The Smooth Entropy Formalism for von Neumann Algebras

Mario Berta*

Institute for Quantum Information and Matter, California Institute of Technology, USA

Fabian Furrer†

Department of Physics, Graduate School of Science, University of Tokyo, Japan and

Institute for Theoretical Physics, Leibniz University Hanover, Germany

Volkher B. Scholz‡

Institute for Theoretical Physics, ETH Zurich, Switzerland

We discuss information-theoretic concepts on infinite-dimensional quantum systems. In particular, we lift the smooth entropy formalism as introduced by Renner and collaborators for finite-dimensional systems to von Neumann algebras. For the smooth conditional min- and max-entropy we recover similar characterizing properties and information-theoretic operational interpretations as in the finite-dimensional case. We generalize the entropic uncertainty relation with quantum side information of Tomamichel and Renner and discuss applications to quantum cryptography. In particular, we prove the possibility to perform privacy amplification and classical data compression with quantum side information modeled by a von Neumann algebra.

I. INTRODUCTION

During the last decades many concepts and techniques have been developed to study quantum information-theoretic tasks using physical systems described by finite-dimensional Hilbert spaces (see, e.g, the books [1, 2]). One conceptually interesting building block is the smooth entropy formalism as introduced by Renner and collaborators [3, 4]. In this work, we extend its scope to more general physical systems modeled by von Neumann algebras. The general aim is the development of a mathematical framework suited to describe quantum informational tasks with resources like bosonic or fermionic quantum fields (see, e.g., the books [5, 6] for further discussions on the algebraic formulation of quantum fields).

A fundamental concept in classical and quantum information theory are entropy measures. They can be defined via an axiomatic approach [7], or operationally, in the sense that they quantitatively characterize fundamental tasks in information theory [8]. If the resources are independent and identically distributed, the relevant measures in the asymptotic limit turn out to be the von Neumann entropy [9] and Umegaki's relative entropy [10]. The definition of these entropies in the setup of von Neumann algebras and the investigation of their properties are closely connected to developments in the algebraic formulation of quantum theory. Early contributors, among others, are Araki, Benatti, Connes, Fannes, Narnhofer, Petz, Thirring, and Uhlmann (see, e.g, the book [11] and references therein).

In order to analyze resources of general form, Renner and collaborators developed the smooth entropy formalism (see, e.g., [3, 4] and references therein). The fundamental entropic quantities are

* berta@caltech.edu
† furrer@eve.phys.s.u-tokyo.ac.jp
‡ scholz@phys.ethz.ch

the smooth conditional min- and max-entropy, which characterize the optimal performance of basic information-theoretic tasks for arbitrary resources. For independent and identically distributed resources, the conditional von Neumann entropy is recovered in the asymptotic limit of infinitely many repetitions [12, Theorem 1].

In this paper, we extend the smooth entropy formalism to the algebraic approach of quantum mechanics. This enables to study information-theoretic problems with infinite-dimensional quantum systems, like for instance quantum fields of bosons and fermions or other continuous variable systems (see, e.g., the review article [13] and references therein). In the special case that the von Neumann algebra is equal to the algebra of all linear bounded operators on some separable Hilbert space, the smooth entropy formalism has been studied in [14]. It was shown that many results from the finite-dimensional case carry over via an inductive limit taken over all finite-dimensional subspaces. However, the assumption of a full algebra is often too restrictive. For example, the von Neumann algebra of a field of free bosons at finite temperature is not of this type [15].

Let us briefly summarize how the paper is organized. We start in Section II A with a brief introduction to von Neumann algebras, followed by a discussion of the relevant quantum information-theoretic concepts (Section II B). We then proceed in Section III A with the definition of the conditional min- and max-entropy. In Sections III B and III C, we define and discuss the smooth conditional min- and max-entropy. This is followed by a discussion of their properties (Section III D), as well as an extension to min- and max-relative entropy (Section III E). Finally, we discuss applications in quantum information theory (Section IV). This includes the operational meaning of the conditional min- and max-entropy (Section IV A), the special case of classical quantum systems (Section IV B), uncertainty relations for the smooth conditional min- and max-entropy (Section IV C), as well as applications in quantum cryptography (Section IV D). We end with a summary of our results and a presentation of some perspectives concerning applications (Section V).

II. PRELIMINARIES

Here we recall some basic concepts and mathematical tools needed to describe quantum information theory in the framework of von Neumann algebras. For an introduction to the theory of von Neumann algebras we refer the reader to the books [16, 17].

A. Mathematical Background

C*-algebras. A $*$-algebra is an algebra $\mathcal{A}$, which is also a vector space over $\mathbb{C}$, together with an operation $*$ called involution satisfying $A^{**} = A$, $(AB)^* = B^*A^*$ and $(\alpha A + \beta B)^* = \bar{\alpha}A^* + \bar{\beta}B^*$ for all $A, B \in \mathcal{A}$ and $\alpha, \beta \in \mathbb{C}$. If a $*$-algebra is equipped with a sub-multiplicative norm for which the involution is isometric and the algebra complete, it is called a Banach $*$-algebra.

Definition 1. *A C^*-algebra is a Banach $*$-algebra $\mathcal{A}$ with the property*

$$\|A^*A\| = \|A\|^2 , \tag{1}$$

for all $A \in \mathcal{A}$.

Note that the set of all linear, bounded operators on a Hilbert space $\mathcal{H}$, denoted by $\mathcal{B}(\mathcal{H})$, is a C^*-algebra with the usual operator norm (induced by the norm on $\mathcal{H}$), and the adjoint operation. Furthermore, each norm closed $*$-subalgebra of $\mathcal{B}(\mathcal{H})$ is a C^*-algebra. A representation of a C^*-algebra $\mathcal{A}$ is a $*$-homomorphism $\pi : \mathcal{A} \to \mathcal{B}(\mathcal{H})$ on a Hilbert space $\mathcal{H}$. A $*$-homomorphism is a linear

map compatible with the $*$-algebraic structure, that is, $\pi(AB) = \pi(A)\pi(B)$ and $\pi(A^*) = \pi(A)^*$. We call a representation π faithful if it is an isometry, which is equivalent to say that it is a $*$-isomorphism from $\mathcal{A}$ to $\pi(\mathcal{A})$. A basic theorem in the theory of C^*-algebras says that each $\mathcal{A}$ is isomorphic to a norm closed $*$-subalgebra of a $\mathcal{B}(\mathcal{H})$ with suitable $\mathcal{H}$ [16, Theorem 2.1.10]. Hence, each C^*-algebra can be seen as a norm closed $*$-subalgebra of a $\mathcal{B}(\mathcal{H})$.

An element $b \in \mathcal{A}$ is called positive if $b = a^*a$ for $a \in \mathcal{A}$, and the set of all positive elements is denoted by $\mathcal{A}_+$. A linear functional ω in the dual space $\mathcal{A}^*$ of $\mathcal{A}$ is called positive if $\omega(a) \geq 0$ for all $a \in \mathcal{A}_+$. The set of all positive functionals $\mathcal{A}^*_+$ defines a positive cone in $\mathcal{A}^*$ with the usual ordering $\omega_1 \geq \omega_2$ if $(\omega_1 - \omega_2) \in \mathcal{A}^*_+$, and we say that ω_1 majorizes ω_2. The norm on the dual space of $\mathcal{A}$ is defined as

$$\|\omega\| := \sup_{x \in \mathcal{A}, \|x\| \leq 1} |\omega(x)| \,. \tag{2}$$

A positive functional $\omega \in \mathcal{A}^*$ with $\|\omega\| = 1$ is called a state. A state ω is called pure if the only positive linear functionals which are majorized by ω are given by $\lambda \cdot \omega$ for $0 \leq \lambda \leq 1$. If $\mathcal{A} = \mathcal{B}(\mathcal{H})$ we have that the pure states are exactly the functionals $\omega_\xi(x) = \langle \xi \, | x\xi \, \rangle$, where $|\xi\rangle \in \mathcal{H}$.

Von Neumann algebras. We consider a subset of linear bounded operators $\mathcal{T} \subset \mathcal{B}(\mathcal{H})$ on a Hilbert space $\mathcal{H}$. The commutant $\mathcal{T}'$ of $\mathcal{T}$ is defined as $\mathcal{T}' = \{a \in \mathcal{B}(\mathcal{H}) : [a, x] = 0, \forall\, x \in \mathcal{T}\}$, where $[a, x] := ax - xa$.

Definition 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 $\mathcal{M}'' = \mathcal{M}$.*

Beside the above definition, there exist other ways to characterize a von Neumann algebra. One rises in the bicommutant theorem [16, Lemma 2.4.11]: a $*$-subalgebra $\mathcal{M} \subset \mathcal{B}(\mathcal{H})$ containing the identity is σ-weakly closed if and only if $\mathcal{M}'' = \mathcal{M}$. (The σ-weak topology on $\mathcal{B}(\mathcal{H})$ is the locally convex topology induced by the semi-norms $A \mapsto |\mathrm{Tr}(\tau A)|$ for trace-class operators $\tau \in \mathcal{B}(\mathcal{H})$, see [16, Chapter 2.4.1].) From this we can conclude that a von Neumann algebra $\mathcal{M}$ is also norm closed and therefore a C^*-algebra. We note that a norm closed subalgebra is not necessarily σ-weakly closed. Thus, a C^*-algebra on $\mathcal{H}$ is not always a von Neumann algebra. The definition of a von Neumann algebra can even 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.

In the following $\mathcal{M}$ denotes a von Neumann algebra. A representation π of a von Neumann algebra $\mathcal{M}$ is a $*$-representation on a Hilbert space $\mathcal{H}$ that is σ-weakly continuous. Thus, the image $\pi(\mathcal{M})$ is again a von Neumann algebra. We say that two von Neumann algebras are isomorphic if there exists a faithful representation mapping one into the other.

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 [16, Lemma 2.4.11], $\mathcal{M} \vee \hat{\mathcal{M}}$ is just the σ-weak closure of $\mathcal{M} \cup \hat{\mathcal{M}}$.

Functionals on von Neumann algebras. A linear functional $\omega : \mathcal{M} \to \mathbb{C}$ is called normal if for any monotone increasing net of operators $x_\alpha \in \mathcal{M}$ with least upper bound x, $\omega(x_\alpha)$ converges to $\omega(x)$. Equivalently, it is σ-weakly continuous [18, Chapter 7, Theorem 7.1.12]. We denote the set of linear, normal functionals on $\mathcal{M}$ by $\mathcal{N}(\mathcal{M})$.

We equip $\mathcal{N}(\mathcal{M})$ with the usual norm as given in (2). Then the set $\mathcal{N}(\mathcal{M})$ is a Banach space and moreover it is the predual of $\mathcal{M}$, which means that its dual space is $\mathcal{M}$. The cone of positive

elements in $\mathcal{N}(\mathcal{M})$ is denoted by $\mathcal{N}^+(\mathcal{M})$. We have that $\|\omega\| = \omega(\mathbb{1})$ for all $\omega \in \mathcal{N}^+(\mathcal{M})$, where $\mathbb{1}$ denotes the identity element in $\mathcal{M}$. We call functionals $\omega \in \mathcal{N}^+(\mathcal{M})$ with $\|\omega\| \leq 1$ 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

$$\mathcal{S}(\mathcal{M}) := \{\omega \in \mathcal{N}^+(\mathcal{M}) : \|\omega\| = 1\}\,. \tag{3}$$

For $\mathcal{M} \subset \mathcal{B}(\mathcal{H})$, we have that for any $\omega \in \mathcal{N}^+(\mathcal{M})$ exists a positive trace-class operator ρ on $\mathcal{H}$, such that

$$\omega_\rho(x) = \mathrm{Tr}(\rho x) = \omega(x) \quad \forall x \in \mathcal{M}\,. \tag{4}$$

If ω is normalized, such an operator ρ is called a density operator. A particular example is a vector state $\omega_\xi(x) = \langle \xi\, | x \xi\, \rangle$, given by some unit vector $|\xi\rangle \in \mathcal{H}$. The Gelfand-Naimark-Segal (GNS) construction [19, 20] asserts that for every state ω there exists a Hilbert space $\mathcal{H}_\omega$, together with a unit vector $|\xi_\omega\rangle \in \mathcal{H}_\omega$ and a representation $\pi_\omega : \mathcal{M} \to \mathcal{B}(\mathcal{H})$ such that $\omega = \omega_{\xi_\omega} \circ \pi_\omega$, i.e.,

$$\omega(x) = \langle \xi_\omega | \pi_\omega(x) \xi_\omega \rangle \quad \forall x \in \mathcal{M}\,. \tag{5}$$

Moreover, the vector $|\xi_\omega\rangle$ is cyclic, that is, $\mathcal{H}_\omega$ is the closure of $\{\pi_\omega(x)|\xi_\omega\rangle : x \in \mathcal{M}\}$.

Weights on von Neumann algebras. In addition to normal states, we also consider weights. A weight φ on a von Neumann algebra $\mathcal{M}$ is a map from the positive elements in $\mathcal{M}$ into the positive reals, being possibly infinite, satisfying

$$\varphi(x+y) = \varphi(x) + \varphi(y) \quad \text{and} \quad \varphi(\lambda x) = \lambda \varphi(x), \quad \text{for} \quad \forall x, y \in \mathcal{M}_+,\ \lambda \geq 0\,. \tag{6}$$

A weight is called semi-finite if the set $\{x \in \mathcal{M}_+ \,:\, \varphi(x) < \infty\}$ is σ-weakly dense in $\mathcal{M}$ [17, Chapter VII, Definition 1.1]. It is called faithful if $\varphi(x) \neq 0$ for any non-zero element $x \in \mathcal{M}_+$. Moreover, a weight φ is called normal if, similar to the case of linear functionals, $\varphi(x_\alpha)$ converges to $\varphi(x)$ for any monotone increasing net of operators $x_\alpha \in \mathcal{M}$ with least upper bound x. A prime example of a semi-finite normal weight is the trace on $\mathcal{B}(\mathcal{H})$, with $\mathcal{H}$ being an infinite-dimensional Hilbert space. Here normality of a weight is defined similar as for functionals.

B. Algebraic Quantum Theory

Systems. We associate to every physical system a von Neumann algebra, which is generated by the physical observables. According to Davies [21], we use the most general notion of an observable and define it as a positive operator valued measure (POVM), which consists of a measurable space (X, Σ) with σ-algebra Σ defining the values of the possible measurement outcomes together with a σ-additive function $E : \Sigma \to \mathcal{M}_+$ such that $E(X) = \mathbb{1}$. Henceforth, we consider only observables with a discrete outcome range X described by a collection of positive operators $\{E_x\}_{x \in X}$ in $\mathcal{M}$ satisfying $\sum_x E_x = \mathbb{1}$. A measurement is called projective or of von Neumann type if the operators E_x are projections. The state of a physical system is represented by a functional $\omega \in \mathcal{S}(\mathcal{M})$. The probability distribution generated by a measurement described by the observable $\{E_x\}_x$ is computed via $p_x = \omega(E_x)$.

Dynamics. The possible evolution of a quantum system is described by normal completely positive unital maps $\mathcal{E} : \mathcal{M}_B \to \mathcal{M}_A$. These are called quantum channels. This corresponds to a description in the Heisenberg picture (see [22] for proper definitions). The corresponding pre-dual

map $\mathcal{E}_*$ in the Schrödinger picture is defined via the relation $\mathcal{E}_*(\omega)(a) = \omega(\mathcal{E}(a))$ for all $a \in \mathcal{M}_B$ and is also completely positive. It maps $\mathcal{S}(\mathcal{M}_A)$ into $\mathcal{S}(\mathcal{M}_B)$. Note that if we consider all linear bounded operators on a Hilbert space $\mathcal{H}$, a state ω is usually associated with a density matrix ρ via $\omega(\cdot) = \mathrm{Tr}[\cdot\rho]$. In this case the unitality of $\mathcal{E}$ translates to $\mathrm{Tr}[\mathcal{E}_*(\rho)] = \mathrm{Tr}[\rho]$ and is referred to as trace preserving. However, a von Neumann algebra does not always admit a trace, and this property translates to norm conservation on $\mathcal{N}^+(\mathcal{M})$.

Multipartite systems. A multipartite system is a composite of different physical subsystems $A, B, \ldots, Z$ associated with mutually commuting von Neumann algebras $\mathcal{M}_A, \mathcal{M}_B, \ldots, \mathcal{M}_Z$ acting on the same Hilbert space $\mathcal{H}$. (If they act on different Hilbert spaces, we just consider their action on the tensor product of the Hilbert spaces.) The corresponding von Neumann algebra of the multipartite system is given by

$$\mathcal{M}_{AB\ldots Z} := \mathcal{M}_A \vee \mathcal{M}_B \vee \ldots \vee \mathcal{M}_Z \,, \tag{7}$$

where $\mathcal{M}_A \vee \mathcal{M}_B$ denotes the von Neumann algebra generated by $\mathcal{M}_A$ and $\mathcal{M}_B$. The considered subsystems are always labeled by subscripts. For example, a state on $\mathcal{M}_{ABC}$ is denoted by ω_{ABC} while ω_{AB} is the restriction of ω_{ABC} onto $\mathcal{M}_{AB}$. We remark that this characterization handles both bosonic and fermionic theories, since the von Neumann algebras correspond to observable quantities, which always commute if space-like separated (see [5, Chapter III.1] for a discussion).

Purifications. An important concept in quantum information theory is purification, which is essentially the completion of a system by adding a complementary system. The idea of purification is to choose an extension ω of a state ω_A such that ω is a pure state. The name is justified by the property that no further extension of the system shows any correlation with the purification ω [17, 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 ω on $\mathcal{M}$, then it follows that $\tilde{\omega}(xy) = \tilde{\omega}(x)\tilde{\omega}(y)$ for all $x \in \mathcal{M}$ and $y \in \mathcal{M}' \cap \tilde{\mathcal{M}}$, where $\mathcal{M}'$ denotes the commutant of $\mathcal{M}$.

Definition 3. *Let $\omega \in \mathcal{S}_\leq(\mathcal{M})$. A purification of ω is a triple $(\pi, \mathcal{H}, |\xi\rangle)$, where π is a representation of $\mathcal{M}$ on a Hilbert space $\mathcal{H}$ and $\xi \in \mathcal{H}$ such that $\omega(x) = \langle \xi \,|\pi(x)\xi\,\rangle$ for all $x \in \mathcal{M}$. We call $\pi(\mathcal{M})$ the relevant and $\pi(\mathcal{M})'$ the complementary system of the purification $(\pi, \mathcal{H}, |\xi\rangle)$.*

The GNS construction as reviewed in Section II A can be rephrased as every state admits a purification. We say for short 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 ω_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 $x \in \mathcal{M}_{A'B}$. Note that we use a less restrictive notion of purification compared to the one of Woronowicz [23], which only applies to factor states. This has the consequence that the state $\omega_{A'B}$ is in general not a pure state for $\mathcal{M}_{A'B}$. For any von Neumann algebra $\mathcal{M}$, there exists a representation π on a Hilbert space $\mathcal{H}$, such that every state on $\mathcal{M}$ has a purification in $\mathcal{H}$. We call such a representation a standard form of $\mathcal{M}$ [17, Chapter IX.1].

Full algebras. Special systems of interest are full algebras of all linear bounded operators on a separable Hilbert space: $\mathcal{M}_A = \mathcal{B}(\mathcal{H}_A)$. This von Neumann algebra possesses a tracial weight τ_A (a weight satisfying $\tau(x^*x) = \tau(xx^*)\ \forall x \in \mathcal{M}$), which is unique if we require that it takes the value one on minimal projections. We denote this weight by τ_A, which can be identified with the usual trace on $\mathcal{H}_A$.

Moreover, we are interested in multipartite systems where only the first system is a full algebra $\mathcal{M}_A = \mathcal{B}(\mathcal{H}_A)$. If $\mathcal{M}_B$ is another von Neumann algebra, we construct the von Neumann tensor product of $\mathcal{M}_A$ with $\mathcal{M}_B$, denoted by $\mathcal{M}_A \otimes \mathcal{M}_B$. For $\mathcal{M}_B \subset \mathcal{B}(\mathcal{H}_B)$, the tensor product $\mathcal{M}_A \otimes \mathcal{M}_B$

is the von Neumann algebra generated by the *-subalgebra $\mathcal{M}_A \otimes_{\text{alg}} \mathcal{M}_B \subset \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_B)$ with $\otimes_{\text{alg}}$ the algebraic tensor product. We briefly recall a few properties for $\mathcal{M}_A \otimes \mathcal{M}_B$, a detailed discussion can be found in [17, Chapter IV.5]. If $\mathcal{M}'_A$ and $\mathcal{M}'_B$ are the commutants, then we have $(\mathcal{M}_A \otimes \mathcal{M}_B)' = \mathcal{M}'_A \otimes \mathcal{M}'_B$. For $\sigma \in \mathcal{S}(\mathcal{M}_B)$ there exists a normal conditional expectation $\hat{\sigma} : \mathcal{M}_A \otimes \mathcal{M}_B \to \mathcal{M}_A$ such that for any $\chi \in \mathcal{S}(\mathcal{M}_A)$ we have $\chi(\hat{\sigma}(a \otimes b)) = \chi(a)\sigma(b)$ [17, Chapter IV.5 & Chapter IX, Theorem 4.2]. This ensures the existence of the product state $\chi \otimes \sigma$. Likewise, we denote by $\varphi \otimes \sigma$ the normal semi-finite weight given by $\varphi \circ \hat{\sigma}$.

Finally, if $\mathcal{M}_A$ and $\mathcal{M}_B$ are two commuting subalgebras in some $\mathcal{B}(\mathcal{H})$ and $\mathcal{M}_A$ is a full algebra (on some Hilbert space), then we can decompose the Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$, with $\mathcal{H}_1 \simeq \mathcal{H}_A$ and $\mathcal{B}(\mathcal{H}_1 \otimes \mathcal{H}_2) \supset \mathcal{M}_A \vee \mathcal{M}_B \simeq \mathcal{B}(\mathcal{H}_1) \otimes \mathcal{M}_B$. That is, for subsystems described by full algebras, commuting and tensor product representations agree.

Finite-dimensional systems. Every finite-dimensional von Neumann algebra is equal to a direct sum of full algebras of linear bounded operators on a finite-dimensional Hilbert space. In the following we will treat every finite-dimensional system as a full algebra of linear bounded operators on a finite-dimensional Hilbert space: $\mathcal{M} = \mathcal{B}(\mathbb{C}^n)$.

III. MIN- AND MAX-ENTROPY

Here we discuss the conditional min- and max-entropy (Section III A), the corresponding smoothed versions (Sections III B – III D), as well as the min- and max-relative entropy (Section III E).

A. Conditional Min- and Max-Entropy

In order to define the conditional entropy of A given the side information B, we need a trace on the A-system. For this reason we restrict ourselves in this section to von Neumann algebras of the form $\mathcal{M}_{AB} = \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{M}_B$ (see Section II B for a discussion about such systems). We note that the B-system is fully general.

Definition 4. *Let $\mathcal{M}_{AB} = \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{M}_B$ and $\omega_{AB} \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$. The conditional min-entropy is defined as*

$$\mathrm{H}_{\min}(A|B)_\omega := -\log \inf_{\sigma_B \in \mathcal{N}^+(\mathcal{M}_B)} \left\{ \sigma_B(\mathbb{1}_B) \,:\, \tau_A \otimes \sigma_B - \omega_{AB} \geq 0 \right\}, \tag{8}$$

where τ_A denotes the trace on $\mathcal{B}(\mathcal{H}_A)$.

In order to define the conditional max-entropy, we have to make a few comments on the setup. Let $\pi : \mathcal{M}_A \otimes \mathcal{M}_B \to \mathcal{B}(\mathcal{H})$ be a representation of the von Neumann algebra $\mathcal{M}_A \otimes \mathcal{M}_B$ on a Hilbert space $\mathcal{H}$. Since $\mathcal{M}_A$ is a full algebra, we can decompose the Hilbert space $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$, such that $\pi(\mathcal{M}_A) = \mathcal{B}(\mathcal{H}_1) \otimes \mathbb{1}_{\mathcal{H}_2}$ with $\mathcal{H}_A \simeq \mathcal{H}_1$. Here $\pi(\mathcal{M}_A)$ denotes the von Neumann algebra generated by elements $\pi(x \otimes \mathbb{1})$, $x \in \mathcal{M}_A$. By the properties of the von Neumann tensor product, we have that the purifying system is $\mathcal{M}_C := \pi(\mathcal{M}_A \otimes \mathcal{M}_B)' = \pi(\mathcal{M}_A)' \otimes \pi(\mathcal{M}_B)' = \mathbb{1} \otimes \pi(\mathcal{M}_B)'$. Any vector $|\xi\rangle \in \mathcal{H}$ induces a state on any von Neumann subalgebra of $\mathcal{B}(\mathcal{H})$, and hence also on the von Neumann algebra $\mathcal{M}_{AC} := \pi(\mathcal{M}_A) \otimes \pi(\mathcal{M}_B)' = \mathcal{B}(\mathcal{H}_A) \otimes \pi(\mathcal{M}_B)'$. We denote the corresponding state by ξ_{AC}.

For the definition of the conditional max-entropy, we are interested in such a state if $|\xi\rangle$ is a purification of a state ω_{AB} on $\mathcal{M}_A \otimes \mathcal{M}_B$. Especially, we will define the conditional max-entropy

as the conditional min-entropy of the state ξ_{AC} of the system A given the system C. For this to make sense, we first have to show that the definition is independent of the choice of purification.

Lemma 1. *Let $\mathcal{M}_{AB} = \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{M}_B$, $\omega_{AB} \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$, and $(\pi_i, \mathcal{K}_i, |\xi_i\rangle)$ with $i = 1, 2$ be two purifications of ω_{AB} with $\pi_i(\mathcal{M}_A \otimes \mathbb{1}_B) \simeq \mathcal{M}_{A_i}$ and complementary systems $\mathcal{M}_{C_i}$. Then, we have*

$$\mathrm{H}_{\min}(A_1|C_1)_{\omega^1} = \mathrm{H}_{\min}(A_2|C_2)_{\omega^2}\,, \tag{9}$$

where $\omega^i_{A_iC_i}$ are the restricted states corresponding to $|\xi_i\rangle$.

Proof. The conceptual idea for the proof is from [24, Lemma 13]. It is straightforward to see 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 $a \in \mathcal{M}_{AB}$. It follows for all $x \in \mathcal{M}_{A_2} \otimes \mathcal{M}_{C_2} = \mathcal{B}(\mathcal{H}_1) \otimes \pi_2(\mathcal{M}_B)'$ that

$$\omega^2_{A_2C_2}(x) = \langle \xi_2 | x \xi_2 \rangle = \langle \xi_1 | V^* x V \xi_1 \rangle = \omega^1_{A_1C_1}(V^* x V)\,, \tag{10}$$

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 $(\mathcal{M}_{A_i} \otimes \mathcal{M}_{C_i})' = \mathbb{1} \otimes \pi_i(\mathcal{M}_B)'' = \pi_i(\mathcal{M}_B)$ and that for all $y \in \mathcal{M}_B$

$$V^*xV\pi_1(y) = V^*x\pi_2(y)V = V^*\pi_2(y)xV = \pi_1(y)V^*xV\,. \tag{11}$$

From (10) we get that $\omega^1_{A_1C_1} \leq \tau_{A_1} \otimes \sigma_{C_1}$ implies $\omega^2_{A_2C_2} \leq V^*(\tau_{A_1} \otimes \sigma_{C_1})V$ with $V^*(\tau_{A_1} \otimes \sigma_{C_1})V(x) = \tau_{A_1} \otimes \sigma_{C_1}(V^*xV)$. Note that $\mathcal{M}_{C_2}$ is mapped by V into $\mathcal{M}_{C_1}$, that is, for any $c \in \mathcal{M}_{C_2}$ we find that V^*cV lies in $\mathcal{M}_{C_1}$. This follows from

$$\begin{aligned} \langle \phi | V^*(\mathbb{1}_{A_2} \otimes c)V\pi_1(x)\psi \rangle = \langle \phi | V^*(\mathbb{1}_{A_2} \otimes c)\pi_2(x)V\psi \rangle &= \langle \phi | V^*\pi_2(x)(\mathbb{1}_{A_2} \otimes c)V\psi \rangle & (12)\\ &= \langle \phi | \pi_1(x)V^*(\mathbb{1}_{A_2} \otimes c)V\psi \rangle & (13) \end{aligned}$$

for any $x \in \mathcal{M}_{AB}$ and $\phi, \psi \in \mathcal{K}_2$. This then implies that for $x \in \mathcal{M}_A$,

$$\tau_{A_1} \otimes \sigma_{C_1}(V^*(\pi_2(x) \otimes c)V) = \tau_{A_1}(\pi_1(x))\sigma_{C_1}(V^*(\mathbb{1} \otimes c)V) \tag{14}$$

factorizes and can therefore be written in the form $\tau_{A_2} \otimes \sigma_{C_2}$, where $\sigma_{C_2}(c) = \sigma_{C_1}(V^*\mathbb{1} \otimes cV)$. This follows since the tensor product weight is uniquely determined by its value on elementary tensors. With $\sigma_{C_2}(\mathbb{1}) \leq \sigma_{C_1}(\mathbb{1})$ 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 is symmetric, we get equality. □

With this result at hand, we can use the definition of a purification on von Neumann algebras (Definition 3) to define the conditional max-entropy as the dual quantity of the conditional min-entropy [25, Definition 2].

Definition 5. *Let $\mathcal{M}_{AB} = \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{M}_B$ and $\omega_{AB} \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$. The conditional max-entropy is defined as*

$$\mathrm{H}_{\max}(A|B)_\omega := -\mathrm{H}_{\min}\big(A'|C\big)_\omega\,, \tag{15}$$

with $\omega_{A'B'C}$ an arbitrary purification $(\pi, \mathcal{K}, |\xi\rangle)$ of ω_{AB} with $\mathcal{M}_{A'B'} = \pi(\mathcal{M}_{AB})$ the relevant system, and $\mathcal{M}_C = \pi(\mathcal{M}_{A'B'})'$ the complementary system.

B. Purified Distance

The smooth conditional min- and max-entropy emerge from their non-smooth counterparts by a maximization and minimization, respectively, over states close with respect to a suitable distance measure. The choice of the distance measure influences the properties of the smooth entropies crucially. Here we extend the so-called purified distance [24] to the setting of von Neumann algebras.

Following [26], the fidelity between $\omega, \sigma \in \mathcal{S}(\mathcal{M})$ is defined as

$$F_{\mathcal{M}}(\omega, \sigma) := \sup_{\pi} |\langle \xi_\omega^\pi | \xi_\sigma^\pi \rangle|^2 , \tag{16}$$

where the supremum runs over all representations π of $\mathcal{M}$ for which purifications $|\xi_\omega^\pi\rangle$ and $|\xi_\sigma^\pi\rangle$ of ω and σ exist. We suppress the subscript $\mathcal{M}$ if clear from the context and simply write $F_{\mathcal{M}}(|\xi_\omega\rangle, \sigma)$ instead of $F_{\mathcal{M}}(\omega, \sigma)$ if $|\xi_\omega\rangle$ is a purification of ω. Various properties are known for the fidelity [26–28]. Among them is the monotonicity under quantum channels $\mathcal{E}$,

$$F(\omega, \sigma) \leq F(\mathcal{E}_*(\omega), \mathcal{E}_*(\sigma)) , \tag{17}$$

and moreover that $F_{\mathcal{M}}(\omega, \sigma) \leq F_{\mathcal{N}}(\omega, \sigma)$ for von Neumann algebras $\mathcal{N} \subset \mathcal{M}$. Furthermore, we can fix a particular representation π on $\mathcal{H}$ in which ω, σ admit vector states $|\xi_\omega\rangle, |\xi_\sigma\rangle \in \mathcal{H}$, and get

$$F(\omega, \sigma) = \sup_{U \in \pi(\mathcal{M})'} |\langle \xi_\omega | U \xi_\sigma \rangle|^2 , \tag{18}$$

where the supremum is taken over all elements U in $\pi(\mathcal{M})'$ with $\|U\| \leq 1$ [28].

Following work for finite-dimensional spaces [24, Definition 2], we generalize the fidelity to sets of subnormalized states. We first introduce the concept of a projective embedding. Let $\mathcal{M}$ and $\mathcal{N}$ be 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 $\mathcal{M}$. (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 $p = VV^*$.) This is equivalent to the existence of a projector p in $\mathcal{N}$ and a faithful representation π of $\mathcal{M}$ into $\mathcal{N}$ such that $\pi(\mathcal{M}) = (\mathbb{1} - p) \oplus p\mathcal{N}p$. 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 $p\mathcal{N}p$. (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 $\sigma(\mathbb{1} - p) = 1 - \omega(p)$.) Hence, we can interpret subnormalized states as post-measurement states conditioned on certain outcomes.

Definition 6. *Let $\omega, \sigma \in \mathcal{S}_\leq(\mathcal{M})$. The generalized fidelity between σ and ω is defined as*

$$\mathcal{F}_{\mathcal{M}}(\omega, \sigma) := \sup_{\mathcal{M} \curvearrowright \mathcal{N}} \sup_{\bar{\omega}, \bar{\sigma} \in \mathcal{S}(\mathcal{N})} F_{\mathcal{N}}(\bar{\sigma}, \bar{\omega}) , \tag{19}$$

where the second supremum is taken 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 ω, and similarly for $\bar{\sigma}$.

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

Lemma 2. *Let $\omega, \sigma \in \mathcal{S}_\leq(\mathcal{M})$. Then, we have*

$$\mathcal{F}_{\mathcal{M}}(\omega, \sigma) = F_{\hat{\mathcal{M}}}(\hat{\omega}, \hat{\sigma}) = \left(\sqrt{F_{\mathcal{M}}(\omega, \sigma)} + \sqrt{(1 - \omega(\mathbb{1}))} \sqrt{(1 - \sigma(\mathbb{1}))} \right)^2 , \tag{20}$$

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

Proof. Let $\mathcal{N}$ be such that $\mathcal{M}\curvearrowright\mathcal{N}$ with p the projector such that $\mathcal{M}\cong p\mathcal{N}p$. Furthermore, let $\bar{\omega},\bar{\sigma}$ be extensions of ω,σ on $\mathcal{N}$ satisfying the required properties. 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 representations of $\mathcal{N}$. Note that all such representations π are also representations of $\mathcal{M}$, that $\xi^{\pi}_{\omega}=\pi(p)\xi^{\pi}_{\bar{\omega}}$ is a purification of ω, and that the same also holds for $\xi^{\pi}_{\sigma}=\pi(p)\xi^{\pi}_{\bar{\sigma}}$. We can use the Cauchy-Schwarz inequality to compute

$$|\langle\xi^{\pi}_{\bar{\omega}}|\xi^{\pi}_{\bar{\sigma}}\rangle| = |\langle\xi^{\pi}_{\omega}|\xi^{\pi}_{\sigma}\rangle| + |\langle((\mathbb{1}-p)\xi^{\pi}_{\bar{\omega}}|(\mathbb{1}-p)\xi^{\pi}_{\bar{\sigma}}\rangle \leq |\langle\xi^{\pi}_{\omega}|\xi^{\pi}_{\sigma}\rangle| + \sqrt{(1-\omega(\mathbb{1}))(1-\sigma(\mathbb{1}))}\,. \tag{21}$$

Since this holds for all π, we have that

$$\mathcal{F}_{\mathcal{N}}(\bar{\omega},\bar{\sigma}) \leq \left(\sqrt{F_{\mathcal{M}}(\omega,\sigma)} + \sqrt{(1-\omega(\mathbb{1}))}\sqrt{(1-\sigma(\mathbb{1}))}\right)^2 \tag{22}$$

for all $\mathcal{N}$ such that $\mathcal{M}\curvearrowright\mathcal{N}$ and all suitable $\bar{\omega},\bar{\sigma}$ on $\mathcal{N}$. Hence, we get

$$\mathcal{F}_{\mathcal{M}}(\omega,\sigma) \leq \left(\sqrt{F_{\mathcal{M}}(\omega,\sigma)} + \sqrt{(1-\omega(\mathbb{1}))}\sqrt{(1-\sigma(\mathbb{1}))}\right)^2. \tag{23}$$

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 then defined in the same way as for finite-dimensional spaces [24, Definition 4].

Definition 7. *Let $\omega,\sigma\in\mathcal{S}_{\leq}(\mathcal{M})$. The purified distance between ρ and σ is defined as*

$$\mathcal{P}_{\mathcal{M}}(\omega,\sigma) := \sqrt{1-\mathcal{F}_{\mathcal{M}}(\omega,\sigma)}\,. \tag{24}$$

The name purified distance comes from the finite-dimensional case, where the purified distance between two states corresponds to the minimal l_1-distance between purifications of these states. It is straightforward to see that the same result also holds in the von Neumann case, namely,

$$\mathcal{P}_{\mathcal{M}}(\omega,\sigma) = \frac{1}{2}\inf_{\pi}\||\xi^{\pi}_{\omega}\rangle\langle\xi^{\pi}_{\omega}| - |\xi^{\pi}_{\sigma}\rangle\langle\xi^{\pi}_{\sigma}|\|_1\,, \tag{25}$$

where the infimum runs over all representations of $\mathcal{M}$ in which ω and σ have a vector representation denoted by $|\xi^{\pi}_{\omega}\rangle$ and $|\xi^{\pi}_{\sigma}\rangle$, respectively.

As for the fidelity, we often omit the indication of the von Neumann algebra and moreover write $\mathcal{P}_{\mathcal{M}}(\omega,\sigma)=\mathcal{P}_{\mathcal{M}}(|\xi\rangle,\sigma)$ if $|\xi\rangle$ is a purification of ω. A detailed discussion of the properties of the purified distance can be found in [24]. (Although this discussion is restricted to systems described by finite-dimensional spaces, many of the properties follow in the same way for general systems.) It is for instance easy to see that the purified distance defines a metric on $\mathcal{S}_{\leq}(\mathcal{M})$ that is equivalent to the norm distance on $\mathcal{N}(\mathcal{M})$,

$$\sqrt{\|\omega-\sigma\|+|\omega(\mathbb{1})-\sigma(\mathbb{1})|} \geq \mathcal{P}_{\mathcal{M}}(\sigma,\omega) \geq \frac{1}{2}\Big(\|\omega-\sigma\|+|\omega(\mathbb{1})-\sigma(\mathbb{1})|\Big)\,. \tag{26}$$

Furthermore, the purified distance is monotone under completely positive contractions.

C. Smooth Conditional Min- and Max-Entropy

As in Section III A, we restrict ourselves to von Neumann algebras of the form $\mathcal{M}_{AB}=\mathcal{B}(\mathcal{H}_A)\otimes\mathcal{M}_B$. The smooth entropies are defined using an ϵ-ball with respect to the purified distance,

$$\mathcal{B}^{\epsilon}_{\mathcal{M}}(\omega) := \Big\{\sigma\in\mathcal{S}_{\leq}(\mathcal{M}) : \mathcal{P}_{\mathcal{M}}(\omega,\sigma)\leq\epsilon\Big\}\,. \tag{27}$$

The set $\mathcal{B}^{\epsilon}_{\mathcal{M}}(\omega)$ is referred to as the smoothing set and ϵ is called the smoothing parameter.

Definition 8. *Let $\mathcal{M}_{AB} = \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{M}_B$, $\omega_{AB} \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$, and $\epsilon \geq 0$. The ϵ-smooth conditional min-entropy is defined as*

$$\mathrm{H}^{\epsilon}_{\min}(A|B)_{\omega} := \sup_{\sigma_{AB} \in \mathcal{B}^{\epsilon}_{\mathcal{M}}(\omega_{AB})} \mathrm{H}_{\min}(A|B)_{\sigma} \,. \tag{28}$$

Since the purified distance defines a metric on $\mathcal{S}_{\leq}(\mathcal{M}_{AB})$, we retrieve the conditional min-entropy for $\epsilon = 0$. In order to define the smooth conditional max-entropy as the dual quantity of the smooth conditional min-entropy, we again have to make sure that everything is independent of the choice of the purification.

Lemma 3. *Let $\mathcal{M}_{AB} = \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{M}_B$, $\omega_{AB} \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$, and $(\pi_i, \mathcal{K}_i, |\xi_i\rangle)$ for $i = 1, 2$ two purifications of ω_{AB} with $\mathcal{M}_{A_i} = \pi_i(\mathcal{M}_A)$ and complementary systems $\mathcal{M}_{C_i}$, and $\epsilon \geq 0$. Then, we have*

$$\mathrm{H}^{\epsilon}_{\min}(A_1|C_1)_{\omega^1} = \mathrm{H}^{\epsilon}_{\min}(A_2|C_2)_{\omega^2} \,, \tag{29}$$

where $\omega^i_{A_iC_i}$ are the restricted states corresponding to $|\xi_i\rangle$.

Proof. We observe that due to the symmetry of (29) it is enough to show inequality in one direction. It is straightforward to see 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, it follows from the proof of Lemma 1 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 $V^*\omega^1_{A_1C_1}V = \omega^2_{A_2C_2}$. We have

$$\mathrm{H}^{\epsilon}_{\min}(A_1|C_1)_{\omega^1} = \sup_{\sigma_{A_1C_1} \in \mathcal{B}^{\epsilon}(\omega^1_{A_1C_1})} \mathrm{H}_{\min}(A_1|C_1)_{\omega} \leq \sup_{\sigma_{A_1C_1} \in \mathcal{B}^{\epsilon}(\omega^1_{A_1C_1})} \mathrm{H}_{\min}(A_2|C_2)_{V^*\sigma V} \,, \tag{30}$$

and we are left to prove $V^*\sigma_{A_1C_1}V \in \mathcal{B}^{\epsilon}(\omega^2_{A_2C_2})$ for all $\sigma_{A_1C_1} \in \mathcal{B}^{\epsilon}(\omega^1_{A_1C_1})$. This is equivalent to

$$\mathcal{F}(\omega_{A_1C_1}, \sigma_{A_1C_1}) \leq \mathcal{F}(V^*\omega_{A_1C_1}V, V^*\sigma_{A_1C_1}V) \,. \tag{31}$$

Let $p = VV^*$ be the projector onto the image of V. Note that

$$V^*\omega_{A_1C_1}V(p) = V^*\omega_{A_1C_1}V(\mathbb{1}) \quad \text{and} \quad V^*\sigma_{A_1C_1}V(p) = V^*\sigma_{A_1C_1}V(\mathbb{1}) \tag{32}$$

holds by construction. Since $p\mathcal{M}_{A_2C_2}p$ is a von Neumann algebra and using Definition 6, we find that

$$\begin{aligned}
\mathcal{F}_{\mathcal{M}_{A_2C_2}}(V^*\omega_{A_1C_1}V, V^*\sigma_{A_1C_1}V) &= \mathcal{F}_{p\mathcal{M}_{A_2C_2}p}(V^*\omega_{A_1C_1}V, V^*\sigma_{A_1C_1}V) && (33)\\
&= \sup_{p\mathcal{M}_{A_2C_2}p \curvearrowright \hat{\mathcal{N}}} \sup_{\bar{\omega},\bar{\sigma}} F_{\mathcal{N}}(\bar{\omega}, \bar{\sigma}) && (34)\\
&\geq F_{\hat{\mathcal{M}}_{A_1C_1}}(\hat{\omega}^1_{A_1C_1}, \hat{\sigma}_{A_1C_1}) && (35)\\
&= \mathcal{F}_{\mathcal{M}_{A_1C_1}}(\omega^1_{A_1C_1}, \sigma_{A_1C_1}) \,, && (36)
\end{aligned}$$

where $\hat{\mathcal{M}}_{A_1C_1}, \hat{\omega}^1_{A_1C_1}, \hat{\sigma}_{A_1C_1}$ are as in Lemma 2, 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 $\hat{\omega}^1_{A_1C_1}, \hat{\sigma}_{A_1C_1}$ are extensions of $V^*\omega_{A_1C_1}V, V^*\sigma_{A_1C_1}V$ in accordance with (19). ∎

We are now ready to define the smooth conditional max-entropy.

Definition 9. *Let $\mathcal{M}_{AB} = \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{M}_B$, $\omega_{AB} \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$, and $\varepsilon \geq 0$. The ϵ-smooth conditional max-entropy is defined as*

$$\mathrm{H}^{\epsilon}_{\max}(A|B)_{\omega} := -\mathrm{H}^{\epsilon}_{\min}\big(A'|C\big)_{\omega}\,, \tag{37}$$

with $\omega_{A'B'C}$ an arbitrary purification $(\pi, \mathcal{K}, |\xi\rangle)$ of ω_{AB} with $\mathcal{M}_{A'B'} = \pi(\mathcal{M}_{AB})$ the relevant system, and $\mathcal{M}_C = \pi(\mathcal{M}_{A'B'})'$ the complementary system.

Lemma 3 ensures that the definition of the smooth conditional max-entropy is independent of the purification. Another possible definition of the smooth conditional max-entropy would have been to smooth the conditional max-entropy (in analogy to the definition of the smooth conditional min-entropy). However, as for finite-dimensional spaces, the two approaches are equivalent [24, Lemma 16]. In order to show this, we first need the following lemma.

Lemma 4. *Let $\mathcal{M} \subset \mathcal{B}(\mathcal{H})$, $|\xi\rangle \in \mathcal{H}$ be a vector inducing a state ω on $\mathcal{M}$, and $\sigma \in \mathcal{S}(\mathcal{M})$ with $\mathcal{P}_{\mathcal{M}}(\omega, \sigma) < \infty$. Then, there exists a vector $|\gamma\rangle \in \mathcal{H}$ such that $\langle \gamma\,|x\gamma\,\rangle \leq \sigma(x)\ \forall x \in \mathcal{M}_+$, and moreover*

$$\mathcal{P}_{\mathcal{M}}(\omega, \sigma) = \mathcal{P}_{\mathcal{B}(\mathcal{H})}(|\xi\rangle, |\gamma\rangle)\,. \tag{38}$$

Proof. Let $\pi, \mathcal{K}$ be a tuple of a Hilbert space $\mathcal{K}$ and a representation of $\mathcal{M}$ on $\mathcal{K}$ such that there exists purifying vectors $|\tilde{\xi}\rangle \in \mathcal{K}$ for ω as well as $|\chi\rangle \in \mathcal{K}$ for σ. This can for example be achieved by a GNS construction with respect to the positive functional $\omega + \sigma$ (since we both have $\omega \leq \omega + \sigma$ as well as $\sigma \leq \omega + \sigma$). It follows that there exists a partial isometry $V : \mathcal{H} \to \mathcal{K}$ with $V|\xi\rangle = |\tilde{\xi}\rangle$ satisfying $\pi(x)V = Vx$, $x \in \mathcal{M}$. We then set $|\gamma\rangle = V^*U|\chi\rangle$, where $U \in \pi(\mathcal{M})'$ with $\|U\| \leq 1$ is taken such that $F(\sigma, \omega) = \langle \chi\,|U^*V\xi\,\rangle$. We find for any $x \in \mathcal{M}_+$ that

$$\langle \gamma\,|x\,\gamma\,\rangle = \langle \chi\,|U^*Vx\,V^*U\chi\,\rangle = \langle \chi\,|\,\pi(x)^{1/2}U^*VV^*U\pi(x)^{1/2}\chi\,\rangle \leq \langle \chi\,|\pi(x)\,\chi\,\rangle = \sigma(x)\,, \tag{39}$$

as well as $\mathcal{P}_{\mathcal{M}}(\omega, \sigma) = \mathcal{P}_{\mathcal{B}(\mathcal{H})}(|\xi\rangle, |\gamma\rangle)$. □

We can now show that the smooth conditional max-entropy can be written as an optimization over conditional max-entropies.

Proposition 5. *Let $\mathcal{M}_{AB} = \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{M}_B$, $\omega_{AB} \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$, and $\epsilon \geq 0$. Then, we have*

$$\mathrm{H}^{\epsilon}_{\max}(A|B)_{\omega} = \inf_{\sigma_{AB} \in \mathcal{B}^{\epsilon}(\omega_{AB})} \mathrm{H}_{\max}(A|B)_{\sigma}\,. \tag{40}$$

Proof. Let $(\pi, \mathcal{K}, |\xi\rangle)$ be an arbitrary purification of ω_{AB} with complementary system $\mathcal{M}_C = \pi(\mathcal{M}_{AB})'$. Because of the independence of the smooth conditional min-entropy of a particular purification (Lemma 3), we can assume that π together with $\mathcal{K}$ is a standard form of $\mathcal{M}$. Thus, each state in $\mathcal{M}_{AB}$ admits a purification in $\mathcal{K}$. According to the definition of the smooth entropies we have to show

$$\sup_{\sigma_{AB} \in \mathcal{B}^{\epsilon}_{\mathcal{M}}(\omega_{AB})} \mathrm{H}_{\min}(A|C)_{|\xi_\sigma\rangle} = \sup_{\eta_{AC} \in \mathcal{B}^{\epsilon}(\omega_{AC})} \mathrm{H}_{\min}(A|C)_{\eta}\,, \tag{41}$$

where $|\xi_\sigma\rangle \in \mathcal{K}$ is a purification of σ_{AB}. Since we know that the conditional min-entropy does not depend on the particular choice of the purification $|\xi_\sigma\rangle$ (Lemma 1), we can 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

$$\mathcal{P}_{\mathcal{M}_{AB}}(\omega_{AB}, \sigma_{AB}) = \mathcal{P}_{\mathcal{B}(\mathcal{H})}(|\xi\rangle, |\xi_\sigma\rangle) \geq \mathcal{P}_{\mathcal{M}_{AC}}(|\xi\rangle, |\xi_\sigma\rangle)\,, \tag{42}$$

from which $\leq$ in (41) follows.

For the other direction, let $(\pi, \mathcal{H}, |\xi\rangle)$ be a purification of ω_{AC}, and for any element $\eta_{AC} \in \mathcal{B}^\epsilon(\omega_{AC})$ let $|\gamma(\eta_{AC})\rangle \in \mathcal{H}$ be the vector obtained from applying Lemma 4 to η_{AC}, which in turn induces a subnormalized state $\gamma_{AC}(\eta_{AC})$ on $\mathcal{M}_{AC}$. Since $\gamma_{AC} \leq \sigma_{AC}$, it follows that

$$\sup_{\eta_{AC}\in\mathcal{B}^\epsilon(\omega_{AC})} \mathrm{H}_{\min}(A|C)_\eta \leq \sup_{\gamma_{AC}(\eta_{AC}):\, \eta_{AC}\in\mathcal{B}^\epsilon(\omega_{AC})} \mathrm{H}_{\min}(A|C)_{\gamma_{AC}} \,. \tag{43}$$

But γ_{AC} originates from a vector $|\gamma\rangle$ such that $\mathcal{P}_{\mathcal{B}(\mathcal{H})}(|\xi\rangle, |\gamma\rangle) \leq \varepsilon$ and hence we find

$$\sup_{\eta_{AC}\in\mathcal{B}^\epsilon(\omega_{AC})} \mathrm{H}_{\min}(A|C)_\eta \leq \sup_{|\gamma\rangle\in\mathcal{H}:\, \mathcal{P}_{\mathcal{B}(\mathcal{H})}(|\xi\rangle,|\gamma\rangle)\leq\varepsilon} \mathrm{H}_{\min}(A|C)_{|\gamma\rangle} \tag{44}$$

$$\leq \sup_{|\gamma\rangle\in\mathcal{H}:\, \mathcal{P}_{\mathcal{M}_{AB}}(\xi_{AB},\gamma_{AB})\leq\varepsilon} \mathrm{H}_{\min}(A|C)_{|\gamma\rangle} \,, \tag{45}$$

where the last step follows from the fact that the purified distance is monotone. The assertion follows since $\xi_{AB} = \omega_{AB}$. □

D. Properties of Smooth Entropies

Data Processing. The principle that local operations on the quantum side information B can never increase the knowledge about the A-system is expressed by the data-processing inequality.

Proposition 6. *Let $\omega_{AB} \in \mathcal{S}_\leq(\mathcal{B}(\mathcal{H}_A) \otimes \mathcal{M}_B)$, $\mathcal{E} : \mathcal{M}_C \to \mathcal{M}_B$ be a quantum channel, and $\epsilon \geq 0$. Then, we have*

$$\mathrm{H}^\epsilon_{\min}(A|B)_\omega \leq \mathrm{H}^\epsilon_{\min}(A|C)_{\mathcal{I}_A\otimes\mathcal{E}_*(\omega)} \quad \textit{as well as} \quad \mathrm{H}^\epsilon_{\max}(A|B)_\omega \leq \mathrm{H}^\epsilon_{\max}(A|C)_{\mathcal{I}_A\otimes\mathcal{E}_*(\omega)} \,, \tag{46}$$

where $\mathcal{I}_A : \mathcal{M}_A \to \mathcal{M}_A$ denotes the identity map. Moreover, we have that access to partial information can only increase the entropies, that is,

$$\mathcal{M}_C \subset \mathcal{M}_B \quad \Rightarrow \quad \mathrm{H}^\epsilon_{\min}(A|B)_\omega \leq \mathrm{H}^\epsilon_{\min}(A|C)_\omega \quad \text{and} \quad \mathrm{H}^\epsilon_{\max}(A|B)_\omega \leq \mathrm{H}^\epsilon_{\max}(A|C)_\omega \,. \tag{47}$$

The proof of the first statement is obtained by adapting the one for systems described by finite-dimensional spaces [24, Theorem 18]. The second statement is obtained from the fact that by restricting the state to a subalgebra, the ordering relation in the definition of the min-entropy (4) is only tested on fewer positive elements such that the infimum in (4) is taken over a larger set of states. This then leads to a larger min-entropy and thus, to a larger smooth min-entropy.

Bounds. Here we would like to study when the smooth conditional min- and max-entropy are finite.

Proposition 7. *Let $\mathcal{M}_{AB} = \mathcal{B}(\mathcal{H}_A) \otimes \mathcal{M}_B$ and $\omega_{AB} \in \mathcal{S}(\mathcal{M}_{AB})$. Then, we have*

$$\mathrm{H}_{\min}(A|B)_\omega < \infty \quad \text{and} \quad \mathrm{H}_{\max}(A|B)_\omega > -\infty \,. \tag{48}$$

Proof. The first inequality follows from the data processing inequality (Proposition 6) and the corresponding statement for the unconditional min-entropy (which we will show in Proposition 11 for a more general setup). The second inequality follows from the duality of the conditional min- and max-entropy (Definition 5) and the first inequality. □

Note that the conditional min-entropy can become minus infinity and the conditional max-entropy can become plus infinity [14, Lemma 1]. However, the smooth conditional min- and max-entropy with smoothing parameter $\epsilon > 0$ are always finite.

Proposition 8. *Let $\mathcal{M}_{AB} = \mathcal{B}(\mathcal{H}) \otimes \mathcal{M}_B$, $\omega_{AB} \in \mathcal{S}(\mathcal{M}_{AB})$, and $\varepsilon > 0$. Then, we have*

$$-\infty < \mathrm{H}^{\epsilon}_{\min}(A|B)_{\omega} < \infty \quad \text{and} \quad -\infty < \mathrm{H}^{\epsilon}_{\max}(A|B)_{\omega} < \infty\,. \tag{49}$$

Proof. The inequalities $\mathrm{H}^{\epsilon}_{\min}(A|B)_{\omega} < \infty$ and $\mathrm{H}^{\epsilon}_{\max}(A|B)_{\omega} > -\infty$ follow by the corresponding statements for the non-smooth entropies (Proposition 7). The other two inequalities follow from applying [14, Lemma 2] together with the data processing inequality (Proposition 6). Namely, let $(\pi, \mathcal{H}, |\xi\rangle)$ be a purification of ω. Since $\mathcal{M}_A$ is a full algebra, we can find a decomposition $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$, $\mathcal{H}_1 \simeq \mathcal{H}_A$ and $\mathcal{M}_{AB} = \mathcal{B}(\mathcal{H}_A) \otimes \pi(\mathcal{M}_B) \subset \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_2)$. The vector $|\xi\rangle$ then induces a normal state on $\mathcal{B}(\mathcal{H}_A) \otimes \mathcal{B}(\mathcal{H}_2)$ and we can apply [14, Lemma 2], followed by the restriction onto the subalgebra $\pi(\mathcal{M}_B) \subset \mathcal{B}(\mathcal{H}_2)$. □

E. Min- and Max-Relative Entropy

Instead of conditional entropies we can also define a min- and max-version of relative entropy (as noticed in [29, Definition 1] for finite-dimensional spaces). This will also allow us to define the (unconditional) min- and max-entropy on von Neumann algebras.

Definition 10. *Let $\omega, \sigma \in \mathcal{N}^+(\mathcal{M})$. The max-relative entropy of ω with respect to σ is defined as*

$$\mathrm{D}_{\max}(\omega||\sigma) := \inf\{\mu \in \mathbb{R} : \omega \leq 2^{\mu} \cdot \sigma\}\,, \tag{50}$$

where the infimum of the empty set is defined to be ∞. The min-relative entropy of ω with respect to σ is defined as

$$\mathrm{D}_{\min}(\omega||\sigma) := -\log F(\omega, \sigma)\,. \tag{51}$$

We have the following ordering relation.

Proposition 9. *Let $\omega \in \mathcal{S}(\mathcal{M})$ and $\sigma \in \mathcal{N}^+(\mathcal{M})$. Then, we have*

$$\mathrm{D}_{\min}(\omega||\sigma) \leq \mathrm{D}_{\max}(\omega||\sigma)\,. \tag{52}$$

Proof. If there exists no finite constant c such that $\omega \leq c \cdot \sigma$, then $\mathrm{D}_{\max}(\omega||\sigma) = \infty$, and there is nothing to prove. So let us suppose the opposite, and let $(\pi, \mathcal{K}, |\xi\rangle)$ be a tuple of a Hilbert space and a representation on it such that there exists purifying vectors $|\xi\rangle \in \mathcal{K}$ for ω as well as $|\chi\rangle \in \mathcal{K}$ for σ. Let $\mu \in \mathbb{R}$ such that $\omega \leq 2^{\mu} \cdot \sigma$. By the non-commutative Radon-Nikodym theorem [17, Chapter VII.2] there exists an element $h_{\omega} \in \pi(\mathcal{M})'$ such that $h_{\omega}|\chi\rangle = |\xi\rangle$ as well as $\|h_{\omega}\|^2 \leq 2^{\mu}$. Using the property (18) of the fidelity, we find

$$2^{\mu} \cdot F(\omega, \sigma) \geq 2^{\mu} \Big| \langle \xi \,| \Big(2^{-\mu/2} h_{\omega} \Big) \chi \rangle \Big|^2 = \langle \xi \,| \xi \rangle = 1\,. \tag{53}$$

Taking logarithms proves the assertion. □

The following proposition shows that the min- and max-relative entropy are monotone under quantum channels. The proof of the first statement follows by definition, the proof of the second follows from the monotonicity of the fidelity (17).

Proposition 10. *Let $\omega, \sigma \in \mathcal{S}(\mathcal{M})$. Then, we have for any quantum channel $\mathcal{E}$,*

$$\mathrm{D}_{\max}(\omega||\sigma) \geq \mathrm{D}_{\max}(\mathcal{E}_*(\omega)||\mathcal{E}_*(\sigma)) \quad \text{and} \quad \mathrm{D}_{\min}(\omega||\sigma) \geq \mathrm{D}_{\min}(\mathcal{E}_*(\omega)||\mathcal{E}_*(\sigma))\,. \tag{54}$$

Min- and Max-Entropy. In the case where the system is given by a full algebra $\mathcal{B}(\mathcal{H})$, the unconditional min- and max-entropy are simply obtained from Definition 4 and Definition 5 (see also Proposition 15) with trivial quantum side information. The extension to arbitrary systems can be done similarly as for the von Neumann entropy [11, Chapter II.6].

Definition 11. *Let $\omega_A \in \mathcal{S}(\mathcal{M}_A)$. The min-entropy is defined as*

$$\mathrm{H}_{\min}(A)_\omega := -\sup\left\{D_{\max}(\sigma_{AX}\|\omega_A \otimes \tau_X)|\sigma_{AX} \in \mathcal{S}(\mathcal{M}_A \otimes \ell_X^\infty), \sigma_A = \omega_A\right\}, \tag{55}$$

where $\tau_X(\cdot)$ denotes the trace on the classical system ℓ_X^∞. The max-entropy is defined as

$$\mathrm{H}_{\max}(A)_\omega := -\inf\left\{D_{\min}(\sigma_{AX}\|\omega_A \otimes \tau_X)|\sigma_{AX} \in \mathcal{S}(\mathcal{M}_A \otimes \ell_X^\infty), \sigma_A = \omega_A\right\}. \tag{56}$$

Proposition 11. *Let $\omega_A \in \mathcal{S}(\mathcal{M}_A)$. Then, we have*

$$0 \leq \mathrm{H}_{\min}(A)_\omega < \infty \quad \text{and} \quad \mathrm{H}_{\min}(A)_\omega \leq \mathrm{H}_{\max}(A)_\omega\,. \tag{57}$$

Proof. The first assertion can be deduced directly from the definition of the min-entropy (Definition 11). The second assertion follows by the ordering of the min- and max-relative entropy (Proposition 9). □

Finally, we could also define smoothed versions in the same manner as for the conditional min- and max-entropy.

IV. APPLICATIONS TO QUANTUM INFORMATION THEORY

In the following we restrict ourselves to von Neumann algebras of the form $\mathcal{M}_{AB} = \mathcal{B}(\mathbb{C}^n) \otimes \mathcal{M}_B$, that is, the A-system is finite-dimensional (see Section II B for a discussion about such systems). We note that the B-system is fully general. This setup is well suited for applications in quantum information theory and in particular in quantum cryptography. (We do not want to make any assumptions about the adversarial system B, but our resource, the A-system, is finite.)

A. Operational Interpretation of Conditional Min- and Max-Entropy

Optimal entanglement fidelity. The following proposition generalizes the operational meaning of the conditional min-entropy [25, Theorem 2]. (The difference of a square in comparison to [25, Theorem 2] is due to the different definition of the fidelity.)

Proposition 12. *Let $\mathcal{M}_{AB} = \mathcal{B}(\mathbb{C}^n) \otimes \mathcal{M}_B$, $\omega_{AB} \in \mathcal{S}(\mathcal{M}_{AB})$, and let $|\Phi_{AA'}^n\rangle := \sum_{i=1}^n |\phi_i\rangle \otimes |\psi_i\rangle$, where $\{|\phi_i\rangle\}$ and $\{|\psi_i\rangle\}$ are orthonormal bases of $\mathbb{C}^n$. Then, we have*

$$2^{-\mathrm{H}_{\min}(A|B)_\omega} = \sup_{\mathcal{E}} F((\mathcal{I}_A \otimes \mathcal{E}_*)(\omega_{AB}), |\Phi_{AA'}^n\rangle)\,, \tag{58}$$

where the supremum is taken over all quantum channels $\mathcal{E} : \mathcal{B}(\mathbb{C}^n) \to \mathcal{M}_B$.

The idea of the proof is that $\mathrm{H}_{\min}(A|B)_\omega$ can be written as the solution of an optimization problem over a subcone of $\mathcal{N}^+(\mathcal{M}_{AB})$ for which the theory of ordered vector spaces [30] applies. For $\omega_{AB} = (\omega_B^{ij}) \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$, we write

$$2^{-\mathrm{H}_{\min}(A|B)_\omega} = \inf\{\sigma_B(\mathbb{1}) : \tau_A \otimes \sigma_B \geq \omega_{AB},\, \sigma_B \in \mathcal{N}^+(\mathcal{M}_B)\} \tag{59}$$

$$= \inf\{f_{\mathbb{1}}(\sigma_{AB}) : \sigma_{AB} \geq \omega_{AB},\, \sigma_{AB} \in E\}\,, \tag{60}$$

where $f_{\mathbb{1}}(\eta_{AB}) = \frac{1}{n}\eta_{AB}(\mathbb{1})$ for $\eta_{AB} \in \mathcal{N}(\mathcal{M}_{AB})$, and $E := \{\tau_A \otimes \eta_B : \eta_B \in \mathcal{N}^h(\mathcal{M}_B)\}$ with $\mathcal{N}^h(\mathcal{M}_B)$ the set of hermitian functionals on $\mathcal{M}_B$. We have that E is a subspace of $\mathcal{N}^h(\mathcal{M}_{AB})$ and $f_{\mathbb{1}}$ defines a positive functional on $\mathcal{N}^h(\mathcal{M}_{AB})$. The basic ingredient is the following extension result for positive functionals in ordered vector spaces.

Lemma 13. *[30, Lemma 2.13] Let V be an ordered real vector space with a full cone V^+, $E \subset V$ a subspace which majorizes V^+, $w \in V\backslash E$, and $f : E \to \mathbb{R}$ a positive functional on E. Then, f admits a positive extension $\tilde{f}$ on V such that*

$$\tilde{f}(w) = u_f(w) := \inf\{f(v) \ : \ v \geq w,\, v \in E\}\,. \tag{61}$$

Moreover, it holds for all positive functionals g on V with $g|_E = f$, that $g(w) \leq u_f(w)$.

If we take $V = \mathcal{N}^h(\mathcal{M}_{AB})$ with the cone of all positive functionals $V^+ = \mathcal{N}^+(\mathcal{M}_{AB})$ and E as defined above, then E majorizes V^+. According to the definition of the predual, the set of all positive functionals on V are given by the positive operators in $\mathcal{M}_{AB}$. Hence, by applying Lemma 13 with $f = f_{\mathbb{1}}$, we find the following corollary.

Corollary 14. *Let $\mathcal{M}_{AB} = \mathcal{B}(\mathbb{C}^n) \otimes \mathcal{M}_B$ and $\omega_{AB} = (\omega_B^{ij}) \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$. Then, we have that*

$$2^{-\mathrm{H}_{\min}(A|B)_\omega} = \sup\left\{\sum_{ij}\omega_B^{ij}(M_{ij}) \ : \ (M_{ij}) \in (\mathcal{B}(\mathbb{C}^n) \otimes \mathcal{M}_B)_+,\, \sum_i M_{ii} = \mathbb{1}\right\}. \tag{62}$$

Proof. The linear functional given by (M_{ij}) restricted to E has to be $f_{\mathbb{1}}$, and thus we have $(\tau_A \otimes \sigma_B)((M_{ij})) = \sum_i \sigma_B(M_{ii}) = 1$ for all $\sigma_B \in \mathcal{S}(\mathcal{M}_B)$. Since $(\mathcal{N}(\mathcal{M}_B))^* = \mathcal{M}_B$ this implies $\sum_i M_{ii} = \mathbb{1}$, and the assertion follows. □

The operational form of the conditional min-entropy (Proposition 12) follows from Corollary 14 by the identification of completely positive maps $\mathcal{E} : \mathcal{B}(\mathbb{C}^n) \to \mathcal{M}_B$ with positive elements M of $\mathcal{M}_{AB}$. Given $M = (M_{ij}) \in (\mathcal{B}(\mathbb{C}^n) \otimes \mathcal{M}_B)_+$ with $\sum_i M_{ii} = \mathbb{1}$, we define the map $\mathcal{E}$ via $\mathcal{E}_*(\sigma) = (\sigma(M_{ij})^{ij})$ for $\sigma \in \mathcal{N}(\mathcal{M}_B)$. $\mathcal{E}$ is unital because of $\sum_i M_{ii} = \mathbb{1}$. The states are with respect to the fixed basis in $\mathcal{B}(\mathbb{C}^n)$ given by $\{|\psi_i\rangle\}$, such that for $A = \sum_{ij} a_{ij}|\psi_i\rangle\langle\psi_i|$, $(\sigma(M_{ij})^{ij})(A) = \sum_{ij} a_{ij}\sigma(M_{ij})$. It is straightforward to check that $\mathcal{E}$ is a quantum channel and satisfies

$$F\big((\mathcal{I}_A \otimes \mathcal{E}_*)(\omega_{AB}), |\Phi_{AA'}\rangle\big) = \sum_{ij}\omega_B^{ij}(M_{ij})\,. \tag{63}$$

The converse is obtained by setting for an arbitrary quantum channel $\mathcal{E}$, $M_{ij}^{\mathcal{E}} = \mathcal{E}(|\psi_i\rangle\langle\psi_j|)$. It follows directly from complete positivity and unitality that $M^{\mathcal{E}} = (M_{ij}^{\mathcal{E}})$ is positive and $\sum_i M_{ii}^{\mathcal{E}} = \mathbb{1}$. The relation (63) can be verified straightforwardly.

Optimal decoupling fidelity. The following proposition generalizes the operational meaning of the conditional max-entropy [25, Theorem 3].

Proposition 15. *Let $\mathcal{M}_{AB} = \mathcal{B}(\mathbb{C}^n) \otimes \mathcal{M}_B$ and $\omega_{AB} \in \mathcal{S}_{\leq}(\mathcal{M}_{AB})$. Then, we have that*

$$\mathrm{H}_{\max}(A|B)_\omega = \sup_{\sigma_B \in \mathcal{S}(\mathcal{M}_B)} \log F(\omega_{AB}, \tau_A \otimes \sigma_B)\,. \tag{64}$$

Proof. The statement can be proven in a similar way as for systems described by finite-dimensional spaces [25, Theorem 3]. Recall that each state in $\mathcal{M}_{AB}$ can be purified in the standard form, that is, in $\mathcal{B}(\mathbb{C}^n)\otimes\mathcal{B}(\mathbb{C}^n)\otimes\mathcal{M}_B^\phi$, where $\mathcal{M}_B^\phi$ is a standard form of $\mathcal{M}_B$ [31]. We denote the complementary system by $\mathcal{M}_{A'B'}$ since it consists of a copy of the A-system $\mathcal{M}_{A'} = \mathcal{B}(\mathbb{C}^n)$ 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 $|\xi_\omega\rangle \in \mathcal{K}$ be a purification of ω_{AB} and $|\Phi_{AA'}\rangle$ a non-normalized maximally entangled state on $\mathcal{M}_{AA'}$ as in Proposition 12, thus a purification of τ_A. Then, with $|\eta_\sigma\rangle \in \mathcal{H}_\phi$ a purification of $\sigma \in \mathcal{S}(\mathcal{M}_B)$, we find that

$$F(\omega_{AB}, \tau_A\otimes\sigma_B) = \sup_{U\in\mathcal{M}_{A'B'}} |\langle \xi_\omega | U(\Phi_{AA'}\otimes\eta_\sigma)\rangle|^2 \leq \sup_{U\in\mathcal{M}_{A'B'}} F_{\mathcal{M}_{AA'}}(U|\xi_\omega\rangle, |\Phi_{AA'}\rangle\otimes|\eta_\sigma\rangle)\,, \quad (65)$$

where the supremum is taken over unitaries U in $\mathcal{M}_{A'B'}$. According to Stinespring's dilation theorem [32], applying a unitary followed by a restriction of the state is a quantum channel, such that the state on $\mathcal{M}_{AA'}$ described by $U|\xi_\omega\rangle$ can be obtained by applying a quantum channel $\mathcal{E}^U : \mathcal{M}_{A'} \to M_{A'B'}$ on $\omega_{AA'B'}$. Hence, together with the operational interpretation of the conditional min-entropy (Proposition 12)

$$F(\omega_{AB}, \tau_A\otimes\sigma_B) \leq \sup_U F_{\mathcal{M}_{AA'}}((\mathcal{I}_A\otimes\mathcal{E}_*^U)(\omega_{AA'B'}), |\Phi_{AA'}\rangle) \leq 2^{-\mathrm{H}_{\min}(A|A'B')_\omega} = 2^{\mathrm{H}_{\max}(A|B)_\omega}\,. \quad (66)$$

Taking the supremum over all $\sigma_B \in \mathcal{S}(\mathcal{M}_B)$, we find inequality in one direction. In order to show the other direction, we note that again by the operational form of the conditional min-entropy (Proposition 12), there exists for all $\delta > 0$ a quantum channel $\mathcal{E} : \mathcal{M}_{A'} \to M_{A'B'}$ such that

$$2^{\mathrm{H}_{\max}(A|B)_\omega} \leq F((\mathcal{I}_A\otimes\mathcal{E}_*)(\omega_{AA'B'}), |\Phi_{AA'}\rangle) + \delta\,. \quad (67)$$

Let now $|\xi_{\omega\mathcal{E}}\rangle$ be a purification of $(\mathcal{I}_{AB}\otimes\mathcal{E}_*)(\omega_{ABA'B'})$, 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

$$F((\mathcal{I}_A\otimes\mathcal{E}_*)(\omega_{AA'B'}), |\Phi_{AA'}\rangle) = \sup_{U\in\mathcal{M}_{CBB'}} |\langle \xi_{\omega\mathcal{E}} | U(\Phi_{AA'}\otimes\theta)\rangle|^2 \quad (68)$$

$$\leq \sup_{U\in\mathcal{M}_{CBB'}} F_{\mathcal{M}_{AB}}(|\xi_{\omega\mathcal{E}}\rangle, |\Phi_{AA'}\rangle\otimes|U\theta\rangle)\,. \quad (69)$$

Since the reduced state of $|\xi_{\omega\mathcal{E}}\rangle$ on $\mathcal{M}_{AB}$ is ω_{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 $\mathcal{M}_{CBB'}$, we arrive at

$$2^{\mathrm{H}_{\max}(A|B)_\omega} \leq \sup_{\sigma_B\in\mathcal{S}(\mathcal{M}_B)} F(\omega_{AB}, \tau_A\otimes\sigma_B) + \delta\,. \quad (70)$$

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

Ordering of entropies. Given these alternative formulations we find that the conditional min-entropy is never larger than the conditional max-entropy.

Proposition 16. *Let $\mathcal{M}_{AB} = \mathcal{B}(\mathbb{C}^n)\otimes\mathcal{M}_B$ and $\omega_{AB} \in \mathcal{S}(\mathcal{M}_{AB})$. Then, we have*

$$\mathrm{H}_{\min}(A|B)_\omega \leq \mathrm{H}_{\max}(A|B)_\omega\,. \quad (71)$$

This follows directly from ordering of the min- and max-relative entropy (Proposition 9).

B. Classical Quantum Systems

Of particular interest in quantum information theory are correlations between classical and quantum degrees of freedom. A classical system is specified by the property that all observables commute, and is thus described by an abelian von Neumann algebra. We restrict to classical systems over a finite alphabet X, given by the bounded complex valued sequences on X, $\ell_X^\infty(\mathbb{C})$, supplied with the supremum norm. (For general discrete and continuous classical systems see the follow-up work [33].) We denote a classical system with alphabet X simply by X, and the corresponding algebra by ℓ_X^∞. A bipartite system consisting of a classical part X and a quantum part B is described by the von Neumann algebra

$$\mathcal{M}_{XB} = \ell_X^\infty \otimes \mathcal{M}_B \,, \tag{72}$$

which is isomorphic to the $\mathcal{M}_B$-valued sequences $\ell_X^\infty(\mathcal{M}_B)$. States on $\ell_X^\infty(M_B)$ are called classical quantum states, and can be written as

$$\omega_{XB} = (\omega_B^x)_{x\in X} \;\text{ with }\; \omega_B^x \in \mathcal{S}_\leq(\mathcal{M}_B), \;\text{ such that }\; \omega_{XB}(a) = \sum_x \omega_B^x(a_x) \;\; \forall a = (a_x) \in \mathcal{M}_{XB} \,. \tag{73}$$

We have the norm

$$\|(\omega^x)\|_{\ell^1(\mathcal{N}(\mathcal{M}_B))} = \sum_{x\in X} \|\omega^x\|_{\mathcal{N}(\mathcal{M}_B)} \,. \tag{74}$$

Conditional min-entropy. Consider the algebra $\mathcal{M}_{XB} = \ell_X^\infty \otimes \mathcal{M}_B$ and $\omega_{XB} \in \mathcal{S}(\mathcal{M}_{XB})$. This also defines a state $\omega_{A_{|X|}B}$ on the algebra $\mathcal{M}_{A_{|X|}B} = \mathcal{B}(\mathbb{C}^{|X|}) \otimes \mathcal{M}_B$ by setting $\omega_B^{xy} = \delta_{xy}\omega_x$. This implies

$$\omega_{A_{|X|}B}\left(\sum_{x,y=1}^{|X|} |x\rangle\langle y| \otimes M_{xy}\right) = \sum_x \omega_x(M_{xx}) \,, \quad M = (M_{xy}) \in \mathcal{B}(\mathbb{C}^{|X|}) \otimes \mathcal{M}_B \,, \tag{75}$$

which is a positive normalized functional. As such, we can compute its conditional min-entropy,

$$\mathrm{H}_{\min}(X|B)_\omega := \mathrm{H}_{\min}\big(A_{|X|}|B\big)_\omega \,. \tag{76}$$

It is easily seen that we can also write

$$\mathrm{H}_{\min}(X|B)_\omega = -\log \inf_{\sigma_B \in \mathcal{N}^+(\mathcal{M}_B)} \Big\{ \sigma_B(\mathbb{1}_B) \,:\, \tau_X \otimes \sigma_B - \omega_{XB} \geq 0 \Big\} \,, \tag{77}$$

where τ_X denotes the trace on ℓ_X^∞. Using the results from Section IV A, we find that the conditional min-entropy of a classical quantum state has an operational interpretation as the probability of correctly guessing the classical register X by making use of the quantum side information B [25, Theorem 1].

Corollary 17. *Let $\mathcal{M}_{XB} = \ell_X^\infty \otimes \mathcal{M}_B$ and $\omega_{XB} \in \mathcal{S}(\mathcal{M}_{XB})$. Then, we have $\mathrm{H}_{\min}(X|B)_\omega = -\log p_{\mathrm{guess}}(X|B)_\omega$ with*

$$p_{\mathrm{guess}}(X|B)_\omega = \sup\left\{ \sum_{x\in X} \omega_B^x(E_x) \;:\; E_x \in \mathcal{M}_B,\; E_x \geq 0,\; \sum_{x\in X} E_x = \mathbb{1} \right\} , \tag{78}$$

the guessing probability of the random variable X given the system B.

The result follows directly from Lemma 13 in analogy to the operational form of the fully quantum conditional min-entropy (Corollary 14). Moreover, using the embedding as in (75) also allows to define the smooth conditional min-entropy of classical quantum states as

$$\mathrm{H}_{\min}^{\epsilon}(X|B)_{\omega} := \sup_{\sigma_{XB}\in\mathcal{B}^{\varepsilon}_{\mathcal{M}_{XB}}(\omega_{XB})} \mathrm{H}_{\min}(X|B)_{\sigma}\,. \tag{79}$$

It follows from the data processing for the smooth conditional min-entropy (Proposition 6) that alternatively we could also smooth over the set $\mathcal{B}^{\varepsilon}_{\mathcal{M}_{A_{|X|}B}}(\omega_{A_{|X|}B})$ in the embedding. The proof of this is the same as for finite-dimensional spaces [3, Remark 3.2.4].

Conditional max-entropy. Again considering a classical quantum system $\mathcal{M}_{XB} = \ell_X^{\infty}\otimes\mathcal{M}_B$ and a state $\omega_{XB}\in\mathcal{S}(\mathcal{M}_{XB})$, we can use (75) to define a state on the system $\mathcal{M}_{A_{|X|}B} = \mathcal{B}(\mathbb{C}^{|X|})\otimes\mathcal{M}_B$. This allows us to consider its conditional max-entropy,

$$\mathrm{H}_{\max}(X|B)_{\omega} := \mathrm{H}_{\max}\big(A_{|X|}|B\big)_{\omega}\,. \tag{80}$$

Using the results from Section IV A we find the following characterization.

Corollary 18. *Let $\mathcal{M}_{XB} = \ell_X^{\infty}\otimes\mathcal{M}_B$ and $\omega_{XB}\in\mathcal{S}(\mathcal{M}_{XB})$. Then, we have $\mathrm{H}_{\max}(X|B)_{\omega} = \log F_{\mathrm{dec}}(X|B)_{\omega}$ with*

$$F_{\mathrm{dec}}(X|B)_{\omega} = \sup\left\{\left(\sum_{x\in X}\sqrt{F(\omega_B^x,\sigma_B)}\right)^2\Big|\sigma_B\in\mathcal{S}(\mathcal{M}_B)\right\}. \tag{81}$$

This follows directly from the characterization of the conditional max-entropy in terms of the optimal decoupling fidelity (Proposition 15) together with the fact that the fidelity between two direct sums of states is a sum itself. The smooth conditional max-entropy is then given as

$$\mathrm{H}_{\max}^{\epsilon}(X|B)_{\omega} := \sup_{\sigma_{XB}\in\mathcal{B}^{\varepsilon}_{\mathcal{M}_{XB}}(\omega_{XB})} \mathrm{H}_{\max}(X|B)_{\sigma}\,, \tag{82}$$

and again we might alternatively smooth over the set $\mathcal{B}^{\varepsilon}_{\mathcal{M}_{A_{|X|}B}}(\omega_{A_{|X|}B})$ in the embedding. For a proof we just follow the arguments for finite-dimensional spaces [34, Lemma 3].

C. Entropic Uncertainty Relations with Quantum Side Information

One of the fundamental principles of quantum mechanics is that for a fixed state the outcome distribution of two measurements described by non-commuting observables cannot be deterministic. A lower bound on the uncertainty inherent by two such measurements is called an uncertainty relation. Since entropies are measures of uncertainty, it is natural to quantify this uncertainty using entropy measures, see the review articles [35, 36]. Recently it was realized that if one allows to have quantum information about the system in question, the situation qualitatively changes and one has a subtle interplay between uncertainty and entanglement between the observer and the system [37]. This effect is quantified by means of so-called entropic uncertainty relations with quantum side information [33, 37–40]. Besides the fundamental interest, these relations also have manifold applications in quantum cryptography [41–44].

Measurements. We start with a tripartite quantum state $\omega_{ABC}\in\mathcal{S}(\mathcal{M}_{ABC})$ and two POVMs $\{E_A^x\}_{x\in X}$ and $\{F_A^y\}_{y\in Y}$ on system A with finite outcome ranges X and Y, respectively. We are

then interested in the uncertainty of the outcome distribution of the measurements $\{E_A^x\}$ and $\{F_A^y\}$ given the quantum side information B and C, respectively. We quantify the uncertainty in terms of the smooth conditional min- and max-entropy.

Proposition 19. *Let $\omega_{ABC} \in \mathcal{S}(\mathcal{M}_{ABC})$, $\{E_A^x\}_{x\in X}$ and $\{F_A^y\}_{y\in Y}$ be POVM's on $\mathcal{M}_A$ with finite outcome ranges X and Y, and $\epsilon \geq 0$. Then, we have that*

$$\mathrm{H}_{\min}^{\epsilon}(X|B)_{\omega} + \mathrm{H}_{\max}^{\epsilon}(Y|C)_{\omega} \geq -\log \max_{x,y} \left\| (E_A^x)^{\frac{1}{2}} \cdot (F_A^y)^{\frac{1}{2}} \right\|^2 , \tag{83}$$

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 classical quantum states on $\ell_X^\infty(\mathcal{M}_B)$ and $\ell_Y^\infty(\mathcal{M}_C)$, respectively.

Note that since we started with a fully general tripartite von Neumann algebra $\mathcal{M}_{ABC}$, no approximation techniques (as, e.g., from [14]) can be applied to just lift the result from finite-dimensions. In the work [42], we use the uncertainty relation (83) to analyze the security of continuous variable quantum key distribution protocols. Moreover, in a follow-up work [33], we discuss a non-smooth extension of Proposition 19 for measurements with infinitely many outcomes (discrete and continuous). In the following we will derive Proposition 19 from a more general uncertainty relation that also holds for quantum channels and not only for measurements.

Quantum Channels. Here we start with a tripartite quantum state $\omega_{ABC} \in \mathcal{S}(\mathcal{M}_{ABC})$ and two quantum channels $\mathcal{E} : \mathcal{M}_E \to \mathcal{M}_A$ and $\mathcal{G} : \mathcal{M}_G \to \mathcal{M}_A$ with their domains $\mathcal{M}_E \cong \mathcal{B}(\mathbb{C}^{n'})$ and $\mathcal{M}_G \cong \mathcal{B}(\mathbb{C}^n)$ being matrix algebras. We are then interested in the uncertainties about the quantum systems obtained by the quantum channels $\mathcal{E}$ and $\mathcal{G}$ given systems B and C , respectively.

Let us first introduce some notation. By definition the quantum channel $\mathcal{E} : \mathcal{B}(\mathbb{C}^n) \to \mathcal{M}_A$ is a completely positive, unital map. As we can always embed $\mathcal{M}_A \subset \mathcal{B}(\mathcal{H})$ faithfully for some $\mathcal{H}$, we can apply Stinespring's dilation theorem to $\mathcal{E}$. There exist a Hilbert space $\mathcal{H}'$, a representation π of $\mathcal{B}(\mathbb{C}^{n'})$ on $\mathcal{H}'$ and an isometry $V : \mathcal{H} \to \mathcal{H}'$, such that $\mathcal{E}(x) = V^* \pi(x) V$. If vectors of the form $\pi(x)V|\psi\rangle$, $x \in \mathcal{B}(\mathbb{C}^{n'})$, $|\psi\rangle \in \mathcal{H}$ are dense in $\mathcal{H}'$, then we call the triple $(V, \mathcal{H}, \pi)$ a minimal Stinespring dilation, which always exists. For such a mininmal dilation, we can choose $\mathcal{H}'$ to be isomorphic to $\mathbb{C}^n \otimes \mathbb{C}^d \otimes \mathcal{H}$ with $1 \leq d \leq n$, and π of the form $\pi(x) = x \otimes \mathbb{1}_d \otimes \mathbb{1}_{\mathcal{H}}$. From now, on we always assume that the dilation is minimal, unless otherwise stated.

Lemma 20. *Let $\omega_{ABC} \in \mathcal{S}(\mathcal{M}_{ABC})$, $\mathcal{E} : \mathcal{M}_E \to \mathcal{M}_A$ and $\mathcal{G} : \mathcal{M}_G \to \mathcal{M}_A$ be quantum channels with $\mathcal{M}_E \cong \mathcal{B}(\mathbb{C}^{n'})$ and $\mathcal{M}_G \cong \mathcal{B}(\mathbb{C}^n)$ being matrix algebras, and $\epsilon \geq 0$. If $U : \mathcal{H} \to \mathbb{C}^{n'} \otimes \mathbb{C}^{d'} \otimes \mathcal{H}$ and $V : \mathcal{H} \to \mathbb{C}^n \otimes \mathbb{C}^d \otimes \mathcal{H}$ denote the isometries corresponding to the minimal Stinespring dilation of $\mathcal{E}$ and $\mathcal{G}$, respectively, then we have*

$$\mathrm{H}_{\min}^{\epsilon}(E|B)_{\omega} + \mathrm{H}_{\max}^{\epsilon}(G|C)_{\omega} \geq -\log c(UV^*) , \tag{84}$$

where $\omega_{EB}(x) := \omega_{AB}(\mathcal{E}(x))$, $\omega_{GC}(y) := \omega_{AC}(\mathcal{G}(y))$, and

$$c(VU^*) := \inf\left\{ c > 0 \,:\, c\,\bar{\mathrm{Tr}}_{n'} - \mathcal{J}_{V^*U} \text{ is completely positive} \right\} . \tag{85}$$

Here $\mathcal{J}_{VU^*} : \mathcal{B}(\mathbb{C}^{n'}) \otimes \mathcal{M}_B \to \mathcal{B}(\mathbb{C}^d) \otimes \mathcal{B}(\mathcal{H})$ is the completely positive mapping

$$\mathcal{J}_{VU^*}(x) := \mathrm{Tr}_n[VU^* x \otimes \mathbb{1}_{d'} UV^*] , \tag{86}$$

and $\bar{\mathrm{Tr}}_{n'} : \mathcal{B}(\mathbb{C}^{n'}) \otimes \mathcal{M}_B \to \mathcal{B}(\mathbb{C}^d) \otimes \mathcal{B}(\mathcal{H})$ denotes the partial trace with respect to $\mathbb{C}^{n'}$ together with tensoring the identity on $\mathbb{C}^d$,

$$\bar{\mathrm{Tr}}_{n'}(x) := \sum_{i=1}^{n'} x_{ii} \otimes \mathbb{1}_d \quad \text{for} \quad (x)_{ij} \in \mathcal{B}(\mathbb{C}^{n'}) \otimes \mathcal{M}_B . \tag{87}$$

We remark that $c(VU^*)$ does not depend on the choice of the particular minimal Stinespring dilations U, V, as all of these are connected by either a unitary on $\mathbb{C}^{d'}$ or on $\mathbb{C}^d$. Thus, they either do not influence the mapping $\mathcal{J}_{V^*U}$ or the mapping $\bar{\mathrm{Tr}}_{n'}$ and hence have no effect on the constant $c(VU^*)$.

Proof of Lemma 20. The proof relies on the ideas developed for finite-dimensional quantum systems [38], and can be regarded as the dual version of it. Let $\mathcal{H}$ be a Hilbert space such that $\mathcal{M}_{ABC} \subset \mathcal{B}(\mathcal{H})$ is faithfully embedded and there exists a purifying vector $|\psi\rangle \in \mathcal{H}$ for ω_{ABC}, that is, $\omega_{ABC}(x) = \langle \psi \, | x \, \psi \rangle$. We denote by $U : \mathcal{H} \to \mathbb{C}^{n'} \otimes \mathbb{C}^{d'} \otimes \mathcal{H}$ and $V : \mathcal{H} \to \mathbb{C}^n \otimes \mathbb{C}^d \otimes \mathcal{H}$ the isometries of the minimal Stinespring dilations corresponding to $\mathcal{E}$ and $\mathcal{G}$, respectively (as explained in the discussion preceding the proposition). Since $\mathcal{M}_A \subset \mathcal{M}_C'$, we have $\mathcal{G}(\mathcal{B}(\mathbb{C}^n)) \subset \mathcal{M}_C'$, and by Arveson's commutant lifting theorem [45, Theorem 1.3.1], there exists a representation

$$\pi_C : \mathcal{M}_C \to \mathcal{B}(\mathbb{C}^n \otimes \mathbb{1}_d \otimes \mathbb{1}_{\mathcal{H}})' = \mathbb{1}_n \otimes \mathcal{B}(\mathbb{C}^d) \otimes \mathcal{B}(\mathcal{H}) \tag{88}$$

such that we have $\pi_C(y)V = Vy$ for $y \in \mathcal{M}_C$. It follows that the map $\tilde{\mathcal{G}} : \mathcal{B}(\mathbb{C}^n) \otimes \mathcal{M}_C \to \mathcal{B}(\mathcal{H})$ defined by

$$\tilde{\mathcal{G}}(x \otimes y) = V^*(x \otimes \mathbb{1}_d \otimes \pi_C(y))V = \mathcal{G}(x)y \tag{89}$$

for $x \in \mathcal{B}(\mathbb{C}^n)$, $y \in \mathcal{M}_C$ extends to a completely positive unital map $\tilde{\mathcal{G}} : \mathcal{B}(\mathbb{C}^n) \otimes \mathcal{M}_C \to \mathcal{M}_{AC}$. Due to the fact that $|\psi\rangle$ is a purification of ω_{ABC}, we have that

$$\langle V\psi \, | x \otimes \mathbb{1}_d V\psi \, \rangle = \langle \psi \, | \tilde{\mathcal{G}}(x)\psi \, \rangle = \omega_{ABC}(\tilde{\mathcal{G}}(x)) = \omega_{GC}(x) \tag{90}$$

for $x \in \mathcal{M}_{GC} \cong \mathcal{B}(\mathbb{C}^n) \otimes \mathcal{M}_B$, implying that $V|\psi\rangle$ is a purification of ω_{GC} on $\mathbb{C}^n \otimes \mathbb{C}^d \otimes \mathcal{H}$ with representation given by $\mathrm{id}_{\mathcal{B}(\mathbb{C}^n)} \otimes \pi_C$, with $\mathrm{id}_{\mathcal{B}(\mathbb{C}^n)}$ being the defining representation of $\mathcal{B}(\mathbb{C}^n)$ on $\mathbb{C}^n$. Since the commutant of $\mathcal{B}(\mathbb{C}^n)$ in $\mathcal{B}(\mathbb{C}^n \otimes \mathbb{C}^d \otimes \mathcal{H})$ equals $\mathbb{1}_n \otimes \mathcal{B}(\mathbb{C}^d \otimes \mathcal{H})$, the complementary system is computed as the commutant $\mathcal{M}_D = \pi_C(\mathcal{M}_C)' \cap \mathcal{B}(\mathbb{C}^d \otimes \mathcal{H})$ of $\pi_C(\mathcal{M}_C)$ in $\mathcal{B}(\mathbb{C}^d \otimes \mathcal{H})$. An analogues argument constructs a channel $\tilde{\mathcal{E}} : \mathcal{B}(\mathbb{C}^{n'}) \otimes \mathcal{M}_B \to \mathcal{M}_{AB}$ starting from $\mathcal{E}$, providing a purification $U|\psi\rangle$ of ω_{EB} on $\mathbb{C}^{n'} \otimes \mathbb{C}^{d'} \otimes \mathcal{H}$ with complementary system $\mathcal{M}_{\tilde{D}}$. Here we denoted $\mathcal{M}_{\tilde{D}} = \pi_B(\mathcal{M}_B)'$, with π_B being the representation of $\mathcal{M}_B$ obtained from repeating the above arguments for $\mathcal{E}$. Since by definition of the smooth conditional max-entropy (Definition 9)

$$\mathrm{H}_{\max}^{\epsilon}(G|C)_{\omega} = -\mathrm{H}_{\min}^{\epsilon}(G|D)_{V|\psi\rangle} \, , \tag{91}$$

we have to show that

$$\mathrm{H}_{\min}^{\epsilon}(G|D)_{V|\psi\rangle} \leq \mathrm{H}_{\min}^{\epsilon}(E|B)_{U|\psi\rangle} + \log c \quad \text{where } c = c(V^*U) \text{ as in (85)} \, . \tag{92}$$

We first prove the proposition for $\epsilon = 0$. By the operational characterization of the conditional min-entropy (Corollary 14) the last inequality amounts to

$$\begin{aligned} &\sup \Big\{ \langle \psi \, | U^* x \otimes \mathbb{1}_{d'} \, U\psi \, \rangle \, : \, x \in (\mathcal{B}(\mathbb{C}^{n'}) \otimes \mathcal{M}_B)_+ \, , \mathrm{Tr}_{n'}(x) \leq \mathbb{1}_{\mathcal{H}} \Big\} \\ &\leq c \cdot \sup \Big\{ \langle \psi \, | V^* \, y \, V\psi \, \rangle \, : \, y \in (\mathcal{B}(\mathbb{C}^n) \otimes \mathcal{M}_D)_+ \, , \mathrm{Tr}_n(y) \leq \mathbb{1}_d \otimes \mathbb{1}_{\mathcal{H}} \Big\} \, . \end{aligned} \tag{93}$$

Since V^*V projects onto $\mathcal{H}$ and $U|\psi\rangle = UV^*V|\psi\rangle$, we have

$$\langle \psi \, | U^* x \otimes \mathbb{1}_{d'} \, U\psi \, \rangle = \langle \psi \, | V^*VU^* x \otimes \mathbb{1}_{d'} \, UV^*V\psi \, \rangle \, . \tag{94}$$

Let us now consider the expression $VU^*x\otimes \mathbb{1}_{d'}\, UV^*$. If this would be an element of $(\mathcal{B}(\mathbb{C}^n)\otimes\mathcal{M}_D)_+$, the assertion would follow from

$$\mathrm{Tr}_n(VU^*\, x\otimes \mathbb{1}_{d'}\, UV^*) \;\leq\; c\cdot \mathbb{1}_d\otimes \mathrm{Tr}_{n'}(x)\,, \tag{95}$$

where $x\in\mathcal{B}(\mathbb{C}^{n'})\otimes\mathcal{M}_B$. However, this follows directly from the definition of the constant $c(VU^*)$, so only the assumption needs to be checked. For that, note that since $\tilde{\mathcal{E}}$ maps into $\mathcal{M}_{AB}\subset\mathcal{M}'_C$, again by Arveson's commutant lifting theorem we can find a representation $\tilde{\pi}_C:\mathcal{M}_C\to(\mathrm{id}_{\mathcal{B}(\mathbb{C}^{n'})}\otimes \pi_B(\mathcal{B}(\mathbb{C}^{n'})\otimes\mathcal{M}_B))'\subset\mathcal{B}(\mathbb{C}^{n'd'}\otimes\mathcal{H})$ satisfying $Uy=\tilde{\pi}_C(y)U$ and hence

$$\begin{aligned} VU^*x\otimes\mathbb{1}_{d'}\,UV^*\pi_C(y) = VU^*x\otimes\mathbb{1}_{d'}\,UyV^* &= VU^*\tilde{\pi}_C(y)x\otimes\mathbb{1}_{d'}\,UV^* &(96)\\ &= \pi_C(y)VU^*x\otimes\mathbb{1}_{d'}\,UV^*\,, &(97)\end{aligned}$$

which implies $VU^*x\otimes\mathbb{1}_{d'}\,UV^*\in\pi_C(\mathcal{M}_C)'=\mathcal{B}(\mathbb{C}^n)\otimes\mathcal{M}_D$. Since $x\in(\mathcal{B}(\mathbb{C}^{n'})\otimes\mathcal{M}_B)_+$, the expression $VU^*x\otimes\mathbb{1}_{d'}\,UV^*$ also defines a positive operator. This concludes the proof for $\epsilon=0$.

For $\epsilon>0$, take $\gamma^\epsilon_{GD}\in\mathcal{B}^\epsilon(\gamma_{GD})$, where γ_{GD} denotes the vector state $V|\psi\rangle$ restricted to $\mathcal{B}(\mathbb{C}^n)\otimes\mathcal{M}_D$. Let $(\pi_{GD},\mathcal{K})$ be a representation $\pi_{GD}:\mathcal{B}(\mathbb{C}^n)\otimes\mathcal{M}_D\to\mathcal{B}(\mathcal{K})$ on $\mathcal{K}$ such that there exists purifying vectors $|\xi\rangle$ and $|\xi^\varepsilon\rangle$ for γ_{GD} and γ^ε_{GD}, respectively, with $\mathcal{F}(|\xi\rangle,|\xi^\epsilon\rangle)\geq 1-\epsilon^2$. Moreover, there exists an isometry $W:\mathbb{C}^{nd}\otimes\mathcal{H}\to\mathcal{K}$ satisfying $Wx=\pi_{GD}(x)W$ for $x\in\mathcal{B}(\mathbb{C}^n)\otimes\mathcal{M}_D$ and $WV|\psi\rangle=|\xi\rangle$. We find using that the purified distance is monotone under partial isometries

$$\begin{aligned} \mathcal{F}(U|\psi\rangle,UV^*W^*|\xi^\epsilon\rangle) = \mathcal{F}(UV^*V|\psi\rangle,UV^*W^*|\xi^\epsilon\rangle) &= \mathcal{F}(UV^*W^*|\xi\rangle,UV^*W^*|\xi^\epsilon\rangle) &(98)\\ &\geq \mathcal{F}(W^*|\xi\rangle,W^*|\xi^\epsilon\rangle) &(99)\\ &\geq 1-\varepsilon^2\,, &(100)\end{aligned}$$

and hence $UV^*W^*|\xi^\epsilon\rangle_{EB}\in\mathcal{B}^\epsilon(U|\psi\rangle_{EB})$, where $UV^*W^*|\xi^\epsilon\rangle_{EB}$ (resp. $U|\psi\rangle_{EB}$) denotes the state on $\mathcal{M}_{EB}$ induced by the vector $UV^*W^*|\xi^\epsilon\rangle$ (resp. $U|\psi\rangle$). Moreover, we find for any $y=VU^*x\otimes\mathbb{1}_{d'}\,UV^*$ with $x\in(\mathcal{B}(\mathbb{C}^{n'})\otimes\mathcal{M}_B)_+$ that

$$\langle W^*\xi^\varepsilon\,|yW^*\xi^\varepsilon\,\rangle = \langle\xi^\varepsilon\,|\sqrt{\pi_{GD}(y)}WW^*\sqrt{\pi_{GD}(y)}\xi^\varepsilon\,\rangle \leq \langle\xi^\varepsilon\,|\pi_{GD}(y)\xi^\varepsilon\,\rangle = \gamma^\varepsilon_{GD}(y)\,, \tag{101}$$

since $y=VU^*x\otimes\mathbb{1}_{d'}\,UV^*\in(\mathcal{B}(\mathbb{C}^n)\otimes\mathcal{M}_D)_+$ as before. Thus, repeating the steps for the $\varepsilon=0$ case and using (101) yields the assertion. □

Finally, we obtain the proof of Proposition 19 from Lemma 20.

Proof of Proposition 19. Since a measurement is a quantum channel with domain being an abelian von Neumann algebra we can make use of Lemma 20. Assume for simplicity that $|X|=|Y|=n$, and think of ℓ^∞_n as the subalgebra of diagonal matrices in $\mathcal{B}(\mathbb{C}^n)$. We then define the maps $\mathcal{G}:\mathcal{B}(\mathbb{C}^n)\to\mathcal{M}_A$, $\mathcal{E}:\mathcal{B}(\mathbb{C}^n)\to\mathcal{M}_A$ as being the projection onto the subalgebra of diagonal matrices followed by the measurement,

$$\mathcal{G}\left(\sum_{x,x'}a_{x,x'}|x\rangle\langle x'|\right) = a_{x,x}E^x_A\,, \tag{102}$$

for $\sum_{x,x'}a_{x,x'}|x\rangle\langle x'|\in\mathcal{B}(\mathbb{C}^n)$ and correspondingly for $\mathcal{E}$. A corresponding isometry for $E:\ell^\infty_n\to\mathcal{M}_A$, $e_x\mapsto E^x_A$ can then be chosen of the form

$$V\,:\,\mathcal{H}\to\mathbb{C}^n\otimes\mathbb{C}^n\otimes\mathcal{H}\quad\text{with}\quad V|\psi\rangle := \sum_{i=x}^{n}(E^x_A)^{\frac{1}{2}}|\psi\rangle|x\rangle|x\rangle\,, \tag{103}$$

and analogously U for $F : \ell_n^\infty \to \mathcal{M}_A$, $e_y \mapsto F_A^y$. Here $\{e_x\}$ denotes the canonical basis for ℓ_n^∞. However, these isometries are generally not minimal. This problem can be resolved by projecting onto the span of the respective representations. Let P (Q) be the projector onto the subspace of $\mathbb{C}^n \otimes \mathbb{C}^n \otimes \mathcal{H}$ spanned by $aV|\psi\rangle$ ($aU|\psi\rangle$), for $a \in \mathcal{B}(\mathbb{C}^n)$ and $|\psi\rangle \in \mathcal{H}$. It then follows that PV and QU are minimal Stinespring dilations.

For $A \in (\mathcal{B}(\mathbb{C}^n) \otimes \mathcal{M}_B)_+$, we find that

$$\mathrm{Tr}_n[PVU^*Q(A \otimes \mathbb{1}_{d'})QUV^*P] = \mathrm{Tr}_n\Big[PV\tilde{\mathcal{E}}(A \otimes \mathbb{1}_{d'})V^*P\Big] = \mathrm{Tr}_n\left[PV\sum_{y\in Y} F_A^y\, A_{yy} V^*P\right], \quad (104)$$

where we used the extension $\tilde{\mathcal{E}} : \mathcal{B}(\mathbb{C}^n) \otimes \mathcal{M}_B \to \mathcal{M}_{AB}$ of $\mathcal{E}$ constructed in the proof of Lemma 20. Moreover, for any $\sigma \in \mathcal{N}^+(\mathcal{B}(\mathbb{C}^n \otimes \mathcal{H}))$, $\sigma = (\sigma)_{xx'}$, we have

$$(\sigma \otimes \mathrm{Tr}_n)\left(PV\sum_{y\in Y} F_A^y\, A_{yy} V^*P\right) = (\sigma \otimes \mathrm{Tr}_n)\left(PV\sum_{y\in Y} F_A^y\, A_{yy} V^*P\right). \quad (105)$$

Since $\mathcal{G}(\mathcal{B}(\mathbb{C}^n)) \subset \mathcal{M}_A \subset \mathcal{M}_B'$, we can find by Arveson's commutant lifting theorem [45, Theorem 1.3.1] a representation $\pi_B : \mathcal{M}_B \to (\mathcal{B}(\mathbb{C}^n) \otimes \mathbb{1}_n \otimes \mathbb{1}_{\mathcal{H}})' = \mathbb{1}_n \otimes \mathcal{B}(\mathbb{C}^n) \otimes \mathcal{B}(\mathcal{H})$ such that $PVb = P\pi_B(b)V = \pi_B(b)PV$. This shows that P both commutes with $V\sum_{y\in Y} F_A^y V^*$ (by construction) as well as with $\pi_B(\mathcal{M}_B)$ and we find

$$\begin{aligned}
(\sigma \otimes \mathrm{Tr}_n)\left(PV\sum_{y\in Y} F_A^y\, A_{yy} V^*P\right) &= (\sigma \otimes \mathrm{Tr}_n)\left(PV\sum_{y\in Y} F_A^y\, V^*P\pi_B(A_{yy})\right) && (106)\\
&\leq (\sigma \otimes \mathrm{Tr}_n)\left(V\sum_{y\in Y} F_A^y\, A_{yy} V^*\right) && (107)\\
&= \sum_{x,y=1}^n \sigma_{xx}((E_A^x)^{\frac{1}{2}} F_A^y (E_A^x)^{\frac{1}{2}} A_{yy}) && (108)\\
&\leq \max_{x,y}\left\|(E_A^x)^{\frac{1}{2}} F_A^y (E_A^x)^{\frac{1}{2}}\right\| \cdot \sum_{x,y=1}^n \sigma_{xx}(A_{yy})\,. && (109)
\end{aligned}$$

The result follows since (109) implies the bound

$$c(VU^*) \leq \max_{x,y}\left\|(E_A^x)^{\frac{1}{2}} \cdot (F_A^y)^{\frac{1}{2}}\right\|^2. \quad (110)$$

□

D. Quantum Key Distribution

One goal in quantum information theory is a tight characterization of information-theoretic tasks involving quantum systems. We focus on the particular task of quantum key distribution for which the basic information-theoretic tasks can be characterized by smooth conditional min- and max-entropies if only finite-dimensional spaces are involved [3]. We prove that this remains true even when quantum systems are modeled by von Neumann algebras. We first describe the task of quantum key distribution and divide it into two subtasks, which are then characterized by the smooth conditional min- and max-entropy.

We consider a tripartite setting with space-like separated parties Alice (A), Bob (B), and Eve (E). The goal for Alice and Bob is to create a uniformly distributed random bit string, the key, which is known to both of them (correctness condition), but not to the adversary Eve (security condition). Mathematically, we model Alice and Bob as a bipartite system $\mathcal{M}_{AB} = \mathcal{M}_A \vee \mathcal{M}_B$ with von Neumann algebras $\mathcal{M}_A$ and $\mathcal{M}_B$, and denote the state they share by $\omega_{AB} \in \mathcal{S}(\mathcal{M}_{AB})$. Furthermore, we assign to Eve the complementary system $\mathcal{M}_E$ of a purification ω_{ABE} of ω_{AB}. After Alice measured her system by applying some POVM $\{E_A^x\}_{x\in X} \subset \mathcal{M}_A$, $|X| < \infty$ the resulting post-measurement state is modeled by a classical quantum state $\omega_{XBE} \in \mathcal{S}(\ell_X^\infty \otimes \mathcal{M}_{BE})$. Bob then wants to determine Alice's bit string and for that he receives a classical message M from Alice. Based on this, Bob chooses his measurement to optimize the success probability to obtain the same bit string. This task is known as data compression with quantum side information and was linked to the smooth conditional max-entropy in finite dimensions [46, Theorem 1]. In the last step Alice and Bob extract a secure key from the bit string they share. This is referred to as privacy amplification and in finite dimensions it has been shown that the remaining correlation with Eve's system after this step can be quantified by the smooth conditional min-entropy [47, Theorem 6]. In the following, we discuss these two information-theoretic tasks in detail for our more generalized setting.

Privacy amplification against quantum side information. We commence with a classical quantum state $\omega_{XE} \in \mathcal{S}(\ell_X^\infty \otimes \mathcal{M}_E)$ between Alice and Eve. As outlined in the introduction, the task of privacy amplification is to extract a secure key from ω_{XE}, that is, a uniformly distributed bit string K on Alice's side that is uncorrelated with Eve's system E. This is described by a classical quantum state $\frac{1}{|K|}\tau_K \otimes \sigma_E$, where $\frac{1}{|K|}\tau_K$ is the tracial state on ℓ_K^∞ and $\sigma_E \in \mathcal{S}(\mathcal{M}_E)$. Note that K is a classical random variable generated from X. We follow [3] and call a state $\omega_{KE} \in \mathcal{S}_\leq(\ell_K^\infty \otimes \mathcal{M}_E)$ ϵ-secure if

$$\left\| \omega_{KE} - \frac{1}{|K|}\tau_K \otimes \omega_E \right\| \leq \epsilon \,. \tag{111}$$

The basic idea how to achieve an ϵ-secure key from an input ω_{XE} is to randomly combine several indices x into a single one, and thereby reducing (hashing) the alphabet from X to K with $|K| < |X|$. This process can be accomplished by using two-universal hash functions. A family of $\{X, K\}$-hash functions is a set $\{\mathcal{F}, \mathcal{P}_\mathcal{F}\}_{X,K}$, where every element $f \in \mathcal{F}$ is a function $f : X \to K$, called hash function, and $\mathcal{P}_\mathcal{F}$ 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 $x \neq y$

$$\mathcal{P}_\mathcal{F}(f(x) = f(y)) \leq \frac{1}{|K|} \,. \tag{112}$$

We refer to [48, 49] for the existence proof of families of two-universal $\{X, K\}$-hash functions for every two finite alphabets X, K with $|K| \leq |X|$. Given a hash function $f : X \to K$, we define the operator T_f from $\mathcal{S}_\leq(\ell_X^\infty)$ to $\mathcal{S}_\leq(\ell_K^\infty)$ through

$$(T_f u)(i) := \sum_{x\in X : f(x)=i} u(x) \quad \text{for} \quad u \in \mathcal{S}_\leq(\ell_X^\infty) \quad \text{and} \quad i \in K \,, \tag{113}$$

which implements the action of the hash function on the state space. We are now ready to state the main result of this section.

Proposition 21. *Let X, K be sets of finite cardinality with $|K| \leq |X|$, $\{\mathcal{F}, \mathcal{P}_\mathcal{F}\}_{X,K}$ a family of two-universal $\{X, K\}$-hash functions, $\omega_{XE} = (\omega_E^x)_{x\in X} \in \mathcal{S}_\leq(\ell_X^\infty \otimes \mathcal{M}_E)$, and $\epsilon \geq 0$. Denoting by*

$\mathbb{E}_{\mathcal{F}}$ the expectation with respect to $\mathcal{P}_{\mathcal{F}}$, we have

$$\mathbb{E}_{\mathcal{F}}\left\|(T_f\otimes\mathcal{I})(\omega_{XE})-\frac{1}{|K|}\tau_K\otimes\omega_E\right\|\leq\sqrt{|K|\cdot 2^{-\mathrm{H}^{\epsilon}_{\min}(X|E)_\omega}}+4\epsilon\,. \tag{114}$$

We note that our proof is different from the one for finite-dimensional systems presented in [47]. Our proof strategy is inspired by the purely classical results [50–52]. We show the statement for $\epsilon=0$, from which the $\epsilon>0$ case is obtained by a simple application of the triangle inequality (see [3, Section 5.6] for details).

Proof. Recall that the norm on $\ell^1(\mathcal{N}(\mathcal{M}_E))$ is inherited from the dual of $\ell^\infty_X\otimes\mathcal{M}_E$, such that the left hand side of (114) is simply the expectation value $\mathbb{E}_{\mathcal{F}}$ of

$$\sum_{i\in K}\sup_{a_i\in\mathcal{M}_E\|a_i\|=1}\left|\sum_{x\in X:f(x)=i}\omega^x_E(a_i)-\frac{1}{|K|}\omega_E(a_i)\right|. \tag{115}$$

Because $|X|$ is finite, we can assume that there exists a $\sigma_E\in\mathcal{S}(\mathcal{M}_E)$ such that $\omega^x_E\leq\lambda\cdot\sigma_E$ for all $x\in X$ and suitable $\lambda>0$ (take for instance $\sigma_E=\sum_x\omega^x_E$). We choose $(\pi_\sigma,\mathcal{H}_\sigma,|\xi_\sigma\rangle)$ to be a purification of σ_E such that $|\xi_\sigma\rangle$ is cyclic. This is always possible according to the GNS construction. We denote by $D_x\in\pi_\sigma(\mathcal{M}_E)'$ ($D\in\pi_\sigma(\mathcal{M}_E)'$) the corresponding Radon-Nikodym derivatives [17, Chapter VII.2] of ω^x_E (ω_E) with respect to σ_E. That is, $D_x|\xi_\sigma\rangle$ ($D|\xi_\sigma\rangle$) is a purification of ω^x_E (ω_E) and we have $\omega^x_E\leq\|D_x\|^2\sigma$. Since $|\xi_\sigma\rangle$ is cyclic it follows that $\sum_x D^*_xD_x|\xi_\sigma\rangle=D^*D|\xi_\sigma\rangle$. We can then write

$$\sum_{x\in X:f(x)=i}\omega^x_E(a_i)-\frac{1}{|K|}\omega_E(a_i)=\left\langle\left(\sum_{x\in X:f(x)=i}D^*_xD_x-\frac{1}{|K|}D^*D\right)\xi_\sigma\middle|\pi_\sigma(a_i)\xi_\sigma\right\rangle, \tag{116}$$

where we used the fact that D_x as well as D are elements of the commutant of $\pi_\sigma(\mathcal{M}_E)$. We now insert this expression into (115), take the expectation $\mathbb{E}_{\mathcal{F}}$ and apply the Cauchy-Schwarz inequality to the sum over $i\in K$ and $f\in\mathcal{F}$, which yields

$$\begin{aligned}&\mathbb{E}_{\mathcal{F}}\left\|(T_f\otimes\mathcal{I})(\omega_{XE})-\frac{1}{|K|}\tau_K\otimes\omega_E\right\|\\&\qquad\leq\sqrt{|K|}\left(\mathbb{E}_{\mathcal{F}}\sum_{i\in K}\left\langle\xi_\sigma\middle|\left(\sum_{x\in X:f(x)=i}D^*_xD_x-\frac{1}{|K|}D^*D\right)^2\xi_\sigma\right\rangle\right)^{\frac{1}{2}}.\end{aligned} \tag{117}$$

Using that $\mathbb{E}_{\mathcal{F}}\sum_{i\in K}\sum_{x\in X:f(x)=i}=\sum_{x\in X}$ and the identity $\sum_x D^*_xD_x|\xi_\sigma\rangle=D^*D|\xi_\sigma\rangle$, we can compute

$$\begin{aligned}&\mathbb{E}_{\mathcal{F}}\sum_{i\in K}\left\langle\xi_\sigma\middle|\left(\sum_{x\in X:f(x)=i}D^*_xD_x-\frac{1}{|K|}D^*D\right)^2\xi_\sigma\right\rangle\\&=\mathbb{E}_{\mathcal{F}}\sum_{i\in K}\left\langle\xi_\sigma\middle|\left(\sum_{x\in X:f(x)=i}D^*_xD_x\right)^2\xi_\sigma\right\rangle-\frac{1}{|K|}\langle\xi_\sigma|D^*DD^*D\xi_\sigma\rangle\,.\end{aligned} \tag{118}$$

The sum in the first term can be written as

$$\mathbb{E}_{\mathcal{F}}\sum_{i\in K}\Big(\sum_{x\in X:f(x)=i}D^*_xD_x\Big)^2=\sum_{x\in X}\sum_{y\in X}D^*_xD_xW_{xy}D^*_yD_y\,, \tag{119}$$

where $W_{xy} := \mathbb{E}_{\mathcal{F}} \sum_{i\in K} \delta_{f(x)=i}\ \delta_{f(y)=i}$. Note that this defines a positive $|X| \times |X|$-matrix which can be upper bounded by $P_{\tau_X} + \mathbb{1}_X$, with $\mathbb{1}_X$ the $|X| \times |X|$-identity matrix and P_{τ_X} the projector onto the vector corresponding to the uniform distribution on X, normalized to trace one. This follows from the definition of two-universal hash functions (112). Using these facts, we obtain

$$\mathbb{E}_{\mathcal{F}} \sum_{i\in K} \left\langle \xi_\sigma \middle| \left(\sum_{x\in X: f(x)=i} D_x^* D_x - \frac{1}{|K|} D^* D \right)^2 \xi_\sigma \right\rangle \leq \sum_{x\in X} \langle \xi_\sigma \, | D_x^* D_x D_x^* D_x \xi_\sigma \, \rangle \, . \tag{120}$$

The expression on the right hand side can be estimated further by employing $\langle \xi_\sigma \, | \sum_{x\in X} D_x^* D_x \xi_\sigma \, \rangle = \omega_E(\mathbb{1}) \leq 1$. Hence, we find

$$\sum_{x\in X} \langle \xi_\sigma \, | D_x^* D_x D_x^* D_x \xi_\sigma \, \rangle \leq \max_{x\in X} \| D_x^* D_x \| \left\langle \xi_\sigma \middle| \sum_{x\in X} D_x^* D_x \xi_\sigma \right\rangle \leq 2^{-\mathrm{H}_{\min}(X|E)_\omega} \, , \tag{121}$$

where we also took the infimum over all suitable $\sigma_E \in \mathcal{S}(\mathcal{M}_E)$ that majorize every ω_E^x. Putting the steps together, we arrive at

$$\mathbb{E}_{\mathcal{F}} \left\| (T_f \otimes \mathcal{I})(\omega_{XE}) - \frac{1}{|K|} \tau_K \otimes \omega_E \right\| \leq \sqrt{|K| \cdot 2^{-\mathrm{H}_{\min}(X|E)_\omega}} \, . \tag{122}$$

□

Data compression with quantum side information. We consider a classical random variable X correlated to a quantum state on a von Neumann algebra $\mathcal{M}_B$. This is modeled by a classical quantum state $\omega_{XB} \in \mathcal{S}(\ell_X^\infty \otimes \mathcal{M}_B)$. A one-way classical communication protocol to transmit X from Alice to Bob consists of a classical encoding map $\mathcal{E} : \ell_C^\infty \to \ell_X^\infty$ on Alice's side, and a decoding map $\mathcal{D} : \ell_X^\infty \to \ell_C^\infty \otimes \mathcal{M}_B$ on Bob's side, where $\mathcal{E}$ and $\mathcal{D}$ are quantum channels. The classical alphabet C (code space) specifies the number of bits, $\log |C|$, that are transmitted. The pre-dual of the decoding map can be written as $\mathcal{D}_* = \{\mathcal{D}_*^c\}_{c\in C}$, where the map $\mathcal{D}_*^c$ onto the classical outcome X is described by a POVM $\{D_x^c\}_{x\in X}$. In the following every such protocol is specified by the triple $(\mathcal{E}, \mathcal{D}, C)$.

Definition 12. *Let X be a set of finite cardinality and $\omega_{XB} \in \mathcal{S}(\ell_X^\infty \otimes \mathcal{M}_B)$. The error probability of a protocol $(\mathcal{E}, \mathcal{D}, C)$ for ω_{XB} is defined as*

$$p_{\mathrm{err}}(\omega_{XB}; \mathcal{E}, \mathcal{D}) := 1 - \sum_x \omega_B^x (D_x^{\mathcal{E}_*(x)}) \, , \tag{123}$$

where $D_x^{\mathcal{E}_*(x)} = \sum_c (\mathcal{E}_*(x))_c D_x^c$.

The main result is the following quantification of the achievable error probability.

Proposition 22. *Let X be a set of cardinality $|X|$, $\omega_{XB} \in \mathcal{S}(\ell_X^\infty \otimes \mathcal{M}_B)$, 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*

$$p_{\mathrm{err}}(\omega_{XB}; \mathcal{E}, \mathcal{D}) \leq \sqrt{\frac{1}{|C|} \cdot 2^{\mathrm{H}_{\max}^\epsilon(X|B)_\omega + 3}} + 2\epsilon \, . \tag{124}$$

Our proof is along the line of the arguments for quantum side information modeled by finite-dimensional spaces [46, Theorem 1]. In particular, for the encoding we employ the property of a family of two-universal hash functions $\mathcal{F}$ as in (112). We show that the averaged error probability over a family of two-universal hash functions $\mathcal{F}$ is bounded as in (124), and 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 ω_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 to distinguish the ensemble $\{\omega_B^x\}_{x \in f^{-1}(c)}$ [53]. Adapted pretty good measurement means that we have to add $\epsilon \mathbb{1}$ ($\epsilon > 0$) to certain operators in order to take their inverse. Eventually, we take the limit $\epsilon \to 0$.

The error analysis in the finite-dimensional case is crucially based on an operator inequality from [54, 55], whereas we use the following generalization to von Neumann algebras.

Lemma 23. *[56, Proposition 1.1] Let $\phi, \eta \in \mathcal{S}_{\leq}(\mathcal{M})$, s_+ be the support projection onto the positive part of $\phi - \eta$, and $s_- = \mathbb{1} - s_+$. Then, we have*

$$\phi(s_-) + \eta(s_+) \leq \mathcal{F}_{\mathcal{M}}(\phi, \eta)^{\frac{1}{2}} . \tag{125}$$

V. DISCUSSION AND OUTLOOK

We generalized the smooth entropy formalism to von Neumann algebras and discussed various properties in this framework. We showed that the characterizations of privacy amplification and data compression in terms of the smooth conditional min- and max-entropy still hold. The results in this paper can be used to extend one-shot quantum information-theoretic tasks to more general quantum systems described by continuous variables and in particular fermionic and bosonic quantum fields. For example, by building on the results given here, we prove security of a squeezed state continuous variable quantum key distribution protocol [33, 42]. Since the smooth min- and max-entropy have also been used in thermodynamics (see, e.g., [57]), the generalization to the von Neumann algebra setting is also interesting from a physical perspective. Especially as quantum mechanical systems of interest in thermodynamics often possess an infinite number of degrees of freedom. One could also generalize the formalism for quantum side information to operator systems [58]. Operationally, this corresponds to a restriction of the actual measurements that are allowed to perform on the physical system. This restriction could be conducted at a fundamental level, by excluding the elements of the von Neumann algebra that are unphysical in the sense that they cannot be observed. For a task like data compression with quantum side information, this would allow to constraint the quantum measurements at the decoder.

ACKNOWLEDGMENTS

We thank Renato Renner for instructive discussions about privacy amplification. We would also like to thank Marco Tomamichel for many insightful discussions about the smooth entropy formalism, and for detailed feedback on the first version of this paper. We acknowledge discussions with Matthias Christandl, Reinhard F. Werner, Michael Walter, and Joseph M. Renes. We thank an anonymous reviewer for pointing out an error in the proof of Lemma 20 and a detailed explanation of how to fix it. MB and VBS are both grateful for the hospitality and the inspiring working environment at the Institute Mittag-Leffler in Djursholm, Sweden, where this work was started. Most of this work was done while MB was at ETH Zurich, and FF and VBS were at the University

of Hanover. MB acknowledges funding provided by the Institute for Quantum Information and Matter, an NSF Physics Frontiers Center (NFS Grant PHY-1125565) with support of the Gordon and Betty Moore Foundation (GBMF-12500028). Additional funding support was provided by the ARO grant for Research on Quantum Algorithms at the IQIM (W911NF-12-1-0521). FF acknowledges support from the Graduiertenkolleg 1463 of the Leibniz University Hanover and by the Japan Society for the Promotion of Science (JSPS) by KAKENHI grant No. 24-02793, and FF and VBS both acknowledge support by the BMBF project QUOREP as well as the DFG cluster of excellence QUEST.

[1] M. M. Wilde, *Quantum Information Theory* (Cambridge University Press, 2013).
[2] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information* (Cambridge University Press, 2000).
[3] R. Renner, *Security of Quantum Key Distribution*, Ph.D. thesis, ETH Zurich (2005), arXiv:0512258 [quant-ph].
[4] M. Tomamichel, *Quantum Information Processing with Finite Resources — Mathematical Foundations* (Springer, 2015).
[5] R. Haag, *Local Quantum Physics: Fiels, Particles, Algebras* (Springer, 1992).
[6] D. Ruelle, *Statistical Mechanics: Rigorous Results* (World Scientific, 1999).
[7] A. Rényi, Proceedings of the 4th Berkeley Symposium on Mathematics, Statistics and Probability , 547 (1960).
[8] C. E. Shannon, Bell System Technical Journal **27**, 379 (1948).
[9] J. von Neumann, *Mathematische Grundlagen der Quantenmechanik* (Springer, 1932).
[10] H. Umegaki, Kodai Math. Sem. Rep. **14**, 59 (1962).
[11] M. Ohya and D. Petz, *Quantum Entropy and Its Use* (Springer, 1993).
[12] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. on Inf. Theory **55**, 5840 (2009).
[13] C. Weedbrook, S. Pirandola, R. García-Patrón, N. Cerf, T. Ralph, J. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[14] F. Furrer, J. Aberg, and R. Renner, Commun. Math. Phys. **306**, 165 (2011).
[15] H. Araki and E. J. Woods, Publications Research Institute for Mathematical Science Series A **4**, 51 (1968).
[16] O. Bratteli and D. W. Robinson, *Operator Algebras and Quantum Statistical Mechanics 1-2* (Springer, 1981).
[17] M. Takesaki, *Theory of Operator Algebras* (Springer, 2002).
[18] R. V. Kadison and J. R. Ringrose, *Fundamentals of the Theory of Operator Algebras: Advanced theory*, Fundamentals of the Theory of Operator Algebras (Academic Press, 1986).
[19] I. M. Gelfand and M. A. Naimark, Mat. Sbornik **12**, 197 (1943).
[20] I. E. Segal, Bull. Am. Math. Soc. **53**, 73 (1947).
[21] E. B. Davies, *Quantum theory of open systems* (London, New York : Academic Press, 1976).
[22] V. I. Paulsen, *Completely bounded maps and operator algebras* (Cambridge University Press, 2002).
[23] S. L. Woronowicz, Communications in Mathematical Physics **78**, 221 (1972).
[24] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. on Inf. Theory **56**, 4674 (2010).
[25] R. König, R. Renner, and C. Schaffner, IEEE Trans. on Inf. Theory **55**, 4337 (2009).
[26] D. Bures, Trans. Amer. Math. Soc. **135**, 199 (1969).
[27] A. Uhlmann, Report on Mathematical Physics **9**, 273 (1976).
[28] P. M. Alberti, Letters in Mathematical Physics **7**, 25 (1983).
[29] N. Datta, IEEE Trans. on Inf. Theory **55**, 2816 (2009).
[30] V. I. Paulsen and M. Tomforde, Indiana University Mathematics Journal **58**, 1319 (2009).
[31] L. M. Schmitt and G. Wittstock, Math. Scand. **51**, 241 (1982).
[32] W. F. Stinespring, Proc. Am. Math. Soc. **6**, 211 (1955).
[33] F. Furrer, M. Berta, M. Tomamichel, V. B. Scholz, and M. Christandl, J. Math. Phys. **55**, 122205 (2014).

[34] J. M. Renes and R. Renner, IEEE Trans. on Inf. Theory **58**, 1985 (2012).
[35] S. Wehner and A. Winter, New J. Phys. **12**, 025009 (2010).
[36] I. Bialynicki-Birula and L. Rudnicki, in *Statistical Complexity*, edited by K. Sen (Springer Netherlands, Dordrecht, 2011) pp. 1–34.
[37] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nat. Phys. **6**, 659 (2010).
[38] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).
[39] P. J. Coles, R. Colbeck, L. Yu, and M. Zwolak, Phys. Rev. Lett. **108**, 210405 (2012).
[40] R. L. Frank and E. H. Lieb, Commun. Math. Phys. **323**, 487 (2013).
[41] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nat. Commun. **3**, 634 (2012).
[42] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Phys. Rev. Lett. **109**, 100502 (2012).
[43] M. Berta, O. Fawzi, and S. Wehner, in *Proc. CRYPTO*, LNCS, Vol. 7417, edited by R. Safavi-Naini and R. Canetti (Springer Berlin Heidelberg, 2012) pp. 776–793.
[44] F. Dupuis, O. Fawzi, and S. Wehner, in *Proc. CRYPTO*, LNCS, Vol. 8043, edited by R. Canetti and J. A. Garay (Springer, 2013) pp. 326–343.
[45] W. B. Arveson, Acta Mathematica **123**, 141 (1969).
[46] J. M. Renes, Proc. Roy. Soc. A **467**, 1604 (2010).
[47] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, IEEE Trans. on Inf. Theory **57**, 5524 (2011).
[48] J. L. Carter and M. N. Wegman, J. Comp. Syst. Sci. **18**, 143 (1979).
[49] M. N. Wegman and J. L. Carter, J. Comp. Syst. Sci. **22**, 265 (1981).
[50] C. H. Bennett, G. Brassard, and J.-M. Robert, SIAM J. on Comput. **17**, 210 (1988).
[51] R. Impagliazzo, L. A. Levin, and M. Luby, Proceedings of 21st Annual ACM Symposium on Theory of Computing , 12 (1989).
[52] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, IEEE Trans. on Inf. Theory **41**, 1915 (1995).
[53] P. Hausladen and W. K. Wootters, Journal of Modern Optics **41**, 2385 (1994).
[54] M. Hayashi and H. Nagaoka, IEEE Trans. on Inf. Theory **49**, 1753 (2003).
[55] K. M. R. Audenaert, J. Calsamiglia, R. Muñoz Tapia, E. Bagan, L. Masanes, A. Acin, and F. Verstraete, Phys. Rev. Lett. **98**, 160501 (2007).
[56] Y. Ogata, Letters in Mathematical Physics **97**, 0377 (2011).
[57] L. del Rio, J. Aberg, R. Renner, O. Dahlsten, and V. Vedral, Nature **474**, 61 (2011).
[58] V. I. Paulsen, I. G. Todorov, and M. Tomforde, Proceedings of the London Mathematical Society **102**, 25 (2011).