pi_n^- \otimes \pi_n^+$. The observables and also the state are constructed in the same manner as for the other cases and the other combinations $\pi_n^+ \otimes \pi_n^+$ and $\pi_n^- \otimes \pi_n^-$ are not possible because the operator $\frac{1}{n}(\hat{X}_1 \otimes \hat{X}_1 + ... + \hat{X}_n \otimes \hat{X}_n)$ does not has an eigenvalue $+1$.. Obviously, since $\pi_n^+$ can be transformed to $\pi_n^-$ by complex conjugation, and also the state of the different quantum representations are linked by complex conjugation, the two different cyclic quantum representations are anti-unitary.

For an extremal quantum correlation matrix, we have that all c-systems are isometrically isomorph and thus, the representations are unitarily equivalent. Hence, we obtain the following statement [Tsi85].

**Corollary 7.4.6.** ***(Tsirelson '85)*** *Let $C$ be an extremal correlation matrix in $\mathcal{Q}_{\text{cor}}$. Then, it follows that each cyclic quantum representation of $C$ is Clifford. Moreover, if the c-systems of $\mathbb{P}$ is of even rank, then there exists a unique cyclic quantum representation up to unitary equivalence. If the c-systems of $\mathbb{P}$ is of odd rank, then there exist exactly two unitary non-equivalent cyclic quantum representations.*

We note that for the above representations of the Clifford algebras always follows that $\langle A_j \rangle = \langle B_j \rangle = 0$ for every $j$. From this it follows that the correlation table $\mathbb{P}$ belonging to an extremal correlation matrix with even rank is also algebraically unique. But it does not have to be an extremal point in general.

Corollary 7.4.6 implies that in the $(2, 2, 2)$ case every extremal correlation matrix except the deterministic ones are algebraically unique. To see this, note that the possible extremal quantum correlation matrices can be described by a c-system $x_1, x_2, y_1, y_2$ such that $||x_i|| = ||y_j|| = 1$ and the linear span of $\{x_1, x_2\}$ is equal to the one of $\{y_1, y_2\}$ [Tsi85]. The rank of the c-system is then the dimension of the linear span of $\{x_1, x_2\}$. Thus, we have the case where $x_1$ and $x_2$ are linearly independent which corresponds to an even rank system where a unique quantum representation exists. If $x_1$ and $x_2$ are not linearly independent, i.e. a odd rank system, we can conclude that $x_1, x_2, y_1, y_2$ are all parallel or antiparallel to each other. Thus, we find the possible correlations to be $w(A_i B_j) = P(i, j) = (-1)^{a_i + b_j}$ with fixed $a_i, b_j = \pm 1$. But obviously, these correlation matrices correspond to deterministic (classical) points.

# 8. Conclusion and Outlook

The topics covered in this thesis can be divided into three main parts. The first part (Chapters 3-5) generalizes information theoretic considerations in the one-shot regime to arbitrary quantum systems including continuous-variable systems. In the second part (Chapter 6), we apply the results developed in the first part to continuous-variable quantum key distribution and present the first quantitative security analysis of such a protocol providing security against coherent attacks. The third part (Chapter 7) contains a characterization and discussion of correlation tables providing security for device-independent quantum key distribution in an error-free scenario. In the following, we summarize the main results for each of the three parts in turn and discuss some open questions.

## 8.1. Non-Asymptotic Information Theory with General Quantum Systems

The generalization of one-shot information theory is accomplished by extending the smooth min- and max-entropy formalism introduced for finite-dimensional systems in [Ren05, KRS09, TCR10] to general quantum and classical systems. We start in Chapter 3 with a discussion of an algebraic approach to quantum mechanics. Space-like separated systems are described by commuting von Neumann algebras (c.f. [Haa92]), which differs from Hilbert space quantum mechanics where one usually assumes a tensor product structure. The concept of a purification then requires a generalization to states on a general von Neumann algebra. While this was already discussed for factor states in [Wor72], we introduce a more general definition based on an operational approach (see Section 3.2). In Section 3.4, we introduce the concept of a projective embedding of a von Neumann algebra. This is motivated by the need to describe sub-normalized post-selected states in order to generalize the purified distance defined in [TCR10]. This distance is adapted for smooth entropies such that desired properties, for example duality, are preserved.

In Chapter 4, we introduce the smooth min- and max-entropies for quantum, classical or hybrid systems modeled by von Neumann algebras. We show that these entropies satisfy the data-processing inequality expressing the principle that classical post-processing cannot increase the amount of information. For systems modeled on type I factors (bounded operators on a separable Hilbert space), we derive in Section 4.5.3 a bound for the smooth-entropies of i.i.d. sources by the von Neumann entropy, and show convergence in the asymptotic limit under certain conditions. In Section 4.6, a Hahn-Banach like extension theorem is used to show the operational meaning of the non-smooth min- and max-entropies for arbitrary side-information. A main result is the characterization of privacy amplification by

the smooth min-entropy in Section 4.8. Existing proofs in the finite-dimensional case [Ren05, TSSR10] are usually not applicable since they rely on a bound of the trace norm by means of a two-norm, which does not hold in infinite dimensions.

In order to study information theoretic properties of continuous-variable systems in the one-shot regime, we extend the conditional min- and max-entropies to continuous outcomes in Section 5.2. We show that they can be approximated by considering their discrete counterparts in the limit where the coarse-graining goes to zero. This is then applied to study the uncertainty of position and momentum measurements (see Section 5.3). In particular, we show that arbitrary side-information can be included into the entropic uncertainty relation for position and momentum operators expressed by min- and max-entropy derived in [BB06]. We further discuss the entropic uncertainty relation for the smooth min- and max-entropy for a finite measurement precision, which is more relevant for practical applications. For non-smoothed versions, we show that the inequality is tight for any precision in the sense that there exists a state for which equality holds.

**Outlook.** One of the motivations for the generalization of the smooth min- and max-entropies to von Neumann algebras was to enable a more physically accurate description of the quantum systems. This includes that in general not all observables lying in the set of all bounded operators on a Hilbert space are physical. The description by means of von Neumann algebras can only partially suffice this requirement since the product of two observables has not to be an observable. It would therefore be interesting to constrain to the vector space spanned by the physical observables, which corresponds mathematically to the theory of operator systems. This would for instance allow one to restrict the read-out measurements of Bob's quantum memory in the information reconciliation task discussed in Section 4.9. On the other hand, in privacy amplification (see Section 4.8), a restriction of Eve's measurement could enhance the bound on the extractable secure key.

The tasks that we have considered have been restricted to a classical-quantum resource. It remains to be seen whether tasks like quantum stage merging in which the resource is fully quantum can be quantified for systems modeled on an arbitrary von Neumann algebra. Another task requiring a fully quantum description is the decoupling property of quantum systems [HHYW08, Dup09, DBWR10]. This property is of great interest since it can be linked to other problems in quantum information theory [DST].

As yet, the smooth differential min- and max-entropies lack an operational interpretation. It would therefore be interesting to consider non-asymptotic information theoretic questions for continuous-variable systems, like for instance capacities of Gaussian channels. Another question that remains open is whether the uncertainty relation with quantum side-information given in Theorem 5.3.3 for the non-smooth min- and max-entropies also holds for the smooth versions.

## 8.2. Continuous-Variable Quantum Key Distribution

We set the optimal finite-key length formula for one-way classical post-processing as derived by Renner in [Ren05] on a rigorous footing for continuous-variable protocols. The explicit formula reads

$$\ell \approx \mathrm{H}_{\min}^{\epsilon}(\mathrm{X_A}|\mathrm{E})_{\omega} - \mathrm{leak_{EC}} - \mathrm{O}(\log \frac{1}{\epsilon'}) \,,$$

and reduces the laborious task of a finite-key security analysis to the estimation of the smooth min-entropy of Alice's raw key $X_A$ given Eve's knowledge $E$. We accomplish this for a continuous-variable protocol and present the first quantitative security analysis against coherent attacks. We employ the uncertainty relation for smooth min- and max-entropies with quantum side-information as first introduced in [TR11], then generalized to continuous-variable systems in Theorem 5.3.1. This allows us to bound the smooth min-entropy by the correlations of the raw keys of Alice and Bob quantified via the smooth max-entropy, that is we have

$$\mathrm{H}_{\min}^{\epsilon}(\mathrm{X}|\mathrm{E})_{\omega} \geq -\mathrm{n}\log \mathrm{c} - \mathrm{H}_{\max}^{\epsilon}(\mathrm{X_A}|\mathrm{X_B})_{\omega}. \tag{8.1}$$

The protocol for which the security analysis is presented is an entanglement based protocol, where a two-mode squeezed state is measured via homodyne detection [CLA01]. The application of the uncertainty relation requires to use squeezed states.This is to ensure that the balance between the complementary of the measurements expressed by the constant $c$ in (8.1) and the correlations of the raw keys $\mathrm{H}_{\max}^{\epsilon}(\mathrm{X_A}|\mathrm{X_B})_{\omega}$ does not become negative.

The finite-key rate is plotted in Figure 6.2 for squeezing strengths recently realized in experiments [EHD$^+$11b, EHD$^+$11a]. The comparison to the case of collective attacks (see Figure 6.4) shows that the finite-key rates computed in the case of coherent attacks are not optimal. The reason for this is that the uncertainty relation is not tight for two-mode squeezed states, as considered in the protocol. This is in contrast to the finite-dimensional case where the optimal asymptotic rates were achieved by employing the same proof technique [TLGR12].

An important advantage of the presented proof technique is that the experimental parameters only enters via the computation of the complementarity constant $c$ for Alice's measurement choices (c.f. Equation (8.1)). This implies that the security analysis is robust in deviations from the ideal implementations which is crucial for practical applications. Furthermore, since the source is assumed to be located in Alice's lab, the reference signal (local oscillator) used for the homodyne detection is directly included in the security analysis (c.f. [HML08]). On the other side, the explicit assumption that the source is located in Alice's lab has the drawback that it forbids the application of reverse reconciliation [GG02]. However, this could only bring small improvements since the bound on the smooth min-entropy is symmetric in Alice's and Bob's data.

In the case of collective attacks, we apply the asymptotic equipartition property from Theorem 4.5.3 to obtain a bound on the smooth min-entropy by the von Neumann entropy. The correction term to the von Neumann entropy, which characterizes the finite resource effect, goes like $O(\frac{1}{\sqrt{n}})$ (where $n$ is the length of the raw key) and is improved compared to the estimations given in [LGG10].

**Outlook.** The general finite-key rate formula can be applied to any continuous-variable protocol and offers a convenient way to prove security. The formula in the case of collective attacks permits a simple adaption of the asymptotic key rates given by the Devetak-Winter formula [DW05] to the finite-key regime. Hence, these key rate formulas provide a basic and general starting point for a finite-key security analysis independent of the specific implementation. This means that difficult problems such as the characterization of the optimal attacks can be avoided.

One big advantage of the proof technique based on the application of the uncertainty relation is that it relies only on a few assumptions. It would therefore be desirable to enhance the bounds and close the gap in the asymptotic limit by a "weak" state dependent version of the uncertainty relation (c.f. [HT11a]), which only exploits trusted knowledge. This knowledge can for instance be the reduced state on Alice's side since the source is assumed to be located in Alice's lab.

In order to narrow the gap between the theoretical assumptions in the security proof and the experimental implementations, it would be desirable to have a more realistic description of the homodyne detection than simple projections onto the spectrum of canonically conjugated operators of one mode. This only enters the finite-key rate formula in the computation of the overlap in the uncertainty relation and can therefore easily be adjusted. For instance, if the amplitude and phase measurements are not perfectly orthogonal and instead deviate by an angle of $\theta$, then the constant $c$ in Equation (8.1) changes by $c \mapsto \cos\theta c + \sin\theta$.

## 8.3. Device-Independent Quantum Key Distribution and Extremal Correlations

We characterize all the secure quantum correlation tables that are monogamous in the sense that any extension to any further commuting quantum measurement is uncorrelated. This property then implies that an eavesdropper cannot have more information about the measurement outcomes of the honest parties than the statistical frequencies thereof. Given that the randomness in the outcome distributions and the correlations between the honest parties are large enough, this enables the extraction of a secure key by classical post-processing (c.f. [ILL89]). A prominent example of such a secure correlation table is the one that maximally violates the CHSH-inequality [Tsi85]. The main result is given in Theorem 7.3.2. It states that the secure correlation tables are exactly the extremal ones in the convex set generated by all quantum correlation tables. This generalizes an idea from [BLM$^+$05], which was used to prove security against individual attacks of a eavesdropper limited by the non-signaling principle [BHK05].

In order to study general correlation experiments, we introduce the universal C*-algebra specified by the number of parties $N$, measurements $M$ and outcomes $K$ (see Definition 7.3.3). We then consider the property of an extremal quantum correlation table to uniquely determine the quantum representation, that is, the quantum state and the observables. We show that this property is related to an even stronger notion of security, called algebraically secure (see Theorem 7.3.8). An algebraically secure correlation table is defined via the property that also every other measurement

which lies in the algebra generated by the observables leads to a secure correlation table. Surprisingly, this is not a rare property among extremal correlation tables. We show in Section 7.4.3 that many extremal correlation tables for an experiment with two parties and binary measurements exhibit this property, including the one corresponding to the maximal violation of the CHSH-inequality.

After linking the security of a correlation table to its extremality, we then discuss different methods of how to verify that a correlation table is extremal. A common verification is to see whether a correlation table maximizes a Tsirelson inequality. This problem can be expressed as a hierarchy of semi-definite programs [DLTW08, NPA08]. However, since this hierarchy is infinite, it is in general not efficiently solvable. We find that the problem of determine all the extremal points is closely related to determine the boundary states of the universal C*-algebra [Ave08], which would decide Tsirelson's problem [SW08], and thus, also Connes embedding problem [JNP$^+$11]. Hence, a general solution of the problem is hardly possible and instead we focus on concrete configurations. The case of $N$ parties where each can perform two binary measurements is completely determined by the irreducible representations of the universal C*-algebra of two-projections (see Section 7.4.1). This, together with ideas from [DLTW08], enabled us to find a parameterized family of extremal correlation tables for the simplest case of $N = 2$ parties. The case of two parties and arbitrary numbers of binary measurements at each site was characterized by Tsirelson [Tsi85] and is discussed in Section 7.4.3.

**Outlook.** The characterization of secure correlation tables shed new light on the requirements that have to be satisfied in order to be useful for device-independent quantum key distribution. A natural extension would be to consider almost secure correlation tables. The security in that case has to be determined by a distance to the closest extremal correlation table. However, linking different distance measures to an operational meaning is far from trivial. A natural measure of security of a correlation table $\mathbb{P}$ with a direct interpretation would be to define the distance as the maximal possible weight of the deterministic points maximized over all convex combinations of $\mathbb{P}$ into extremal correlation tables. This idea was for instance used in the device-independent security proof in [BHK05]. This measure depends crucially on the geometry of the convex set of quantum correlation tables. It would thus be interesting to study this geometry in more detail, especially, around extremal correlation tables which are possible candidates for practical implementations of device-independent quantum key distribution protocols including the one maximizing the CHSH-inequality or Mermin's inequalities [Mer90].

The different cases specified by the number of parties $N$, measurements $M$ and outcomes $K$, are related to different notions of security of two-party quantum key distribution protocols. In the situation where $(N, M, K)$ is $(2, 2, 2)$, we can under the assumption of individual attacks, directly estimate the correlation table $\mathbb{P}$. From this we can then determine the maximal possible weight of deterministic points, previously discussed, and infer security of the device-independent quantum key distribution protocol in analogy to [BHK05]. The case $(2n, 2, 2)$ would then corre-

spond to $n$ choices of two commuting binary measurements at each site as discussed in [HR10, MPA11]. Finally, the case $(2, 2^n, 2^n)$ corresponds to coherent attacks in a protocol based on $n$ choices of two possible binary measurements. Since only little is known about the C*-algebra corresponding to the $(2, 2^n, 2^n)$ case, finding extremal correlation tables or even verifying that a correlation table is close to an extremal one is generally extremely difficult.

# A. Technical Results

## A.1. Gaussian Extremality

In the following we show that the infimum $\inf_\omega H(X_A|E)_\omega$ taken over all states $\omega_{AB}$ with covariance matrix $\Gamma$ is attained for the Gaussian representative. Even though the argument is in analogy to [GPC06], we give it here for the sake of completeness. See also [NGA06] for a similar result.

The main tool is the nice result from [RWW06] which classifies functions which are optimized by Gaussian states. In particular, if one can show that a function $f(\omega_{AB})$ is (i) lower semi-continuous in trace norm, (ii) invariant under local unitary transformations, and (iii) strongly superadditive, i.e. $f(\omega_{ABA'B'}) \geq f(\omega_{AB}) + f(\omega_{A'B'})$ where equality holds if $\omega_{ABA'B'} = \omega_{AB} \otimes \omega_{A'B'}$, then it follows that $f(\omega_{AB}) \geq f(\omega_{AB}^\Gamma)$. Here, $\omega_{AB}^\Gamma$ denotes the Gaussian representative of the family of states with same covariance matrix $\Gamma$.

Consider now the function $f(\omega_{AB}) = H(X|E)_\omega$ where $\omega_{ABE}$ is a purification of $\omega_{AB}$ and $\omega_{XBE}$ is obtained by applying the measurement used in our protocol on the A system. The conditional von Neumann entropy is defined in accordance with [Kuz11], that is, $H(A|B)_\rho = H(A)_\rho - H(\rho_{AB}||\rho_A \otimes \rho_B)$ where $H(\rho||\sigma)$ denotes the relative entropy. In this definition we require that $H(A)_\rho$ is finite. Note that the classical alphabet $\mathcal{X}$ on which $\omega_X$ is defined is finite such that $H(X)_\omega$ is always finite and the conditional entropy is well-defined. Because $0 \leq H(X|B)_\rho \leq H(X)_\rho \leq \log|\mathcal{X}|$ holds for any finite-dimensional B systems, we obtain the same result for infinite-dimensional Hilbert spaces via the finite-dimensional approximation property of the conditional von Neumann entropy as shown in [Kuz11].

We show now that $f$ satisfies the properties (i)-(iii) from which the extremality of the Gaussian state follows. The properties (i) and (ii) are obtained in a similar way as in [GPC06]. In order to show property (iii) one takes a purification $\omega_{ABA'B'E}$ of $\omega_{ABA'B'}$ which is of course also a purification of $\omega_{AB}$ and $\omega_{A'B'}$. The following chain of inequalities for the von Neumann entropies

$$\begin{aligned} H(XX|E)_\omega &= H(X|X'E)_\omega + H(X'|XE)_\omega \\ &\quad + I(X:X'|E)_\omega \\ &\geq H(X|A'B'E) + H(X|ABE) \end{aligned}$$

holds for finite-dimensional systems due to $I(X:X'|E)_\omega \geq 0$ and since $X$ $(X')$ is obtained from $AB$ $(A'B')$ via a trace preserving completely positive map. But this can be lifted to infinite-dimensions via the finite-dimensional approximation property [Kuz11] as the entropies are all finite. Hence, we obtain the strong super-

additivity

$$\begin{aligned} f(\omega_{ABA'B'}) &= H(XX|E)_\omega \\ &\geq H(X|A'B'E) + H(X|ABE) \\ &= f(\omega_{AB}) + f(\omega_{A'B'})\,. \end{aligned}$$

The equality in the case of $\omega_{AB} \otimes \omega_{A'B'}$ follows from the additivity of the von Neumann entropy.

## A.2. The Conditional von Neumann Entropy for Finite Spacing

The goal is to calculate $H(X_A|E)_\omega$ for a two mode squeezed Gaussian state $\omega_{AB}$. For the proper definition and the properties of conditional von Neumann entropies for infinite-dimensional systems, we refer to [Kuz11]. Let $\omega_{ABC}$ be a Gaussian purification of $\omega_{AB}$ with $\omega_E$ a two mode Gaussian state. We first rewrite the entropy as

$$\begin{aligned} H(X_A|E)_\omega &= H(X_AE)_\omega - H(E)_\omega \\ &= H(E|X_A)_\omega + H(X_A)_\omega - H(AB)_\omega\ , \end{aligned}$$

where we used that $\omega_{ABE}$ is pure and therefore $H(E) = H(AB)$. Note also that in our case the alphabet $\mathcal{X}$ is finite. Since $\omega_{AB}$ is a two mode Gaussian state the entropy $H(AB)_\omega$ is just a function of the symplectic invariants and can be calculated [SIDS04].

For the computation of the other entropies, we assume for simplicity that the correlations in amplitude and phase are symmetric, and do the calculation for the amplitude measurement with corresponding operator denoted by $X$. The measurement operators for a projection onto the interval $I_k$, $k \in \mathcal{X}$, are described by $E_k = \mu_x(I_k)$, where $\mu_x$ is the spectral measure of $X$. The post-measurement states are then given by $\omega^k_{ABE} = 1/p_k(E_k\omega_{ABE}E_k^\dagger)$, where $p_k = \mathrm{Tr}\,[\omega_{ABE}E_k]$. The entropy $H(X_A)_\omega$ is the Shannon entropy of the classical distribution $\{p_k\}$.

Let us turn to the estimation of $H(E|X_A)_\omega$. First, we note that

$$H(E|X_A)_\omega = \sum_k p_k H(E)_{\omega^k}\ ,$$

which reduces the problem to calculate $H(E)_{\omega^k}$ for every $k \in \mathcal{X}$. For that we introduce the normalized post measurement state $\omega_{BE}(x)$ conditioned that Alice measures the amplitude $x \in \mathbb{R}$. Furthermore, we denote by $p(x)$ the probability that Alice measures $x$. Since $\omega_{AE}$ is a Gaussian state, one can show that $\omega_E(x) = \mathrm{U}(v(x))\omega_E(0)\mathrm{U}(v(x))^\dagger$, where $\mathrm{U}(v)$ denotes the Weyl operator which corresponds to a phase space translation and $v$ is a continuous function which depends on $\Gamma_{AE}$. Hence, we obtain that $H(E)_{\omega(x)} = H(E)_{\omega(0)}$ for all $x$.

**Proposition A.2.1.** *Let $\omega_{AB}$ be a two mode squeezed Gaussian state, $\omega_{ABE}$ a Gaussian purification, and $\omega_{BE}(x)$ and $\omega^k_{BE}$ as defined above. Then, it follows that $H(E)_{\omega^k} \geq H(E)_{\omega(0)}$ and, thus, $H(E|X_A)_\omega \geq H(E)_{\omega(0)}$.*

*Proof.* The proof exploits the concavity of the von Neumann entropy and the fact that the state $\omega_E^k$ can be approximated in trace class by a finite convex combination of states $\omega_E(x)$. Note that we can write $\omega_E^k = 1/p_k \int_{I_k} p(x)\omega_E(x)\mathrm{dx}$ where the integral converges weakly. As discussed above we also have the relation $\omega_E(x) = \mathrm{U}(v(x))\omega_E(0)\mathrm{U}(v(x))^\dagger$. Since $\mathrm{U}(v)$ is strongly continuous in $v$, we have $x \mapsto \omega_{BE}(x)$ and, thus, $x \mapsto \omega_E(x)$ are trace class continuous. Hence, we know that the Lebesgue integral $\int_{I_k} p(x)\omega_E(x)\mathrm{dx}$ converges even in trace norm, and furthermore, it is equal to the Riemann integral. So we can approximate $\omega_E^k$ in trace norm via step functions

$$\rho_E^l = \frac{1}{p_k} \sum_{j=1}^{N_l} p(x_j^l)|J_j^l|\omega_E(x_j^l) \ ,$$

where it holds for all $l$ that $I_k = \bigcup_j J_j^l$, the $x_j^l \in J_j^l$ are chosen such that $\sum_{j=1}^{N_l} p(x_j^l)|J_j^l| = p_k$, and $\sup_j |J_j^l| \to 0$ for $l \to \infty$. Furthermore, as $\omega_E(x)$ is a Gaussian state, we have that for $H = Q_E^2 + P_E^2$ the expectation value $\mathrm{Tr}\,[\omega_E(x)H]$ is bounded and continuous in $x$, so $\mathrm{Tr}\left[\rho_E^l H\right] \to \mathrm{Tr}\left[\omega_E^k H\right]$ for $l \to \infty$ [1]. Using that the von Neumann entropy is continuous for sequences of states with finite energy [Weh78], we find that $H(E)_{\omega^k} = \lim_{l\to\infty} H(\rho_E^l)$, and thus,

$$\begin{aligned} H(\omega_E^k) &= \lim_{l\to\infty} H(\rho_E^l) \\ &\geq \lim_{l\to\infty} \frac{1}{p_k} \sum_{j=1}^{N_l} p(x_j^l)|J_j^l| H(\omega_E(x_j^l)) = H(\omega_E(0)) \ . \end{aligned}$$

The inequality is due to the concavity of the von Neumann entropy [Weh78] and the last equality holds because $H(\omega_E(x))$ is independent of $x$. □

Using this proposition we finally get

$$H(X_A|E)_\omega \geq H(E)_{\omega(0)} + H(X_A)_\omega - H(AB)_\omega \ ,$$

where the right-hand side can be calculated since $\omega_E(0)$ and $\omega_{AB}$ are Gaussian states (see, e.g., [SIDS04]). Note also that the only dependence on the interval length $\delta$ in this formula is due to $H(X_A)_\omega$.

[1] We also use that $x < \infty$ for $x \in I_k$ since $I_k \subset \mathbb{R}$ for all $k$.

# Bibliography


[ABG+07] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, *Device-independent security of quantum cryptography against collective attacks*, Physical Review Letters **98** (2007), 230501.

[ACMT+07] K. M. R. Audenaert, J. Calsamiglia, R. Munoz-Tapia, E. Bagan, L. Masanes, A. Acin, and F. Verstraete, *Discriminating States: The Quantum Chernoff Bound*, Physical Review Letters **98** (2007), 160501.

[AF04] R. Alicki and M. Fannes, *Continuity of quantum conditional information*, J. Phys. A **37** (2004), L55.

[AKMB11] S. Abruzzo, H. Kampermann, M. Mertz, and D. Bruß, *Quantum key distribution with finite resources: Secret key rates via Rényi entropies*, Physical Review A **84** (2011), 032321.

[Alb83] P. M. Alberti, *A note on the transition probability over C*-algebras*, Letters in Mathematical Physics **7** (1983), 25–32.

[Ara75] H. Araki, *Relative entropy of states of von Neumann algebras*, Publications of the Research Institute for Mathematical Sciences **11** (1975), no. 3, 809–833.

[Ave08] W. Aversen, *The noncommutative Choquet boundary*, Journal of the American Mathematical Society **21** (2008), 1065–1084.

[BB84] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (1984), 175–179.

[BB06] I. Bialynicki-Birula, *Formulation of the uncertainty relations in terms of the Rényi entropies*, Physical Review A **74** (2006), 052101.

[BBCM95] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, *Generalized privacy amplification*, IEEE Transactions on Information Theory **41** (1995), no. 6, 1915–1923.

[BBM75] I. Bialynicki-Birula and J. Mycielski, *Uncertainty relations for information entropy in wave mechanics*, Communications in Mathematical Physics **44** (1975), 129–132.

[BBM92] C. H. Bennett, G. Brassard, and N. D. Mermin, *Quantum cryptography without Bell's theorem*, Physical Review Letters **68** (1992), 557–559.

[BBR88] C. H. Bennett, G. Brassard, and J.-M. Robert, *Privacy amplification by public discussion*, SIAM Journal on Computing **17** (1988), no. 2, 210–229.

[BBR11] I. Bialynicki-Birula and L. Rudnicki, *Entropic Uncertainty Relations in Quantum Physics*, Statistical Complexity, Ed. K. D. Sen, Springer, 2011, p. 1.

[BCC+10] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, *The uncertainty principle in the presence of quantum memory*, Nature Physics **6** (2010), 659.

[BD09] F. Brandão and N. Datta, *One-shot rates for entanglement manipulation under non-entangling maps*, IEEE Transactions on Information Theory **57** (2009), 1754.

[BD10a] F. Buscemi and N. Datta, *Distilling entanglement from arbitrary resources*, Journal of Mathematical Physics **51** (2010), 102201.

[BD10b] ———, *General theory of assisted entanglement distillation.*

[BD10c] ———, *The quantum capacity of channels with arbitrarily correlated noise*, IEEE Transactions on Information Theory **56** (2010), 1447.

[BD11] ———, *Entanglement cost in practical scenarios*, Physical Review Letters **106** (2011), 130503.

[Bec75] W. Beckner, *Inequalities in Fourier analysis*, The Annals of Mathematics **102** (1975), no. 1, pp. 159–182 (English).

[Bel64] J. S. Bell, *On the Einstein Podolsky Rosen paradox*, Physics **1** (1964), no. 3, 195–200.

[Ber08] M. Berta, *Single-shot quantum state merging*, Master's thesis, ETH Zürich, 2008, arXiv:0912.4495v1.

[BFS11] M. Berta, F. Furrer, and V. B. Scholz, *The Smooth Entropy Formalism on von Neumann Algebras*, arXiv:1107.5460v1 (2011).

[BHJ25] M. Born, W. Heisenberg, and P. Jordan, *Zur Quantenmechanik II*, Zeitschrift für Physik **35** (1925), 557–615.

[BHK05] J. Barrett, L. Hardy, and A. Kent, *No signaling and quantum key distribution*, Physical Review Letters **95** (2005), 010503.

[BJ25] M. Born and P. Jordan, *Zur Quantenmechanik*, Zeitschrift für Physik **34** (1925), 858–888.

[BKP06] J. Barrett, A. Kent, and S. Pironio, *Maximally nonlocal and monogamous quantum correlations*, Physical Review Letters **97** (2006), 170409.

[BLM+05] J. Barrett, N. Linden, S. Massar, S. Pironio, S. Popescu, and D. Roberts, *Nonlocal correlations as an information-theoretic resource*, Physical Review A **71** (2005), 022101.

[BOHL+05] M. Ben-Or, M. Horodecki, D. Leung, D. Mayers, and J. Oppenheim, *The universal composable security of quantum key distribution*, Theory of Cryptography (Joe Kilian, ed.), Lecture Notes in Computer Science, vol. 3378, Springer Berlin / Heidelberg, 2005, pp. 386–406.

[Bor26] M. Born, *Zur Quantenmechanik der Stossvorgänge*, Zeitschrift für Physik A **37** (1926), 12, 863–867.

[BR79] O. Bratteli and D. W. Robinson, *Operator algebras and quantum statistical mechanics 1*, Springer, 1979.

[BR81] ———, *Operator algebras and quantum statistical mechanics 2*, Springer, 1981.

[BS94] G. Brassard and L. Salvail, *Secret-key reconciliation by public discussion*, Lecture Notes in Computer Science, vol. 765, Springer-Verlag, 1994, pp. 410–423.

[Bur69] D. Bures, *An extension of Kakutani's theorem on infinite product measures to the tensor product of semifinite W*-algebras*, Transactions of the American Mathematical Society **135** (1969), 199–212.

[BvL05] S. L. Braunstein and P. van Loock, *Quantum information with continuous variables*, Reviews of Modern Physics **77** (2005), 513–577.

[Can01] R. Canetti, *Universally composable security: a new paradigm for cryptographic protocols*, Proc. IEEE Int. Conf. on Cluster Comput., 2001, pp. 136–145.

[CCYZ12] P. J. Coles, R. Colbeck, L. Yu, and M. Zwolak, *Uncertainty relations from simple entropic properties*, Physical Review Letters **108** (2012), 210405.

[CHSH69] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, *Proposed experiment to test local hidden-variable theories*, Physical Review Letters **23** (1969), 880–884.

[CK78] I. Csiszar and J. Körner, *Broadcast channels with confidential messages*, IEEE Transactions on Information Theory **24** (1978), no. 3, 339 – 348.

[CKMR07] M. Christandl, R. König, G. Mitchison, and R. Renner, *One-and-a-half quantum de Finetti theorems*, Communications in Mathematical Physics **273** (2007), 473.

[CKR09] M. Christandl, R. König, and R. Renner, *Post-selection technique for quantum channels with applications to quantum cryptography*, Physical Review Letters **102** (2009), 020504.

[CLA01] N. J. Cerf, M. Lévy, and G. Van Assche, *Quantum distribution of Gaussian keys using squeezed states*, Physical Review A **63** (2001), 052311.

[CM96] C. Cachin and U. Maurer, *Smoothing probability distributions and smooth entropy (extended abstract)*, Proceedings of International Symposium on Information Theory, ISIT 97, 1996.

[CT91] T. M. Cover and J. A. Thomas, *Elements of information theory*, J. Wiley & Sons, Inc., New York, 1991.

[CT07] C. D. Charalambos and R. Tourky, *Cones and duality, graduate studies in mathematics vol. 84*, American Mathematical Society, 2007.

[CW79] J. L. Carter and M. N. Wegman, *Universal classes of hash functions*, Journal of Computer and System Sciences **18** (1979), 143–154.

[CYGG] P. J. Coles, L. Yu, V. Gheorghiu, and R. B. Griffiths, *Information-theoretic treatment of tripartite systems and quantum channels*, Physical Review A **83**, 062338.

[CYZ11] P. J. Coles, L. Yu, and M. Zwolak, *Relative entropy derivation of the uncertainty principle with quantum side information*, arXiv:1105.4865v1.

[Dat09] N. Datta, *Max- relative entropy of entanglement, alias log robustness*, International Journal of Quantum Information **7** (2009), 475.

[Dav76] E. B. Davies, *Quantum theory of open systems*, London, New York : Academic Press, 1976.

[DBWR10] F. Dupuis, M. Berta, J. Wullschleger, and R. Renner, *The decoupling theorem*, arXiv:1012.6044v1.

[Deu83] D. Deutsch, *Uncertainty in quantum measurements*, Physical Review Letters **50** (1983), 631–633.

[DLTW08] A. C. Doherty, Y.-C. Liang, B. Toner, and S. Wehner, *The quantum moment problem and bounds on entangled multi-prover games*, Proceedings of IEEE Conference on Computational Complexity 2008 (2008), 199.

[DST] F. Dupuis, O. Szehr, and M. Tomamichel, *A decoupling approach to classical data transmission over quantum channels*, arXiv:1207.0067 **2012**.

[Dup09] F. Dupuis, *The decoupling approach to quantum information theory*, Ph.D. thesis, Université de Montréal, 2009, arXiv:1004.1641v1.

[DW03] I. Devetak and A. Winter, *Classical data compression with quantum side information*, Physical Review A **68** (2003), no. 4, 042301.

[DW05] ———, *Distillation of secret key and entanglement from quantum state*, Proceedings of Royal Society A **461** (2005), 207.

[EHD+11a] T. Eberle, V. Händchen, J. Duhme, T. Franz, R.F. Werner, and R. Schnabel, *Gaussian Entanglement for Quantum Key Distribution from a Single-Mode Squeezing Source*, arXiv:1110.3977 (2011).

[EHD+11b] ———, *Strong Einstein-Podolsky-Rosen entanglement from a single squeezed light source*, Physical Review A **83** (2011), 052329.

[Eke91] A. Ekert, *Quantum cryptography based on Bell's theorem*, Physical Review Letters **67** (1991), 661–663.

[FAR11] F. Furrer, J. Aberg, and R. Renner, *Min- and max-entropy in infinite dimensions*, Communications in Mathematical Physics **306** (2011), no. 1, 165–186.

[FFB+11] F. Furrer, T Franz, M. Berta, V.B. Scholz, M. Tomamichel, A. Leverrier, and R.F. Werner, *Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks*, arxiv:1112.2179 (2011), Accepted for publication in Physical Review Letters.

[FFW11] T. Franz, F. Furrer, and R. F. Werner, *Extremal Quantum Correlations and Cryptographic Security*, Physical Review Letters **106** (2011), 250502.

[Fin82] A. Fine, *Hidden variables, joint probability, and the Bell inequalities*, Physical Review Letters **48** (1982), 291–295.

[FL11] R.L. Frank and E.H. Lieb, *Entropy and the uncertainty principle*, arXiv:1109.1209v1 (2011).

[Fur09] F. Furrer, *Min- and max-entropies as generalized entropy measures in infinite-dimensional quantum systems*, Master's thesis, ETH Zürich, 2009.

[GG02] F. Grosshans and P. Grangier, *Continuous variable quantum cryptography using coherent states*, Physical Review Letters **88** (2002), 057902.

[GM87] A. Garg and N. D. Mermin, *Detector inefficiencies in the Einstein-Podolsky-Rosen experiment*, Physical Review D **35** (1987), 3831–3835.

[GN43] I. Gelfand and M. Neumark, *On the imbedding of normed rings into the ring of operators in Hilbert space*, Sbornik: Mathematics **12** (1943), 197–217.

[GP01] D. Gottesman and J. Preskill, *Secure quantum key distribution using squeezed states*, Physical Review A **63** (2001), 022309.

[GPC06] R. García-Patrón and N. J. Cerf, *Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution*, Physical Review Letters **97** (2006), 190503.

[HÏ0] E. Hänggi, *Device-independent quantum key distribution*, Ph.D. thesis, ETH Zurich, 2010.

[Haa92] R. Haag, *Local quantum physics: Fields, particles, algebras*, Springer, 1992.

[HD11] M.-H. Hsieh and N. Datta, *One-shot entanglement-assisted classical communication*, arXiv:1105.3321v1.

[Hei25] W. Heisenberg, *über quantentheoretische Umdeutung kinematischer und mechanischer Beziehungen.*, Zeitschrift für Physik **33** (1925), 879–893.

[Hei27] W. Heisenberg, *Zur Quantenmechanik einfacher Bewegungstypen*, Zeitschrift für Physik **43** (1927), 172.

[HHYW08] P. Hayden, M. Horodecki, J. Yard, and A. Winter, *A decoupling approach to the quantum capacity*, Open Systems & Information Dynamics **15** (2008), 1, pp. 7–9.

[Hil00] M. Hillery, *Quantum cryptography with squeezed states*, Physical Review A **61** (2000), 022309.

[HJ57] I. I. Hirschman Jr., *A note on entropy*, American Journal of Mathematics **79** (1957), no. 1, pp. 152–156 (English).

[HML08] H. Häseler, T. Moroder, and N. Lütkenhaus, *Testing quantum devices: Practical entanglement verification in bipartite optical systems*, Physical Review A **77** (2008), 032303.

[HN03] M. Hayashi and H. Nagaoka, *General formulas for capacity of classical-quantum channels*, IEEE Transactions on Information Theory **49** (2003), no. 7, 1753–1768.

[Hol98] A. S. Holevo, *The capacity of the quantum communication channel with general signal states*, IEEE Transactions on Information Theory **44** (1998), 269.

[HOW05] M. Horodecki, J. Oppenheim, and A. Winter, *Partial quantum information*, Nature **436** (2005), 673–676.

[HOW06] ———, *Quantum state merging and negative information*, Communications in Mathematical Physics **269** (2006), 107.

[HP91] F. Hiai and D. Petz, *The proper formula for relative entropy and its asymptotics in quantum probability*, Communications in Mathematical Physics **143** (1991), no. 1, 99–114.

[HR10] E. Hänggi and R. Renner, *Device-independent quantum key distribution with commuting measurements*, arXiv:1009.1833.

[HS10] A. S. Holevo and M. E. Shirokov, *Mutual and coherent information for infinite-dimensional quantum channels*, Problems of Information Transmission **46** (2010), 201–217.

[HT11a] E. Hänggi and M. Tomamichel, *The link between uncertainty relations and non-locality*, arXiv:1108.5349 (2011).

[HT11b] M. Hayashi and T. Tsurumaru, *Concise and tight security analysis of the Bennett-Brassard 1984 protocol with finite key lengths*, arXiv:1107.0589 (2011).

[HW94] P. Hausladen and W. K. Wootters, *A pretty good measurement for distinguishing quantum states*, Journal of Modern Optics **41** (1994), no. 12, 2385.

[ILL89] R. Impagliazzo, L. A. Levin, and M. Luby, *Pseudo-random generation from one-way functions*, Proceedings of 21st Annual ACM Symposium on Theory of Computing (1989), 12–24.

[JKJL11] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, *Long-distance continuous-variable quantum key distribution with a gaussian modulation*, Physical Review A **84** (2011), 062317.

[JNP+11] M. Junge, M. Navascues, C. Palazuelos, D. Perez-Garcia, V. B. Scholz, and R. F. Werner, *Connes' embedding problem and Tsirelson's problem*, Journal of Mathematical Physics **52** (2011), 012102.

[Ken27] E. H. Kennard, *Zur Quantenmechanik einfacher Bewegungstypen*, Zeitschrift für Physik A **44** (1927), 326–352.

[KGR05] B. Kraus, N. Gisin, and R. Renner, *Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication*, Physical Review Letters **95** (2005), 080501.

[Kiu] J. Kiukas, *Private communication.*

[Kle31] O. Klein, *Zur quantenmechanischen Begründung des zweiten Hauptsatzes der Wärmelehre.*, Zeitschrift für Physik A **72** (1931), 767 – 775.

[KMR05] R. König, U. M. Maurer, and R. Renner, *On the power of quantum memory*, IEEE Transactions on Information Theory **51** (2005), no. 7, 2391–2401.

[Koa06] M. Koashi, *Unconditional security of quantum key distribution and the uncertainty principle*, Journal of Physics: Conference Series **36** (2006), 98.

[Kra83] K. Kraus, *States, effects, and operations fundamental notions of quantum theory, lecture notes in physics, vol. 190*, Berlin ; New York : Springer-Verlag, 1983.

[KRBM07] R. König, R. Renner, A. Bariska, and U. Maurer, *Small accessible quantum information does not imply security*, Physical Review Letters **98** (2007), 140502.

[KRS09] R. König, R. Renner, and C. Schaffner, *The operational meaning of min- and max-entropy*, IEEE Transactions on Information Theory **55** (2009), no. 9, 4674–4681.

[KSW08] D. Kretschmann, D. Schlingemann, and R.F. Werner, *The information-disturbance tradeoff and the continuity of Stinespring's representation*, Information Theory, IEEE Transactions on **54** (2008), no. 4, 1708 – 1717.

[Kuz11] A. A. Kuznetsova, *Conditional entropy for infinite-dimensional quantum systems*, Theory Probab. Appl. **55** (2011), 709.

[KW10] J. Kiukas and R. F. Werner, *Maximal violation of Bell inequalities by position measurements*, Journal of Mathematical Physics **51** (2010), 072105.

[LAM+11] L. Lydersen, M. K. Akhlaghi, A H. Majedi, J. Skaar, and V. Makarov, *Controlling a superconducting nanowire single-photon detector using tailored bright illumination*, New Journal of Physics **13** (2011), no. 11, 113042.

[Lar98] J.-Å. Larsson, *Bell's inequality and detector inefficiency*, Physical Review A **57** (1998), 3304–3308.

[LBGP+07] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, *Quantum key distribution over* 25 km *with an all-fiber continuous-variable system*, Physical Review A **76** (2007), 042305.

[LGG10] A. Leverrier, F. Grosshans, and P. Grangier, *Finite-size analysis of a continuous-variable quantum key distribution*, Physical Review A **81** (2010), 062343.

[Lin73] G. Lindblad, *Entropy, information and quantum measurements*, Comm. Math. Phys. **33** (1973), 305–322.

[Lin74] ———, *Expectations and entropy inequalities for finite quantum systems*, Comm. Math. Phys. **39** (1974), 111–119.

[LP64] H. J. Landau and H. O. Pollak, *Prolate spheroidal wave functions, Fourier analysis and uncertainty-II*, The Bell System Technical Journal **40** (1964), no. 6, 65–84.

[Lus12] N. Lusin, *Sur les propriétés des fonctions measurables*, Comptes rendus de l'Académie des sciences Paris **154** (1912), 1688–1690.

[Mas03] L. Masanes, *Necessary and sufficient condition for quantum-generated correlations*, arXiv:quant-ph/0309137 (2003).

[May96] D. Mayers, *Quantum key distribution and string oblivious transfer in noisy channels*, Advances in Cryptology CRYPTO'96 (Neal Koblitz, ed.), Lecture Notes in Computer Science, vol. 1109, Springer Berlin / Heidelberg, 1996, pp. 343–357.

[MD09] M. Mosonyi and N. Datta, *Generalized relative entropies and the capacity of classical-quantum channels*, Journal of Mathematical Physics **50** (2009), 072104.

[Mer90] N. D. Mermin, *Extreme quantum entanglement in a superposition of macroscopically distinct states*, Physical Review Letters **65** (1990), 1838–1840.

[MPA11] L. Masanes, S. Pironio, and A. Acin, *Secure device-independent quantum key distribution with causally independent measurement devices*, Nature Communications **2** (2011), 238.

[MQR09] J. Müller-Quade and R. Renner, *Composability in quantum cryptography*, New J. Phys. **11** (2009), 085006.

[MU88] H. Maassen and J. B. M. Uffink, *Generalized entropic uncertainty relations*, Physical Review Letters **60** (1988), 1103–1106.

[Mur90] G. J. Murphy, *C*-algebras and operator theory*, Academic Press, INC, 1990.

[MY98] D. Mayers and A. Yao, *Quantum cryptography with imperfect apparatus*, Foundations of Computer Science, 1998. Proceedings.39th Annual Symposium on, 1998, pp. 503 –509.

[NC00] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, 2000.

[NGA06] M. Navascués, F. Grosshans, and A. Acín, *Optimality of Gaussian attacks in continuous-variable quantum cryptography*, Physical Review Letters **97** (2006), 190502.

[NPA08] M. Navascues, S. Pironio, and A. Acin, *A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations*, New Journal of Physics **10** (2008), 073013.

[Oga10] Y. Ogata, *A generalization of the inequality of Audenaert et al.*, arXiv:1011.1340v1.

[OP93] M. Ohya and D. Petz, *Quantum entropy and its use*, Springer Verlag Berlin, Heidelberg, New York, 1993.

[Pau02] V. I. Paulsen, *Completely bounded maps and operator algebras*, Cambridge University Press, 2002.

[Ped68] G. K. Pederson, *Measurem theory in C*-algebras II*, Math. Scand. 22 **22** (1968), 63–74.

[Ped08] F. Pedrocchi, *An infinite dimensional quantum de Finetti theorem: tests of robustness*, Master's thesis, ETH Zürich, 2008.

[Pet85] D. Petz, *Quasientropies for states of a von Neumann algebra*, Publications of the Research Institute for Mathematical Sciences **21** (1985), no. 4, 787–800.

[Pet86] ———, *Properties of the relative entropy of states of von Neumann algebras*, Acta Mathematics Hungary **47** (1986), no. 1-2, 65–72.

[PR94] S Popescu and D. Rohrlich, *Quantum nonlocality as an axiom*, Foundations of Physics **24** (1994), 379–385.

[Proa] *http://qig.itp.uni-hannover.de/qiproblems/1.*

[Prob] *http://qig.itp.uni-hannover.de/qiproblems/33.*

[PT09] V. I. Paulsen and M. Tomforde, *Vector spaces with an order unit*, Indiana University Mathematics Journal **58** (2009), no. 3, 1319–1360.

[Rae89] Sinclair A. M. Raeburn, I., *The C*-algebra generated by two projections*, Mathematica Scandenavica **65** (1989), 278–290.

[Ral99] T. C. Ralph, *Continuous variable quantum cryptography*, Physical Review A **61** (1999), 010303.

[RB09] J. M. Renes and J.-C. Boileau, *Conjectured strong complementary information tradeoff*, Physical Review Letters **103** (2009), 020402.

[RC09] R. Renner and J. I. Cirac, *De Finetti representation theorem for infinite dimensional quantum systems and applications to quantum cryptography*, Physical Review Letters **102** (2009), 110504.

[Rei00] M. D. Reid, *Quantum cryptography with a predetermined key, using continuous-variable einstein-podolsky-rosen correlations*, Physical Review A **62** (2000), 062308.

[Rén60] A. Rényi, *On measures of information and entropy*, Proceedings of the 4th Berkeley Symposium on Mathematics, Statistics and Probability (1960), 547–561.

[Ren05] Renato Renner, *Security of quantum key distribution*, Ph.D. thesis, ETH Zurich, 2005.

[Ren07] R. Renner, *Symmetry of large physical systems implies independence of subsystems*, Nature Physics **3** (2007), 645.

[RGK05] Renato Renner, Nicolas Gisin, and Barbara Kraus, *Information-theoretic security proof for quantum-key-distribution protocols*, Physical Review A **72** (2005), 012332.

[RK05] R. Renner and R. König, *Universally composable privacy amplification against quantum adversaries*, Springer Lecture Notes in Computer Science **3378** (2005), 407.

[RR11] J. M. Renes and R. Renner, *Noisy channel coding via privacy amplification and information reconciliation*, IEEE Transactions on Information Theory **57** (2011), 7377.

[RR12] ———, *One-shot classical data compression with quantum side information and the distillation of common randomness or secret keys*, IEEE Transactions on Information Theory **58** (2012), 1985.

[RS78] M. Reed and B. Simon, *Methods of modern mathematical physics, Vol. i: Functional analysis*, NewYork Academic Press, 1978.

[RW04] R. Renner and S. Wolf, *Smooth Rényi entropy and applications*, Proceedings of IEEE International Symposium Information Theory (2004), 233.

[RW05] ———, *Simple and tight bounds for information reconciliation and privacy amplification*, Springer Lecture Notes in Computer Science **3788** (2005), 199.

[RWW06] R. Renner, S. Wolf, and J. Wullschleger, *The single-serving channel capacity*, Proceedings of IEEE International Symposium on Information Theory (2006), 1424–1427.

[Sak65] S. Sakai, *A Radon-Nikodym theorem in W*-algebras*, Bulletin American Mathematical Society **71** (1965), no. 1, 149–152.

[SBPC+09] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, *The security of practical quantum key distribution*, Reviews of Modern Physics **81** (2009), 1301.

[Sch26a] E. Schrödinger, *Quantisierung als Eigenwertproblem*, Annalen der Physik (1926), 361–377.

[Sch26b] ———, *An undulatory theory of the mechanics of atoms and molecules*, Physical Review **28** (1926), 1049–1070.

[Sch95] B. Schumacher, *Quantum coding*, Physics Review A **51** (1995), 2738–2747.

[Seg47] I. E. Segal, *Irreducible representations of operator algebras*, Bulletin American Mathematical Society **53** (1947), 73–88.

[Ser74] R.J. Serfling, *Probability inequalities for the sum in sampling without replacement*, Annals of Statistics **2** (1974), 39–48.

[Sha48] C. E. Shannon, *A mathematical theory of communication*, Bell System Technical Journal **27** (1948), 379–423, 623–656.

[SIDS04] A. Serafini, F. Illuminati, and S. De Siena, *Symplectic invariants, entropic measures and correlations of gaussian states*, Journal of Physics B **37** (2004), L21.

[Sim96] Barry Simon, *Graduate studies in mathematics vol. 10, representations of finite and compact groups*, American Mathematical Society, 1996.

[Sio58] Maurice Sion, *On general minimax theorems.*, Pacific Journal of Mathematics **8** (1958), 171–176.

[SLS10] L. Sheridan, T. P. Le, and V. Scarani, *Finite-key security against coherent attacks in quantum key distribution*, New Journal of Physics **12** (2010), 123019.

[SP00] P.W. Shor and J. Preskill, *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol*, Physical Review Letters **85** (2000), 441–444.

[SRLL02] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, *Continuous Variable Quantum Cryptography: Beating the 3 db Loss Limit*, Physical Review Letters **89** (2002), 167901.

[Sto30] M. H. Stone, *Linear transformations in hilbert space III. Operational methods and group theory*, Proceedings of the National Academy of Sciences **16** (1930), 172–175.

[SW71] D. Slepian and J. Wolf, *Noiseless coding of correlated information sources*, IEEE Transactions on Information Theory **19** (1971), 461.

[SW97] B. Schumacher and M. D. Westmoreland, *Sending classical information via noisy quantum channels*, Physics Review A **56** (1997), 131.

[SW08] V. B. Scholz and R. F. Werner, *Tsirelson's problem*, arXiv:0812.4305v1.

[Tak01] M. Takesaki, *Theory of operator algebras 1*, Springer, 2001.

[Tak02a] ———, *Theory of operator algebras 2*, Springer, 2002.

[Tak02b] ———, *Theory of operator algebras 3*, Springer, 2002.

[TCR09] M. Tomamichel, R. Colbeck, and R. Renner, *A fully quantum asymptotic equipartition property*, IEEE Transactions on Information Theory **55** (2009), 5840–5847.

[TCR10] ———, *Duality between smooth min- and max-entropies*, IEEE Transactions on Information Theory **56** (2010), 4674.

[TKI03] K. Tamaki, M. Koashi, and N. Imoto, *Unconditionally secure key distribution based on two nonorthogonal states*, Physical Review Letters **90** (2003), 167904.

[TLGR12] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, *Tight finite-key analysis for quantum cryptography*, Nature Communications **3** (2012), 634, arXiv:1103.4130v1.

[Tom12] M. Tomamichel, *A framework for non-asymptotic quantum information theory*, Ph.D. thesis, ETH Zürich, 2012.

[TR11] M. Tomamichel and R. Renner, *The uncertainty relation for smooth entropies*, Physical Review Letters **106** (2011), 110506.

[Tsi80] B. S. Tsirelson, *Quantum generalizations of Bell's inequality.*, Letters in Mathematical Physics **4** (1980), 93–100.

[Tsi85] B. S. Tsirel'son, *Quantum analogues of the Bell inequalities. the case of two spatially separated domains*, Journal of Soviet mathematics **36** (1985), no. 4, 557–570.

[Tsi93] B. S. Tsirelson, *Some results and problems on quantum Bell-type inequalities*, Hadronic Journal Supplement **8** (1993), 329.

[TSSR10] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, *Leftover hashing against quantum side information*, Proceedings of IEEE Symposium on Information Theory (2010), 2703–2707.

[Uhl76] A. Uhlmann, *The transition probability in the state space of a *-algebra*, Report on Mathematical Physics **9** (1976), 273.

[Unr10] D. Unruh, *Universally composable quantum multi-party computation*, vol. 6110, 2010, pp. 486–505.

[vAIC05] G. van Assche, S. Iblisdir, and N. J. Cerf, *Secure coherent-state quantum key distribution protocols with efficient reconciliation*, Physical Review A **71** (2005), 052304.

[vN29] J. von Neumann, *Zur Algebra der Funktionaloperationen und Theorie der normalen Operatoren*, Mathematische Annalen **34** (1929), 370–427.

[vN31] ———, *Die Eindeutigkeit der Schrödingerschen Operatoren*, Mathematische Annalen **104** (1931).

[WC81] M. N. Wegman and J. L. Carter, *New hash functions an their use in authentication and set equality*, Journal of Computer and System Sciences **22** (1981), 265–279.

[Weh78] A. Wehrl, *General properties of entropy*, Reviews of Modern Physics **50** (1978), 2.

[Wie84] S. Wiesner, *Conjugate coding*, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (1984), 175–179, Originally written c. 1970 but unpublished.

[Wil11] M. Wilde, *From classical to quantum shannon theory*, ArXiv:1106.1445 (2011).

[WLB+04] C. Weedbrook, A.M. Lance, W.P. Bowen, T. Symul, T.C. Ralph, and P.K. Lam, *Quantum cryptography without switching*, Physical Review Letters **93** (2004), 170504.

[Wor72] S. L. Woronowicz, *On the purification of factor states*, Communications in Mathematical Physics **78** (1972), 221–235.

[WPGP+12] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T.C. Ralph, J. H. Shapiro, and S. Lloyd, *Gaussian quantum information*, Reviews of Modern Physics **84** (2012), 621–669.

[WR12] L. Wang and R. Renner, *One-shot classical-quantum capacity and hypothesis testing*, Physical Review Letters **108** (2012), 200501.

[WW10] S. Wehner and A. Winter, *Entropic uncertainty relations - a survey*, New Journal of Physics **12** (2010), 025009.

# Curriculum Vitae

Fabian Furrer

## Personalien



| | |
|---|---|
| Email | fabian.furrer@itp.uni-hannover.de |
| Homepage | http://www.itp.uni-hannover.de/~furrer/ |
| Geburtsdatum | 24.04.1982 |
| Geburtsort | Zürich, Schweiz |
| Staatsangehörigkeit | Schweiz |



## Schulen und Ausbildungen

| | |
|---|---|
| Sept. 2009 – Nov. 2012 | Promotionsstudium an der Leibniz Universität Hannover am Institute für Theoretische Physik, Gruppe Quanteninformationstheorie.<br>Betreuer: Prof. Dr. R. F. Werner,<br>Co-Betreuer Prof. Dr. E. Schrohe.<br>Angeschlossen an das Graduiertenkolleg 1463 für Analysis, Geometrie und Stringtheorie. |
| Okt. 2007 – März 2009 | Master Studium in Physik an der ETH Zürich<br>Titel: Master of Science in Physics |
| Okt. 2004 – Okt. 2007 | Bachelor Studium in Physik an der ETH Zürich<br>Titel: Bachelor of Science in Physics |
| Aug. 2002 – Juni 2004 | Besuch der Kantonalen Maturitätsschule für Erwachsene Zürich |
| Aug. 1998 – Aug. 2002 mit | Absolvierung der Berufslehre als Automechaniker (leicht)<br>Berufsmatura bei Unique Flughafen Zürich AG |
| Aug. 1995 – Aug. 1998 | Besuch der Sekundarschule in Dübendorf (Zürich) |
| Aug. 1989 – Aug. 1995 | Besuch der Grundschule in Zürich |