Commun. Math. Phys. 306, 165–186 (2011)
Digital Object Identifier (DOI) 10.1007/s00220-011-1282-1

Communications in
Mathematical
Physics

Min- and Max-Entropy in Infinite Dimensions

Fabian Furrer[1], **Johan Åberg**[2], **Renato Renner**[2]

[1] Institute for Theoretical Physics, Leibniz Universität Hannover, 30167 Hannover, Germany.
E-mail: fabian.furrer@itp.uni-hannover.de
[2] Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland.
E-mail: jaaberg@phys.ethz.ch; renner@phys.ethz.ch

Received: 10 June 2010 / Accepted: 1 February 2011
Published online: 25 June 2011 –

Abstract: We consider an extension of the conditional min- and max-entropies to infinite-dimensional separable Hilbert spaces. We show that these satisfy characterizing properties known from the finite-dimensional case, and retain information-theoretic operational interpretations, e.g., the min-entropy as maximum achievable quantum correlation, and the max-entropy as decoupling accuracy. We furthermore generalize the smoothed versions of these entropies and prove an infinite-dimensional quantum asymptotic equipartition property. To facilitate these generalizations we show that the min- and max-entropy can be expressed in terms of convergent sequences of finite-dimensional min- and max-entropies, which provides a convenient technique to extend proofs from the finite to the infinite-dimensional setting.

1. Introduction

Entropy measures are fundamental to information theory. For example, in classical information theory a central role is played by the Shannon entropy [1] and in quantum information theory by the von Neumann entropy. Their usefulness partially stems from the fact that they have several convenient mathematical properties (e.g. strong subadditivity) that facilitate a 'calculus' of information and uncertainty. Indeed, entropy measures can even be characterized axiomatically in terms of such properties [2]. However, equally important for their use in information theory is the fact that they are related to operational quantities. This means that they characterize the optimal efficiency by which various information-theoretic tasks can be solved. One example of such a task is source coding, where one considers a source that randomly outputs data according to some given probability distribution. The question of interest is how much memory is needed in order to store and faithfully regenerate the data. Another example is channel coding, where the aim is to reliably transmit information over a channel. Here we ask how many bits (or qubits in the quantum case) one can optimally transmit per use of the channel [1,3,4].

The operational relevance of Shannon and von Neumann entropy is normally limited to the case when one considers the asymptotic limit over infinitely many instances of a random experiment, which are independent and identically distributed (iid) or can be described by a Markov process. In the case of source coding this corresponds to assuming an iid repetition of the source. In the limit of infinitely many such repetitions, the average number of bits one needs to store per output is given by the Shannon entropy of the distribution of the source [1]. In the general case, where we have more complicated types of correlations, or where we only consider finite instances, the role of the Shannon or von Neumann entropies appears to be taken over by other measures of entropy, referred to as the smooth min- and max-entropies [5]. For example, in [6,7] it was found that the smooth max-entropy characterizes one-shot data compression, i.e., when we wish to compress a single output of an information source. Furthermore, in [8] it was proved that in one single use of a classical channel, the transmission can be characterized by the difference between a smooth min- and max-entropy. The von Neumann entropy of a state can be regained via the quantum asymptotic equipartition property (AEP) [5,9], by applying these measures to asymptotically many iid repetitions of the state. This allows us to derive properties of the von Neumann entropy from the smooth min- and max-entropies, a technique that has been used for an alternative proof of the quantum reverse Shannon theorem [10], and to derive an entropic uncertainty relation [11]. The min- and max-entropies furthermore generalize the spectral entropy rates [12] (that are defined in an asymptotic sense) which themselves have been introduced as generalizations of the Shannon entropy [13,14]. Closely related quantities are the relative min- and max-entropies [15], which have been applied to entanglement theory [16,17] as well as channel capacity [18].

So far, the investigations of the operational relevance and properties of the min- and max-entropy and their smoothed versions have been almost exclusively focused on quantum systems with finite-dimensional Hilbert spaces. Here we consider the min- and max-entropy in infinite-dimensional separable Hilbert spaces. Since the modeling in vast parts of quantum physics is firmly rooted in infinite-dimensional Hilbert spaces, it appears that such a generalization is crucial for the application of these tools. For example, it has recently been shown that the smooth min- and max-entropies are the relevant measures of entropy in certain statistical mechanics settings [19,20]. An extension of these ideas to, e.g., quantized classical systems, would require an infinite-dimensional version of the min- and max-entropy. Another example is quantum key distribution (QKD), where in the finite-dimensional case the smooth min-entropy bounds the length of the secure key that can be extracted from an initial raw key [5]. The generalization to infinite dimensions has therefore direct relevance for continuous variable QKD (for references see, e.g., Sect. II.D. 3 of [21]). In such a scheme one uses the quadratures of the electromagnetic field to establish a secret key (as opposed to other schemes that use, e.g., the polarization degree of freedom of single photons). Since such QKD methods are based on the generation of coherent states and measurement of quadratures, it appears rather unavoidable to use infinite-dimensional Hilbert spaces to model the states of the field modes. Beyond the obvious application to continuous variable quantum key distribution, one can argue that there are several quantum cryptographic tasks that today are analyzed in finite-dimensional settings, which strictly speaking would require an analysis in infinite-dimensions, since there is in general no reason to assume the Hilbert spaces of the adversary's systems to be finite.

As indicated by the above discussion, an extension of the min- and max-entropies to an infinite-dimensional setting does not only require that we can reproduce known mathematical properties of these measures, but also that we should retain their operational

interpretations. A complete study of this two-fold goal would bring us far beyond the scope of this work. However, here we pave the way for this development by introducing an infinite-dimensional generalization of the min- and max-entropy, and demonstrating a collection of 'core' properties and operational interpretations. In particular, we derive (under conditions detailed below) a quantum AEP for a specific choice of an infinite-dimensional conditional von Neumann entropy. On a more practical level we introduce a technique that facilitates the extension of results proved for the finite-dimensional case to the setting of separable Hilbert spaces. More precisely, we show that the conditional min- and max-entropies for infinite-dimensional states can be expressed as limits of entropies obtained by finite-dimensional truncations of the original state (Proposition 1). This turns out to be a convenient tool for generalizations, and we illustrate this on the various infinite-dimensional extensions that we consider.

The ϵ-smoothed min-and max-entropies are defined in terms of the 'un-smoothed' ($\epsilon = 0$) min- and max-entropies (which we simply refer to as 'min- and max-entropy'). In Sect. 2.1 we extend these 'plain' min- and max-entropies to separable Hilbert spaces. Section 2.2 contains the main technical tool, Proposition 1, by which the infinite-dimensional min- and max-entropies can be expressed as limits of sequences of finite-dimensional entropies. The proof of Proposition 1 is given in Appendix B. In Sect. 3 we consider properties of the min- and max-entropy, e.g., additivity and the data processing inequality. Section 4 focuses on the generalization of operational interpretations. In Sect. 5 we consider the extension of the ϵ-smooth min- and max-entropies, for $\epsilon > 0$. In Sect. 6 we bound the smooth min- and max-entropy of an iid state on a system A conditioned on a system B in terms of the conditional von Neumann entropy (Proposition 8). This result relies on the assumption that A has finite von Neumann entropy. If A furthermore has a finite-dimensional Hilbert space (but the Hilbert space of B is allowed to be separable) we prove that these smooth entropies converge to the conditional von Neumann entropy (Corollary 1), which corresponds to a quantum AEP. The paper ends with a short summary and outlook in Sect. 7.

2. Min- and Max-Entropy

2.1. Definition of the conditional min- and max-entropy. Associated to each quantum system is a Hilbert space H, which we assume to be separable in all that follows. We denote the bounded operators by $\mathcal{L}(H) = \{A : H \to H \mid \|A\| < \infty\}$, where $\|A\| = \sup_{\||\psi\rangle\|=1} \|A|\psi\rangle\|$ is the standard operator norm. Among these, the trace class operators satisfy the additional feature of having a finite trace norm $\|T\|_1 := \operatorname{tr}|T| = \operatorname{tr}\sqrt{T^\dagger T}$. The set of trace class operators is denoted by $\tau_1(H) := \{T \in \mathcal{L}(H) \mid \|T\|_1 < \infty\}$.

We consider states which can be represented as density operators, i.e., normal states [22], and denote the set of all these states as $\mathcal{S}(H) := \{\rho \in \tau_1(H) \mid \rho \geq 0, \|\rho\|_1 = 1\}$. It is often convenient to allow non-normalized density operators, which form the positive cone $\tau_1^+(H) \subset \tau_1(H)$ consisting of all non-negative trace class operators.

We define the conditional min- and max-entropy of bipartite quantum systems analogously to the finite-dimensional case [23].[1]

Definition 1. *Let H_A and H_B be separable Hilbert spaces and $\rho_{AB} \in \tau_1^+(H_A \otimes H_B)$. The min-entropy of ρ_{AB} conditioned on $\sigma_B \in \tau_1^+(H_B)$ is defined by*

$$H_{\min}(\rho_{AB}|\sigma_B) := -\log \inf\{\lambda \in \mathbb{R} | \lambda \operatorname{id}_A \otimes \sigma_B \geq \rho_{AB}\}, \tag{1}$$

[1] Max-entropy as we define it in Eq. (3) is related to the Rényi 1/2-entropy (see Sect. 3.2 or [23,24]). In the original definition [5] max-entropy was defined in terms of the Rényi 0-entropy.

where we let $H_{\min}(\rho_{AB}|\sigma_B) := -\infty$ *if the condition* $\lambda \,\mathrm{id}_A \otimes \sigma_B \geq \rho_{AB}$ *cannot be satisfied for any* $\lambda \in \mathbb{R}$. *Moreover, we define the min-entropy of* ρ_{AB} *conditioned on B by*

$$H_{\min}(\rho_{AB}|B) := \sup_{\sigma_B \in \mathcal{S}(H_B)} H_{\min}(\rho_{AB}|\sigma_B). \tag{2}$$

The max-entropy of ρ_{AB} *conditioned on B is defined as the dual of the min-entropy*

$$H_{\max}(\rho_{AB}|B) := -H_{\min}(\rho_{AC}|C), \tag{3}$$

where ρ_{ABC} *is a purification of* ρ_{AB}.

In the definition above, and in all that follows, we let "log" denote the binary logarithm. The reduction of a state to a subsystem is indicated by the labels of the Hilbert space, e.g., $\rho_A = \mathrm{tr}_C\, \rho_{AC}$. Note that the max-entropy $H_{\max}(\rho_{AB}|B)$ as defined in (3) is independent of the choice of the purification ρ_{ABC}, and thus well-defined. This follows from the fact that two purifications can only differ by a partial isometry on the purifying system, and the min-entropy $H_{\min}(\rho_{AC}|C)$ is invariant under these partial isometries on subsystem C.

The two optimizations in the definition of $H_{\min}(\rho_{AB}|B)$, in Eqs. (1) and (2), can be combined into

$$H_{\min}(\rho_{AB}|B) = -\log\left(\inf\{\mathrm{tr}\,\tilde{\sigma}_B \mid \tilde{\sigma}_B \in \tau_1^+(H_B), \mathrm{id}_A \otimes \tilde{\sigma}_B \geq \rho_{AB}\}\right). \tag{4}$$

For convenience we introduce the following two quantities:

$$\Lambda(\rho_{AB}|\sigma_B) := 2^{-H_{\min}(\rho_{AB}|\sigma_B)} = \inf\{\lambda \in \mathbb{R} | \lambda \,\mathrm{id}_A \otimes \sigma_B \geq \rho_{AB}\}, \tag{5}$$

$$\Lambda(\rho_{AB}|B) := 2^{-H_{\min}(\rho_{AB}|B)} = \inf\{\mathrm{tr}\,\tilde{\sigma}_B \mid \tilde{\sigma}_B \in \tau_1^+(H_B), \mathrm{id}_A \otimes \tilde{\sigma}_B \geq \rho_{AB}\}. \tag{6}$$

2.2. Finite-dimensional approximations of min- and max-entropies. In this section we present the main result, Proposition 1, that provides a method to express the conditional min- and max-entropy as a limit of min- and max-entropies of finite-dimensional systems. The rough idea is to choose sequences $\{P_k^A\}_{k=1}^{\infty}$ and $\{P_k^B\}_{k=1}^{\infty}$ of projectors[2] onto finite-dimensional subspaces $U_k^A \subset H_A$ and $U_k^B \subset H_B$, respectively, both converging to the identity. Then we define a sequence of non-normalized states as $\rho_{AB}^k = (P_k^A \otimes P_k^B)\rho_{AB}(P_k^A \otimes P_k^B)$. The min- or max-entropy of ρ_{AB}^k can now be treated as if the underlying Hilbert space would be $U_k^A \otimes U_k^B$ (Lemma 8), and therefore finite-dimensional. Proposition 1 shows that, as $k \to \infty$, these finite-dimensional entropies approach the desired infinite-dimensional entropy. As we will see, this provides a convenient method to extend properties from the finite to the infinite setting.

When we say that an operator sequence Q_k converges to Q in the weak operator topology we intend that $\lim_{k\to 0}\langle\chi|Q - Q_k|\psi\rangle = 0$ for all $|\chi\rangle, |\psi\rangle \in H$. The sequence converges in the strong operator topology if $\lim_{k\to 0} \|(Q-Q_k)|\psi\rangle\| = 0$ for all $|\psi\rangle \in H$.

Definition 2. *Let* $\{P_k^A\}_{k\in\mathbb{N}} \subset \mathcal{L}(H_A)$, $\{P_k^B\}_{k\in\mathbb{N}} \subset \mathcal{L}(H_B)$ *be sequences of projectors such that for each* $k \in \mathbb{N}$ *the projection spaces* $U_k^A \subset H_A, U_k^B \subset H_B$ *of* P_k^A, P_k^B *are finite-dimensional,* $P_k^A \leq P_{k'}^A$ *and* $P_k^B \leq P_{k'}^B$ *for all* $k \leq k'$, *and* P_k^A, P_k^B *converge in*

[2] With "projector" we intend a bounded operator P such that $P^2 = P$ and $P^\dagger = P$, which in the mathematics literature usually is referred to as an "orthogonal projector".

the weak operator topology to the identity. We refer to such a sequence (P_k^A, P_k^B) *as a generator of projected states. For* $\rho_{AB} \in \mathcal{S}(H_A \otimes H_B)$ *we define the (non-normalized) states*

$$\rho_{AB}^k := (P_k^A \otimes P_k^B)\rho_{AB}(P_k^A \otimes P_k^B), \tag{7}$$

which we call the projected states of ρ_{AB} *relative to* (P_k^A, P_k^B)*. Moreover, we refer to*

$$\hat{\rho}_{AB}^k := \frac{\rho_{AB}^k}{\operatorname{tr} \rho_{AB}^k} \tag{8}$$

as the normalized projected states of ρ_{AB} *relative to* (P_k^A, P_k^B)*.*

Note that a sequence of projectors that converges in the weak operator topology to the identity also converges in the strong operator topology to the identity. As a matter of convenience, we can thus in all that follows regard the generators of projected states to converge in the strong operator topology. One may also note that the sequence of projected states ρ_{AB}^k (as well as the normalized projected states $\hat{\rho}_{AB}^k$) converges to ρ_{AB} in the trace norm (see Corollary 2 in Appendix A). The normalized projected states in Eq. (8) are of course only defined if $\operatorname{tr} \rho_{AB}^k \neq 0$. However, this is true for all sufficiently large k due to the trace norm convergence to ρ_{AB}.

Proposition 1. *For* $\rho_{AB} \in \mathcal{S}(H_A \otimes H_B)$*, let* $\{\rho_{AB}^k\}_{k\in\mathbb{N}}$ *be the projected states of* ρ_{AB} *relative to a generator* (P_k^A, P_k^B)*, and* $\hat{\rho}_{AB}^k$ *the corresponding normalized projected states. Furthermore, let* $\sigma_B \in \mathcal{S}(H_B)$ *and define the operators* $\sigma_B^k := P_k^B \sigma_B P_k^B$ *and* $\hat{\sigma}_B^k := \operatorname{tr}(\sigma_B^k)^{-1}\sigma_B^k$*. Then, the following three statements hold*:

$$H_{\min}(\rho_{AB}|\sigma_B) = \lim_{k\to\infty} H_{\min}(\rho_{AB}^k|\sigma_B^k) = \lim_{k\to\infty} H_{\min}\left(\hat{\rho}_{AB}^k|\hat{\sigma}_B^k\right), \tag{9}$$

and the infimum in Eq. (1) *is attained if* $H_{\min}(\rho_{AB}|\sigma_B)$ *is finite.*

$$H_{\min}(\rho_{AB}|B) = \lim_{k\to\infty} H_{\min}(\rho_{AB}^k|B_k) = \lim_{k\to\infty} H_{\min}\left(\hat{\rho}_{AB}^k|B_k\right), \tag{10}$$

and the supremum in Eq. (2) *is attained if* $H_{\min}(\rho_{AB}|B)$ *is finite.*

$$H_{\max}(\rho_{AB}|B) = \lim_{k\to\infty} H_{\max}(\rho_{AB}^k|B_k) = \lim_{k\to\infty} H_{\max}\left(\hat{\rho}_{AB}^k|B_k\right). \tag{11}$$

Here, B_k *denotes the restriction of system* B *to the projection space* U_k^B *of* P_k^B*.*

The proof of this proposition is found in Appendix B. When we say that the infimum in (1) is attained, it means that there exists a finite λ' such that $\lambda' \operatorname{id}_A \otimes \sigma_B - \rho_{AB} \geq 0$ and $H_{\min}(\rho_{AB}|\sigma_B) = -\log \lambda'$. Similarly, that the supremum in (2) is attained, means that there exists a $\sigma_B' \in \tau_1^+(H_B)$ satisfying $\operatorname{id} \otimes \sigma_B' \geq \rho_{AB}$ such that $H_{\min}(\rho_{AB}|B) = H_{\min}(\rho_{AB}|\sigma_B')$.

Given the above proposition, a natural question is if $H_{\min}(\rho_{AB}|B)$ and $H_{\max}(\rho_{AB}|B)$ are trace norm continuous in general. In the finite-dimensional case [24] it is known that these entropies are continuous with a Lipschitz constant depending on the dimension of H_A. However, the following example shows that they are in general not continuous in

the infinite-dimensional case. Let $\{|k\rangle\}_{k=0,1,\ldots}$ be an arbitrary orthonormal basis of the Hilbert space H_A. For each $n = 1, 2, \ldots$ let

$$\rho_n = (1 - \frac{1}{n})|0\rangle\langle 0| + \frac{1}{n^2}\sum_{k=1}^{n}|k\rangle\langle k|. \tag{12}$$

One can see that ρ_n converges in the trace norm to $|0\rangle\langle 0|$ as $n \to \infty$, while $\lim_{n\to\infty} H_{\max}(\rho_n) = 2$, and $H_{\max}(|0\rangle\langle 0|) = 0$. Hence, the max-entropy is not continuous. ($H_{\max}(\rho)$ without conditioning means that we condition on a trivial subsystem B. See Eq. (19).) The duality, Eq. (3), yields an example also for the min-entropy.

3. Properties of Min- and Max-Entropy

3.1. Additivity and the data processing inequality. Proposition 1 can be used as a tool to generalize known finite-dimensional results to the infinite-dimensional case. A simple example is the ordering property [9]

$$H_{\min}(\rho_{AB}|B) \leq H_{\max}(\rho_{AB}|B), \tag{13}$$

which is obtained by a direct application of Proposition 1. Another example is the additivity, which in the finite-dimensional case was proved in [5]. A direct generalization of the proof techniques they employed appears rather challenging, while Proposition 1 makes the generalization straightforward.

Proposition 2. *Let $\rho_{AB} \in \mathcal{S}(H_A \otimes H_B)$ and $\rho_{A'B'} \in \mathcal{S}(H_{A'} \otimes H_{B'})$ for H_A, $H_{A'}$, H_B, and $H_{B'}$ separable Hilbert spaces. Then, it follows that*

$$H_{\min}(\rho_{AB} \otimes \rho_{A'B'}|BB') = H_{\min}(\rho_{AB}|B) + H_{\min}(\rho_{A'B'}|B'), \tag{14}$$
$$H_{\max}(\rho_{AB} \otimes \rho_{A'B'}|BB') = H_{\max}(\rho_{AB}|B) + H_{\max}(\rho_{A'B'}|B'). \tag{15}$$

The proof is a simple application of the approximation scheme in Proposition 1 combined with Lemma 6 and the finite-dimensional version of Proposition 2, and therefore omitted.

For the sake of completeness we note that the data processing inequalities [5] also hold in the infinite-dimensional setting. In this case, however, there is no need to resort to Proposition 1, as the proof in [5] can be generalized directly.

Proposition 3. *Let $\rho_{ABC} \in \tau_+(H_A \otimes H_B \otimes H_C)$ for separable Hilbert spaces H_A, H_B and H_C. Then, it follows that*

$$H_{\min}(\rho_{ABC}|BC) \leq H_{\min}(\rho_{AB}|B), \tag{16}$$
$$H_{\max}(\rho_{ABC}|BC) \leq H_{\max}(\rho_{AB}|B). \tag{17}$$

The data processing inequalities can be regarded as the min- and max-entropy counterparts of the strong subadditivity of the von Neumann entropy (and are sometimes directly referred to as "strong subadditivity"). One reason for this is that the standard formulation of the strong subadditivity of von Neumann entropy [25–27], $H(\rho_{ABC}) + H(\rho_B) \leq H(\rho_{AB}) + H(\rho_{BC})$, can be recast in the same form.

3.2. Entropy of pure states, and a bound for general states. Here we briefly consider the fact that the min-entropy can take the value $-\infty$, and the max-entropy can take the value $+\infty$. For this purpose we discuss the special case of pure states, as well as the case of no conditioning (i.e., if there is no subsystem B). Based on this we obtain a general bound which says that the conditional min- and max-entropies of a state ρ_{AB} are finite if the operator $\sqrt{\rho_A}$ is trace class. Moreover it turns out that the min-entropy cannot attain the value $+\infty$, while the max-entropy cannot attain $-\infty$.

Lemma 1. *The min-entropy of $\rho_{AB} = |\psi\rangle\langle\psi|$, where $|\psi\rangle \in H_A \otimes H_B$, is given by*

$$H_{\min}(\rho_{AB}|B) = -2\log \operatorname{tr} \sqrt{\rho_A}. \tag{18}$$

From this lemma we can conclude that $H_{\min}(\rho_{AB}|B)$ is finite if and only if $\sqrt{\rho_A}$ is trace class. Otherwise $H_{\min}(\rho_{AB}|B) = -\infty$. If the Schmidt decomposition [28] of ψ is given by $\sum_{k=1}^{\infty} r_k |a_k\rangle|b_k\rangle$, we have $\operatorname{tr}\sqrt{\rho_A} = \sum_{k=1}^{\infty} r_k$, such that a finite Schmidt rank always implies that $H_{\min}(\rho_{AB}|B)$ is finite. Recall that the Schmidt coefficients characterize the entanglement of a pure state, and, roughly speaking, that the more uniformly the Schmidt coefficients are distributed the stronger is the entanglement (see for instance [28]). This suggests that pure states with $H_{\min}(\rho_{AB}|B) = -\infty$ are entangled in a rather strong sense.

Proof. Let $|\psi\rangle = \sum_{k=1}^{\infty} r_k |a_k\rangle|b_k\rangle$ be the Schmidt decomposition of $|\psi\rangle$, and $\tilde{\sigma}_B \in \tau_1^+(H_B)$ any operator that satisfies $\mathrm{id}_A \otimes \tilde{\sigma}_B \geq \rho_{AB}$. For each $n \in \mathbb{N}$ define $|\chi_n\rangle = \sum_{k=1}^{n} |a_k\rangle|b_k\rangle$. It follows that

$$\operatorname{tr}\tilde{\sigma}_B \geq \langle\chi_n|\,\mathrm{id}_A \otimes \tilde{\sigma}_B|\chi_n\rangle \geq \langle\chi_n|\rho_{AB}|\chi_n\rangle = \left(\sum_{k=1}^{n} r_k\right)^2,$$

and thus, by taking the infimum over all $\tilde{\sigma}_B$ with $\mathrm{id}_A \otimes \tilde{\sigma}_B \geq \rho_{AB}$, as well as the supremum over all n, we find $\Lambda(\rho_{AB}|B) \geq (\operatorname{tr}\sqrt{\rho_A})^2$. Especially, we see that if $\operatorname{tr}\sqrt{\rho_A} = +\infty$, then $\Lambda(\rho_{AB}|B) = +\infty$ (and thus $H_{\min}(\rho_{AB}|B) = -\infty$). In the following we assume that $\operatorname{tr}\sqrt{\rho_A} < +\infty$, i.e., $\sqrt{\rho_A} \in \tau_1^+(H_A)$. We show that the lower bound $\Lambda(\rho_{AB}|B) \geq (\operatorname{tr}\sqrt{\rho_A})^2$ is attained, by proving that $\tilde{\sigma}_B := \operatorname{tr}(\sqrt{\rho_A})\sqrt{\rho_B}$ satisfies $id_A \otimes \tilde{\sigma}_B \geq \rho_{AB}$. By using the Schmidt decomposition of ψ we compute for an arbitrary $\eta \in H_A \otimes H_B$,

$$\begin{aligned}\langle\eta|(\mathrm{id} \otimes \tilde{\sigma}_B - \rho_{AB})|\eta\rangle &= \operatorname{tr}(\sqrt{\rho_A}) \sum_{k,l=1}^{\infty} |c_{k,l}|^2 r_l - \left|\sum_{k=1}^{\infty} c_{k,k} r_k\right|^2 \\ &\geq \sum_{l=1}^{\infty} r_l \sum_{k=1}^{\infty} |c_{k,k}|^2 r_k - \left|\sum_{k=1}^{\infty} c_{k,k} r_k\right|^2 \geq 0,\end{aligned}$$

where $c_{k,l} = (\langle a_k|\langle b_l|)|\eta\rangle$, and the last step follows from the Cauchy-Schwarz inequality. Hence, $\mathrm{id}_A \otimes \tilde{\sigma}_B - \rho_{AB}$ is positive and therefore $\operatorname{tr}(\tilde{\sigma}_B) \geq \Lambda(\rho_{AB}|B)$. Combined with $\Lambda(\rho_{AB}|B) \geq (\operatorname{tr}\sqrt{\rho_A})^2$, we find $H_{\min}(\rho_{AB}|B) = -\log \Lambda(\rho_{AB}|B) = -2\log \operatorname{tr}\sqrt{\rho_A}$.

The duality (3) allows us to rewrite Lemma 1 by using the unconditional max-entropy. For every $\rho \in \mathcal{S}(H)$ this yields the quantum 1/2-Rényi entropy (cf. [23]),

$$H_{\max}(\rho) = 2\log \operatorname{tr}\sqrt{\rho} = H_{\frac{1}{2}}(\rho), \tag{19}$$

if $\sqrt{\rho}$ is trace-class. Otherwise $H_{\max}(\rho) = +\infty$.

The unconditional min-entropy is obtained by conditioning on a trivial subsystem B. One can see that

$$H_{\min}(\rho) = -\log \|\rho\|. \tag{20}$$

For a pure state $\rho_{AB} = |\psi\rangle\langle\psi| \in \mathcal{S}(H_A \otimes H_B)$, the max-entropy is given by

$$H_{\max}(\rho_{AB}|B) = \log \|\rho_A\|. \tag{21}$$

To see this one can apply the duality (3) where we purify the pure state ρ_{AB} with a trivial system C, and next use Eq. (20).

By combining these facts with the data processing inequality, $H_{\min}(\rho_{ABC}|BC) \leq H_{\min}(\rho_{AB}|B) \leq H_{\min}(\rho_A)$ and $H_{\max}(\rho_{ABC}|BC) \leq H_{\max}(\rho_{AB}|B) \leq H_{\max}(\rho_A)$, for ρ_{ABC} a purification of ρ_{AB}, we find the following bounds on the min- and max-entropy.

Proposition 4. *For every state $\rho_{AB} \in S(H_A \otimes H_B)$ it holds that*

$$-2\log \operatorname{tr} \sqrt{\rho_A} \leq H_{\min}(\rho_{AB}|B) \leq -\log \|\rho_A\|, \tag{22}$$

$$\log \|\rho_A\| \leq H_{\max}(\rho_{AB}|B) \leq 2\log \operatorname{tr} \sqrt{\rho_A}. \tag{23}$$

Hence, $H_{\min}(\rho_{AB}|B)$ and $H_{\max}(\rho_{AB}|B)$ are finite if $\sqrt{\rho_A}$ is trace-class.

4. Operational Interpretations of Min- and Max-Entropy

Min- and max-entropy can be regarded as answers to operational questions, i.e., they quantify the optimal solution to certain information-theoretic tasks. Max-entropy $H_{\max}(\rho_{AB}|B)$ answers the question of how distinguishable ρ_{AB} is from states that are maximally mixed on A, while uncorrelated with B [23] (see also Definition 3 below). This is a useful concept, e.g., in quantum key distribution, where one ideally would have a maximally random key uncorrelated with the eavesdropper's state. Thus, the above distinguishability quantifies how well this is achieved. Min-entropy $H_{\min}(\rho_{AB}|B)$ is related to the question of how close one can bring the state ρ_{AB} to a maximally entangled state on the bipartite system AB, allowing only local quantum operations on the B system [23]. In the special case that A is classical (i.e., we have a classical-quantum state, see Eq. (31) below) one finds that $H_{\min}(\rho_{AB}|B)$ is related to the guessing probability, i.e., our best chance to correctly guess the value of the classical system A, given the quantum system B. In the following sections we show that these results can be generalized to the case that H_B is infinite-dimensional. These generalizations are for instance crucial in cryptographic settings, where there is a priori no reason to expect an eavesdropper to be limited to a finite-dimensional Hilbert space, while it is reasonable to assume the key to be finite. The operational interpretations of the min- and max-entropy exhibit a direct dependence on the dimension of the A system, which is why a naive generalization to an infinite-dimensional A appears challenging, and will not be considered here.

4.1. Max-entropy as decoupling accuracy. To define decoupling accuracy we use fidelity $F(\rho, \sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1$ as a distance measure between states.

Definition 3. *For a finite-dimensional Hilbert space H_A and an arbitrary separable Hilbert space H_B, we define the decoupling accuracy of $\rho_{AB} \in \tau_1^+(H_A \otimes H_B)$ w.r.t. the system B as*

$$d(\rho_{AB}|B) := \sup_{\sigma_B \in \mathcal{S}(H_B)} d_A F(\rho_{AB}, \tau_A \otimes \sigma_B)^2. \tag{24}$$

Here, d_A is the dimension of H_A, and $\tau_A := d_A^{-1}\,\mathrm{id}_A$ is the maximally mixed state on A.

Note that in infinite-dimensional Hilbert spaces there is no trace class operator which can be regarded as a generalization of the maximally mixed state in finite dimensions. We must thus require system A to be finite-dimensional in order to keep the decoupling accuracy well-defined. In [23], Proposition 5 was proved in the case where H_B is assumed to be finite-dimensional. Below we use Proposition 1 to extend the assertion to the infinite-dimensional case.

Proposition 5. *Let H_A be a finite-dimensional and H_B a separable Hilbert space. It follows that*

$$d(\rho_{AB}|B) = 2^{H_{\max}(\rho_{AB}|B)}, \tag{25}$$

for each $\rho_{AB} \in \tau_1^+(H_A \otimes H_B)$.

In the following we will need to consider physical operations (channels) on states, i.e., trace preserving completely positive maps [29]. By $\mathrm{TPCPM}(H_A, H_B)$ we denote the set of all trace preserving completely positive maps $\mathcal{E} : \tau_1(H_A) \to \tau_1(H_B)$. Let $\mathcal{I}$ denote the identity map.

Proof. Let us take projected states ρ_{AB}^k relative to a generator of the form (id_A, P_k^B) (this is a proper generator since $\dim H_A < \infty$). Denote the space onto which P_k^B projects by U_k^B and set $P_k := \mathrm{id}_A \otimes P_k^B$. The finite-dimensional version of Proposition 5 together with Proposition 1 yield $d(\rho_{AB}^k|B_k) = 2^{H_{\max}(\rho_{AB}^k|B_k)} \to 2^{H_{\max}(\rho_{AB}|B)}$, as $k \to \infty$.

In order to prove $d(\rho_{AB}|B) \leq 2^{H_{\max}(\rho_{AB}|B)}$ we construct a suitable TPCPM and use the fact that the fidelity can only increase under its action [30]. For each $k \in \mathbb{N}$ choose a normalized state $|\theta_k\rangle \in H_A \otimes H_B$ such that $P_k|\theta_k\rangle = 0$. We define a channel $\mathcal{E}_k \in \mathrm{TPCPM}(H_A \otimes H_B, H_A \otimes H_B)$ as $\mathcal{E}_k(\eta) = P_k \eta P_k + q_k(\eta)|\theta_k\rangle\langle\theta_k|$, with $q_k(\eta) := \mathrm{tr}[\eta(\mathrm{id} - P_k)]$. Then, for all $\sigma_B \in \mathcal{S}(H_B)$ we find

$$\begin{aligned} F(\rho_{AB}, \tau_A \otimes \sigma_B) &\leq F\left(\mathcal{E}_k(\rho_{AB}), \mathcal{E}_k(\tau_A \otimes \sigma_B)\right) \\ &= \left\| \sqrt{\rho_{AB}^k}\sqrt{\tau_A \otimes \sigma_B^k} + \sqrt{q_k(\rho_{AB}) q_k(\tau_A \otimes \sigma_B)}|\theta_k\rangle\langle\theta_k| \right\|_1 \\ &\leq \left\| \sqrt{\rho_{AB}^k}\sqrt{\tau_A \otimes \sigma_B^k} \right\|_1 + \sqrt{q_k(\rho_{AB})} = F(\rho_{AB}^k, \tau_A \otimes \sigma_B^k) + \sqrt{q_k(\rho_{AB})}, \end{aligned}$$

where $\sigma_B^k := P_k^B \sigma_B P_k^B$. The second line is due to the fact that $|\theta_k\rangle$ is orthogonal to the support of both ρ_{AB}^k and $\tau_A \otimes \sigma_B^k$. The last line follows by the triangle inequality and $q_k(\tau_A \otimes \sigma_B) \leq 1$. By taking the supremum over all $\sigma_B \in \mathcal{S}(H_B)$ we obtain

$$\sqrt{d(\rho_{AB}|B)} \leq \sqrt{d(\rho_{AB}^k|B_k)} + \sqrt{d_A\,\mathrm{tr}[\rho_{AB}(\mathrm{id} - P_k)]} \to 2^{\frac{1}{2}H_{\max}(\rho_{AB}|B)},$$

as $k \to \infty$. It remains to show $d(\rho_{AB}|B) \geq 2^{H_{\max}(\rho_{AB}|B)}$. For this purpose we use that the fidelity can be reformulated as

$$F(\rho, \sigma) = \sup_{|\phi\rangle} F(|\psi\rangle, |\phi\rangle), \tag{26}$$

where $|\psi\rangle$ is a purification of ρ, and the supremum is taken over all purifications $|\phi\rangle$ of σ [31]. Let us fix an arbitrary $k \in \mathbb{N}$ and a $\sigma_B \in \mathcal{S}(H_B)$. Assume $|\psi_{ABC}\rangle$ to be a purification of ρ_{AB}, and note that $|\psi^k_{ABC}\rangle := \tilde{P}_k|\psi_{ABC}\rangle$, with $\tilde{P}_k = P_k \otimes \mathrm{id}_C$, is a purification of ρ^k_{AB}. Let $|\phi\rangle \in H_A \otimes H_B \otimes H_C$ be an arbitrary purification of $\tau_A \otimes \sigma_B$. According to (26) it follows that

$$\begin{aligned} F(\rho_{AB}, \tau_A \otimes \sigma_B) &\geq F(|\psi_{ABC}\rangle, |\phi\rangle) = |\langle\psi_{ABC}|\phi\rangle| \\ &= |\langle\psi_{ABC}|\tilde{P}_k|\phi\rangle + \langle\psi_{ABC}|\,\mathrm{id} - \tilde{P}_k|\phi\rangle| \\ &\geq |\langle\psi^k_{ABC}|\phi\rangle| - \|(\mathrm{id} - \tilde{P}_k)|\psi_{ABC}\rangle\|, \end{aligned}$$

where the last line is obtained by the reverse triangle inequality and the Cauchy-Schwarz inequality. By taking the supremum over all the purifications $|\phi\rangle$ of $\tau_A \otimes \sigma_B$ in the above inequality, Eq. (26) yields $F(\rho_{AB}, \tau_A \otimes \sigma_B) \geq F(\rho^k_{AB}, \tau_A \otimes \sigma_B) - \|(\mathrm{id} - \tilde{P}_k)|\psi_{ABC}\rangle\|$. As this holds for all $\sigma_B \in \mathcal{S}(H_B)$ and all k, we obtain with the definition of the decoupling accuracy:

$$d(\rho_{AB}|B) \geq \lim_{k\to\infty} \left(\sqrt{d(\rho^k_{AB}|B_k)} - \sqrt{d_A}\,\|(\mathrm{id} - \tilde{P}_k)|\psi_{ABC}\rangle\|\right)^2 = 2^{H_{\max}(\rho_{AB}|B)}.$$

4.2. Min-entropy as maximum achievable quantum correlation. Assume a bipartite quantum system consisting of a finite-dimensional A system and an arbitrary B system. We can then define a maximally entangled state between the A and B system as

$$|\Psi_{AB}\rangle := \frac{1}{\sqrt{d_A}} \sum_{k=1}^{d_A} |a_k\rangle|b_k\rangle. \tag{27}$$

Here, d_A denotes the dimension of H_A, $\{a_k\}_{k=1}^{d_A}$ an arbitrary orthonormal basis of H_A and $\{b_k\}_{k=1}^{d_A}$ an arbitrary orthonormal system in H_B, where we assume that $\dim(H_A) \leq \dim(H_B)$.

Definition 4. *For H_A a finite-dimensional and H_B a separable Hilbert space (with $\dim H_A \leq \dim H_B$), we define the quantum correlation of a state $\rho_{AB} \in \mathcal{S}(H_A \otimes H_B)$ relative to B as*

$$q(\rho_{AB}|B) := \sup_{\mathcal{E}} d_A F\left((\mathcal{I}_A \otimes \mathcal{E})\rho_{AB}, |\Psi_{AB}\rangle\langle\Psi_{AB}|\right)^2, \tag{28}$$

where the supremum is taken over all $\mathcal{E}$ in TPCPM(H_B, H_B), and $|\Psi_{AB}\rangle$ is given by (27).

Due to the invariance of the fidelity under unitaries [30], the definition of $q(\rho_{AB}|B)$ is independent of the choice of the maximally entangled state $|\Psi_{AB}\rangle$. The quantum correlation can be rewritten as

$$q(\rho_{AB}|B) = \sup_{\mathcal{E}} d_A \langle\Psi_{AB}|(\mathcal{I}_A \otimes \mathcal{E})\rho_{AB}|\Psi_{AB}\rangle. \tag{29}$$

The min-entropy is directly linked to the quantum correlation as shown in [23] for the finite-dimensional case. We extend this result to a B system with a separable Hilbert space.

Proposition 6. *Let H_A be a finite-dimensional and H_B be a separable Hilbert space. It follows that*

$$q(\rho_{AB}|B) = 2^{-H_{\min}(\rho_{AB}|B)}, \tag{30}$$

for each $\rho_{AB} \in \mathcal{S}(H_A \otimes H_B)$.

Proof. Let $\{\rho_{AB}^k\}_{k\in\mathbb{N}}$ be the projected states of ρ_{AB} relative to a generator of the form (id_A, P_k^B), and set $P_k := \mathrm{id}_A \otimes P_k^B$. Let us denote the projection space of P_k^B by U_k^B and assume that $|b_l\rangle \in U_k^B, l = 1, ..., d_A$, for all k, with $|b_l\rangle$ as in Eq. (27). By the already proved finite-dimensional version of Proposition 6 and Proposition 1, we obtain $q(\rho_{AB}^k|B_k) = \Lambda(\rho_{AB}^k|B_k) \to \Lambda(\rho_{AB}|B)$.

We begin to prove $\Lambda(\rho_{AB}|B) \leq q(\rho_{AB}|B)$. Fix k and choose $\mathcal{E}_k \in \mathrm{TPCPM}(U_k^B, U_k^B)$ such that $q(\rho_{AB}^k|B_k) = d_A\langle\Psi_{AB}|(\mathcal{I}_A \otimes \mathcal{E}_k)\rho_{AB}^k|\Psi_{AB}\rangle$. Define $\tilde{\mathcal{E}}_k(\rho) = \mathcal{E}_k(P_k\rho P_k) + (\mathrm{id}_B - P_k^B)\rho(\mathrm{id}_B - P_k^B)$, which is a valid quantum operation in $\mathrm{TPCPM}(H_B, H_B)$. As $\tilde{\mathcal{E}}_k$ is just one possible TPCPM, it follows that

$$q(\rho_{AB}|B) \geq d_A\langle\Psi_{AB}|(\mathcal{I}_A \otimes \tilde{\mathcal{E}}_k)\rho_{AB}|\Psi_{AB}\rangle \geq q(\rho_{AB}^k|B_k).$$

We thus find $q(\rho_{AB}|B) \geq \lim_{k\to\infty} q(\rho_{AB}^k|B_k) = \Lambda(\rho_{AB}|B)$.

We next prove $\Lambda(\rho_{AB}|B) \geq q(\rho_{AB}|B)$. Let $\mathcal{E}$ be an arbitrary $\mathrm{TPCPM}(H_B, H_B)$. As a special instance of Stinespring dilations we know that there exists an ancilla H_R together with an unitary $U_{BR} \in \mathcal{L}(H_B \otimes H_R)$ and a state $|\theta_R\rangle \in H_R$, such that $\mathcal{E}(\sigma_B) = \mathrm{tr}_R[U_{BR}(\sigma_B \otimes |\theta_R\rangle\langle\theta_R|)U_{BR}^\dagger]$ [29]. With $|\psi_{ABC}\rangle$ a purification of ρ_{AB}, it follows according to (26) that

$$\begin{aligned} F\left((\mathcal{I}_A \otimes \mathcal{E})\rho_{AB}, |\Psi_{AB}\rangle\langle\Psi_{AB}|\right) &= \sup_{\eta_{CR}} F\left((\mathrm{id} \otimes U_{BR})|\psi_{ABC}\rangle|\theta_R\rangle, |\Psi_{AB}\rangle|\eta_{CR}\rangle\right) \\ &\leq \sup_{\eta_{CR}} F\left(\rho_{AC}, \tau_A \otimes \mathrm{tr}_R(|\eta_{CR}\rangle\langle\eta_{CR}|)\right), \end{aligned}$$

where the last inequality is due to the monotonicity of fidelity under the partial trace and $\tau_A = d_A^{-1}\,\mathrm{id}_A = \mathrm{tr}_B(|\Psi_{AB}\rangle\langle\Psi_{AB}|)$. The optimization over all pure states η_{CR} can be replaced by the optimization over all density operators on H_C. Then, with Proposition 5 it follows that

$$\begin{aligned} d_A F((\mathcal{I}_A \otimes \mathcal{E})\rho_{AB}, |\Psi_{AB}\rangle\langle\Psi_{AB}|)^2 &\leq \sup_{\sigma_C} d_A F(\rho_{AC}, \tau_A \otimes \sigma_C)^2 = 2^{H_{\max}(\rho_{AC}|C)} \\ &= 2^{-H_{\min}(\rho_{AB}|B)} = \Lambda(\rho_{AB}|B). \end{aligned}$$

Since this holds for all $\mathcal{E} \in \mathrm{TPCPM}(H_B, H_B)$, we obtain $q(\rho_{AB}|B) \leq \Lambda(\rho_{AB}|B)$.

The quantum correlation and its relation to min-entropy applied to classical quantum states connects the min-entropy with the optimal guessing probability. Imagine a source that produces the quantum states $\rho_B^x \in \mathcal{S}(H_B)$ at random, according to the probability distribution $P_X(x)$. The average output is characterized by the classical-quantum state,

$$\rho_{XB} = \sum_{x\in X} P_X(x)|x\rangle\langle x| \otimes \rho_B^x, \tag{31}$$

where X denotes the (finite) alphabet of the classical system describing the source and $\{|x\rangle\}_{x\in X}$ is an orthonormal basis spanning H_X. We define the guessing probability $g(\rho_{XB}|B)$ as the probability to correctly guess x, permitting an optimal measurement strategy on subsystem B. Formally, this can be expressed as

$$g(\rho_{XB}|B) := \sup_{\{M_x\}} \sum_{x\in X} P_X(x)\,\mathrm{tr}(\rho_B^x M_x), \tag{32}$$

where the supremum is taken over all positive operator valued measures (POVM) on H_B. By POVM on H_B we intend a set $\{M_x\}_{x\in X}$ of positive operators which sum up to the identity. For finite-dimensional H_B it is known [23] that the guessing probability is linked to the min-entropy by

$$g(\rho_{XB}|B) = 2^{-H_{\min}(\rho_{XB}|B)}. \tag{33}$$

We will now use Proposition 6 to show that Eq. (33) also holds for separable H_B.

Let ρ_{XB} be a state as defined in Eq. (31), and construct the state $|\Psi_{XB}\rangle := |X|^{-1/2}\sum_{x\in X}|x\rangle|x_B\rangle$, where $\{|x_B\rangle\}_{x\in X}$ is an arbitrary orthonormal set in H_B. We now define $Q(\rho_{XB},\mathcal{E}) := d_A\langle\Psi_{XB}|(\mathcal{I}_X\otimes\mathcal{E})\rho_{XB}|\Psi_{XB}\rangle$ (cf. Eq. (29)) and $G(\rho_{XB},\{M_x\}) := \sum_{x\in X} P_X(x)\,\mathrm{tr}(\rho_B^x M_x)$ (cf. Eq. (32)). Then,

$$Q(\rho_{XB},\mathcal{E}) = \sum_{x\in X} P_X(x)\,\mathrm{tr}[\mathcal{E}^*(|x_B\rangle\langle x_B|)\rho_B^x], \tag{34}$$

where $\mathcal{E}^*$ denotes the adjoint operation of $\mathcal{E}$. Let $\{M_x\}$ be an arbitrary $|X|$-element POVM on H_B. One can see that the TPCPM $\mathcal{E}(\rho) := \sum_{x\in X}\mathrm{tr}(M_x\rho)|x_B\rangle\langle x_B|$ satisfies $\mathcal{E}^*(|x_B\rangle\langle x_B|) = M_x$. Thus, by Eq. (34), we find $Q(\rho_{XB},\mathcal{E}) = G(\rho_{XB},\{M_x\})$. Since the POVM was arbitrary, it follows that $q(\rho_{XB}|B) \geq g(\rho_{XB}|B)$.

Next, let $\mathcal{E}$ be an arbitrary TPCPM on H_B. Define $P = \sum_{x\in X}|x_B\rangle\langle x_B|$ and

$$M_x = \mathcal{E}^*(|x_B\rangle\langle x_B|) + \frac{1}{|X|}\mathcal{E}^*(\mathrm{id}_B - P), \quad x\in X.$$

One can verify that $\{M_x\}$ is a POVM on H_B. By using Eq. (34) we can see that $G(\rho_{XB},\{M_x\}) \geq Q(\rho_{XB},\mathcal{E})$. This implies $g(\rho_{XB}|B) \geq q(\rho_{XB}|B)$, and thus $g(\rho_{XB}|B) = q(\rho_{XB}|B)$.

5. Smooth Min- and Max-Entropy

The entropic quantities that usually appear in operational settings are the smooth min- and max-entropies [8,6,23]. They result from the non-smoothed versions by an optimization procedure over states close to the original state. The closeness is defined by an appropriate metric on the state space, and a smoothing parameter specifies the maximal distance to the original state. The choice of metric has varied in the literature, but here we follow [24].

By $\mathcal{S}_{\leq}(H)$ we denote the set of positive trace class operators with trace norm smaller than or equal to 1. We define the generalized fidelity on $\mathcal{S}_{\leq}(H)$ by $\bar{F}(\rho,\sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1 + \sqrt{(1-\mathrm{tr}\,\rho)(1-\mathrm{tr}\,\sigma)}$, which induces a metric on $\mathcal{S}_{\leq}(H)$ via

$$P(\rho,\sigma) := \sqrt{1-\bar{F}(\rho,\sigma)^2}, \tag{35}$$

referred to as the purified distance.

Definition 5. *For $\epsilon > 0$, we define the ϵ-smooth min- and max-entropy of $\rho_{AB} \in \mathcal{S}_{\leq}(H_A \otimes H_B)$ conditioned on B as*

$$H_{\min}^{\epsilon}(\rho_{AB}|B) := \sup_{\tilde{\rho}_{AB} \in \mathcal{B}^{\epsilon}(\rho_{AB})} H_{\min}(\tilde{\rho}_{AB}|B), \tag{36}$$

$$H_{\max}^{\epsilon}(\rho_{AB}|B) := \inf_{\tilde{\rho}_{AB} \in \mathcal{B}^{\epsilon}(\rho_{AB})} H_{\max}(\tilde{\rho}_{AB}|B), \tag{37}$$

where the smoothing set $\mathcal{B}^{\epsilon}(\rho_{AB})$ is defined with respect to the purified distance

$$\mathcal{B}^{\epsilon}(\rho_{AB}) := \{\tilde{\rho}_{AB} \in \mathcal{S}_{\leq}(H_A \otimes H_B) | P(\rho_{AB}, \tilde{\rho}_{AB}) \leq \epsilon\}. \tag{38}$$

Closely related to this particular choice of smoothing set is the invariance of the smooth entropies under (partial) isometries acting locally on each of the subsystems. This can be used to show the duality relation of the smooth entropies, namely, for all states ρ_{AB} on $H_A \otimes H_B$ it follows that

$$H_{\min}^{\epsilon}(\rho_{AB}|B) = -H_{\max}^{\epsilon}(\rho_{AC}|C), \tag{39}$$

where ρ_{ABC} is an arbitrary purification of ρ_{AB} on an ancilla H_C. A proof for the finite-dimensional case can be found in [24], which allows a straightforward modification to infinite dimensions.

A useful property of the smooth entropies is the data processing inequality.

Proposition 7. *Let be $\rho_{ABC} \in \mathcal{S}_{\leq}(H_A \otimes H_B \otimes H_C)$, then it follows that*

$$H_{\min}^{\epsilon}(\rho_{ABC}|BC) \leq H_{\min}^{\epsilon}(\rho_{AB}|B),$$
$$H_{\max}^{\epsilon}(\rho_{ABC}|BC) \leq H_{\max}^{\epsilon}(\rho_{AB}|B).$$

Proof. Using the data processing inequality for the min-entropy, Eq. (16), we obtain

$$H_{\min}^{\epsilon}(\rho_{ABC}|BC) = \sup_{\tilde{\rho}_{ABC} \in \mathcal{B}^{\epsilon}(\rho_{ABC})} H_{\min}(\tilde{\rho}_{ABC}|BC) \leq \sup_{\tilde{\rho}_{ABC} \in \mathcal{B}^{\epsilon}(\rho_{ABC})} H_{\min}(\mathrm{tr}_C\, \tilde{\rho}_{ABC}|B).$$

Thus, it is sufficient to show that $\mathrm{tr}_C(\mathcal{B}^{\epsilon}(\rho_{ABC})) \subseteq \mathcal{B}^{\epsilon}(\rho_{AB})$. But this follows directly from the fact that the purified distance does not increase under partial trace [24], i.e., $P(\rho_{ABC}, \tilde{\rho}_{ABC}) \geq P(\rho_{AB}, \tilde{\rho}_{AB})$.

The data processing inequality of the smooth max-entropy follows from the duality (39),

$$H_{\max}^{\epsilon}(\rho_{ABC}|BC) = -H_{\min}^{\epsilon}(\rho_{AD}|D) \leq -H_{\min}^{\epsilon}(\rho_{ACD}|CD) = H_{\max}^{\epsilon}(\rho_{AB}|B),$$

where ρ_{ABCD} is a purification of ρ_{ABC}.

6. An Infinite-Dimensional Quantum Asymptotic Equipartition Property

In the finite-dimensional case the quantum asymptotic equipartition property (AEP) says that the conditional von Neumann entropy can be regained as an asymptotic quantity from the conditional smooth min- and max-entropy [5,9]. (For a discussion on why the AEP can be formulated in terms of entropies, see [32].) More precisely, $\lim_{\epsilon \to 0} \lim_{n \to \infty} \frac{1}{n} H_{\min}^{\epsilon}(\rho_{AB}^{\otimes n}|B^n) = H(\rho_{AB}|B)$ and $\lim_{\epsilon \to 0} \lim_{n \to \infty} \frac{1}{n} H_{\max}^{\epsilon}(\rho_{AB}^{\otimes n}|B^n) = H(\rho_{AB}|B)$. For the infinite-dimensional case we derive an upper (lower) bound to the conditional von Neumann entropy in terms of the smooth

min-(max-)entropy. We then use these bounds to prove the above limits in the case where H_A is finite-dimensional. To this end we need a well defined notion of conditional von Neumann entropy in the infinite-dimensional case. Here we use the definition introduced in [33], which in turn is based on an infinite-dimensional extension of the relative entropy [34–37]. For $\rho, \sigma \in \tau_1^+(H)$ the relative entropy can be defined as

$$H(\rho\|\sigma) := \sum_{jk} |\langle a_j|b_k\rangle|^2 (a_j \log a_j - a_j \log b_k + b_k - a_j), \tag{40}$$

where $\{|a_j\rangle\}_j$ is an arbitrary orthonormal eigenbasis of ρ with corresponding eigenvalues a_j, and analogously for $\{|b_k\rangle\}_k$, b_k, and σ. The relative entropy is always positive, possibly $+\infty$, and equal to 0 if and only if $\rho = \sigma$ [35]. For states ρ_{AB} with $H(\rho_A) < +\infty$, the conditional von Neumann entropy can be defined as [33]

$$H(\rho_{AB}|B) := H(\rho_A) - H(\rho_{AB}\|\rho_A \otimes \rho_B). \tag{41}$$

For many applications it appears reasonable to assume $H(\rho_A)$ to be finite, e.g., in cryptographic settings it would correspond to restricting the states of the 'legitimate' users.

Similarly as for the min- and max-entropy, the conditional von Neumann entropy can be approximated by projected states [33], i.e., for $\rho_{AB} \in \mathcal{S}(H_A \otimes H_B)$ satisfying $H(\rho_A) < \infty$ with corresponding normalized projected states $\hat{\rho}_{AB}^k$ it follows that

$$\lim_{k\to\infty} H(\hat{\rho}_{AB}^k|B) = H(\rho_{AB}|B). \tag{42}$$

In the finite-dimensional case it has been shown [9] that the min-, max- and, von Neumann entropy can be ordered as

$$H_{\min}(\rho_{AB}|B) \leq H(\rho_{AB}|B) \leq H_{\max}(\rho_{AB}|B). \tag{43}$$

A direct application of Proposition 1 and (42) shows that this remains true in the infinite-dimensional case, if $H(\rho_A) < \infty$. Note, however, that the ordering between min- and max-entropy (13) does not hold for their smoothed versions.

Proposition 8. *Let $\rho_{AB} \in \mathcal{S}(H_A \otimes H_B)$ be such that $H(\rho_A) < \infty$. For any $\epsilon > 0$ it follows that*

$$\frac{1}{n} H_{\min}^{\epsilon}(\rho_{AB}^{\otimes n}|B^n) \geq H(\rho_{AB}|B) - \frac{1}{\sqrt{n}} 4\log(\eta)\sqrt{\log\frac{2}{\epsilon^2}}, \tag{44}$$

$$\frac{1}{n} H_{\max}^{\epsilon}(\rho_{AB}^{\otimes n}|B^n) \leq H(\rho_{AB}|B) + \frac{1}{\sqrt{n}} 4\log(\eta)\sqrt{\log\frac{2}{\epsilon^2}} \tag{45}$$

for $n \geq (8/5)\log(2/\epsilon^2)$, and $\eta = 2^{-\frac{1}{2}H_{\min}(\rho_{AB}|B)} + 2^{\frac{1}{2}H_{\max}(\rho_{AB}|B)} + 1$.

Note that it is not clear under what conditions the limits $n \to \infty, \epsilon \to 0$ exist for the left hand side of Eqs. (44) and (45). If they do, Proposition 8 implies $\lim_{\epsilon\to 0}\lim_{n\to\infty} \frac{1}{n} H_{\min}^{\epsilon}(\rho_{AB}^{\otimes n}|B^n) \geq H(\rho_{AB}|B)$ and $\lim_{\epsilon\to 0}\lim_{n\to\infty} \frac{1}{n} H_{\max}^{\epsilon}(\rho_{AB}^{\otimes n}|B^n) \leq H(\rho_{AB}|B)$. For the case of a finite-dimensional H_A we show that these inequalities can be replaced with equalities (Corollary 1).

It should be noted that in the classical case a lower bound on the min-entropy and an upper bound on the max-entropy, analogous to Eqs. (44) and (45), correspond [32] to the AEP in classical probability theory [38]. Since in the finite-dimensional quantum

case, the step from Proposition 8 to Corollary 1 is directly obtained [9] via Fannes' inequality [39], the limits in Corollary 1 are usually referred to as 'the quantum AEP' [9]. In the infinite-dimensional case the relation between Proposition 8 and Corollary 1 appears less straightforward, and it is thus not entirely clear what should be regarded as constituting 'the quantum AEP'. We will not pursue this question here, but merely note that it is the inequalities in Proposition 8, rather than the limits in Corollary 1, that are the most relevant for applications [5]. However, for the sake of simplicity we continue to refer to Corollary 1 as a quantum AEP.

We prove Proposition 8 after the following lemma.

Lemma 2. *Let $\rho_{AB} \in \mathcal{S}(H_A \otimes H_B)$ and let $\{\hat{\rho}^k_{AB}\}_{k=1}^{\infty}$ be a sequence of normalized projected states. For any fixed $1 > t > 0$, there exists a $k_0 \in \mathbb{N}$ such that*

$$H^{\epsilon}_{\min}(\rho_{AB}|B) \geq H^{t\epsilon}_{\min}(\hat{\rho}^k_{AB}|B), \quad \forall k \geq k_0. \tag{46}$$

Proof. In the following let $t \in (0, 1)$ be fixed. According to the definition of the smooth min-entropy in Eq. (36), it is enough to show that $\mathcal{B}^{t\epsilon}(\hat{\rho}^k_{AB}) \subseteq \mathcal{B}^{\epsilon}(\rho_{AB})$ for all $k \geq k_0$. Note that the purified distance is compatible with trace norm convergence, i.e., $\|\rho_{AB} - \hat{\rho}^k_{AB}\|_1 \to 0$ implies that $P(\hat{\rho}^k_{AB}, \rho_{AB}) \to 0$. Hence, there exists a k_0 such that $P(\hat{\rho}^k_{AB}, \rho_{AB}) < (1-t)\epsilon$ for all $k \geq k_0$. For $k \geq k_0$ and $\tilde{\rho}_{AB} \in \mathcal{B}^{t\epsilon}(\hat{\rho}^k_{AB})$ we thus find $P(\tilde{\rho}_{AB}, \rho_{AB}) \leq P(\tilde{\rho}_{AB}, \hat{\rho}^k_{AB}) + P(\hat{\rho}^k_{AB}, \rho_{AB}) < \epsilon$, such that $\tilde{\rho}_{AB} \in \mathcal{B}^{\epsilon}(\rho_{AB})$.

Proof (Proposition 8). Let (P^A_k, P^B_k) be a generator of projected states. The pair of n-fold tensor products of the projections, $\left((P^A_k)^{\otimes n}, (P^B_k)^{\otimes n}\right)$, is also a generator of projected states. If we now fix $1 > t > 0$ and $n \in \mathbb{N}$, it follows by Lemma 2 that we can find a $k_0 \in \mathbb{N}$ such that $H^{\epsilon}_{\min}(\rho^{\otimes n}_{AB}|B^n) \geq H^{t\epsilon}_{\min}((\hat{\rho}^k_{AB})^{\otimes n}|B^n)$ for every $k \geq k_0$. Since Eq. (44) is valid for the finite-dimensional case [9], we can apply it to $H^{t\epsilon}_{\min}((\hat{\rho}^k_{AB})^{\otimes n}|B^n)$ to obtain

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

for any $n \geq (8/5)\log(2/(t\epsilon)^2)$, and $\eta_k = 2^{-\frac{1}{2}H_{\min}(\hat{\rho}^k_{AB}|B)} + 2^{\frac{1}{2}H_{\max}(\hat{\rho}^k_{AB}|B)} + 1$. Hence

$$\frac{1}{n} H^{\epsilon}_{\min}(\rho^{\otimes n}_{AB}|B^n) \geq H(\hat{\rho}^k_{AB}|B) - \frac{1}{\sqrt{n}} 4 \log(\eta_k) \sqrt{\log \frac{2}{(t\epsilon)^2}}, \tag{47}$$

for all $k \geq k_0$. Since the left-hand side of Eq. (47) is independent of k we can use (42) and Proposition 1, to find

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

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

For the second part we use the duality of the conditional von Neumann entropy, i.e., $H(\rho_{AB}|B) = -H(\rho_{AC}|C)$ for a purification ρ_{ABC} [33]. This, together with the duality relation for smooth min- and max-entropy (39) leads directly to (45).

Corollary 1. *Let H_A be a finite-dimensional and H_B a separable Hilbert space. For all $\rho_{AB} \in \mathcal{S}(H_A \otimes H_B)$ it follows that*

$$\lim_{\epsilon\to 0}\lim_{n\to\infty}\frac{1}{n}H_{\min}^{\epsilon}(\rho_{AB}^{\otimes n}|B^n) = H(\rho_{AB}|B), \tag{48}$$

$$\lim_{\epsilon\to 0}\lim_{n\to\infty}\frac{1}{n}H_{\max}^{\epsilon}(\rho_{AB}^{\otimes n}|B^n) = H(\rho_{AB}|B). \tag{49}$$

Proof. Let $\epsilon > 0$ be sufficiently small, and let (id_A, P_k^B) be a generator of projected states ρ_{AB}^k, with corresponding normalized projected states $\hat{\rho}_{AB}^k$. Let $\sigma_{AB} \in \mathcal{B}^{\epsilon}(\rho_{AB})$, with projected states σ_{AB}^k, and normalized projected states $\hat{\sigma}_{AB}^k$. By $H_{\min}(\sigma_{AB}^k|B) = H_{\min}(\hat{\sigma}_{AB}^k|B) + \log\operatorname{tr}\sigma_{AB}^k$ and (43) we find $H_{\min}(\sigma_{AB}^k|B_k) \leq H(\hat{\sigma}_{AB}^k|B)$, where $\hat{\sigma}_{AB}^k = (\operatorname{tr}\sigma_{AB}^k)^{-1}\sigma_{AB}^k$. Since $H(\hat{\sigma}_{AB}^k|B_k)$ is finite-dimensional we can use Fannes' inequality [39] to obtain (for k sufficiently large) $H(\hat{\sigma}_{AB}^k|B_k) \leq H(\hat{\rho}_{AB}^k|B_k) + 4\Delta_k \log d_A + 4H_{\mathrm{bin}}(\Delta_k)$, with $d_A = \dim(H_A)$, $\Delta_k = \|\hat{\rho}_{AB}^k - \hat{\sigma}_{AB}^k\|_1$, and $H_{\mathrm{bin}}(t) = -t\log t - (1-t)\log(1-t)$. Due to the general relation $\|\rho-\sigma\|_1 \leq 2P(\rho,\sigma)$ (see Lemma 6 in [24]), we have $\|\rho_{AB} - \sigma_{AB}\|_1 \leq 2\epsilon$ for all $\sigma_{AB} \in \mathcal{B}^{\epsilon}(\rho_{AB})$, which yields $\lim_{k\to\infty}\Delta_k = \|\rho_{AB} - \hat{\sigma}_{AB}\|_1 \leq 4\epsilon$, where $\hat{\sigma}_{AB} = \sigma_{AB}/\operatorname{tr}(\sigma_{AB})$. Combined with (42) this leads to $H_{\min}^{\epsilon}(\rho_{AB}|B) = \sup_{\sigma_{AB}\in\mathcal{B}^{\epsilon}(\rho_{AB})}\lim_{k\to\infty}H_{\min}(\sigma_{AB}^k|B) \leq H(\rho_{AB}|B) + 16\epsilon\log d_A + 4H_{\mathrm{bin}}(4\epsilon)$. Applied to an n-fold tensor product this gives

$$\frac{1}{n}H_{\min}^{\epsilon}(\rho_{AB}^{\otimes n}|B^n) \leq H(\rho_{AB}|B) + 16\epsilon\log d_A + \frac{4}{n}H_{\mathrm{bin}}(4\epsilon). \tag{50}$$

Equation (48) follows by combining (50) with the lower bound in (44), taking the limits $n\to\infty$ and $\epsilon\to 0$. Equation (49) follows directly by the duality of the conditional von Neumann entropy [33] together with the duality of the smooth min- and max-entropy (39).

7. Conclusion and Outlook

We have extended the min- and max-entropies to separable Hilbert spaces, and shown that properties and operational interpretations, known from the finite-dimensional case, remain valid in the infinite-dimensional setting. These extensions are facilitated by the finding (Proposition 1) that the infinite-dimensional min- and max-entropies can be expressed in terms of convergent sequences of finite-dimensional entropies. We bound the smooth min- and max-entropies of iid states (Proposition 8) in terms of an infinite-dimensional generalization of the conditional von Neumann entropy $H(A|B)$, introduced in [33], which is defined when the von Neumann entropy of system A is finite, $H(A) < \infty$. Under the additional assumption that the Hilbert space of system A has finite dimension we furthermore prove that the smooth entropies of iid states converge to the conditional von Neumann entropy (Corollary 1), corresponding to a quantum asymptotic equipartition property (AEP). Whether these conditions can be relaxed is an open question. In the general case where $H(A)$ is not necessarily finite, this would however require a more general definition of the conditional von Neumann entropy than the one used here.

For information-theoretic purposes it appears reasonable to require extensions of the conditional von Neumann entropy to be compatible with the AEP, i.e., that the conditional von Neumann entropy can be regained from the smooth min- and max-entropy in

the asymptotic iid limit. This enables generalizations of operational interpretations of the conditional von Neumann entropy. For example, in the finite-dimensional asymptotic case the conditional von Neumann entropy characterizes the amount of entanglement needed for state merging [40], i.e., the transfer of a quantum state shared by two parties to only one of the parties. An infinite-dimensional generalization of one-shot state merging [41], together with the AEP, could be used to extend this result to the infinite-dimensional case.

Some other immediate applications of this work are in continuous variable quantum key distribution, and in statistical mechanics, where it has recently been shown [19,20] that the smooth min- and max-entropies play a role. Our techniques may also be employed to derive an infinite-dimensional generalization of the entropic uncertainty relation [11]. Such a generalization would be interesting partially because it could find applications in continuous variable quantum information processing, but also because it may bring this information-theoretic uncertainty relation into the same realm as the standard uncertainty relation.

Acknowledgements. We thank Roger Colbeck and Marco Tomamichel for helpful comments and discussions, and an anonymous referee for very valuable suggestions. Fabian Furrer acknowledges support from the Graduiertenkolleg 1463 of the Leibniz University Hannover. We furthermore acknowledge support from the Swiss National Science Foundation (grant No. 200021-119868).

A. Technical Lemmas

In the following, each Hilbert space is assumed to be separable. Let us define the positive cone $\mathcal{L}^+(H) := \{T \in \mathcal{L}(H) | \ T \geq 0\}$ in $\mathcal{L}(H)$. The next two lemmas follow directly from the definition of positivity of an operator.

Lemma 3. *If $T \in \mathcal{L}^+(H)$, then for each $S \in \mathcal{L}(H)$ it follows that $STS^\dagger \in \mathcal{L}^+(H)$.*

Lemma 4. *The positive cone $\mathcal{L}^+(H)$ is sequentially closed in the weak operator topology, i.e., for $\{T_k\}_{k\in\mathbb{N}} \subset \mathcal{L}^+(H)$ such that T_k converge to $T \in \mathcal{L}(H)$ in the weak operator topology, it follows that $T \geq 0$.*

The following lemma is a special case of a theorem by Grümm [42] (see also [43], pp. 25–29, for similar results).

Lemma 5. *Let $A_k, A \in \mathcal{L}(H)$, such that $\sup_k \|A_k\| < +\infty$, and $A_k \to A$ in the strong operator topology, and let $T \in \tau_1(H)$. Then $\lim_{k\to\infty} \|A_k T - AT\|_1 = 0$ and $\lim_{k\to\infty} \|TA_k - TA\|_1 = 0$.*

Corollary 2. *If P_k is a sequence of projectors on H that converges in the strong operator topology to the identity, and if $\rho \in \tau_1^+(H)$, then $\lim_{k\to\infty} \|P_k \rho P_k - \rho\|_1 = 0$.*

Lemma 6. *If sequences of projectors P_k^A and P_k^B on H_A and H_B, respectively, converge in the strong operator topology to the identity, then $P_k^A \otimes P_k^B$ converges in the strong operator topology to id_{AB}.*

Lemma 7. *Let $\{T_k\}_{k\in\mathbb{N}} \subset \tau_1(H_B)$ be a sequence that converges in the weak* topology to $T \in \tau_1(H_B)$. Then, the sequence $\mathrm{id}_A \otimes T_k$ in $\mathcal{L}(H_A \otimes H_B)$ converges to $\mathrm{id}_A \otimes T$ in the weak operator topology.*

Proof. For each $\psi \in H_A \otimes H_B$ we find that $\langle\psi| \operatorname{id} \otimes T_k |\psi\rangle = \operatorname{tr}(T_k K_\psi^B)$, where $K_\psi^B = \operatorname{tr}_A |\psi\rangle\langle\psi|$ is the reduced operator. Since K_ψ^A is trace class (and thus compact) the statement follows immediately.

B. Proof of Proposition 1

In order to derive Proposition 1 we proceed as follows: In Sect. B.1 we show that the min- and max-entropy of a projected state can be reduced to an entropy on a finite-dimensional space. In Sect. B.2 we show that the min- and max-entropies are monotonic over the sequences of projected states. Finally we prove the limits listed in Proposition 1. Note that in what follows we mostly make use of the quantities $\Lambda(\rho_{AB}|\sigma_B)$ and $\Lambda(\rho_{AB}|B)$, as defined in Eqs. (5) and (6), rather than the min- and max-entropies per se.

B.1. Reduction. Here we show that the min- and max-entropy of a projected state can be considered as effectively finite-dimensional, in the sense that restricting the Hilbert space to the support of the projected states does not change the value of the entropies.

Lemma 8. *Let P_A, P_B be projectors onto closed subspaces $U_A \subseteq H_A$ and $U_B \subseteq H_B$, respectively, $\tilde{\rho}_{AB} \in \tau_1^+(H_A \otimes H_B)$, and $\tilde{\sigma}_B \in \tau_1^+(H_B)$.*

i) *If $(P_A \otimes \operatorname{id}_B)\tilde{\rho}_{AB}(P_A \otimes \operatorname{id}_B) = \tilde{\rho}_{AB}$ it follows that*

$$\Lambda(\tilde{\rho}_{AB}|\tilde{\sigma}_B) = \inf\{\lambda \in \mathbb{R} | \lambda P_A \otimes \tilde{\sigma}_B \geq \tilde{\rho}_{AB}\}. \tag{51}$$

ii) *If $(\operatorname{id}_A \otimes P_B)\tilde{\rho}_{AB}(\operatorname{id}_A \otimes P_B) = \tilde{\rho}_{AB}$ it follows that*

$$\Lambda(\tilde{\rho}_{AB}|B) = \Lambda(\tilde{\rho}_{AB}|U_B), \tag{52}$$

where $\Lambda(\tilde{\rho}_{AB}|U_B)$ means that the infimum in Eq. (6) is taken only over the set $\tau_1^+(U^B)$.

The proof is straightforward and left to the reader. In the particular case of projected states ρ_{AB}^k relative to a generator (P_k^A, P_k^B), the evaluation of $\Lambda(\rho_{AB}^k|\sigma_B^k)$ and $\Lambda(\rho_{AB}^k|B)$, where $\sigma_B^k = P_k^B \sigma_B P_k^B$, can be restricted to the finite-dimensional Hilbert space $U_k^A \otimes U_k^B$ given by the projection spaces of P_k^A and P_k^B. Especially, we can conclude that the infima of Eqs. (5) and (6), and consequently the infimum in (1) and the supremum in (2), are attained for projected states, since these are optimizations of continuous functions over compact sets.

B.2. Monotonicity. The next lemma considers the monotonic behaviour of the min- and max-entropies with respect to sequences of projected states.

Lemma 9. *For $\rho_{AB} \in \mathcal{S}(H_A \otimes H_B)$, $\sigma_B \in \mathcal{S}(H_B)$, let $\{\rho_{AB}^k\}_{k=1}^\infty$ and $\{\sigma_B^k\}_{k=1}^\infty$ be projected states relative to a generator (P_k^A, P_k^B).*

i) *It follows that $\Lambda(\rho_{AB}^k|\sigma_B^k)$ and $\Lambda(\rho_{AB}^k|B)$ are monotonically increasing in k, where the first sequence is bounded by $\Lambda(\rho_{AB}|\sigma_B)$ and the latter by $\Lambda(\rho_{AB}|B)$.*
ii) *For an arbitrary but fixed purification ρ_{ABC} of ρ_{AB} with purifying system H_C, let $\rho_{AC}^k = \operatorname{tr}_B \rho_{ABC}^k$ and $\rho_{ABC}^k = (P_k^A \otimes P_k^B \otimes \operatorname{id}_C)\rho_{ABC}(P_k^A \otimes P_k^B \otimes \operatorname{id}_C)$. Then it follows that $\Lambda(\rho_{AC}^k|C)$ is monotonically increasing and bounded by $\Lambda(\rho_{AC}|C)$.*

Note that ρ^k_{AC} as defined in the lemma is not a projected state in the sense of Definition 2. Translated to min- and max-entropies, the lemma above says that $H_{\min}(\rho^k_{AB}|\sigma^k_B)$ and $H_{\min}(\rho^k_{AB}|B)$ are monotonically increasing while $H_{\max}(\rho^k_{AB}|B)$ is monotonically decreasing. But in general, the monotonicity does not hold for *normalized* projected states.

Proof. Set $P_k := P^A_k \otimes P^B_k$ and recall that $\Lambda(\rho^k_{AB}|\sigma^k_B) = \inf\{\lambda \in \mathbb{R} |\, \lambda P^A_k \otimes \sigma^k_B \geq \rho^k_{AB}\}$ according to Lemma 8. To show the first part of i) note that for $k' \leq k$ the equations

$$P_{k'} P_k (\lambda \,\mathrm{id} \otimes \sigma_B - \rho_{AB}) P_{k'} P_k = P_{k'} (\lambda P^A_k \otimes \sigma^k_B - \rho^k_{AB}) P_{k'} = \lambda P^A_{k'} \otimes \sigma^{k'}_B - \rho^{k'}_{AB}$$

hold, which imply via Lemma 3 that $\Lambda(\rho^{k'}_{AB}|\sigma^{k'}_B) \leq \Lambda(\rho^k_{AB}|\sigma^k_B) \leq \Lambda(\rho_{AB}|\sigma_B)$. For the second part, let $\tilde{\sigma}_B \in \tau^+_1(H_B)$ be the optimal state such that $\Lambda(\rho^k_{AB}|B) = \mathrm{tr}\,\tilde{\sigma}_B$ and $P^A_k \otimes \tilde{\sigma}_B \geq \rho^k_{AB}$. But then we obtain that $P^A_{k'} \otimes P^B_{k'} \tilde{\sigma}_B P^B_{k'} - \rho^{k'}_{AB} \geq 0$ and therefore also $\Lambda(\rho^{k'}_{AB}|B) \leq \Lambda(\rho^k_{AB}|B)$. The upper bound follows in the same manner.

In order to show ii) we define the sets $\mathcal{M}_k := \{\tilde{\sigma}_C \in \tau^+_1(H_C) |\, \mathrm{id}_A \otimes \tilde{\sigma}_C \geq \rho^k_{AC}\}$ such that $\Lambda(\rho^k_{AC}|C) = \inf_{\tilde{\sigma}_C \in \mathcal{M}_k} \mathrm{tr}\,\tilde{\sigma}_C$. To conclude the monotonicity we show that $\mathcal{M}_{k'} \supset \mathcal{M}_k$ for $k' \leq k$. If $\mathcal{M}_k = \emptyset$, the statement is trivial. Assume $\tilde{\sigma}_C \in \mathcal{M}_k$. Using $P^B_{k'} \leq P^B_k$ we find

$$\mathrm{id}_A \otimes \tilde{\sigma}_C \geq P^A_k \,\mathrm{tr}_B(P^B_k \rho_{ABC} P^B_k) P^A_k \geq P^A_k \,\mathrm{tr}_B(P^B_{k'} \rho_{ABC} P^B_{k'}) P^A_k.$$

Together with Lemma 3, this yields $P^A_{k'} \otimes \tilde{\sigma}_C \geq \rho^{k'}_{AC}$ and thus $\tilde{\sigma}_C \in \mathcal{M}_{k'}$. A similar argument provides the upper bound $\Lambda(\rho^k_{AC}|C) \leq \Lambda(\rho_{AC}|C)$.

B.3. Limits. After the above discussion on general properties of the min- and max-entropies of projected states we are now prepared to prove Proposition 1. For the sake of convenience we divide the proof into three lemmas.

Lemma 10. *For $\rho_{AB} \in \mathcal{S}(H_A \otimes H_B)$ and $\sigma_B \in \mathcal{S}(H_B)$, let $\{\rho^k_{AB}\}_{k=1}^\infty$ be the projected states of ρ_{AB} relative to a generator (P^A_k, P^B_k), and let $\sigma^k_B := P^B_k \sigma_B P^B_k$. It follows that*

$$\Lambda(\rho_{AB}|\sigma_B) = \lim_{k\to\infty} \Lambda(\rho^k_{AB}|\sigma^k_B), \tag{53}$$

and the infimum in Eq. (5) is attained if $\Lambda(\rho_{AB}|\sigma_B)$ is finite.

Proof. That the infimum is attained follows directly from the definition. To show (53) we prove that $\Lambda(\rho_{AB}|\sigma_B)$ is lower semi-continuous in (ρ_{AB}, σ_B) with respect to the product topology induced by the trace norm topology on each factor. Since this means that $\liminf_{k\to\infty} \Lambda(\rho^k_{AB}|\sigma^k_B) \geq \Lambda(\rho_{AB}|\sigma_B)$, the combination with Lemma 9 results directly in (53). To show lower semi-continuity recall that it is equivalent to say that all lower level sets $\Lambda^{-1}((-\infty, t]) = \{(\rho_{AB}, \sigma_B) |\, \Lambda(\rho_{AB}|\sigma_B) \leq t\}$, for $t \in \mathbb{R}$ have to be closed. But this follows by rewriting $\Lambda^{-1}((-\infty, t])$ as $\{(\rho_{AB}, \sigma_B) |\, t\,\mathrm{id} \otimes \sigma_B \geq \rho_{AB}\}$.

Lemma 11. *For $\rho_{AB} \in \mathcal{S}(H_A \otimes H_B)$, let $\{\rho^k_{AB}\}_{k=1}^\infty$ be the projected states of ρ_{AB} relative to a generator (P^A_k, P^B_k). It follows that*

$$\Lambda(\rho_{AB}|B) = \lim_{k\to\infty} \Lambda(\rho^k_{AB}|B), \tag{54}$$

and the infimum in Eq. (6) is attained if $\Lambda(\rho_{AB}|B)$ is finite.

Proof. Let $\mu_k := \Lambda(\rho_{AB}^k|B) = \Lambda(\rho_{AB}^k|B_k)$, where the last equality is due to Lemma 8. By Lemma 9 this sequence is monotonically increasing, and we can thus define $\mu := \lim_{k\to\infty} \mu_k \in \mathbb{R} \cup \{+\infty\}$. In addition, Lemma 9 also yields $\mu \leq \Lambda(\rho_{AB}|B)$. Hence, the case $\lambda = +\infty$ is trivial, and it remains to show $\mu \geq \Lambda(\rho_{AB}|B)$, for $\mu < \infty$.

For each $k \in \mathbb{N}$ let $\tilde{\sigma}_B^k$ be an optimal state such that $\Lambda(\rho_{AB}^k|B) = \operatorname{tr} \tilde{\sigma}_B^k$ and $\mathrm{id} \otimes \tilde{\sigma}_B^k \geq \rho_{AB}^k$. Note that due to positivity $\operatorname{tr} \tilde{\sigma}_B^k = \|\tilde{\sigma}_B^k\|_1 \leq \mu$, such that $\tilde{\sigma}_B^k$ is a bounded sequence in $\tau_1(H_B)$. Since the trace class operators $\tau_1(H_B)$ is the dual space of the compact operators $\mathcal{K}(H_B)$ [44], we can apply Banach Alaoglu's theorem [44,45] to find a subsequence $\{\tilde{\sigma}_B^k\}_{k\in\Gamma}$ with a weak* limit $\tilde{\sigma}_B \in \tau_1(H_B)$, i.e., $\operatorname{tr}(K\tilde{\sigma}_B^k) \to \operatorname{tr}(K\tilde{\sigma}_B)$ $(k \in \Gamma)$ for all $K \in \mathcal{K}(H_B)$, such that $\|\tilde{\sigma}_B\|_1 \leq \mu$. Obviously, $\tilde{\sigma}_B$ is also positive. According to Lemma 7, $\mathrm{id} \otimes \tilde{\sigma}_B^k$ (for $k \in \Lambda$) converges in the weak operator topology to $\mathrm{id} \otimes \tilde{\sigma}_B$, and so does $\mathrm{id} \otimes \tilde{\sigma}_B^k - \rho_{AB}^k$ to $\mathrm{id} \otimes \tilde{\sigma}_B - \rho_{AB}$. But then we can conclude that $\mathrm{id} \otimes \tilde{\sigma}_B - \rho_{AB} \geq 0$ such that $\Lambda(\rho_{AB}|B) \leq \operatorname{tr} \tilde{\sigma}_B \leq \mu$.

Lemma 12. *For $\rho_{AB} \in \mathcal{S}(H_A \otimes H_B)$, let ρ_{ABC} be a purification with purifying system H_C, and (P_k^A, P_k^B) be a generator of projected states. It follows that*

$$\Lambda(\rho_{AC}|C) = \lim_{k\to\infty} \Lambda(\rho_{AC}^k|C), \tag{55}$$

where $\rho_{AC}^k = \operatorname{tr}_B[(P_k^A \otimes P_k^B \otimes \mathrm{id}_C)\rho_{ABC}(P_k^A \otimes P_k^B \otimes \mathrm{id}_C)]$.

Proof. Let $\nu_k := \Lambda(\rho_{AC}^k|C)$. Due to Lemma 9 this sequence is monotonically increasing, so we can define $\nu := \lim_{k\to\infty} \nu_k \in \mathbb{R} \cup \{+\infty\}$, and conclude that $\nu \leq \Lambda(\rho_{AC}|C)$. Thus, the case $\nu = +\infty$ is trivial. It thus remains to show $\nu \geq \Lambda(\rho_{AC}|C)$ for $\nu < +\infty$. As proved in Lemma 11, the infimum in Eq. (6) is attained even if the underlying Hilbert spaces are infinite-dimensional. Thereby there exists for each $k \in \mathbb{N}$ a state $\tilde{\sigma}_C^k$ such that $\mathrm{id} \otimes \tilde{\sigma}_C^k \geq \rho_{AC}^k$ and $\operatorname{tr} \tilde{\sigma}_C^k = \Lambda(\rho_{AC}^k|C)$. Now we can proceed in the same manner as in the proof of Lemma 11 to construct a weak* limit $\tilde{\sigma}_C \in \tau_1^+(H_B)$ that satisfies $\mathrm{id}_A \otimes \tilde{\sigma}_C \geq \rho_{AC}$, and is such that $\Lambda(\rho_{AC}|C) \leq \operatorname{tr} \tilde{\sigma}_C \leq \nu \leq \Lambda(\rho_{AC}|C)$. This completes the proof.

Of course, Lemma 10 and 11 can directly be rewritten in terms of min-entropies and yield the first two statements of Proposition 1. The part for the normalized projected states follows via $H_{\min}(\hat{\rho}_{AB}^k|\hat{\sigma}_B^k) = H_{\min}(\rho_{AB}^k|\sigma_B^k) - \log \operatorname{tr} \sigma_B^k + \log \operatorname{tr} \rho_{AB}^k$, and $H_{\min}(\hat{\rho}_{AB}^k|B) = H_{\min}(\rho_{AB}^k|B) + \log \operatorname{tr} \rho_{AB}^k$.

In order to obtain the convergence stated for the max-entropy in Proposition 1, note that $(P_k^A \otimes P_k^B \otimes \mathrm{id}_C)\rho_{ABC}(P_k^A \otimes P_k^B \otimes \mathrm{id}_C)$ is a purification of ρ_{AB}^k, whenever ρ_{ABC} is a purification of ρ_{AB}. Hence, $H_{\max}(\rho_{AB}^k|B) = -H_{\min}(\rho_{AC}^k|C) = \log \Lambda(\rho_{AC}^k|C)$. For normalized states use $H_{\max}(\hat{\rho}_{AB}^k|B_k) = H_{\max}(\rho_{AB}^k|B_k) - \log \operatorname{tr} \rho_{AB}^k$.

References

1. Shannon, C.E.: A Mathematical Theory of Communication. Bell System Technical Journal **27**, 379–423 and 623–656 (1948)
2. Rényi, A.: On measures of entropy and information. *Proc. of the 4th Berkley Symp. on Math. Statistics and Prob.* **1**, Berkeley, CA: Univ. of Calif. Press, 1961, pp. 547–561
3. Barnum, H., Nielsen, M.A., Schumacher, B.: Information transmission through a noisy quantum channel. Phys. Rev. A **57**, 4153–4175 (1998)
4. Schumacher, B.: Quantum coding. Phys. Rev. A **51**, 2738–2747 (1995)
5. Renner, R.: Security of Quantum Key Distribution. Ph.D. thesis, Swiss Fed. Inst. of Technology, Zurich, 2005, Available at http://arXiv.org/abs/quant-ph/0512258v2, 2006

6. Renner, R., Wolf, S.: Smooth Renyi entropy and applications *Proc. 2004 IEEE International Symposium on Information Theory*, Piscataway, NJ: IEEE, 2004, p. 233
7. Renes, J. M., Renner, R.: One-Shot Classical Data Compression with Quantum Side Information and the Distillation of Common Randomness or Secret Keys. http://arXiv.org/abs/1008.0452v2 [quant-ph], 2010
8. Renner, R., Wolf, S., Wullschleger, J.: The Single-Serving Channel Capacity *Proc. 2006 IEEE International Symposium on Information Theory*, Piscataway, NJ: IEEE, 2006, pp. 1424–1427
9. Tomamichel, M., Colbeck, R., Renner, R.: A Fully Quantum Asymptotic Equipartition Property. IEEE Trans. Inf. Th. **55**, 5840–5847 (2009)
10. Berta, M., Christandl, M., Renner, R.: A Conceptually Simple Proof of the Quantum Reverse Shannon Theorem. http://arXiv.org/abs/0912.3805v1 [quant-ph], 2009
11. Berta, M., Christandl, M., Colbeck, R., Renes, J.M., Renner, R.: The uncertainty principle in the presence of quantum memory. Nature Physics **6**, 659–662 (2010)
12. Datta, N., Renner, R.: Smooth Entropies and the Quantum Information Spectrum. IEEE Trans. Inf. Theor. **55**, 2807–2815 (2009)
13. Han, T. S.: *Information-Spectrum Methods in Information Theory*. New York: Springer-Verlag, 2002
14. Han, T.S., Verdu, S.: Approximation theory of output statistics. IEEE Trans. Inform. Theory **39**, 752–772 (1993)
15. Datta, N.: Min- and Max-Relative Entropies and a New Entanglement Monotone. IEEE Trans. Inf. Theor. **55**, 2816–2826 (2009)
16. Brandão, F.G.S.L., Datta, N.: One-shot rates for entanglement manipulation under non-entangling maps. IEEE Trans. Inf. Theor. **57**, 1754 (2011)
17. Buscemi, F., Datta, N.: Entanglement Cost in Practical Scenarios. Phys. Rev. Lett **106**, 130503 (2011)
18. Mosonyi, M., Datta, N.: Generalized relative entropies and the capacity of classical-quantum channels. J. Math. Phys. **50**, 072104 (2009)
19. Dahlsten, O.C.O., Renner, R., Rieper, E., Vedral, V.: Inadequacy of von Neumann entropy for characterizing extractable work. New J. Phys. **13**, 053015 (2011)
20. del Rio L., Åberg J., Renner R., Dahlsten O., Vedral, V.: The thermodynamic meaning of negative entropy. Nature **474**, 61–63 (2011)
21. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dušek, M., Lütkenhaus, N., Peev, M.: The security of practical quantum key distribution. Rev. Mod. Phys. **81**, 1301–1350 (2009)
22. Bratteli, O., Robinson, D. W.: *Operator Algebras and Quantum Statistical Mechanics I*. New York: Springer-Verlag, 1979
23. König, R., Renner, R., Schaffner, C.: The Operational Meaning of Min- and Max-Entropy. IEEE Trans. Inf. Th. **55**, 4337–4347 (2009)
24. Tomamichel, M., Colbeck, R., Renner, R.: Duality Between Smooth Min- and Max-Entropies. IEEE Trans. Inf. Th. **56**, 4674–4681 (2010)
25. Lieb, E.H., Ruskai, M.B.: A Fundamental Property of Quantum-Mechanical Entropy. Phys. Rev. Lett. **30**, 434–436 (1973)
26. Lieb, E.H.: Convex trace functions and the Wigner-Yanase-Dyson conjecture. Adv. Math. **11**, 267–288 (1973)
27. Lieb, E.H., Ruskai, M.B.: Proof of the strong subadditivity of quantum-mechanical entropy. J. Math. Phys. **14**, 1938–1941 (1973)
28. Owari, M., Braunstein, S.L., Nemoto, K., Murao, M.: Epsilon-convertibility of entangled states and extension of Schmidt rank in infinite-dimensional systems. Quant. Inf. and Comp. **8**, 30–52 (2008)
29. Kraus, K.: Lecture Notes in Physics **190**, *States, Effects, and Operations*. Berlin Heidelberg: Springer-Verlag, 1983
30. Nielsen, M.L., Chuang, I.L.: *Quantum Computation and Quantum Information*. Cambridge: Cambridge University Press, 2000
31. Uhlmann, A.: The transition probability in the state space of a *-algebra. Rep. Math. Phys. **9**, 273–279 (1976)
32. Holenstein, H., Renner, R.: On the Randomness of Independent Experiments. IEEE Trans. Inf. Theor. **57**(4), 1865–1871 (2011)
33. Kuznetsova, A.A.: Quantum conditional entropy for infinite-dimensional systems. Theory Probab. Appl. **55**, 782–790 (2010)
34. Klein, O.: Zur quantenmechanischen Begründung des zweiten Hauptsatzes der Wärmelehre. Z. F. Phys. A **72**, 767–775 (1931)
35. Lindblad, G.: Entropy, Information and Quantum Measurements. Commun. Math. Phys. **33**, 305–322 (1973)
36. Lindblad, G.: Expectations and Entropy Inequalities for Finite Quantum Systems. Commun. Math. Phys. **39**, 111–119 (1974)
37. Holevo, A.S., Shirokov, M.E.: Mutual and Coherent Information for Infinite-Dimensional Quantum Channels. Probl. Inf. Transm. **46**, 201–217 (2010)

38. Cover, T.M., Thomas, J.A.: *Elements of Information Theory*. 2nd ed. New York: Wiley, 2006
39. Alicki, R., Fannes, M.: Continuity of quantum conditional information. J. Phys. A **37**, L55–L57 (2004)
40. Horodecki, M., Oppenheim, J., Winter, A.: Partial quantum information. Nature **436**, 673–676 (2005)
41. Berta, M.: Single-shot Quantum State Merging. Diploma thesis, ETH Zurich, February 2008, available at http://arXiv.org/abs/0912.4495v1 [quant-ph], 2009
42. Grümm, H.R.: Two theorems about $\mathcal{C}_p$. Rep. Math. Phys. **4**, 211–215 (1973)
43. Simon, B.: *Trace Ideals and Their Applications*. 2nd ed. Providence, RI: Amer. Math. Soc., 2005
44. Reed, M., Simon, B.: *Methods of Modern Mathematical Physics, Vol. I: Functional Analysis*. New York: Academic Press, 1978
45. Hille, E., Phillips, R.S.: *Functional Analysis and Semi-Groups*. Providence, RI: Amer. Math. Soc., 1957

Communicated by M.B. Ruskai