Uncertainty Relations from Simple Entropic Properties

Patrick J. Coles, Roger Colbeck, Li Yu, and Michael Zwolak

Phys. Rev. Lett. **108**, 210405 — Published 23 May 2012

DOI: 10.1103/PhysRevLett.108.210405

Uncertainty relations from simple entropic properties

Patrick J. Coles,[1] Roger Colbeck,[2] Li Yu,[1] and Michael Zwolak[3]

[1]*Department of Physics, Carnegie Mellon University, Pittsburgh, Pennsylvania 15213, USA*
[2]*Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, ON N2L 2Y5, Canada*
[3]*Department of Physics, Oregon State University, Corvallis, OR 97331, USA*

Uncertainty relations provide constraints on how well the outcomes of incompatible measurements can be predicted, and, as well as being fundamental to our understanding of quantum theory, they have practical applications such as for cryptography and witnessing entanglement. Here we shed new light on the entropic form of these relations, showing that they follow from a few simple entropic properties, including the data processing inequality. We prove these relations without relying on the exact expression for the entropy, and hence show that a single technique applies to several entropic quantities, including the von Neumann entropy, min- and max-entropies and the Rényi entropies.

PACS numbers: 03.67.-a, 03.67.Hk

Uncertainty relations form a central part of our understanding of quantum mechanics, and give a dramatic illustration of the separation between quantum and classical physics. They provide fundamental constraints on how well the outcomes of various incompatible measurements can be predicted, as first noted by Heisenberg in the case of position and momentum measurements [1]. This and other early uncertainty relations [2, 3] were formulated using the standard deviation as the measure of uncertainty.

With the advent of information theory, it became natural to develop relations using entropies to measure uncertainty [4–8]. Furthermore, the most recent versions also account for the possibility of observers holding additional side-information which they can use to predict the measurement outcomes [9–11], and the measurements can be arbitrary POVMs (Positive Operator Valued Measures) [12, 13], which can be thought of as projective measurements on a possibly enlarged space (see, e.g. [14]). When formulated in this way, uncertainty relations can be applied more directly to problems related to information processing tasks (data compression, transmission over noisy channels, etc.), or to cryptography, since the quantities involved (conditional entropies) have direct operational meanings.

Applications of the uncertainty principle go right back to the first work on quantum cryptography [15], which discussed a proposal for quantum money, amongst other things. However, because they did not account for the possibility of quantum side information, the uncertainty relations available at the time could not be directly applied to prove security against arbitrary adversaries, and served only an intuitional purpose. Following the discovery of uncertainty relations that account for the possibility of quantum side information, there have been many direct applications. They have been used, for example, as experimentally efficient entanglement witnesses [11, 16, 17], to provide tight finite-key rates in quantum key distribution [18] and to prove security of certain position-based quantum cryptography protocols [19, 20].

One way to think about uncertainty relations is in the following tripartite scenario. Consider a system, A, that will be measured using one of two measurements, X and Z, which can be described in terms of their POVM elements, $\{X_j\}$ and $\{Z_k\}$ (in this work, we take these sets to be finite). If X is measured, an observer (Bob) holding information B is asked to predict the outcome of this measurement, while if Z is measured, a second observer (Charlie) holding C is asked to predict the outcome. In general, the information B and C held by the observers may be quantum, and, most generally, the state before measurement is described by a tripartite density operator, ρ_{ABC}. Uncertainty relations provide quantitative limits on the prediction accuracy, often giving a *trade-off* between Bob's ability to predict X and Charlie's ability to predict Z.

There are many different ways to measure uncertainty, and for much of this paper, we need not specify precisely which measure we are using. We use H_K to denote a generic measure of uncertainty, which we call a K-entropy. $H_K(X|B)$ is then a measure of the uncertainty about the outcome of measurement X given B and, likewise, $H_{\widehat{K}}(Z|C)$ is a measure of the uncertainty about the outcome of measurement Z given C, where, for our uncertainty relations, we require the unspecified entropies, H_K and $H_{\widehat{K}}$, to be closely related as explained later. A tripartite uncertainty relation then gives a lower bound on $H_K(X|B) + H_{\widehat{K}}(Z|C)$ which depends on the measurements X and Z, and reflects their complementarity. For example, in the case where X and Z are composed of commuting projectors, so that there exist states for which both predictions can be correctly made, this lower bound will be trivial (i.e. 0).

In this work, we show that such uncertainty relations follow from a few simple entropic properties. Among them, the data-processing inequality forms a central part. Roughly speaking, this states that if B provides information about A, then processing B cannot decrease the uncertainty about A, which is clearly what one would

expect from an uncertainty measure.

We also obtain relations for the bipartite case where only one measurement will be made (i.e. where we only ask Bob to predict the outcome of the measurement of X). The state-independent relation we obtain is trivial if X is projective (then there is always a state for which $H_K(X|B) = 0$), but gives an interesting bound for more general measurements. Furthermore, we give an additional relation that depends on the entropy of the initial state.

More precisely, our main result is that for any entropy H_K that satisfies a particular set of properties (stated below), the relations

$$H_K(X|B) + H_{\widehat{K}}(Z|C) \geqslant \log \frac{1}{c(X,Z)}, \tag{1}$$

$$H_K(X|B) \geqslant \log \frac{1}{c(X)}, \quad \text{and} \tag{2}$$

$$H_K(X|B) \geqslant \log \frac{1}{c'(X)} + H_K(A|B) \tag{3}$$

hold for any state ρ_{ABC}, where $c(X,Z) = \max_{jk} \|\sqrt{X_j}\sqrt{Z_k}\|_\infty^2$, $c(X) = c(X,\{\mathbb{1}\})$ and $c'(X) = \max_j \mathrm{Tr}(X_j)$ (the infinity norm of an operator is its largest singular value) [35]. In (3), $H_K(A|B)$ is the conditional K-entropy of A given B, and in (1), $H_{\widehat{K}}$ is the entropy dual to H_K in the sense that for any pure state ρ_{ABC}, $H_K(A|B) + H_{\widehat{K}}(A|C) = 0$.

In particular, our proof applies to the von Neumann entropy, the min- and max-entropies, and a range of Rényi entropies. For the tripartite relation, the first two cases were already known [11–13], while the latter is new, and for the bipartite relations we extend previous work on this idea [13, 21, 22] to allow for other entropies or quantum side information. To emphasize, the main contribution of the present work is that it provides a unified proof of these relations.

Entropic Properties.—As mentioned above, we are interested in the uncertainties of POVM outcomes. A POVM, X, can be specified via a set of operators $\{X_j\}$ that satisfy $X_j \geqslant 0$, $\sum_j X_j = \mathbb{1}$. We also define an associated TPCPM (Trace Preserving Completely Positive Map), $\mathcal{X}$, from $\mathcal{H}_A$ to $\mathcal{H}_X$ given by

$$\mathcal{X} : \rho_A \mapsto \sum_j |j\rangle\langle j|_X \mathrm{Tr}(X_j \rho_A), \tag{4}$$

where $\{|j\rangle\}$ form an orthonormal basis in $\mathcal{H}_X$. Thus, for a state ρ_{AB}, we can define the conditional K-entropy of X given B, denoted $H_K(X|B)$, as the conditional K-entropy of the state $(\mathcal{X} \otimes \mathcal{I})(\rho_{AB})$.

A (bipartite) conditional entropy is a map from the set of density operators on a Hilbert space $\mathcal{H}_{AB}$ to the real numbers. In turns out to be convenient to consider a generalized quantity, $D_K(S||T)$, which maps two positive semi-definite operators to the real numbers. Such quantities are often called relative entropies. We consider relative K-entropies that are constructed such that they generalize the respective conditional K-entropies in the sense that, depending on the entropy, either $H_K(A|B) = -D_K(\rho_{AB}||\mathbb{1} \otimes \rho_B)$, or $H_K(A|B) = \max_{\sigma_B}[-D_K(\rho_{AB}||\mathbb{1}\otimes\sigma_B)]$ where σ_B is any (normalized) density operator on $\mathcal{H}_B$.

We now introduce the properties of D_K that allow us to prove our uncertainty relations:

(a) Decrease under TPCPMs: If $\mathcal{E}$ is a TPCPM, then $D_K(\mathcal{E}(S)||\mathcal{E}(T)) \leqslant D_K(S||T)$.

(b) Being unaffected by null subspaces: $D_K(S \oplus 0||T \oplus T') = D_K(S||T)$, where $\oplus$ denotes direct sum.

(c) Multiplying the second argument: If c is a positive constant, then $D_K(S||cT) = D_K(S||T) + \log \frac{1}{c}$.

(d) Zero for identical states: For any density operator ρ, $D_K(\rho||\rho) = 0$.

Property (a) implies the increase of $H_K(A|B)$ under TPCPMs on B, i.e. the data processing inequality—doing operations on B cannot decrease the uncertainty about A. It also implies that D_K is invariant under isometries U, i.e.,

$$D_K(USU^\dagger||UTU^\dagger) = D_K(S||T). \tag{5}$$

This can be seen by invoking (a) twice in succession, first with the TPCPM corresponding to U, then with a TPCPM that undoes U, establishing that $D_K(S||T) \geqslant D_K(USU^\dagger||UTU^\dagger) \geqslant D_K(S||T)$, and hence (5).

The uncertainty relation (1) is expressed in terms of the entropy H_K and its dual $H_{\widehat{K}}$, the latter being defined by $H_{\widehat{K}}(A|B) := -H_K(A|C)$, where ρ_{ABC} is a purification of ρ_{AB}. That this is independent of the chosen purification (and hence that $H_{\widehat{K}}$ is well-defined) is ensured by the invariance of $H_K(A|B)$ under local isometries (shown in the Supplemental Material [36]), and the fact that purifications are unique up to isometries on the purifying system (see, for example, [14]). This definition also ensures that $H_{\widehat{K}}(A|B)$ inherits many natural properties of $H_K(A|B)$, for example, increase under TPCPMs on B and invariance under local isometries.

We proceed by giving some examples of entropies that fit these criteria. The first is the von Neumann entropy, which can be defined via the von Neumann relative entropy. For two positive operators, S and T, this is given by

$$D(S||T) := \lim_{\xi \to 0} \frac{1}{\mathrm{Tr}S}(\mathrm{Tr}(S \log S) - \mathrm{Tr}(S \log(T + \xi\mathbb{1}))).$$

Note that if T is invertible, the limit is not needed, and if part of S lies outside the support of T then $D(S||T) = \infty$. For a density operator ρ_{AB}, we can then

define the conditional von Neumann entropy of A given B by $H(A|B) := -D(\rho_{AB}||\mathbb{1} \otimes \rho_B)$. The von Neumann entropy is its own dual, i.e. for any pure state ρ_{ABC}, we have $H(A|B) = -H(A|C)$.

A second class of entropies to which our results apply are a range of Rényi entropies [23, 24] (for examples of their application, see e.g. [25]). For positive operators, S and T, and for $\alpha \in (0,1) \cup (1,2]$, the Rényi relative entropy of order α is defined by

$$D_\alpha(S||T) := \lim_{\xi \to 0} \frac{1}{\alpha - 1} \log \mathrm{Tr}(S^\alpha (T + \xi \mathbb{1})^{1-\alpha}).$$

Furthermore, we define

$$\begin{aligned} D_0(S||T) &:= \lim_{\alpha \to 0+} D_\alpha(S||T) \quad \text{and} \\ D_1(S||T) &:= \lim_{\alpha \to 1} D_\alpha(S||T) = D(S||T). \end{aligned}$$

Hence, the von Neumann relative entropy can be seen as the special case $\alpha = 1$. The relative entropy D_α gives rise to the conditional Rényi entropy

$$H_\alpha(A|B) := -D_\alpha(\rho_{AB}||\mathbb{1} \otimes \rho_B),$$

which satisfies the duality relation that $H_\alpha(A|B) = -H_{2-\alpha}(A|C)$ for pure ρ_{ABC} [26].

Furthermore, the min and max relative entropies

$$\begin{aligned} D_{\min}(S||T) &:= \log \min\{\lambda : S \leqslant \lambda T\} \\ D_{\max}(S||T) &:= -2 \log \mathrm{Tr} \sqrt{\sqrt{S} T \sqrt{S}} \end{aligned}$$

can be used to define the related conditional entropies [27, 28]

$$\begin{aligned} H_{\min}(A|B) &:= \max_{\sigma_B} [-D_{\min}(\rho_{AB}||\mathbb{1} \otimes \sigma_B)] \\ H_{\max}(A|B) &:= \max_{\sigma_B} [-D_{\max}(\rho_{AB}||\mathbb{1} \otimes \sigma_B)] \end{aligned}$$

which satisfy the duality relation $H_{\min}(A|B) = -H_{\max}(A|C)$ [28]. We also consider the entropies

$$\widehat{H}_\alpha(A|B) := \max_{\sigma_B} [-D_\alpha(\rho_{AB}||\mathbb{1} \otimes \sigma_B)].$$

While in general we do not have alternative expressions for the duals of the latter entropies, it has been shown [29] that $\widehat{H}_{\min}(A|B) = -\widehat{H}_0(A|C)$ for pure ρ_{ABC}, where $\widehat{H}_{\min}(A|B) := -D_{\min}(\rho_{AB}||\mathbb{1} \otimes \rho_B)$.

Main Results.—Our main result is that the properties discussed above are sufficient to establish the following uncertainty relations [36].

Theorem 1. Let $X = \{X_j\}$ and $Z = \{Z_k\}$ be arbitrary POVMs on A, and $H_K(A|B)$ be such that either $H_K(A|B) = -D_K(\rho_{AB}||\mathbb{1} \otimes \rho_B)$ or $H_K(A|B) = \max_{\sigma_B}[-D_K(\rho_{AB}||\mathbb{1} \otimes \sigma_B)]$, for all ρ_{AB}, where D_K satisfies Properties (a)–(c). It follows that for all ρ_{ABC}

$$H_K(X|B) + H_{\widehat{K}}(Z|C) \geqslant \log \frac{1}{c(X,Z)},$$

where $c(X,Z) = \max_{j,k} \|\sqrt{Z_k}\sqrt{X_j}\|_\infty^2$.

The ideas behind this proof are illustrated below where we give a proof for the special case where H_K is the von Neumann entropy, and X and Z are composed of rank-one projectors.

We also have the following single-measurement uncertainty relation.

Lemma 2. Let $X = \{X_j\}$ be an arbitrary POVM on A, and suppose that H_K and its related D_K satisfy the conditions given in Theorem 1, as well as Property (d). Then, for all ρ_{AB},

$$H_K(X|B) \geqslant \log \frac{1}{c(X)}, \tag{6}$$

where $c(X) := c(X, \{\mathbb{1}\}) = \max_j \|X_j\|_\infty$.

Proof. This follows from Theorem 1 by setting $Z = \{\mathbb{1}\}$ and using the fact that $H_{\widehat{K}}(Z|C) = 0$ in this case (see Lemma S4 in the Supplemental Material). □

However, there is an alternative single-measurement relation, which can give a stronger bound than (6).

Lemma 3. Let $X = \{X_j\}$ be an arbitrary POVM on A, and $H_K(A|B)$ be such that either $H_K(A|B) = -D_K(\rho_{AB}||\mathbb{1} \otimes \rho_B)$ or $H_K(A|B) = \max_{\sigma_B}[-D_K(\rho_{AB}||\mathbb{1} \otimes \sigma_B)]$, for all ρ_{AB}, where D_K satisfies Properties (a)–(c). It follows that

$$H_K(X|B) \geqslant \log \frac{1}{c'(X)} + H_K(A|B),$$

where $c'(X) = \max_j \mathrm{Tr}(X_j)$.

We remark that the bounds in these results can be generalized in the following way. Suppose Π is a projector on $\mathcal{H}_A$ whose support includes the support of ρ_A. The above results hold if $c(X,Z)$ is replaced by $c(X,Z;\Pi) := \max_{j,k} \|\sqrt{Z_k}\Pi\sqrt{X_j}\|_\infty^2$, and if $c'(X)$ is replaced by $c'(X;\Pi) = \max_j \mathrm{Tr}(X_j\Pi)$. See [30] for further ways to take advantage of knowledge of the state to derive tighter uncertainty relations for the von Neumann entropy.

We have shown that, in order to establish that a particular entropy satisfies these uncertainty relations, it suffices to verify that it satisfies a few properties. (Recall that for any entropy satisfying our properties, its dual is automatically well defined; it is not necessary to have an alternative expression for it in order for (1) to hold.)

Lemma 4. All examples of relative entropies defined above satisfy Properties (a) through (d).

Proof. Properties (b), (c), and (d) follow directly from the definitions of these entropies. Property (a) was discussed in, e.g., [14] for the von Neumann relative entropy, in [24, 26] for the Rényi relative entropies (D_0 being a special case), and in [27] for the min relative entropy. For the max relative entropy, it follows because the fidelity is monotonically increasing under TPCPMs [31]. □

This implies that the dual entropy pairs (H, H), $(H_\alpha, H_{2-\alpha})$, $(H_{\min}, H_{\max})$ and $(\widehat{H}_{\min}, \widehat{H}_0)$ each satisfy Eq. (1), and that the entropies H, H_α, $H_{\min}$, $H_{\max}$, $\widehat{H}_\alpha$ and $\widehat{H}_{\min}$ each satisfy Eqs. (2) and (3).

Illustration of the proof technique.—In order to illustrate how our properties combine to yield uncertainty relations, we give a proof in the special case of the von Neumann entropy and where $X = \{|X_j\rangle\langle X_j|\}$ and $Z = \{|Z_k\rangle\langle Z_k|\}$ are orthonormal bases. Although more straightforward, this proof features all of the essential ideas of its generalization. We note that in this case $c(X, Z) = \max_{j,k} |\langle X_j|Z_k\rangle|^2$, and the resulting uncertainty relation,

$$H(X|B) + H(Z|C) \geqslant \log \frac{1}{c(X, Z)}, \tag{7}$$

is the one conjectured in [10] and proven in [11].

We first show that all relative K-entropies are decreasing under increases of its second argument.

Lemma 5. If $D_K(S||T)$ satisfies Properties (a) and (b), then for all positive operators S and T, and for $\tilde{T} \geqslant T$,

$$D_K(S||T) \geqslant D_K(S||\tilde{T}). \tag{8}$$

Proof. Denote $\mathcal{H}_\mu$ as the Hilbert space on which S, T and $\tilde{T}$ are defined and introduce $\mathcal{H}_\nu$ as an isomorphic Hilbert space. Let $\{|\mu_j\rangle\}$ and $\{|\nu_j\rangle\}$ be orthonormal bases for $\mathcal{H}_\mu$ and $\mathcal{H}_\nu$ and let $\mathcal{H} = \mathcal{H}_\mu \oplus \mathcal{H}_\nu$. We also introduce a TPCPM acting on operators on $\mathcal{H}$, $\mathcal{F} : S \mapsto F_1 S F_1^\dagger + F_2 S F_2^\dagger$, with $F_1 = \sum_j |\mu_j\rangle\langle\mu_j|$ and $F_2 = \sum_j |\mu_j\rangle\langle\nu_j|$. For $W := \tilde{T} - T$, we have

$$\begin{aligned} D_K(S||T) &\overset{(b)}{=} D_K(S \oplus 0||T \oplus W) \\ &\overset{(a)}{\geqslant} D_K(\mathcal{F}(S \oplus 0)||\mathcal{F}(T \oplus W)) \\ &\overset{(b)}{=} D_K(S \oplus 0||(T + W) \oplus 0) = D_K(S||\tilde{T}). \end{aligned}$$

□

Now, define the isometry $V_X := \sum_j |j\rangle \otimes X_j$ associated with the X measurement on system A, and the state $\tilde{\rho}_{XABC} := V_X \rho_{ABC} V_X^\dagger$. We proceed to give the proof for the case of pure ρ_{ABC}. The impure case follows by considering a purification, ρ_{ABCD}, and using $H(X|C) \geqslant H(X|CD)$ (from Property (a)). Applying the duality to $\tilde{\rho}_{XABC}$ gives:

$$\begin{aligned} H(X|C) &= -H(X|AB) = D(\tilde{\rho}_{XAB}||\mathbb{1} \otimes \tilde{\rho}_{AB}) \\ &\overset{(b)}{=} D(V_X \rho_{AB} V_X^\dagger||V_X \sum_j X_j \rho_{AB} X_j V_X^\dagger) \\ &\overset{(5)}{=} D(\rho_{AB}||\sum_j X_j \rho_{AB} X_j) \\ &\overset{(a)}{\geqslant} D(\overline{\rho}_{ZB}||\sum_{j,k} |\langle X_j|Z_k\rangle|^2 Z_k \otimes \mathrm{Tr}_A\{X_j \rho_{AB}\}) \\ &\overset{(8)}{\geqslant} D(\overline{\rho}_{ZB}||c(X, Z)\mathbb{1} \otimes \rho_B) \\ &\overset{(c)}{=} \log(1/c(X, Z)) + D(\overline{\rho}_{ZB}||\mathbb{1} \otimes \rho_B) \\ &= \log(1/c(X, Z)) - H(Z|B), \end{aligned} \tag{9}$$

where we have used $\overline{\rho}_{ZB} := \sum_k Z_k \rho_{AB} Z_k$.

We note that our proof technique points to a method for finding states that satisfy the uncertainty relation (7) with equality. In the case of pure states ρ_{ABC} and mutually unbiased bases X and Z (for which $|\langle X_j|Z_k\rangle|$ is independent of j, k), the only inequality remaining is a single use of Property (a) (the fourth line of (9)). In this case, (7) is satisfied with equality if Property (a) is saturated, for the particular TPCPM used in the proof.

For the von Neumann relative entropy, (a) is satisfied with equality [32, 33] if and only if there exists a TPCPM, $\hat{\mathcal{E}}$, that undoes the action of $\mathcal{E}$ on S and T, i.e.

$$(\hat{\mathcal{E}} \circ \mathcal{E})(S) = S, \quad (\hat{\mathcal{E}} \circ \mathcal{E})(T) = T. \tag{10}$$

Hence, states of minimum uncertainty are closely connected to the *reversibility* of certain quantum operations. For specific examples, we refer the reader to [34].

Acknowledgements.—We thank Robert Griffiths for helpful conversations. Research at Carnegie Mellon was supported by the Office of Naval Research and by the National Science Foundation through Grant No. PHY-1068331. Research at Perimeter Institute was supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Research and Innovation.

[1] W. Heisenberg, Zeitschrift für Physik **43**, 172 (1927).
[2] H. P. Robertson, Phys. Rev. **34**, 163 (1929).
[3] E. Schrödinger, Proceedings of The Prussian Academy of Sciences Physics-Mathematical Section **XIX**, 296 (1930).
[4] I. Białynicki-Birula and J. Mycielski, Communications in Mathematical Physics **44**, 129 (1975).
[5] D. Deutsch, Physical Review Letters **50**, 631 (1983).
[6] K. Kraus, Physical Review D **35**, 3070 (1987).
[7] H. Maassen and J. B. M. Uffink, Physical Review Letters **60**, 1103 (1988).
[8] S. Wehner and A. Winter, New Journal of Physics **12**, 025009 (2010).

[9] M. J. W. Hall, Phys. Rev. Lett. **74**, 3307 (1995).

[10] J. M. Renes and J.-C. Boileau, Phys. Rev. Lett. **103**, 020402 (2009).

[11] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, Nature Physics **6**, 659 (2010).

[12] M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).

[13] P. J. Coles, L. Yu, V. Gheorghiu, and R. B. Griffiths, Phys. Rev. A **83**, 062338 (2011).

[14] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000), 5th ed.

[15] S. Wiesner, SIGACT News **15**, 78 (1983).

[16] C.-F. Li, J.-S. Xu, X.-Y. Xu, K. Li, and G.-C. Guo, Nature Physics **7**, 752 (2011).

[17] R. Prevedel, D. R. Hamel, R. Colbeck, K. Fisher, and K. J. Resch, Nature Physics **7**, 757 (2011).

[18] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nature Communications **3**, 634 (2012).

[19] A. Kent, W. J. Munro, and T. P. Spiller, Physical Review A **84**, 012326 (2011).

[20] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner, in *Proceedings of the 31st Annual Cryptology Conference (CRYPTO 11)* (Santa Barbara, CA, USA, 2011), pp. 429–446.

[21] M. Krishna and K. Parthasarathy, Indian J. of Statistics **Ser. A 64**, 842 (2002).

[22] A. E. Rastegin (2008), eprint `arXiv:0807.2691` [quant-ph].

[23] A. Rényi, in *Proceedings 4th Berkeley Symposium on Mathematical Statistics and Probability* (1961), pp. 547–561.

[24] D. Petz, Reports on Mathematical Physics **23**, 57 (1984).

[25] M. Mosonyi and F. Hiai, IEEE Trans. Inf. Theory **57**, 2474 (2011).

[26] M. Tomamichel, R. Colbeck, and R. Renner, IEEE Trans. Inf. Theory **55**, 5840 (2009).

[27] R. Renner, Ph.D. thesis, ETH Zürich (2005), URL `http://arxiv.org/abs/quant-ph/0512258`.

[28] R. Konig, R. Renner, and C. Schaffner, IEEE Trans. Inf. Theory **55**, 4337 (2009).

[29] M. Berta, Master's thesis, ETH Zürich (2008), available at `http://arxiv.org/abs/0912.4495`.

[30] E. Hänggi and M. Tomamichel (2011), eprint `arXiv:1108.5349` [quant-ph].

[31] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Physical Review Letters **76**, 2818 (1996).

[32] D. Petz, Rev. Math. Phys. **15**, 79 (2003).

[33] P. Hayden, R. Jozsa, D. Petz, and A. Winter, Commun. Math. Phys. **246**, 359 (2004).

[34] P. J. Coles, L. Yu, and M. Zwolak (2011), eprint `arXiv:1105.4865` [quant-ph].

[35] While the base of the logarithm is conventionally taken to be 2, so that entropies are measured in *bits*, our results apply for any base, provided the same one is used throughout.

[36] See the Supplemental Material for proofs and elaboration of our results.