The Uncertainty Principle in the Presence of Quantum Memory

Mario Berta,[1,2] Matthias Christandl,[1,2] Roger Colbeck,[3,1,4] Joseph M. Renes,[5] and Renato Renner[1]

[1]*Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland.*
[2]*Faculty of Physics, Ludwig-Maximilians-Universität München, 80333 Munich, Germany.*
[3]*Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, ON N2L 2Y5, Canada.*
[4]*Institute of Theoretical Computer Science, ETH Zurich, 8092 Zurich, Switzerland.*
[5]*Institute for Applied Physics, Technische Universität Darmstadt, 64289 Darmstadt, Germany.*

(Dated: 26th July 2010)

The uncertainty principle [1] lies at the heart of quantum theory, illuminating a dramatic difference with classical mechanics. The principle bounds the uncertainties of the outcomes of any two observables on a system in terms of the expectation value of their commutator. It implies that an observer cannot predict the outcomes of two incompatible measurements to arbitrary precision. However, this implication is only valid if the observer does not possess a quantum memory, an unrealistic assumption in light of recent technological advances [2]. In this work we strengthen the uncertainty principle to one that applies even if the observer has a quantum memory. We provide a lower bound on the uncertainty of the outcomes of two measurements which depends on the entanglement between the system and the quantum memory. We expect our uncertainty principle to have widespread use in quantum information theory, and describe in detail its application to quantum cryptography.

Uncertainty relations constrain the potential knowledge an observer can have about the physical properties of a system. Although classical theory does not limit the knowledge an observer can simultaneously have about arbitrary properties of a particle, such a limit does exist in quantum theory, where, for example, the position and momentum cannot be simultaneously known. This lack of knowledge has been termed uncertainty, and was quantified by Heisenberg using the standard deviation.[1] For two observables, R and S, the resulting bound on the uncertainty can be expressed in terms of the commutator [3]:

$$\Delta R \cdot \Delta S \geq \frac{1}{2}|\langle [R,S] \rangle|. \tag{1}$$

Inspired by information theory, uncertainty has since been quantified using the Shannon Entropy [4]. The first uncertainty relations of this type were by Białynicki-Birula and Mycielski [5] and Deutsch [6]. Later, Maassen and Uffink [7] improved Deutsch's result to show that

$$H(R) + H(S) \geq \log_2 \frac{1}{c}, \tag{2}$$

where $H(R)$ denotes the Shannon entropy of the probability distribution of the outcomes when R is measured. The term $\frac{1}{c}$ quantifies the complementarity of the observables,[2] similarly to the commutator in Equation (1).

One way to think about uncertainty relations is via the following game (the uncertainty game) between two players, Alice and Bob. Before the game commences, Alice and Bob agree on two measurements R and S. The game proceeds as follows: Bob creates a quantum state of his choosing and sends it to Alice. Alice then performs one of the two measurements and announces her choice of measurement to Bob. Bob's task is then to minimize his uncertainty about Alice's measurement outcome. This is illustrated in Figure 1.

Equation (2) bounds Bob's uncertainty in the case that he has no quantum memory. However, if he does have access to a quantum memory, this bound can be beaten. To do so, Bob should maximally entangle his quantum memory with the state he sends to Alice. Then, for any measurement she chooses, there is a measurement on Bob's memory which gives the same outcome as Alice obtains. Hence, for any observables, R and S, the uncertainties $H(R)$ and $H(S)$ vanish, in clear violation of Equation (2). More generally, the violation depends on the amount of entanglement between the system and the quantum memory.

We now proceed to state our uncertainty relation. It holds in the presence of quantum memory and provides a bound on the uncertainties of the measurement outcomes which depends on the amount of entanglement between the system, A, and the quantum memory, B. Mathematically, it is the following relation:[3]

$$H(R|B) + H(S|B) \geq \log_2 \frac{1}{c} + H(A|B). \tag{3}$$

Bob's uncertainty about the outcome of measurement R is denoted by the conditional von Neumann entropy,

[1] For observable R, we denote its standard deviation $\Delta R := \sqrt{\langle R^2 \rangle - \langle R \rangle^2}$, where $\langle R \rangle$ denotes the expectation value of R.

[2] For non-degenerate observables, $c := \max_{j,k} |\langle \psi_j | \phi_k \rangle|^2$ where $|\psi_j\rangle$ and $|\phi_k\rangle$ are the eigenvectors of R and S, respectively.

[3] A related uncertainty relation has been conjectured in the literature [8], which is implied by the relation we derive.

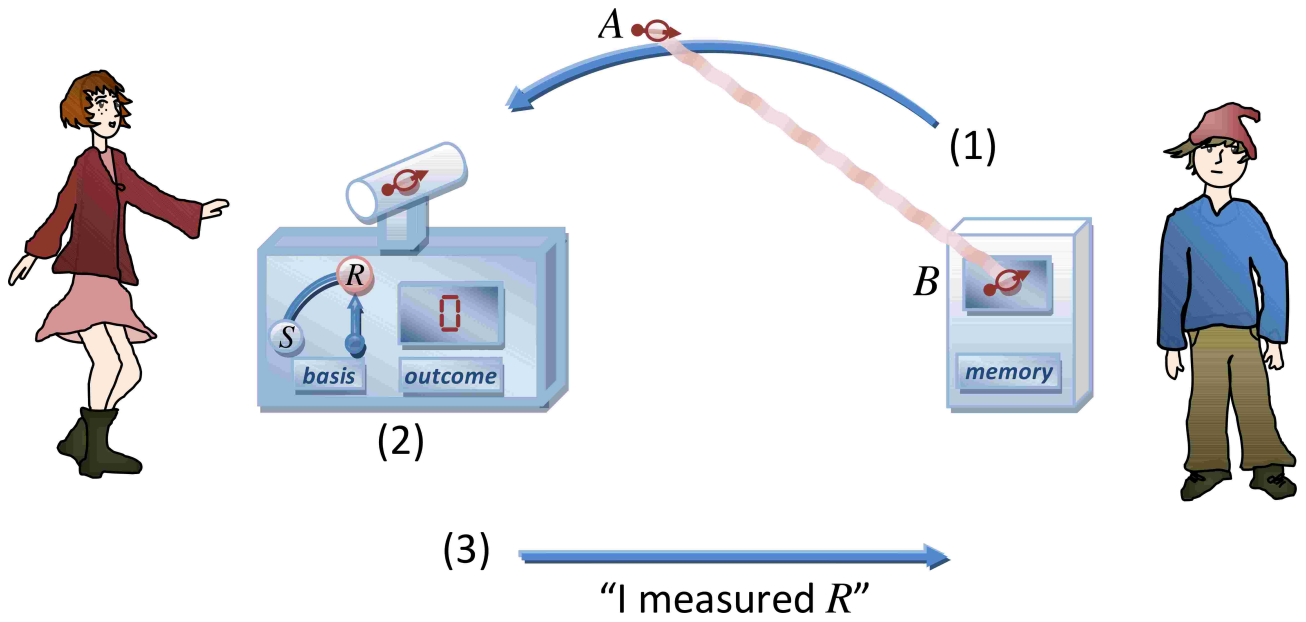

FIG. 1: Illustration of the uncertainty game. (1) Bob sends a state to Alice, which may, in general, be entangled with his quantum memory. (2) Alice measures either R or S and notes her outcome. (3) Alice announces her measurement choice to Bob. Bob's goal is then to minimize his uncertainty about Alice's measurement outcome.

$H(R|B)$, which directly generalizes the Shannon entropy, $H(R)$, to the case that Bob has a quantum memory, B, and likewise for S.[4] The additional term $H(A|B)$ appearing on the right hand side quantifies the amount of entanglement between the system and the memory. We discuss some instructive examples:

1. If the state, A, and memory, B, are maximally entangled, then $H(A|B) = -\log_2 d$, where d is the dimension of the system sent to Alice. Since $\log_2 \frac{1}{c}$ cannot exceed $\log_2 d$, the bound (3) reduces to $H(R|B)+H(S|B) \geq 0$, which is trivial, since the conditional entropy of a system after measurement given the quantum memory cannot be negative. As discussed above, Bob can guess both R and S perfectly with such a strategy.

2. If A and B are not entangled[5] then $H(A|B) \geq 0$. Since $H(R|B) \leq H(R)$ and $H(S|B) \leq H(S)$ for all states, we recover Maassen and Uffink's bound, Equation (2).

3. In the absence of the quantum memory, B, we can reduce the bound (3) to $H(R) + H(S) \geq \log_2 \frac{1}{c} + H(A)$. If the state of the system, A, is pure, then $H(A) = 0$ and we again recover the bound of Maassen and Uffink, Equation (2). However, if the system, A, is in a mixed state then $H(A) > 0$ and the resulting bound is stronger than Equation (2) even when there is no quantum memory.

4. In terms of new applications, the most interesting case is when A and B are entangled, but not maximally so. Since a negative conditional entropy $H(A|B)$ is a signature of entanglement, the uncertainty relation takes into account the entanglement between the system and the memory. It is therefore qualitatively different from existing classical bounds.

Aside from its fundamental significance, our result also has potential application to the development of future quantum technologies. One obvious candidate is in the field of quantum cryptography. In the 1970s and 80s, Wiesner [9], and Bennett and Brassard [10] proposed new cryptographic protocols based on quantum theory, most famously the BB84 quantum key distribution protocol [10]. Their intuition for security lay in the uncertainty principle. In spite of providing the initial intuition, the majority of security proofs to date have been founded on entanglement distillation and privacy amplification (see e.g. [11–16]), rather than the uncertainty principle [17]. In any cryptographic task, in order to prove security against a technologically unbounded eavesdropper, it is necessary to allow the eavesdropper access to a quantum memory. We therefore anticipate the use of our uncertainty relation in this field. By way of illustration, we discuss its potential application for the task of quantum key distribution.

[4] More precisely, $H(R|B)$ is the conditional von Neumann entropy of the state $(\sum_j |\psi_j\rangle\langle\psi_j| \otimes \mathbb{1})\rho_{AB}(\sum_j |\psi_j\rangle\langle\psi_j| \otimes \mathbb{1})$, where ρ_{AB} is the joint state of the system and the memory and $|\psi_j\rangle$ are the eigenvectors of the observable R.

[5] In other words, the state takes the form $\rho_{AB} = \sum_j p_j \rho_A^j \otimes \rho_B^j$, for probabilities p_j and quantum states ρ_A^j and ρ_B^j.

Based on the idea by Ekert [18], the security of quantum key distribution protocols are usually analysed by assuming that the eavesdropper creates a quantum state and distributes parts of it to the two users, Charlie and Diana[6]. In practice, Charlie and Diana do not provide the eavesdropper with this luxury, but a security proof that applies even in this case will certainly imply security when Charlie and Diana distribute the states themselves. In order to generate their key, Charlie and Diana will measure the states they receive using measurements chosen at random. To ensure that they generate the same key, they communicate their measurement choices to one another. In the worst case, this communication is overheard in its entirety by the eavesdropper who is trying to obtain the key. This scenario can be seen as an instance of the uncertainty game described in the previous section, where Charlie and Diana take the role of Alice and the eavesdropper takes the role of Bob.

We now explain how our uncertainty relation can be used to bound the eavesdropper's knowledge about Charlie and Diana's measurement outcomes and hence guarantee the security of the key. In order to use our relation, Charlie and Diana need to bound the right hand side of Equation (3). In other words, they need to bound how entangled their systems are with those of the eavesdropper. Remarkably, they can do so without access to the eavesdropper's memory. Quantum systems have the property that the more entangled Charlie is with Diana, the less entangled he is with any other systems, including the eavesdropper's memory. This property is often called monogamy of entanglement [19, 20]. Charlie and Diana can hence bound their entanglement with the eavesdropper by showing that they are highly entangled with one another, for instance by communicating some of their measurement results to one another and verifying that they violate a Bell inequality.

Charlie and Diana can then use our uncertainty relation, Equation (3), to bound the eavesdropper's information about their measurement outcomes. If it is too high, they abort the protocol and discard their insecure key. Otherwise, they can generate a secure key.

[6] Note that Charlie and Diana do not take the roles analogous to those of Alice and Bob in the uncertainty game (see later).

Uncertainties about any quantity are always measured relative to the knowledge of an observer. An observer with little knowledge will have high uncertainty while one with more knowledge will have less uncertainty. Previous uncertainty relations give useful bounds with respect to classical knowledge, but do not apply when the knowledge takes the form of data in a quantum memory. In this Letter, we have introduced an uncertainty principle which applies to this new paradigm and uncovered a stark difference. A new term must be added to the classical bound which accounts for any entanglement between the system and the quantum memory. We have illustrated the significance of this term using the two player uncertainty game. Moreover, as we have illustrated using key distribution as an example, our uncertainty relation is likely to have numerous applications in quantum information processing.

The full proofs of the results contained here can be found in the Supplementary Information at the end of this document.

Acknowledgements

We thank Robert König, Jonathan Oppenheim and Marco Tomamichel for discussions and Lídia del Rio for the illustration (Figure 1). MB and MC acknowledge support by the Excellence Network of Bavaria and the German Science Foundation (DFG). JMR acknowledges the support of CASED (www.cased.de). RC and RR acknowledge support from the Swiss National Science Foundation.

[1] Heisenberg, W. Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. *Zeitschrift für Physik* **43**, 172–198 (1927). English translation available in [21].

[2] Julsgaard, B., Sherson, J., Cirac, J. I., Fiurášek, J. & Polzik, E. S. Experimental demonstration of quantum memory for light. *Nature* **432**, 482–486 (2004).

[3] Robertson, H. P. The uncertainty principle. *Physical Review* **34**, 163–164 (1929).

[4] Shannon, C. E. Communication theory of secrecy systems. *Bell System Technical Journal* **28**, 656–715 (1949).

[5] Białynicki-Birula, I. & Mycielski, J. Uncertainty relations for information entropy in wave mechanics. *Communications in Mathematical Physics* **44**, 129–132 (1975).

[6] Deutsch, D. Uncertainty in quantum measurements. *Physical Review Letters* **50**, 631–633 (1983).

[7] Maassen, H. & Uffink, J. B. Generalized entropic uncertainty relations. *Physical Review Letters* **60**, 1103–1106 (1988).

[8] Renes, J. M. & Boileau, J.-C. Conjectured strong complementary information tradeoff. *Physical Review Letters* **103**, 020402 (2009).

[9] Wiesner, S. Conjugate coding. *Sigact News* **15**, 78–88 (1983). Originally written c. 1970 but unpublished.

[10] Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, 175–179 (IEEE, 1984).

[11] Deutsch, D. *et al.* Quantum privacy amplification and the

security of quantum cryptography over noisy channels. *Physical Review Letters* **77**, 2818–2821 (1996).

[12] Lo, H.-K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283**, 2050–2056 (1999).

[13] Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters* **85**, 441–444 (2000).

[14] Christandl, M., Renner, R. & Ekert, A. A generic security proof for quantum key distribution (2004). URL `http://arxiv.org/abs/quant-ph/0402131`.

[15] Renner, R. & König, R. Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography Conference, TCC 2005*, vol. 3378 of *Lecture Notes in Computer Science*, 407–425 (Springer, 2005).

[16] Renner, R. *Security of Quantum Key Distribution*. Ph.D. thesis, ETH Zürich (2005). URL `http://arxiv.org/abs/quant-ph/0512258`.

[17] Koashi, M. Unconditional security of quantum key distribution and the uncertainty principle. *Journal of Physics: Conference Series* **36**, 98–102 (2006).

[18] Ekert, A. Quantum cryptography based on Bell's theorem. *Physical Review Letters* **67**, 661–663 (1991).

[19] Coffman, V., Kundu, J. & Wootters, W. K. Distributed entanglement. *Physical Review A* **61**, 052306 (2000).

[20] Koashi, M. & Winter, A. Monogamy of quantum entanglement and other correlations. *Physical Review A* **69**, 022309 (2004).

[21] Wheeler, J. A. & Zurek, W. H. (eds.) *Quantum Theory and Measurement* (Princeton University Press, Princeton, 1983).

Supplementary Information

Here we present the full proof of our main result, the uncertainty relation given in Equation (3) of the main manuscript (Theorem 1 below).

In order to state our result precisely, we introduce a few definitions. Consider two measurements described by orthonormal bases $\{|\psi_j\rangle\}$ and $\{|\phi_k\rangle\}$ on a d-dimensional Hilbert space $\mathcal{H}_A$ (note that they are not necessarily complementary). The measurement processes are then described by the completely positive maps

$$\mathcal{R} : \rho \mapsto \sum_j \langle\psi_j|\rho|\psi_j\rangle |\psi_j\rangle\langle\psi_j| \quad \text{and}$$
$$\mathcal{S} : \rho \mapsto \sum_k \langle\phi_k|\rho|\phi_k\rangle |\phi_k\rangle\langle\phi_k|$$

respectively. We denote the square of the overlap of these measurements by c, i.e.

$$c := \max_{j,k} |\langle\psi_j|\phi_k\rangle|^2. \tag{4}$$

Furthermore, we assume that $\mathcal{H}_B$ is an arbitrary finite-dimensional Hilbert space. The von Neumann entropy of A given B is denoted $H(A|B)$ and is defined via $H(A|B) := H(AB) - H(B)$, where for a state ρ on $\mathcal{H}_A$ we have $H(A) := -\mathrm{tr}(\rho \log \rho)$.

The statement we prove is then

Theorem 1. *For any density operator ρ_{AB} on $\mathcal{H}_A \otimes \mathcal{H}_B$,*

$$H(R|B) + H(S|B) \geq \log_2 \frac{1}{c} + H(A|B), \tag{5}$$

where $H(R|B)$, $H(S|B)$, and $H(A|B)$ denote the conditional von Neumann entropies of the states $(\mathcal{R} \otimes \mathcal{I})(\rho_{AB})$, $(\mathcal{S} \otimes \mathcal{I})(\rho_{AB})$, and ρ_{AB}, respectively.

In the next section, we introduce the smooth min- and max- entropies and give some properties that will be needed in the proof.

Before that, we show that the statement of our main theorem is equivalent to a relation conjectured by Boileau and Renes [1].

Corollary 2. *For any density operator ρ_{ABE} on $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$,*

$$H(R|E) + H(S|B) \geq \log_2 \frac{1}{c}. \tag{6}$$

Proof. To show that our result implies (6), we first rewrite (5) as $H(RB) + H(SB) \geq \log_2 \frac{1}{c} + H(AB) + H(B)$. In the case that ρ_{ABE} is pure, we have $H(RB) = H(RE)$ and $H(AB) = H(E)$. This yields the expression $H(RE) + H(SB) \geq \log_2 \frac{1}{c} + H(E) + H(B)$, which is equivalent to (6). The result for arbitrary states ρ_{ABE} follows by the concavity of the conditional entropy (see e.g. [2]).

That (6) implies (5) can be seen by taking ρ_{ABE} as the state which purifies ρ_{AB} in (6) and reversing the argument above. □

1. (Smooth) min- and max-entropies—definitions

As described above, we prove a generalized version of (5), which is formulated in terms of smooth min- and max-entropies. This section contains the basic definitions, while Section 5 b summarizes the properties of smooth entropies needed for this work. For a more detailed discussion of the smooth entropy calculus, we refer to [3–6].

We use $\mathcal{U}_=(\mathcal{H}) := \{\rho : \rho \geq 0, \mathrm{tr}\rho = 1\}$ to denote the set of normalized states on a finite-dimensional Hilbert space $\mathcal{H}$ and $\mathcal{U}_\leq(\mathcal{H}) := \{\rho : \rho \geq 0, \mathrm{tr}\rho \leq 1\}$ to denote the set of subnormalized states on $\mathcal{H}$. The definitions below apply to subnormalized states.

The conditional min-entropy of A given B for a state $\rho \in \mathcal{U}_{\leq}(\mathcal{H}_{AB})$ is defined as[7]

$$H_{\min}(A|B)_\rho := \sup_\sigma H_{\min}(A|B)_{\rho|\sigma} \ ,$$

where the supremum is over all normalized density operators $\sigma \in \mathcal{U}_{=}(\mathcal{H}_B)$ and where

$$H_{\min}(A|B)_{\rho|\sigma} := -\log_2 \inf\{\lambda : \ \rho_{AB} \leq \lambda \, \mathbb{1}_A \otimes \sigma_B\} \ .$$

In the special case where the B system is trivial, we write $H_{\min}(A)_\rho$ instead of $H_{\min}(A|B)_\rho$. It is easy to see that $H_{\min}(A)_\rho = -\log_2 \|\rho_A\|_\infty$ and that for $\rho \leq \tau$, $H_{\min}(A|B)_\rho \geq H_{\min}(A|B)_\tau$.

Furthermore, for $\rho \in \mathcal{U}_{\leq}(\mathcal{H}_A)$, we define

$$H_{\max}(A)_\rho := 2 \log_2 \mathrm{tr}\sqrt{\rho} \ .$$

It follows that for $\rho \leq \tau$, $H_{\max}(A)_\rho \leq H_{\max}(A)_\tau$ (since the square root is operator monotone).

In our proof, we also make use of an intermediate quantity, denoted $H_{-\infty}$. It is defined by

$$H_{-\infty}(A)_\rho := -\log_2 \sup\{\lambda : \ \rho_A \geq \lambda \, \Pi_{\mathrm{supp}(\rho_A)}\} \, ,$$

where $\Pi_{\mathrm{supp}(\rho_A)}$ denotes the projector onto the support of ρ_A. In other words, $H_{-\infty}(A)_\rho$ is equal to the negative logarithm of the smallest non-zero eigenvalue of ρ_A. This quantity will not appear in our final statements but will instead be replaced by a smooth version of $H_{\max}$ (see below and Section 5 b).

The *smooth* min- and max-entropies are defined by extremizing the non-smooth entropies over a set of nearby states, where our notion of nearby is expressed in terms of the *purified distance*. It is defined as (see [6])

$$P(\rho, \sigma) := \sqrt{1 - \bar{F}(\rho, \sigma)^2} \ , \tag{7}$$

where $\bar{F}(\cdot, \cdot)$ denotes the generalized fidelity (which equals the standard fidelity if at least one of the states is normalized),

$$\bar{F}(\rho, \sigma) := \left\| \sqrt{\rho \oplus (1 - \mathrm{tr}\rho)} \sqrt{\sigma \oplus (1 - \mathrm{tr}\sigma)} \right\|_1 \ . \tag{8}$$

(Note that we use $F(\rho, \sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1$ to denote the standard fidelity.)

The purified distance is a distance measure; in particular, it satisfies the triangle inequality $P(\rho, \sigma) \leq P(\rho, \tau) + P(\tau, \sigma)$. As its name indicates, $P(\rho, \sigma)$ corresponds to the minimum trace distance[8] between purifications of ρ and σ. Further properties are stated in Section 5 a.

We use the purified distance to specify a ball of subnormalized density operators around ρ:

$$\mathcal{B}^\varepsilon(\rho) := \{\rho' : \rho' \in \mathcal{U}_{\leq}(\mathcal{H}), P(\rho, \rho') \leq \varepsilon\} \ .$$

Then, for any $\varepsilon \geq 0$, the *ε-smooth min- and max-entropies* are defined by

$$\begin{aligned} H_{\min}^\varepsilon(A|B)_\rho &:= \sup_{\rho' \in \mathcal{B}^\varepsilon(\rho)} H_{\min}(A|B)_{\rho'} \\ H_{\max}^\varepsilon(A)_\rho &:= \inf_{\rho' \in \mathcal{B}^\varepsilon(\rho)} H_{\max}(A)_{\rho'} \ . \end{aligned}$$

In the following, we will sometimes omit the subscript ρ when it is obvious from context which state is implied.

---

[7] In the case of finite dimensional Hilbert spaces (as in this work), the infima and suprema used in our definitions can be replaced by minima and maxima.

[8] The trace distance between two states τ and κ is defined by $\frac{1}{2}\|\tau - \kappa\|_1$ where $\|\Gamma\|_1 = \mathrm{tr}\sqrt{\Gamma\Gamma^\dagger}$.

2. Overview of the proof

The proof of our main result, Theorem 1, is divided into two main parts, each individually proven in the next sections.

In the first part, given in Section 3, we prove the following uncertainty relation, which is similar to the main result but formulated in terms of the quantum entropies $H_{\min}$ and $H_{-\infty}$.

Theorem 3. *For any $\rho_{AB} \in \mathcal{U}_{\leq}(\mathcal{H}_{AB})$ we have*

$$H_{\min}(R|B)_{(\mathcal{R}\otimes\mathcal{I})(\rho)} + H_{-\infty}(SB)_{(\mathcal{S}\otimes\mathcal{I})(\rho)} \geq \log_2 \frac{1}{c} + H_{\min}(AB)_\rho \ .$$

The second part of the proof involves *smoothing* the above relation and yields the following theorem (see Section 4)[9].

Theorem 4. *For any $\rho \in \mathcal{U}_{=}(\mathcal{H}_{AB})$ and $\varepsilon > 0$,*

$$H_{\min}^{5\sqrt{\varepsilon}}(R|B)_{(\mathcal{R}\otimes\mathcal{I})(\rho)} + H_{\max}^{\varepsilon}(SB)_{(\mathcal{S}\otimes\mathcal{I})(\rho)} \geq \log_2 \frac{1}{c} + H_{\min}^{\varepsilon}(AB)_\rho - 2\log_2 \frac{1}{\varepsilon} \ .$$

From Theorem 4, the von Neumann version of the uncertainty relation (Theorem 1) can be obtained as an asymptotic special case for i.i.d. states. More precisely, for any $\sigma \in \mathcal{U}_{=}(\mathcal{H}_{AB})$ and for any $n \in \mathbb{N}$, we evaluate the inequality for $\rho = \sigma^{\otimes n}$ where $\mathcal{R}\otimes\mathcal{I}$ and $\mathcal{S}\otimes\mathcal{I}$ are replaced by $(\mathcal{R}\otimes\mathcal{I})^{\otimes n}$ and $(\mathcal{S}\otimes\mathcal{I})^{\otimes n}$, respectively. Note that the corresponding overlap is then given by

$$c^{(n)} = \max_{j_1\ldots j_n, k_1\ldots k_n} |\langle\psi_{j_1}|\phi_{k_1}\rangle \ldots \langle\psi_{j_n}|\phi_{k_n}\rangle|^2 = \max_{j,k} |\langle\psi_j^{\otimes n}|\phi_k^{\otimes n}\rangle|^2 = c^n \ .$$

The assertion of the theorem can thus be rewritten as

$$\frac{1}{n} H_{\min}^{5\sqrt{\varepsilon}}(R^n|B^n)_{((\mathcal{R}\otimes\mathcal{I})(\sigma))^{\otimes n}} + \frac{1}{n} H_{\max}^{\varepsilon}(S^n B^n)_{((\mathcal{S}\otimes\mathcal{I})(\sigma))^{\otimes n}} \geq \log_2 \frac{1}{c} + \frac{1}{n} H_{\min}^{\varepsilon}(A^n B^n)_{\sigma^{\otimes n}} - \frac{2}{n}\log_2 \frac{1}{\varepsilon} \ .$$

Taking the limit $n \to \infty$ and then $\varepsilon \to 0$ and using the asymptotic equipartition property (Lemma 9), we obtain $H(R|B) + H(SB) \geq \log_2 \frac{1}{c} + H(AB)$, from which Theorem 1 follows by subtracting $H(B)$ from both sides.

3. Proof of Theorem 3

In this section we prove a version of Theorem 1, formulated in terms of the quantum entropies $H_{\min}$ and $H_{-\infty}$.

We introduce $D_R = \sum_j e^{\frac{2\pi i j}{d}} |\psi_j\rangle\langle\psi_j|$ and $D_S = \sum_k e^{\frac{2\pi i k}{d}} |\phi_k\rangle\langle\phi_k|$ (D_R and D_S are d-dimensional generalizations of Pauli operators). The maps $\mathcal{R}$ and $\mathcal{S}$ describing the two measurements can then be rewritten as

$$\mathcal{R} : \rho \mapsto \frac{1}{d}\sum_{a=0}^{d-1} D_R^a \rho D_R^{-a}$$
$$\mathcal{S} : \rho \mapsto \frac{1}{d}\sum_{b=0}^{d-1} D_S^b \rho D_S^{-b} \ .$$

We use the two chain rules proved in Section 5 b (Lemmas 11 and 12), together with the strong subadditivity of the min-entropy (Lemma 10), to obtain, for an arbitrary density operator $\Omega_{A'B'AB}$,

$$\begin{aligned} H_{\min}(A'B'AB)_\Omega - H_{-\infty}(A'AB)_\Omega &\leq H_{\min}(B'|A'AB)_{\Omega|\Omega} \\ &\leq H_{\min}(B'|AB)_{\Omega|\Omega} \\ &\leq H_{\min}(B'A|B)_\Omega - H_{\min}(A|B)_\Omega. \end{aligned} \quad (9)$$

---

[9] We note that a related relation follows from the work of Maassen and Uffink [7] who derived a relation involving Rényi entropies (the order α Rényi entropy [8] is denoted H_α) and the overlap c (defined in (4)). They showed that $H_\alpha(R)_\rho + H_\beta(S)_\rho \geq \log_2 \frac{1}{c}$, where $\frac{1}{\alpha} + \frac{1}{\beta} = 2$. The case $\alpha \to \infty$, $\beta \to \frac{1}{2}$ yields $H_{\min}(R)_\rho + H_{\max}(S)_\rho \geq \log_2 \frac{1}{c}$.

We now apply this relation to the state $\Omega_{A'B'AB}$ defined as follows[10]:

$$\Omega_{A'B'AB} := \frac{1}{d^2}\sum_{a,b} |a\rangle\langle a|_{A'} \otimes |b\rangle\langle b|_{B'} \otimes (D_R^a D_S^b \otimes \mathbb{1})\rho_{AB}(D_S^{-b} D_R^{-a} \otimes \mathbb{1}) \ ,$$

where $\{|a\rangle_{A'}\}_a$ and $\{|b\rangle_{B'}\}_b$ are orthonormal bases on d-dimensional Hilbert spaces $\mathcal{H}_{A'}$ and $\mathcal{H}_{B'}$.

This state satisfies the following relations:

$$\begin{aligned} H_{\min}(A'B'AB)_\Omega &= 2\log_2 d + H_{\min}(AB)_\rho & (10)\\ H_{-\infty}(A'AB)_\Omega &= \log_2 d + H_{-\infty}(SB)_{(\mathcal{S}\otimes\mathcal{I})(\rho)} & (11)\\ H_{\min}(B'A|B)_\Omega &\leq \log_2 d + H_{\min}(R|B)_{(\mathcal{R}\otimes\mathcal{I})(\rho)} & (12)\\ H_{\min}(A|B)_\Omega &\geq \log_2 \frac{1}{c}. & (13) \end{aligned}$$

Using these in (9) establishes Theorem 3. We proceed by showing (10)–(13).

Relation (10) follows because $\Omega_{A'B'AB}$ is unitarily related to $\frac{1}{d^2}\sum_{a,b} |a\rangle\langle a|_{A'} \otimes |b\rangle\langle b|_{B'} \otimes \rho_{AB}$, and the fact that the unconditional min-entropy is invariant under unitary operations.

To see (11), note that $\Omega_{A'AB}$ is unitarily related to $\frac{1}{d^2}\sum_a |a\rangle\langle a|_{A'} \otimes \sum_b (S^b \otimes \mathbb{1})\rho_{AB}(S^{-b} \otimes \mathbb{1})$ and that $\frac{1}{d}\sum_b (S^b \otimes \mathbb{1})\rho_{AB}(S^{-b} \otimes \mathbb{1}) = (\mathcal{S} \otimes \mathcal{I})(\rho_{AB})$.

To show inequality (12), note that

$$\Omega_{B'AB} = \frac{1}{d^2}\sum_b |b\rangle\langle b|_{B'} \otimes \sum_a (D_R^a D_S^b \otimes \mathbb{1})\rho_{AB}(D_S^{-b} D_R^{-a} \otimes \mathbb{1}).$$

To evaluate the min-entropy, define λ such that $H_{\min}(B'A|B)_\Omega = -\log_2 \lambda$. It follows that there exists a (normalized) density operator σ_B such that

$$\lambda\, \mathbb{1}_{B'A} \otimes \sigma_B \ \geq \ \frac{1}{d^2}\sum_b |b\rangle\langle b|_{B'} \otimes \sum_a (D_R^a D_S^b \otimes \mathbb{1})\rho_{AB}(D_S^{-b} D_R^{-a} \otimes \mathbb{1}).$$

Thus, for all b,

$$\lambda\, \mathbb{1}_A \otimes \sigma_B \ \geq \ \frac{1}{d^2}\sum_a (D_R^a D_S^b \otimes \mathbb{1})\rho_{AB}(D_S^{-b} D_R^{-a} \otimes \mathbb{1}),$$

and in particular, for $b = 0$, we have

$$\begin{aligned} \lambda\, \mathbb{1}_A \otimes \sigma_B \ &\geq \ \frac{1}{d^2}\sum_a (D_R^a \otimes \mathbb{1})\rho_{AB}(D_R^{-a} \otimes \mathbb{1}) \\ &= \ \frac{1}{d}(\mathcal{R} \otimes \mathcal{I})(\rho_{AB}). \end{aligned}$$

We conclude that $2^{-H_{\min}(R|B)_{(\mathcal{R}\otimes\mathcal{I})(\rho)}} \leq \lambda d$, from which (12) follows.

To show (13), we observe that

$$\Omega_{AB} = \frac{1}{d^2}\sum_{ab} (D_R^a D_S^b \otimes \mathbb{1})\rho_{AB}(D_S^{-b} D_R^{-a} \otimes \mathbb{1}) = ((\mathcal{R} \circ \mathcal{S}) \otimes \mathcal{I})(\rho_{AB}) \ .$$

---

[10] The idea behind the use of this state first appeared in [9].

Then,

$$\begin{aligned}((\mathcal{R}\circ\mathcal{S})\otimes\mathcal{I})(\rho_{AB}) &= (\mathcal{R}\otimes\mathcal{I})\left(\sum_k |\phi_k\rangle\langle\phi_k|\otimes \mathrm{tr}_A((|\phi_k\rangle\langle\phi_k|\otimes\mathbb{1})\rho_{AB})\right)\\ &= \sum_{jk} |\langle\phi_k|\psi_j\rangle|^2\,|\psi_j\rangle\langle\psi_j|\otimes \mathrm{tr}_A((|\phi_k\rangle\langle\phi_k|\otimes\mathbb{1})\rho_{AB})\\ &\leq \max_{lm}\left(|\langle\phi_l|\psi_m\rangle|^2\right)\sum_{jk}|\psi_j\rangle\langle\psi_j|\otimes \mathrm{tr}_A((|\phi_k\rangle\langle\phi_k|\otimes\mathbb{1})\rho_{AB})\\ &= \max_{lm}\left(|\langle\phi_l|\psi_m\rangle|^2\right)\,\mathbb{1}_A\otimes\sum_k \mathrm{tr}_A((|\phi_k\rangle\langle\phi_k|\otimes\mathbb{1})\rho_{AB})\\ &= \max_{lm}\left(|\langle\phi_l|\psi_m\rangle|^2\right)\,\mathbb{1}_A\otimes\rho_B.\end{aligned}$$

It follows that $2^{-H_{\min}(A|B)_{((\mathcal{R}\circ\mathcal{S})\otimes\mathcal{I})(\rho)}} \leq \max_{lm}|\langle\phi_l|\psi_m\rangle|^2 = c$, which concludes the proof. □

4. Proof of Theorem 4

The uncertainty relation proved in the previous section (Theorem 3) is formulated in terms of the entropies $H_{\min}$ and $H_{-\infty}$. In this section, we transform these quantities into the smooth entropies $H^\varepsilon_{\min}$ and $H^\varepsilon_{\max}$, respectively, for some $\varepsilon > 0$. This will complete the proof of Theorem 4.

Let $\sigma_{AB}\in\mathcal{U}_{\leq}(\mathcal{H}_{AB})$. Lemma 15 applied to $\sigma_{SB} := (\mathcal{S}\otimes\mathcal{I})(\sigma_{AB})$ implies that there exists a nonnegative operator $\Pi\leq\mathbb{1}$ such that $\mathrm{tr}((\mathbb{1}-\Pi^2)\sigma_{SB})\leq 3\varepsilon$ and

$$H^\varepsilon_{\max}(SB)_{(\mathcal{S}\otimes\mathcal{I})(\sigma)} \geq H_{-\infty}(SB)_{\Pi(\mathcal{S}\otimes\mathcal{I})(\sigma)\Pi} - 2\log_2\frac{1}{\varepsilon}\ . \tag{14}$$

We can assume without loss of generality that Π commutes with the action of $\mathcal{S}\otimes\mathcal{I}$ because it can be chosen to be diagonal in any eigenbasis of σ_{SB}. Hence, $\Pi(\mathcal{S}\otimes\mathcal{I})(\sigma_{AB})\Pi = (\mathcal{S}\otimes\mathcal{I})(\Pi\sigma_{AB}\Pi)$, and

$$\mathrm{tr}((\mathbb{1}-\Pi^2)\sigma_{AB}) = \mathrm{tr}((\mathcal{S}\otimes\mathcal{I})((\mathbb{1}-\Pi^2)\sigma_{AB})) = \mathrm{tr}((\mathbb{1}-\Pi^2)\sigma_{SB}) \leq 3\varepsilon\ . \tag{15}$$

Applying Theorem 3 to the operator $\Pi\sigma_{AB}\Pi$ yields

$$H_{\min}(R|B)_{(\mathcal{R}\otimes\mathcal{I})(\Pi\sigma\Pi)} + H_R(SB)_{(\mathcal{S}\otimes\mathcal{I})(\Pi\sigma\Pi)} \geq \log_2\frac{1}{c} + H_{\min}(AB)_{\Pi\sigma\Pi}\ . \tag{16}$$

Note that $\Pi\sigma\Pi\leq\sigma$ and so

$$H_{\min}(AB)_{\Pi\sigma\Pi} \geq H_{\min}(AB)_\sigma. \tag{17}$$

Using (14) and (17) to bound the terms in (16), we find

$$H_{\min}(R|B)_{(\mathcal{R}\otimes\mathcal{I})(\Pi\sigma\Pi)} + H^\varepsilon_{\max}(SB)_{(\mathcal{S}\otimes\mathcal{I})(\sigma)} \geq \log_2\frac{1}{c} + H_{\min}(AB)_\sigma - 2\log_2\frac{1}{\varepsilon}\ . \tag{18}$$

Now we apply Lemma 18 to ρ_{AB}. Hence there exists a nonnegative operator $\bar{\Pi}\leq\mathbb{1}$ which is diagonal in an eigenbasis of ρ_{AB} such that

$$\mathrm{tr}((\mathbb{1}-\bar{\Pi}^2)\rho_{AB}) \leq 2\varepsilon \tag{19}$$

and $H_{\min}(AB)_{\bar{\Pi}\rho\bar{\Pi}} \geq H^\varepsilon_{\min}(AB)_\rho$. Evaluating (18) for $\sigma_{AB} := \bar{\Pi}\rho_{AB}\bar{\Pi}$ thus gives

$$H_{\min}(R|B)_{(\mathcal{R}\otimes\mathcal{I})(\Pi\bar{\Pi}\rho\bar{\Pi}\Pi)} + H^\varepsilon_{\max}(SB)_{(\mathcal{S}\otimes\mathcal{I})(\bar{\Pi}\rho\bar{\Pi})} \geq \log_2\frac{1}{c} + H^\varepsilon_{\min}(AB)_\rho - 2\log_2\frac{1}{\varepsilon}\ , \tag{20}$$

where Π is diagonal in any eigenbasis of $(\mathcal{S}\otimes\mathcal{I})(\bar{\Pi}\rho_{AB}\bar{\Pi})$ and satisfies

$$\mathrm{tr}((\mathbb{1}-\Pi^2)\bar{\Pi}\rho_{AB}\bar{\Pi}) \leq 3\varepsilon\ . \tag{21}$$

Since $\rho_{AB} \geq \bar{\Pi}\rho_{AB}\bar{\Pi}$, we can apply Lemma 17 to $(\mathcal{S}\otimes\mathcal{I})(\rho_{AB})$ and $(\mathcal{S}\otimes\mathcal{I})(\bar{\Pi}\rho_{AB}\bar{\Pi})$, which gives

$$H_{\max}^{\varepsilon}(SB)_{(\mathcal{S}\otimes\mathcal{I})(\rho)} \geq H_{\max}^{\varepsilon}(SB)_{(\mathcal{S}\otimes\mathcal{I})(\bar{\Pi}\rho\bar{\Pi})} \ . \tag{22}$$

The relation (20) then reduces to

$$H_{\min}(R|B)_{(\mathcal{R}\otimes\mathcal{I})(\Pi\bar{\Pi}\rho\bar{\Pi}\Pi)} + H_{\max}^{\varepsilon}(SB)_{(\mathcal{S}\otimes\mathcal{I})(\rho)} \geq \log_2\frac{1}{c} + H_{\min}^{\varepsilon}(AB)_{\rho} - 2\log_2\frac{1}{\varepsilon} \ . \tag{23}$$

Finally, we apply Lemma 7 to (19) and (21), which gives

$$\begin{aligned} P(\rho_{AB}, \bar{\Pi}\rho_{AB}\bar{\Pi}) &\leq \sqrt{4\varepsilon} \\ P(\bar{\Pi}\rho_{AB}\bar{\Pi}, \Pi\bar{\Pi}\rho_{AB}\bar{\Pi}\Pi) &\leq \sqrt{6\varepsilon} \ . \end{aligned}$$

Hence, by the triangle inequality

$$P(\rho_{AB}, \Pi\bar{\Pi}\rho_{AB}\bar{\Pi}\Pi) \leq (\sqrt{4}+\sqrt{6})\sqrt{\varepsilon} < 5\sqrt{\varepsilon} \ .$$

Consequently, $(\mathcal{R}\otimes\mathcal{I})(\Pi\bar{\Pi}\rho_{AB}\bar{\Pi}\Pi)$ has at most distance $5\sqrt{\varepsilon}$ from $(\mathcal{R}\otimes\mathcal{I})(\rho_{AB})$. This implies

$$H_{\min}^{5\sqrt{\varepsilon}}(R|B)_{(\mathcal{R}\otimes\mathcal{I})(\rho)} \geq H_{\min}(R|B)_{(\mathcal{R}\otimes\mathcal{I})(\Pi\bar{\Pi}\rho\bar{\Pi}\Pi)} \ .$$

Inserting this in (23) gives

$$H_{\min}^{5\sqrt{\varepsilon}}(R|B)_{(\mathcal{R}\otimes\mathcal{I})(\rho)} + H_{\max}^{\varepsilon}(SB)_{(\mathcal{S}\otimes\mathcal{I})(\rho)} \geq \log_2\frac{1}{c} + H_{\min}^{\varepsilon}(AB)_{\rho} - 2\log_2\frac{1}{\varepsilon} \ ,$$

which completes the proof of Theorem 4. □

5. Technical properties

a. *Properties of the purified distance*

The purified distance between ρ and σ corresponds to the minimum trace distance between purifications of ρ and σ, respectively [6]. Because the trace distance can only decrease under the action of a partial trace (see, e.g., [2]), we obtain the following bound.

Lemma 5. *For any $\rho \in \mathcal{U}_{\leq}(\mathcal{H})$ and $\sigma \in \mathcal{U}_{\leq}(\mathcal{H})$,*

$$\|\rho - \sigma\|_1 \leq 2P(\rho,\sigma).$$

The following lemma states that the purified distance is non-increasing under certain mappings.

Lemma 6. *For any $\rho \in \mathcal{U}_{\leq}(\mathcal{H})$ and $\sigma \in \mathcal{U}_{\leq}(\mathcal{H})$, and for any nonnegative operator $\Pi \leq \mathbb{1}$,*

$$P(\Pi\rho\Pi, \Pi\sigma\Pi) \leq P(\rho,\sigma). \tag{24}$$

Proof. We use the fact that the purified distance is non-increasing under any trace-preserving completely positive map (TPCPM) [6] and consider the TPCPM

$$\mathcal{E} : \rho \mapsto \Pi\rho\Pi \oplus \mathrm{tr}(\sqrt{\mathbb{1}-\Pi^2}\rho\sqrt{\mathbb{1}-\Pi^2}).$$

We have $P(\rho,\sigma) \geq P(\mathcal{E}(\rho),\mathcal{E}(\sigma))$, which implies $\bar{F}(\rho,\sigma) \leq \bar{F}(\mathcal{E}(\rho),\mathcal{E}(\sigma))$. Then,

$$\begin{aligned} \bar{F}(\rho,\sigma) &\leq \bar{F}(\mathcal{E}(\rho),\mathcal{E}(\sigma)) \\ &= F(\Pi\rho\Pi,\Pi\sigma\Pi) + \sqrt{(\mathrm{tr}\rho - \mathrm{tr}(\Pi^2\rho))(\mathrm{tr}\sigma - \mathrm{tr}(\Pi^2\sigma))} + \sqrt{(1-\mathrm{tr}\rho)(1-\mathrm{tr}\sigma)} \\ &\leq F(\Pi\rho\Pi,\Pi\sigma\Pi) + \sqrt{(1-\mathrm{tr}(\Pi^2\rho))(1-\mathrm{tr}(\Pi^2\sigma))} \\ &= \bar{F}(\Pi\rho\Pi,\Pi\sigma\Pi), \end{aligned}$$

which is equivalent to the statement of the Lemma.

The second inequality is the relation

$$\sqrt{(\mathrm{tr}\rho - \mathrm{tr}(\Pi^2\rho))(\mathrm{tr}\sigma - \mathrm{tr}(\Pi^2\sigma))} + \sqrt{(1-\mathrm{tr}\rho)(1-\mathrm{tr}\sigma)} \;\leq\; \sqrt{(1-\mathrm{tr}(\Pi^2\rho))(1-\mathrm{tr}(\Pi^2\sigma))},$$

which we proceed to show. For brevity, we write $\mathrm{tr}\rho - \mathrm{tr}(\Pi^2\rho) = r$, $\mathrm{tr}\sigma - \mathrm{tr}(\Pi^2\sigma) = s$, $1-\mathrm{tr}\rho = t$ and $1-\mathrm{tr}\sigma = u$. We hence seek to show

$$\sqrt{rs} + \sqrt{tu} \leq \sqrt{(r+t)(s+u)}.$$

For r, s, t and u nonnegative, we have

$$\begin{aligned}\sqrt{rs} + \sqrt{tu} \leq \sqrt{(r+t)(s+u)} \;&\Leftrightarrow\; rs + 2\sqrt{rstu} + tu \leq (r+t)(s+u)\\ &\Leftrightarrow\; 4rstu \leq (ru+st)^2\\ &\Leftrightarrow\; 0 \leq (ru-st)^2.\end{aligned}$$

□

Furthermore, the purified distance between a state ρ and its image $\Pi\rho\Pi$ is upper bounded as follows.

Lemma 7. *For any $\rho \in \mathcal{U}_{\leq}(\mathcal{H})$, and for any nonnegative operator, $\Pi \leq \mathbb{1}$,*

$$P(\rho, \Pi\rho\Pi) \leq \frac{1}{\sqrt{\mathrm{tr}\rho}}\sqrt{(\mathrm{tr}\rho)^2 - (\mathrm{tr}(\Pi^2\rho))^2}.$$

Proof. Note that

$$\|\sqrt{\rho}\sqrt{\Pi\rho\Pi}\|_1 = \mathrm{tr}\sqrt{(\sqrt{\rho}\Pi\sqrt{\rho})(\sqrt{\rho}\Pi\sqrt{\rho})} = \mathrm{tr}(\Pi\rho)\ ,$$

so we can write the generalized fidelity (see (8)) as

$$\bar{F}(\rho, \Pi\rho\Pi) \;=\; \mathrm{tr}(\Pi\rho) + \sqrt{(1-\mathrm{tr}\rho)(1-\mathrm{tr}(\Pi^2\rho))}\ .$$

For brevity, we now write $\mathrm{tr}\rho = r$, $\mathrm{tr}(\Pi\rho) = s$ and $\mathrm{tr}(\Pi^2\rho) = t$. Note that $0 \leq t \leq s \leq r \leq 1$. Thus,

$$1 - \bar{F}(\rho, \Pi\rho\Pi)^2 \;=\; r + t - rt - s^2 - 2s\sqrt{(1-r)(1-t)}.$$

We proceed to show that $r(1-\bar{F}(\rho,\Pi\rho\Pi)^2) - r^2 + t^2 \leq 0$:

$$\begin{aligned}r(1-\bar{F}(\rho,\Pi\rho\Pi)^2) - r^2 + t^2 \;&=\; r\left(r + t - rt - s^2 - 2s\sqrt{(1-r)(1-t)}\right) - r^2 + t^2\\ &\leq\; r\left(r + t - rt - s^2 - 2s(1-r)\right) - r^2 + t^2\\ &=\; rt - r^2t + t^2 - 2rs + 2r^2s - rs^2\\ &\leq\; rt - r^2t + t^2 - 2rs + 2r^2s - rt^2\\ &=\; (1-r)(t^2 + rt - 2rs)\\ &\leq\; (1-r)(s^2 + rs - 2rs)\\ &=\; (1-r)s(s-r)\\ &\leq\; 0.\end{aligned}$$

This completes the proof. □

Lemma 8. *Let $\rho \in \mathcal{U}_{\leq}(\mathcal{H})$ and $\sigma \in \mathcal{U}_{\leq}(\mathcal{H})$ have eigenvalues r_i and s_i ordered non-increasingly ($r_{i+1} \leq r_i$ and $s_{i+1} \leq s_i$). Choose a basis $|i\rangle$ such that $\sigma = \sum_i s_i |i\rangle\langle i|$ and define $\tilde{\rho} = \sum_i r_i |i\rangle\langle i|$, then*

$$P(\rho, \sigma) \geq P(\tilde{\rho}, \sigma).$$

Proof. By the definition of the purified distance $P(\cdot,\cdot)$, it suffices to show that $\bar{F}(\rho,\sigma) \leq \bar{F}(\tilde{\rho},\sigma)$.

$$\begin{aligned}\bar{F}(\rho,\sigma) - \sqrt{(1-\mathrm{tr}\rho)(1-\mathrm{tr}\sigma)} &= \|\sqrt{\rho}\sqrt{\sigma}\|_1\\ &= \max_U \mathrm{Re}\ \mathrm{tr}(U\sqrt{\rho}\sqrt{\sigma})\\ &\leq \max_{U,V} \mathrm{Re}\ \mathrm{tr}(U\sqrt{\rho}V\sqrt{\sigma})\\ &= \sum_i \sqrt{r_i}\sqrt{s_i} = \bar{F}(\tilde{\rho},\sigma) - \sqrt{(1-\mathrm{tr}\tilde{\rho})(1-\mathrm{tr}\sigma)}.\end{aligned}$$

The maximizations are taken over the set of unitary matrices. The second and third equality are Theorem 7.4.9 and Equation (7.4.14) (on page 436) in [10]. Since $\mathrm{tr}\tilde{\rho} = \mathrm{tr}\rho$, the result follows. □

b. Basic properties of (smooth) min- and max-entropies

Smooth min- and max-entropies can be seen as generalizations of the von Neumann entropy, in the following sense [5].

Lemma 9. *For any $\sigma \in \mathcal{U}_=(\mathcal{H}_{AB})$,*

$$\lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}H_{\min}^{\varepsilon}(A^n|B^n)_{\sigma^{\otimes n}} = H(A|B)_\sigma$$
$$\lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}H_{\max}^{\varepsilon}(A^n)_{\sigma^{\otimes n}} = H(A)_\sigma \ .$$

The von Neumann entropy satisfies the strong subadditivity relation, $H(A|BC) \leq H(A|B)$. That is, discarding information encoded in a system, C, can only increase the uncertainty about the state of another system, A. This inequality directly generalizes to (smooth) min- and max-entropies [3]. In this work, we only need the statement for $H_{\min}$.

Lemma 10 (Strong subadditivity for $H_{\min}$ [3])**.** *For any $\rho \in \mathcal{S}_\leq(\mathcal{H}_{ABC})$,*

$$H_{\min}(A|BC)_{\rho|\rho} \leq H_{\min}(A|B)_{\rho|\rho}. \tag{25}$$

Proof. By definition, we have

$$2^{-H_{\min}(A|BC)_{\rho|\rho}}\mathbb{1}_A \otimes \rho_{BC} - \rho_{ABC} \geq 0 \ .$$

Because the partial trace maps nonnegative operators to nonnegative operators, this implies

$$2^{-H_{\min}(A|BC)_{\rho|\rho}}\mathbb{1}_A \otimes \rho_{B} - \rho_{AB} \geq 0 \ .$$

This implies that $2^{-H_{\min}(A|B)_{\rho|\rho}} \leq 2^{-H_{\min}(A|BC)_{\rho|\rho}}$, which is equivalent to the assertion of the lemma. □

The chain rule for von Neumann entropy states that $H(A|BC) = H(AB|C) - H(B|C)$. This equality generalizes to a family of inequalities for (smooth) min- and max-entropies. In particular, we will use the following two lemmas.

Lemma 11 (Chain rule I)**.** *For any $\rho \in \mathcal{S}_\leq(\mathcal{H}_{ABC})$ and $\sigma_C \in \mathcal{S}_\leq(\mathcal{H}_C)$,*

$$H_{\min}(A|BC)_{\rho|\rho} \leq H_{\min}(AB|C)_\rho - H_{\min}(B|C)_\rho \ .$$

Proof. Let $\sigma_C \in \mathcal{S}_\leq(\mathcal{H}_C)$ be arbitrary. Then, from the definition of the min-entropy we have

$$\begin{aligned}\rho_{ABC} &\leq 2^{-H_{\min}(A|BC)_{\rho|\rho}}\mathbb{1}_A \otimes \rho_{BC} \\ &\leq 2^{-H_{\min}(A|BC)_{\rho|\rho}}2^{-H_{\min}(B|C)_{\rho|\sigma}}\mathbb{1}_{AB} \otimes \sigma_C.\end{aligned}$$

This implies that $2^{-H_{\min}(AB|C)_{\rho|\sigma}} \leq 2^{-H_{\min}(A|BC)_{\rho|\rho}}2^{-H_{\min}(B|C)_{\rho|\sigma}}$ and, hence $H_{\min}(A|BC)_{\rho|\rho} \leq H_{\min}(AB|C)_{\rho|\sigma} - H_{\min}(B|C)_{\rho|\sigma}$. Choosing σ such that $H_{\min}(B|C)_{\rho|\sigma}$ is maximized, we obtain $H_{\min}(A|BC)_{\rho|\rho} \leq H_{\min}(AB|C)_{\rho|\sigma} - H_{\min}(B|C)_\rho$. The desired statement then follows because $H_{\min}(AB|C)_{\rho|\sigma} \leq H_{\min}(AB|C)_\rho$. □

Lemma 12 (Chain rule II)**.** *For any $\rho \in \mathcal{S}_\leq(\mathcal{H}_{AB})$,*

$$H_{\min}(AB)_\rho - H_{-\infty}(B)_\rho \leq H_{\min}(A|B)_{\rho|\rho}.$$

Note that the inequality can be extended by conditioning all entropies on an additional system C, similarly to Lemma 11. However, in this work, we only need the version stated here.

Proof. From the definitions,

$$\begin{aligned}\rho_{AB} &\leq 2^{-H_{\min}(AB)}\mathbb{1}_A \otimes \Pi_{\mathrm{supp}(\rho_B)} \\ &\leq 2^{-H_{\min}(AB)}2^{H_{-\infty}(B)}\mathbb{1}_A \otimes \rho_B.\end{aligned}$$

It follows that $2^{-H_{\min}(A|B)_{\rho|\rho}} \leq 2^{-H_{\min}(AB)}2^{H_{-\infty}(B)}$, which is equivalent to the desired statement. □

The remaining lemmas stated in this appendix are used to transform statements that hold for entropies $H_{\min}$ and H_R into statements for smooth entropies $H_{\min}^{\varepsilon}$ and $H_{\max}^{\varepsilon}$. We start with an upper bound on $H_{-\infty}$ in terms of $H_{\max}$.

Lemma 13. *For any $\varepsilon > 0$ and for any $\sigma \in \mathcal{S}_{\leq}(\mathcal{H}_A)$ there exists a projector Π which is diagonal in any eigenbasis of σ such that $\mathrm{tr}((\mathbb{1} - \Pi)\sigma) \leq \varepsilon$ and*

$$H_{\max}(A)_\sigma > H_{-\infty}(A)_{\Pi\sigma\Pi} - 2\log_2 \frac{1}{\varepsilon} \ .$$

Proof. Let $\sigma = \sum_i r_i |i\rangle\langle i|$ be a spectral decomposition of σ where the eigenvalues r_i are ordered non-increasingly ($r_{i+1} \leq r_i$). Define the projector $\Pi_k := \sum_{i \geq k} |i\rangle\langle i|$. Let j be the smallest index such that $\mathrm{tr}(\Pi_j \sigma) \leq \varepsilon$ and define $\Pi := \mathbb{1} - \Pi_j$. Hence, $\mathrm{tr}(\Pi\sigma) \geq \mathrm{tr}(\sigma) - \varepsilon$. Furthermore,

$$\mathrm{tr}\sqrt{\sigma} \geq \mathrm{tr}(\Pi_{j-1}\sqrt{\sigma}) \geq \mathrm{tr}(\Pi_{j-1}\sigma)\|\Pi_{j-1}\sigma\Pi_{j-1}\|_\infty^{-\frac{1}{2}}.$$

We now use $\mathrm{tr}(\Pi_{j-1}\sigma\Pi_{j-1}) > \varepsilon$ and the fact that $\|\Pi_{j-1}\sigma\Pi_{j-1}\|_\infty$ cannot be larger than the smallest non-zero eigenvalue of $\Pi\sigma\Pi$,[11] which equals $2^{-H_{-\infty}(A)_{\Pi\sigma\Pi}}$. This implies

$$\mathrm{tr}\sqrt{\sigma} > \varepsilon\sqrt{2^{H_{-\infty}(A)_{\Pi\sigma\Pi}}}.$$

Taking the logarithm of the square of both sides concludes the proof. □

Lemma 14. *For any $\varepsilon > 0$ and for any $\sigma \in \mathcal{S}_{\leq}(\mathcal{H}_A)$ there exists a nonnegative operator $\Pi \leq \mathbb{1}$ which is diagonal in any eigenbasis of σ such that $\mathrm{tr}((\mathbb{1} - \Pi^2)\sigma) \leq 2\varepsilon$ and*

$$H^\varepsilon_{\max}(A)_\sigma \geq H_{\max}(A)_{\Pi\sigma\Pi} \ .$$

Proof. By definition of $H^\varepsilon_{\max}(A)_\sigma$, there is a $\rho \in \mathcal{B}^\varepsilon(\sigma)$ such that $H^\varepsilon_{\max}(A)_\sigma = H_{\max}(A)_\rho$. It follows from Lemma 8 that we can take ρ to be diagonal in any eigenbasis of σ. Define

$$\rho' := \rho - \{\rho - \sigma\}_+ = \sigma - \{\sigma - \rho\}_+$$

where $\{\cdot\}_+$ denotes the positive part of an operator. We then have $\rho' \leq \rho$, which immediately implies that $H_{\max}(A)_{\rho'} \leq H_{\max}(A)_\rho$. Furthermore, because $\rho' \leq \sigma$ and because ρ' and σ have the same eigenbasis, there exists a nonnegative operator $\Pi \leq \mathbb{1}$ diagonal in the eigenbasis of σ such that $\rho' = \Pi\sigma\Pi$. The assertion then follows because

$$\mathrm{tr}((\mathbb{1} - \Pi^2)\sigma) = \mathrm{tr}(\sigma) - \mathrm{tr}(\rho') = \mathrm{tr}(\{\sigma - \rho\}_+) \leq \|\rho - \sigma\|_1 \leq 2\varepsilon \ ,$$

where the last inequality follows from Lemma 5 and $P(\rho, \sigma) \leq \varepsilon$. □

Lemma 15. *For any $\varepsilon > 0$ and for any $\sigma \in \mathcal{S}_{\leq}(\mathcal{H}_A)$ there exists a nonnegative operator $\Pi \leq \mathbb{1}$ which is diagonal in any eigenbasis of σ such that $\mathrm{tr}((\mathbb{1} - \Pi^2)\sigma) \leq 3\varepsilon$ and*

$$H^\varepsilon_{\max}(A)_\sigma \geq H_{-\infty}(A)_{\Pi\sigma\Pi} - 2\log_2 \frac{1}{\varepsilon} \ .$$

Proof. By Lemma 14, there exists a nonnegative operator $\bar{\Pi} \leq \mathbb{1}$ such that

$$H^\varepsilon_{\max}(A)_\sigma \geq H_{\max}(A)_{\bar{\Pi}\sigma\bar{\Pi}}$$

and $\mathrm{tr}((\mathbb{1} - \bar{\Pi}^2)\sigma) \leq 2\varepsilon$. By Lemma 13 applied to $\bar{\Pi}\sigma\bar{\Pi}$, there exists a projector $\bar{\bar{\Pi}}$ such that

$$H_{\max}(A)_{\bar{\Pi}\sigma\bar{\Pi}} \geq H_{-\infty}(A)_{\Pi\sigma\Pi} - 2\log_2 \frac{1}{\varepsilon}$$

and $\mathrm{tr}((\mathbb{1} - \bar{\bar{\Pi}})\bar{\Pi}\sigma\bar{\Pi}) \leq \varepsilon$, where we defined $\Pi := \bar{\bar{\Pi}}\bar{\Pi}\bar{\Pi}$. Furthermore, $\bar{\Pi}$, $\bar{\bar{\Pi}}$ and, hence, Π, can be chosen to be diagonal in any eigenbasis of σ. The claim then follows because

$$\mathrm{tr}((\mathbb{1} - \Pi^2)\sigma) = \mathrm{tr}((\mathbb{1} - \bar{\bar{\Pi}}\bar{\Pi}\bar{\Pi}^2)\sigma) = \mathrm{tr}((\mathbb{1} - \bar{\Pi}^2)\sigma) + \mathrm{tr}((\mathbb{1} - \bar{\bar{\Pi}})\bar{\Pi}\sigma\bar{\Pi}) \leq 3\varepsilon.$$

□

[11] If $\Pi\sigma\Pi$ has no non-zero eigenvalue then $H_{-\infty}(A)_{\Pi\sigma\Pi} = -\infty$ and the statement is trivial.

Lemma 16. *Let $\varepsilon \geq 0$, let $\sigma \in \mathcal{S}_{\leq}(\mathcal{H}_A)$ and let $\mathcal{M} : \sigma \mapsto \sum_i |\phi_i\rangle\langle\phi_i|\langle\phi_i|\sigma|\phi_i\rangle$ be a measurement with respect to an orthonormal basis $\{|\phi_i\rangle\}_i$. Then*

$$H_{\max}^{\varepsilon}(A)_{\sigma} \leq H_{\max}^{\varepsilon}(A)_{\mathcal{M}(\sigma)} \ .$$

Proof. The max-entropy can be written in terms of the (standard) fidelity (see also [4]) as

$$H_{\max}(A)_{\sigma} = 2\log_2 F(\sigma_A, \mathbb{1}_A).$$

Using the fact that the fidelity can only increase when applying a trace-preserving completely positive map (see, e.g., [2]), we have

$$F(\sigma_A, \mathbb{1}_A) \leq F(\mathcal{M}(\sigma_A), \mathcal{M}(\mathbb{1}_A)) = F(\mathcal{M}(\sigma_A), \mathbb{1}_A) \ .$$

Combining this with the above yields

$$H_{\max}(A)_{\sigma} \leq H_{\max}(A)_{\mathcal{M}(\sigma)} \ , \tag{26}$$

which proves the claim in the special case where $\varepsilon = 0$.

To prove the general claim, let $\mathcal{H}_S$ and $\mathcal{H}_{S'}$ be isomorphic to $\mathcal{H}_A$ and let U be the isometry from $\mathcal{H}_A$ to $\text{span}\{|\phi_i\rangle_S \otimes |\phi_i\rangle_{S'}\}_i \subseteq \mathcal{H}_S \otimes \mathcal{H}_{S'}$ defined by $|\phi_i\rangle_A \to |\phi_i\rangle_S \otimes |\phi_i\rangle_{S'}$. The action of $\mathcal{M}$ can then equivalently be seen as that of U followed by the partial trace over $\mathcal{H}_{S'}$. In particular, defining $\sigma'_{SS'} := U\sigma_A U^{\dagger}$, we have $\mathcal{M}(\sigma_A) = \sigma'_S$.

Let $\rho' \in \mathcal{S}(\mathcal{H}_{SS'})$ be a density operator such that

$$H_{\max}(S)_{\rho'} = H_{\max}^{\varepsilon}(S)_{\sigma'} \tag{27}$$

and

$$P(\rho'_{SS'}, \sigma'_{SS'}) \leq \varepsilon \ . \tag{28}$$

(Note that, by definition, there exists a state ρ'_S that satisfies (27) with $P(\rho'_S, \sigma'_S) \leq \varepsilon$. It follows from Uhlmann's theorem (see e.g. [2]) and the fact that the purified distance is non-increasing under partial trace that there exists an extension of ρ'_S such that (28) also holds.)

Since $\sigma'_{SS'}$ has support in the subspace $\text{span}\{|\phi_i\rangle_S \otimes |\phi_i\rangle_{S'}\}_i$, we can assume that the same is true for $\rho'_{SS'}$. To see this, define Π as the projector onto this subspace and observe that $\text{tr}_{S'}(\Pi\rho'_{SS'}\Pi)$ cannot be a worse candidate for the optimization in $H_{\max}^{\varepsilon}(S)_{\sigma'}$: From Lemma 8, we can take ρ'_S to be diagonal in the $\{|\phi_i\rangle\}$ basis, i.e. we can write

$$\rho'_S = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i|,$$

where $\lambda_i \geq 0$. We also write

$$\rho_{SS'} = \sum_{ijkl} c_{ijkl} |\phi_i\rangle\langle\phi_j| \otimes |\phi_k\rangle\langle\phi_l|,$$

for some coefficients c_{ijkl}. To ensure $\rho'_S = \text{tr}_{S'}\rho'_{SS'}$, we require $\sum_k c_{ijkk} = \lambda_i \delta_{ij}$. Consider then

$$\begin{aligned} \text{tr}_{S'}(\Pi\rho'_{SS'}\Pi) &= \text{tr}_{S'}\left(\sum_{ij} c_{ijij} |\phi_i\rangle\langle\phi_j| \otimes |\phi_i\rangle\langle\phi_j|\right) \\ &= \sum_i c_{iiii} |\phi_i\rangle\langle\phi_i|. \end{aligned}$$

It follows that $\text{tr}_{S'}(\Pi\rho'_{SS'}\Pi) \leq \rho'_S$ (since $\sum_k c_{iikk} = \lambda_i$ and $c_{iikk} \geq 0$) and hence we have

$$H_{\max}(S)_{\text{tr}_{S'}(\Pi\rho'_{SS'}\Pi)} \leq H_{\max}^{\varepsilon}(S)_{\rho'}.$$

Furthermore, from Lemma 6, we have

$$P(\Pi\rho'_{SS'}\Pi, \sigma'_{SS'}) = P(\Pi\rho'_{SS'}\Pi, \Pi\sigma'_{SS'}\Pi) \leq P(\rho'_{SS'}, \sigma'_{SS'}) \leq \varepsilon,$$

from which it follows that

$$\mathrm{tr}_{S'}(\Pi\rho'_{SS'}\Pi) \in \mathcal{B}^\varepsilon(\sigma'_S).$$

We have hence shown that there exists a state $\rho'_{SS'}$ satisfying (27) and (28) whose support is in $\mathrm{span}\{|\phi_i\rangle_S \otimes |\phi_i\rangle_{S'}\}_i$.

We can thus define $\rho_A := U^\dagger \rho'_{SS'} U$ so that $\rho'_S = \mathcal{M}(\rho_A)$ and hence (27) can be rewritten as

$$H_{\max}(A)_{\mathcal{M}(\rho)} = H^\varepsilon_{\max}(A)_{\mathcal{M}(\sigma)} \ ,$$

and (28) as

$$P(\rho_A, \sigma_A) \leq \varepsilon \ .$$

Using this and (26), we conclude that

$$H^\varepsilon_{\max}(A)_{\mathcal{M}(\sigma)} = H_{\max}(A)_{\mathcal{M}(\rho)} \geq H_{\max}(A)_\rho \geq H^\varepsilon_{\max}(A)_\sigma \ .$$

□

Lemma 17. *Let $\varepsilon \geq 0$, and let $\sigma \in \mathcal{S}_\leq(\mathcal{H}_A)$ and $\sigma' \in \mathcal{S}_\leq(\mathcal{H}_A)$. If $\sigma' \leq \sigma$ then*

$$H^\varepsilon_{\max}(A)_{\sigma'} \leq H^\varepsilon_{\max}(A)_\sigma \ .$$

Proof. By Lemma 16, applied to an orthonormal measurement $\mathcal{M}$ with respect to the eigenbasis of σ, we have

$$H^\varepsilon_{\max}(A)_{\sigma'} \leq H^\varepsilon_{\max}(A)_{\mathcal{M}(\sigma')} \ .$$

Using this and the fact that $\mathcal{M}(\sigma') \leq \mathcal{M}(\sigma) = \sigma$, we conclude that it suffices to prove the claim for the case where σ' and σ are diagonal in the same basis.

By definition, there exists ρ such that $P(\rho, \sigma) \leq \varepsilon$ and $H_{\max}(A)_\rho = H^\varepsilon_{\max}(A)_\sigma$. Because of Lemma 8, ρ can be assumed to be diagonal in an eigenbasis of σ. Hence, there exists an operator Γ which is diagonal in the same eigenbasis such that $\rho = \Gamma\sigma\Gamma$. We define $\rho' := \Gamma\sigma'\Gamma$ for which $\rho' \geq 0$ and $\mathrm{tr}(\rho') \leq \mathrm{tr}(\rho) \leq 1$. Furthermore, since $\rho' \leq \rho$, we have

$$H_{\max}(A)_{\rho'} \leq H_{\max}(A)_\rho = H^\varepsilon_{\max}(A)_\sigma \ .$$

Because σ' and σ can be assumed to be diagonal in the same basis, there exists a nonnegative operator $\Pi \leq \mathbb{1}$ which is diagonal in the eigenbasis of σ (and, hence, of Γ and ρ) such that $\sigma' = \Pi\sigma\Pi$. We then have

$$\rho' = \Gamma\sigma'\Gamma = \Gamma\Pi\sigma\Pi\Gamma = \Pi\Gamma\sigma\Gamma\Pi = \Pi\rho\Pi \ .$$

Using the fact that the purified distance can only decrease under the action of Π (see Lemma 6), we have

$$P(\rho', \sigma') = P(\Pi\rho\Pi, \Pi\sigma\Pi) \leq P(\rho, \sigma) \leq \varepsilon \ .$$

This implies $H^\varepsilon_{\max}(A)_{\sigma'} \leq H_{\max}(A)_{\rho'}$ and thus concludes the proof. □

Lemma 18. *For any $\varepsilon \geq 0$ and for any (normalized) $\sigma \in \mathcal{S}_=(\mathcal{H}_A)$, there exists a nonnegative operator $\Pi \leq \mathbb{1}$ which is diagonal in any eigenbasis of σ such that $\mathrm{tr}((\mathbb{1} - \Pi^2)\sigma) \leq 2\varepsilon$ and*

$$H^\varepsilon_{\min}(A)_\sigma \leq H_{\min}(A)_{\Pi\sigma\Pi} \ .$$

Proof. Let $\rho \in \mathcal{B}^\varepsilon(\sigma)$ be such that $H_{\min}(A)_\rho = H^\varepsilon_{\min}(A)_\sigma$. It follows from Lemma 8 that we can take ρ to be diagonal in an eigenbasis $|i\rangle$ of σ. Let r_i (s_i) be the list of eigenvalues of ρ (σ) and define $\sigma'_A = \sum_i \min(r_i, s_i)|i\rangle\langle i|$. It is easy to see that there exists a nonnegative operator $\Pi \leq \mathbb{1}$ such that $\sigma' = \Pi\sigma\Pi$. Since $\sigma' \leq \rho$, we have

$$H_{\min}(A)_{\Pi\sigma\Pi} = H_{\min}(A)_{\sigma'} \geq H_{\min}(A)_\rho = H^\varepsilon_{\min}(A)_\sigma \ .$$

Furthermore, $\mathrm{tr}((\mathbb{1} - \Pi^2)\sigma) = \mathrm{tr}(\sigma - \sigma') = \sum_{i:\, s_i \geq r_i}(s_i - r_i) \leq \|\sigma - \rho\|_1$. The assertion then follows because, by Lemma 5, the term on the right hand side is bounded by $2P(\sigma, \rho) \leq 2\varepsilon$. □

[1] Renes, J. M. & Boileau, J.-C. Conjectured strong complementary information tradeoff. *Physical Review Letters* **103**, 020402 (2009).

[2] Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).

[3] Renner, R. *Security of Quantum Key Distribution*. Ph.D. thesis, ETH Zürich (2005). URL `http://arxiv.org/abs/quant-ph/0512258`.

[4] König, R., Renner, R. & Schaffner, C. The operational meaning of min- and max-entropy. *IEEE Transactions on Information Theory* **55**, 4337–4347 (2009).

[5] Tomamichel, M., Colbeck, R. & Renner, R. A fully quantum asymptotic equipartition property. *IEEE Transactions on information theory* **55**, 5840–5847 (2009).

[6] Tomamichel, M., Colbeck, R. & Renner, R. Duality between smooth min- and max-entropies (2009). URL `http://arxiv.org/abs/0907.5238`.

[7] Maassen, H. & Uffink, J. B. Generalized entropic uncertainty relations. *Physical Review Letters* **60**, 1103–1106 (1988).

[8] Rényi, A. On measures of information and entropy. In *Proceedings 4th Berkeley Symposium on Mathematical Statistics and Probability*, 547–561 (1961).

[9] Christandl, M. & Winter, A. Uncertainty, monogamy and locking of quantum correlations. *IEEE Transactions on Information Theory* **51**, 3159–3165 (2005).

[10] Horn, R. A. & Johnson, C. R. *Matrix Analysis* (Cambridge University Press, 1985).