Relating different quantum generalizations of the conditional Rényi entropy

Marco Tomamichel, Mario Berta, and Masahito Hayashi

Articles you may be interested in

On quantum Rényi entropies: A new generalization and some properties
Journal of Mathematical Physics **54**, 122203 (2013); 10.1063/1.4838856

Rényi generalizations of the conditional quantum mutual information
Journal of Mathematical Physics **56**, 022205 (2015); 10.1063/1.4908102

Monotonicity of a relative Rényi entropy
Journal of Mathematical Physics **54**, 122201 (2013); 10.1063/1.4838835

Sandwiched Rényi divergence satisfies data processing inequality
Journal of Mathematical Physics **54**, 122202 (2013); 10.1063/1.4838855

α-z-Rényi relative entropies
Journal of Mathematical Physics **56**, 022202 (2015); 10.1063/1.4906367

Correlation detection and an operational interpretation of the Rényi mutual information
Journal of Mathematical Physics **57**, 102201 (2016); 10.1063/1.4964755

Relating different quantum generalizations of the conditional Rényi entropy

Marco Tomamichel,[1,2] Mario Berta,[3,4] and Masahito Hayashi[1,5]

[1]*Centre for Quantum Technologies, National University of Singapore, Singapore 117543, Singapore*
[2]*School of Physics, The University of Sydney, Sydney 2006, Australia*
[3]*Institute for Quantum Information and Matter, Caltech, Pasadena, California 91125, USA*
[4]*Institute for Theoretical Physics, ETH Zurich, 8092 Zürich, Switzerland*
[5]*Graduate School of Mathematics, Nagoya University, Furocho, Chikusaku, Nagoya, 464-860, Japan*

Recently a new quantum generalization of the Rényi divergence and the corresponding conditional Rényi entropies was proposed. Here, we report on a surprising relation between conditional Rényi entropies based on this new generalization and conditional Rényi entropies based on the quantum relative Rényi entropy that was used in previous literature. Our result generalizes the well-known duality relation $H(A|B) + H(A|C) = 0$ of the conditional von Neumann entropy for tripartite pure states to Rényi entropies of two different kinds. As a direct application, we prove a collection of inequalities that relate different conditional Rényi entropies and derive a new entropic uncertainty relation. © *2014 AIP Publishing LLC*. [http://dx.doi.org/10.1063/1.4892761]

I. INTRODUCTION

Recently, there has been renewed interest in finding suitable quantum generalizations of Rényi's[36] entropies and divergences. This is due to the fact that Rényi entropies and divergences have a wide range of applications in classical information theory and cryptography, see, e.g., Ref. 13.

We will review some of the recent progress here, but refer the reader to Ref. 31 for a more in-depth discussion. For our purposes, a quantum system is modeled by a finite dimensional Hilbert space. We denote by $\mathcal{P}$ the set of positive semi-definite operators on that Hilbert space, and by $\mathcal{S}$ the subset of density operators with unit trace.

The following natural quantum generalization of the Rényi divergence has been widely used and has found operational significance, for example, as a cut-off rate in quantum hypothesis testing[28] (see also Refs. 32 and 34). It is usually referred to as *quantum Rényi relative entropy* and for all $\alpha \in (0, 1) \cup (1, \infty)$ given as

$$D_\alpha(\rho \| \sigma) := \frac{1}{\alpha - 1} \log \operatorname{Tr} \left\{ \rho^\alpha \sigma^{1-\alpha} \right\} \tag{1}$$

for arbitrary $\rho \in \mathcal{S}$, $\sigma \in \mathcal{P}$ that satisfy $\rho \ll \sigma$. (The notation $\rho \ll \sigma$ means that σ dominates ρ, i.e., the kernel of σ lies inside the kernel of ρ.)

While this definition has proven useful in many applications, it has a major drawback in that it does not satisfy the data-processing inequality (DPI) for $\alpha > 2$. The DPI states that the quantum Rényi relative entropy is contractive under application of a quantum channel, i.e., $D_\alpha\big(\mathcal{E}[\rho] \big\| \mathcal{E}[\sigma]\big) \leq D_\alpha(\rho \| \sigma)$ for any completely positive trace-preserving map $\mathcal{E}$. Intuitively, this property is very desirable since we want to think of the divergence as a measure of how well ρ can be distinguished from σ, and this can only get more difficult after a channel is applied.

Recently, an alternative quantum generalization has been investigated[30, 31, 42] (see also Ref. 38). It is referred to as *quantum Rényi divergence* (or sandwiched Rényi relative entropy in Ref. 42) and

defined as

$$\widetilde{D}_\alpha(\rho\|\sigma) := \frac{1}{\alpha-1} \log \mathrm{Tr}\left\{\left(\sigma^{\frac{1-\alpha}{2\alpha}}\rho\,\sigma^{\frac{1-\alpha}{2\alpha}}\right)^\alpha\right\} \tag{2}$$

for all $\alpha \in (0,1) \cup (1,\infty)$ and $\rho \in \mathcal{S}$, $\sigma \in \mathcal{P}$ that satisfy $\rho \ll \sigma$. The quantum Rényi divergence has found operational significance in the converse part of quantum hypothesis testing.[29] As such, it satisfies the DPI for all $\alpha \geq \frac{1}{2}$ as was shown by Frank and Lieb[15] and independently by Beigi[6] for $\alpha > 1$. See also earlier work[30,31] where a different proof is given for $\alpha \in (1,2]$. Furthermore, the quantum Rényi divergence has already proven an indispensable tool, for example, in the study of strong converse capacities of quantum channels.[17,42]

The definitions, (1) and (2), are in general different but coincide when ρ and σ commute. For $\alpha \in \{0,1,\infty\}$, we define $D_\alpha(\rho\|\sigma)$ and $\widetilde{D}_\alpha(\rho\|\sigma)$ as the corresponding limit. For $\alpha \to 0$ it has been shown that:[4,14]

$$D_0(\rho\|\sigma) = -\log \mathrm{Tr}\left\{\Pi_\rho\sigma\right\} \tag{3}$$

$$\widetilde{D}_0(\rho\|\sigma) = -\log \max_{i_1,\dots,i_s}\left\{\sum_{j=1}^{s}\lambda_{i_j} : \left\{\Pi_\rho|i_j\rangle\right\} \text{ linearly independent}\right\} \tag{4}$$

with the eigenvalue decomposition $\sigma = \sum_i \lambda_i|i\rangle\langle i|$, $s = \mathrm{rank}(\Pi_\rho\sigma)$, and Π_ρ the projector on the support of ρ. In the limit $\alpha \to 1$ both expressions converge to the quantum relative entropy,[30,31,42] namely

$$D_1(\rho\|\sigma) = \widetilde{D}_1(\rho\|\sigma) = D(\rho\|\sigma) := \mathrm{Tr}\left\{\rho(\log\rho - \log\sigma)\right\}. \tag{5}$$

For $\alpha \to \infty$ the limits have been evaluated in Refs. 31 and 39, respectively:

$$\widetilde{D}_\infty(\rho\|\sigma) = \inf\left\{\lambda \in \mathbb{R} : \rho \leq 2^\lambda\sigma\right\} \tag{6}$$

$$D_\infty(\rho\|\sigma) = \log \max_{i,j}\left\{\frac{\nu_i}{\mu_j} : \langle i|\bar{j}\rangle \neq 0\right\} \tag{7}$$

with the eigenvalue decompositions $\rho = \sum_i \nu_i|i\rangle\langle i|$ and $\sigma = \sum_j \mu_j|\bar{j}\rangle\langle\bar{j}|$.

It has been observed[14,42] that the relation

$$D_\alpha(\rho\|\sigma) \geq \widetilde{D}_\alpha(\rho\|\sigma) \tag{8}$$

follows from the Araki-Lieb-Thirring trace inequality.[1,25] Furthermore, $\alpha \mapsto D_\alpha(\rho\|\sigma)$ and $\alpha \mapsto \widetilde{D}_\alpha(\rho\|\sigma)$ are monotonically increasing functions. For the latter quantity, this was shown in Ref. 31 and independently in Ref. 6.

Finally, very recently Audenaert and Datta[4] defined a more general two parameter family of *α-z-relative Rényi entropies* of the form

$$D_{\alpha,z}(\rho\|\sigma) := \frac{1}{\alpha-1}\log\mathrm{Tr}\left\{\left(\rho^{\frac{\alpha}{z}}\sigma^{\frac{1-\alpha}{z}}\right)^z\right\}, \tag{9}$$

and explored some of its properties. We clearly have $D_\alpha \equiv D_{\alpha,1}$ and $\widetilde{D}_\alpha \equiv D_{\alpha,\alpha}$.

II. QUANTUM CONDITIONAL RÉNYI ENTROPIES

We will in the following consider disjoint quantum systems, denoted by capital letters A, B and C. The sets $\mathcal{P}(A)$ and $\mathcal{S}(A)$ take on the expected meaning.

The conditional von Neumann entropy can be conveniently defined in terms of the quantum relative entropy as follows. For a bipartite state $\rho_{AB} \in \mathcal{S}(AB)$, we define

$$H(A|B)_\rho := H(\rho_{AB}) - H(\rho_B) \tag{10}$$

$$= -D(\rho_{AB}\|1_A \otimes \rho_B) \tag{11}$$

$$= \sup_{\sigma_B \in \mathcal{S}(B)} -D(\rho_{AB}\|1_A \otimes \sigma_B), \tag{12}$$

where $H(\rho) := -\operatorname{Tr}\{\rho \log \rho\}$ is the usual von Neumann entropy. The last equality can be verified using the relation $D(\rho_{AB}\|1_A \otimes \sigma_B) = D(\rho_{AB}\|1_A \otimes \rho_B) + D(\rho_B\|\sigma_B)$ together with the fact that $D(\,\cdot\,\|\,\cdot\,)$ is positive definite.

In the case of Rényi entropies, it is not immediate which expression, (10) and (11), or (12), should be used to define the conditional Rényi entropies. It has been found in the study of the classical special case (see, e.g., Ref. 23 for an overview) that generalizations based on (10) have severe limitations, for example, they cannot be expected to satisfy a DPI. On the other hand, definitions based on the underlying divergence, as in (11) or (12), have proven to be very fruitful and lead to quantities with operational significance. Together with the two proposed quantum generalizations of the Rényi divergence in (1) and (2), this leads to a total of four different candidates for conditional Rényi entropies. For $\alpha \geq 0$ and $\rho_{AB} \in \mathcal{S}(AB)$, we define

$$H_\alpha^\downarrow(A|B)_\rho := -D_\alpha(\rho_{AB}\|1_A \otimes \rho_B), \tag{13}$$

$$H_\alpha^\uparrow(A|B)_\rho := \sup_{\sigma_B \in \mathcal{S}(B)} -D_\alpha(\rho_{AB}\|1_A \otimes \sigma_B), \tag{14}$$

$$\widetilde{H}_\alpha^\downarrow(A|B)_\rho := -\widetilde{D}_\alpha(\rho_{AB}\|1_A \otimes \rho_B), \qquad \text{and,} \tag{15}$$

$$\widetilde{H}_\alpha^\uparrow(A|B)_\rho := \sup_{\sigma_B \in \mathcal{S}(B)} -\widetilde{D}_\alpha(\rho_{AB}\|1_A \otimes \sigma_B). \tag{16}$$

The fully quantum entropy $H_\alpha^\downarrow$ has first been studied in Ref. 39. For the classical and classical-quantum special case this quantity gives a generalization of the leftover hashing lemma[7] for the modified mutual information to Rényi entropies with $\alpha \neq 2$.[19,20]

The classical version of $H_\alpha^\uparrow$ was introduced by Arimoto for an evaluation of the guessing probability.[2] We note that he used another but equivalent expression for $H_\alpha^\uparrow$ that we later explain in Lemma 1. Then, Gallager used $H_\alpha^\uparrow$ (again in the form of Lemma 1) to upper bound the decoding error probability of a random coding scheme for data compression with side-information.[16,43] The classical and classical-quantum special cases of $H_\alpha^\uparrow$ were, for example, also investigated in Refs. 20 and 22 and realize another type of a generalization of the leftover hashing lemma for the L_1-distinguishability in the study of randomness extraction to Rényi entropies with $\alpha \neq 2$.

It follows immediately from the definition and the corresponding property of D_α that these two entropies satisfy a data-processing inequality. Namely, for any quantum operation $\mathcal{E}_{B \to B'}$ with $\tau_{AB'} = \mathcal{E}_{B \to B'}[\rho_{AB}]$ and any $\alpha \in [0, 2]$, we have

$$H_\alpha^\downarrow(A|B)_\rho \leq H_\alpha^\downarrow(A|B')_\tau \qquad \text{and} \qquad H_\alpha^\uparrow(A|B)_\rho \leq H_\alpha^\uparrow(A|B')_\tau, \tag{17}$$

while their classical-quantum versions have been obtained in Ref. 20.

The conditional entropy $\widetilde{H}_\alpha^\uparrow$ was proposed in Ref. 38 and investigated in Ref. 31, whereas $\widetilde{H}_\alpha^\downarrow$ is first considered in this paper. (Since the relative entropies $\widetilde{D}_\alpha$ and D_α are identical for commuting operators, we note that $\widetilde{H}_\alpha^\uparrow = H_\alpha^\uparrow$ as well as $\widetilde{H}_\alpha^\downarrow = H_\alpha^\downarrow$ for classical distributions.) Both definitions satisfy the above data-processing inequality for $\alpha \geq \frac{1}{2}$.

Furthermore, it is easy to verify that all entropies considered are invariant under applications of local isometries on either the A or B systems. Finally, note that the optimization over σ_B can always be restricted to $\sigma_B \gg \rho_B$ for $\alpha > 1$.

We use up and down arrows to express the trivial observation that $H_\alpha^\uparrow(A|B)_\rho \geq H_\alpha^\downarrow(A|B)_\rho$ and $\widetilde{H}_\alpha^\uparrow(A|B)_\rho \geq \widetilde{H}_\alpha^\downarrow(A|B)_\rho$ by definition. Finally, (8) gives us the additional relations $\widetilde{H}_\alpha^\uparrow(A|B)_\rho \geq H_\alpha^\uparrow(A|B)_\rho$ and $\widetilde{H}_\alpha^\downarrow(A|B)_\rho \geq H_\alpha^\downarrow(A|B)_\rho$. These relations are summarized in Figure 1. Moreover, inheriting these properties from the corresponding divergences, all entropies are monotonically decreasing functions of α

For $\alpha = 1$, all definitions coincide with the usual von Neumann conditional entropy (11). For $\alpha = \infty$, two quantum generalizations of the conditional min-entropy emerge, which both have been

$$H_\alpha^\uparrow(A|B)_\rho \longleftarrow \widetilde{H}_\alpha^\uparrow(A|B)_\rho$$

$$H_\alpha^\downarrow(A|B)_\rho \longleftarrow \widetilde{H}_\alpha^\downarrow(A|B)_\rho$$
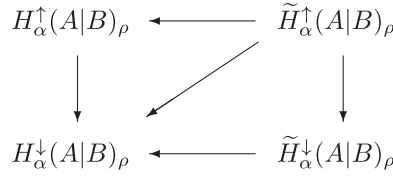
FIG. 1. Overview of the different conditional entropies used in this paper. Arrows indicate that one entropy is larger or equal to the other for all states $\rho_{AB} \in \mathcal{S}(AB)$ and all $\alpha \geq 0$.

studied by Renner.[35] Namely,

$$\widetilde{H}_\infty^\downarrow(A|B)_\rho = \sup\left\{\lambda \in \mathbb{R} : \rho_{AB} \leq 2^{-\lambda}1_A \otimes \rho_B\right\} \qquad \text{and} \qquad (18)$$

$$\widetilde{H}_\infty^\uparrow(A|B)_\rho = \sup\left\{\lambda \in \mathbb{R} : \rho_{AB} \leq 2^{-\lambda}1_A \otimes \sigma_B, \ \sigma_B \in \mathcal{S}(B)\right\}. \qquad (19)$$

(The notation $H_{\min}(A|B)_{\rho|\rho} \equiv \widetilde{H}_\infty^\downarrow(A|B)_\rho$ and $H_{\min}(A|B)_\rho \equiv \widetilde{H}_\infty^\uparrow(A|B)_\rho$ is widely used. However, we prefer our notation as it makes our exposition in this manuscript clearer.) For $\alpha = 2$, we find a quantum generalization of the conditional collision entropy as introduced by Renner:[35]

$$\widetilde{H}_2^\downarrow(A|B)_\rho = -\log \mathrm{Tr}\left\{\left(\rho_{AB}\left(1_A \otimes \rho_B^{-\frac{1}{2}}\right)\right)^2\right\}. \qquad (20)$$

For $\alpha = \frac{1}{2}$, we find the quantum conditional max-entropy first studied by König *et al.*,[24]

$$\widetilde{H}_{\frac{1}{2}}^\uparrow(A|B)_\rho = \sup_{\sigma_B \in \mathcal{S}(B)} 2\log F(\rho_{AB}, 1_A \otimes \sigma_B), \qquad (21)$$

where $F(\cdot, \cdot)$ denotes the fidelity. (The alternative notation $H_{\max}(A|B)_\rho \equiv \widetilde{H}_{\frac{1}{2}}^\uparrow(A|B)_\rho$ is often used.) For $\alpha = 0$, we find a quantum conditional generalization of the Hartley entropy[18] that was initially considered by Renner,[35]

$$H_0^\uparrow(A|B)_\rho = \sup_{\sigma_B \in \mathcal{S}(B)} \log \mathrm{Tr}\{\Pi_{\rho_{AB}} 1_A \otimes \sigma_B\}, \qquad (22)$$

where Π_ρ denotes the projector onto the support of ρ.

III. DUALITY RELATIONS

It is well known that, for any tripartite pure state ρ_{ABC}, the relation

$$H(A|B)_\rho + H(A|C)_\rho = 0 \qquad (23)$$

holds. We call this a *duality relation* for the conditional entropy. To see this, simply write $H(A|B)_\rho = H(\rho_{AB}) - H(\rho_B)$ and $H(A|C)_\rho = H(\rho_{AC}) - H(\rho_C)$ and note that the spectra of ρ_{AB} and ρ_C as well as the spectra of ρ_B and ρ_{AC} agree. The significance of this relation is manifold — for example, it turns out to be useful in cryptography where the entropy of an adversarial party, let us say C, can be estimated using local state tomography by two honest parties, A and B. In the following, we are interested to see if such relations hold more generally for conditional Rényi entropies.

It was shown in Lemma 6 of Ref. 39 that $H_\alpha^\downarrow$ indeed satisfies a duality relation, namely

$$H_\alpha^\downarrow(A|B)_\rho + H_\beta^\downarrow(A|C)_\rho = 0 \qquad \text{when} \quad \alpha + \beta = 2, \ \alpha, \beta \geq 0. \qquad (24)$$

Note that the map $\alpha \mapsto \beta = 2 - \alpha$ maps the interval $[0, 2]$, where data-processing holds, onto itself. This is not surprising. Indeed, consider the Stinespring dilation $\mathcal{U}_{B \to B'B''}$ of a quantum channel $\mathcal{E}_{B \to B'}$. Then, for ρ_{ABC} pure, $\tau_{AB'B''C} = \mathcal{U}_{B \to B'B''}[\rho_{ABC}]$ is also pure and the above duality relation implies that

$$H_\alpha^\downarrow(A|B)_\rho \leq H_\alpha^\downarrow(A|B')_\tau \iff H_\beta^\downarrow(A|C)_\rho \geq H_\beta^\downarrow(A|B''C)_\tau. \qquad (25)$$

Hence, data-processing for α holds if and only if data-processing for β holds.

A similar relation has recently been discovered for $\widetilde{H}_\alpha^\uparrow$ in Ref. 31 and independently in Ref. 6. There, it is shown that

$$\widetilde{H}_\alpha^\uparrow(A|B)_\rho + \widetilde{H}_\beta^\uparrow(A|C)_\rho = 0 \qquad \text{when} \quad \frac{1}{\alpha} + \frac{1}{\beta} = 2, \; \alpha, \beta \geq \frac{1}{2}. \tag{26}$$

As expected, the map $\alpha \mapsto \beta = \frac{\alpha}{2\alpha-1}$ maps the interval $[\frac{1}{2}, \infty]$, where data-processing holds, onto itself.

The purpose of the following is thus to show if a similar relation holds for the remaining two candidates, $H_\alpha^\uparrow$ and $\widetilde{H}_\alpha^\downarrow$. First, we find the following alternative expression for $H_\alpha^\uparrow$ by determining the optimal σ_B in the definition (14).

Lemma 1. Let $\alpha \in (0, 1) \cup (1, \infty)$ and $\rho_{AB} \in \mathcal{S}(AB)$. Then,

$$H_\alpha^\uparrow(A|B)_\rho = \frac{\alpha}{1-\alpha} \log \mathrm{Tr} \left\{ \left(\mathrm{Tr}_A\{\rho_{AB}^\alpha\} \right)^{\frac{1}{\alpha}} \right\}. \tag{27}$$

This generalizes a result by one of the current authors[20] (Lemma 7).

Proof. Recall the definition

$$H_\alpha^\uparrow(A|B)_\rho = \sup_{\sigma_B \in \mathcal{S}(B)} \frac{1}{1-\alpha} \log \mathrm{Tr} \left\{ \rho_{AB}^\alpha \, 1_A \otimes \sigma_B^{1-\alpha} \right\} \tag{28}$$

$$= \sup_{\sigma_B \in \mathcal{S}(B)} \frac{1}{1-\alpha} \log \mathrm{Tr} \left\{ \mathrm{Tr}_A\{\rho_{AB}^\alpha\} \sigma_B^{1-\alpha} \right\}. \tag{29}$$

This can immediately be lower bounded by the expression in (27) by substituting

$$\sigma_B^* = \frac{\left(\mathrm{Tr}_A\{\rho_{AB}^\alpha\} \right)^{\frac{1}{\alpha}}}{\mathrm{Tr} \left\{ \left(\mathrm{Tr}_A\{\rho_{AB}^\alpha\} \right)^{\frac{1}{\alpha}} \right\}} \tag{30}$$

for σ_B. It remains to show that this choice is optimal. We employ the following Hölder and reverse Hölder inequalities (cf. Lemma 6 in the Appendix). For any $A, B \geq 0$, the Hölder inequality states that

$$\mathrm{Tr}\{AB\} \leq \left(\mathrm{Tr}\{A^p\} \right)^{\frac{1}{p}} \left(\mathrm{Tr}\{B^q\} \right)^{\frac{1}{q}} \qquad \text{for all } p, q > 1 \text{ s.t. } \frac{1}{p} + \frac{1}{q} = 1. \tag{31}$$

Furthermore, if $B \gg A$, we also have a reverse Hölder inequality which states that

$$\mathrm{Tr}\{AB\} \geq \left(\mathrm{Tr}\{A^p\} \right)^{\frac{1}{p}} \left(\mathrm{Tr}\{B^q\} \right)^{\frac{1}{q}} \qquad \text{for all } q < 0 < p < 1 \text{ s.t. } \frac{1}{p} + \frac{1}{q} = 1. \tag{32}$$

For $\alpha < 1$, we employ (31) for $p = \frac{1}{\alpha}, q = \frac{1}{1-\alpha}, A = \mathrm{Tr}_A\{\rho_{AB}^\alpha\}$ and $B = \sigma_B^{1-\alpha}$ to find

$$\mathrm{Tr} \left\{ \mathrm{Tr}_A\{\rho_{AB}^\alpha\} \sigma_B^{1-\alpha} \right\} \leq \left(\mathrm{Tr} \left\{ \left(\mathrm{Tr}_A\{\rho_{AB}^\alpha\} \right)^{\frac{1}{\alpha}} \right\} \right)^\alpha \left(\mathrm{Tr}\{\sigma_B\} \right)^{1-\alpha}, \tag{33}$$

which yields the desired upper bound since $\mathrm{Tr}\{\sigma_B\} = 1$. For $\alpha > 1$, we instead use (32). This leads us to (27) upon the same substitutions, concluding the proof. $\qquad\square$

An alternative proof also follows rather directly from a quantum generalization of Sibson's identity, which was introduced by Sharma and Warsi[37] (Lemma 3 in the supplementary material).

This allows us to show our main result.

Theorem 2. *Let $\alpha, \beta \in (0, 1) \cup (1, \infty)$ with $\alpha \cdot \beta = 1$ and let $\rho_{ABC} \in \mathcal{S}(ABC)$ be pure. Then,* $H_\alpha^\uparrow(A|B)_\rho + \widetilde{H}_\beta^\downarrow(A|C)_\rho = 0$.

Proof. Substituting $\beta = \frac{1}{\alpha}$ and employing Lemma 1, it remains to show that

$$H_\alpha^\uparrow(A|B)_\rho = \frac{\alpha}{1-\alpha} \log \operatorname{Tr}\left\{\left(\operatorname{Tr}_A\{\rho_{AB}^\alpha\}\right)^{\frac{1}{\alpha}}\right\} \tag{34}$$

is equal to

$$-\widetilde{H}_\beta^\downarrow(A|C)_\rho = -\frac{1}{1-\beta} \log \operatorname{Tr}\left\{\left(\left(1_A \otimes \rho_C^{\frac{1-\beta}{2\beta}}\right)\rho_{AC}\left(1_A \otimes \rho_C^{\frac{1-\beta}{2\beta}}\right)\right)^\beta\right\} \tag{35}$$

$$= \frac{\alpha}{1-\alpha} \log \operatorname{Tr}\left\{\left(\left(1_A \otimes \rho_C^{\frac{\alpha-1}{2}}\right)\rho_{AC}\left(1_A \otimes \rho_C^{\frac{\alpha-1}{2}}\right)\right)^{\frac{1}{\alpha}}\right\}. \tag{36}$$

In the following we show something stronger, namely, that the operators

$$\operatorname{Tr}_A\{\rho_{AB}^\alpha\} \qquad \text{and} \qquad \left(1_A \otimes \rho_C^{\frac{\alpha-1}{2}}\right)\rho_{AC}\left(1_A \otimes \rho_C^{\frac{\alpha-1}{2}}\right) \tag{37}$$

are unitarily equivalent. This is true since both of these operators are marginals — on B and AC — of the same tripartite rank-1 operator,

$$\left(1_{AB} \otimes \rho_C^{\frac{\alpha-1}{2}}\right)\rho_{ABC}\left(1_{AB} \otimes \rho_C^{\frac{\alpha-1}{2}}\right). \tag{38}$$

To see that this is indeed true, note the first operator in (37) can be rewritten as

$$\operatorname{Tr}_A\{\rho_{AB}^\alpha\} = \operatorname{Tr}_A\left\{\rho_{AB}^{\frac{\alpha-1}{2}} \rho_{AB} \rho_{AB}^{\frac{\alpha-1}{2}}\right\} \tag{39}$$

$$= \operatorname{Tr}_{AC}\left\{\left(\rho_{AB}^{\frac{\alpha-1}{2}} \otimes 1_C\right)\rho_{ABC}\left(\rho_{AB}^{\frac{\alpha-1}{2}} \otimes 1_C\right)\right\} \tag{40}$$

$$= \operatorname{Tr}_{AC}\left\{\left(1_{AB} \otimes \rho_C^{\frac{\alpha-1}{2}}\right)\rho_{ABC}\left(1_{AB} \otimes \rho_C^{\frac{\alpha-1}{2}}\right)\right\}. \tag{41}$$

The last equality can be verified using the Schmidt decomposition of ρ_{ABC} with regards to the partition $AB{:}C$. This concludes the proof. $\qquad\square$

The relation can readily be extended for all $\alpha \geq 0$ and $\beta \geq 0$. The limiting case $\alpha = 1$ is simply the duality of the conditional von Neumann entropy (23), whereas the case $\alpha = 0$, $\beta = \infty$ was also shown in Proposition 3.11 of Ref. 8. (See Lemma 25 of Ref. 41 for a concise proof.) Again, note that the transformation $\alpha \mapsto \beta = \frac{1}{\alpha}$ maps the interval $[0, 2]$ where data-processing holds for $H_\alpha^\uparrow$ to $[\frac{1}{2}, \infty]$ where data-processing holds for $\widetilde{H}_\beta^\downarrow$.

We summarize these duality relations in the following theorem, where we take note that the first and second statements have been shown in Refs. 39, 6, and 31, respectively.

Theorem 3. *For any pure $\rho_{ABC} \in \mathcal{S}(ABC)$, the following holds:*[33]

$$H_\alpha^\downarrow(A|B)_\rho + H_\beta^\downarrow(A|C)_\rho = 0 \qquad \text{for} \qquad \alpha, \beta \in [0, 2],\ \alpha + \beta = 2, \tag{42}$$

$$\widetilde{H}_\alpha^\uparrow(A|B)_\rho + \widetilde{H}_\beta^\uparrow(A|C)_\rho = 0 \qquad \text{for} \qquad \alpha, \beta \in \left[\frac{1}{2}, \infty\right],\ \frac{1}{\alpha} + \frac{1}{\beta} = 2, \tag{43}$$

$$H_\alpha^\uparrow(A|B)_\rho + \widetilde{H}_\beta^\downarrow(A|C)_\rho = 0 \qquad \text{for} \qquad \alpha, \beta \in [0, \infty],\ \alpha \cdot \beta = 1. \tag{44}$$

IV. SOME INEQUALITIES RELATING CONDITIONAL ENTROPIES

Our first application yields relations between different conditional Rényi entropies for arbitrary mixed states. Recently, Mosonyi[27] (Lemma 2.1) used a converse of the Araki-Lieb-Thirring trace

inequality due to Audenaert[3] to find a converse to the ordering relation $D_\alpha(\rho\|\sigma) \geq \widetilde{D}_\alpha(\rho\|\sigma)$, namely,

$$\widetilde{D}_\alpha(\rho\|\sigma) \geq \alpha \cdot D_\alpha(\rho\|\sigma) + \log \text{Tr}\left\{\rho^\alpha\right\} + (\alpha - 1)\log\|\sigma\|. \tag{45}$$

Here, we follow a different approach and show that inequalities of a similar type for the conditional entropies are a direct corollary of the duality relations in Theorem 3.

Corollary 4. Let $\rho_{AB} \in \mathcal{S}(AB)$. Then, the following inequalities hold for $\alpha \in \left[\frac{1}{2}, \infty\right]$:

$$H_\alpha^\uparrow(A|B)_\rho \leq \widetilde{H}_\alpha^\uparrow(A|B)_\rho \leq H_{2-\frac{1}{\alpha}}^\uparrow(A|B)_\rho, \tag{46}$$

$$H_\alpha^\downarrow(A|B)_\rho \leq H_\alpha^\uparrow(A|B)_\rho \leq H_{2-\frac{1}{\alpha}}^\downarrow(A|B)_\rho, \tag{47}$$

$$\widetilde{H}_\alpha^\downarrow(A|B)_\rho \leq \widetilde{H}_\alpha^\uparrow(A|B)_\rho \leq \widetilde{H}_{2-\frac{1}{\alpha}}^\downarrow(A|B)_\rho, \tag{48}$$

$$H_\alpha^\downarrow(A|B)_\rho \leq \widetilde{H}_\alpha^\downarrow(A|B)_\rho \leq H_{2-\frac{1}{\alpha}}^\downarrow(A|B)_\rho. \tag{49}$$

Proof. Note that the first inequality on each line follows directly from the relations depicted in Figure 1. Next, consider an arbitrary purification $\rho_{ABC} \in \mathcal{S}(ABC)$ of ρ_{AB}. The relations of Figure 1, for any $\gamma \geq 0$, applied to the marginal ρ_{AC} are given as

$$\widetilde{H}_\gamma^\uparrow(A|C)_\rho \geq \widetilde{H}_\gamma^\downarrow(A|C)_\rho \geq H_\gamma^\downarrow(A|C)_\rho, \qquad \text{and} \tag{50}$$

$$\widetilde{H}_\gamma^\uparrow(A|C)_\rho \geq H_\gamma^\uparrow(A|C)_\rho \geq H_\gamma^\downarrow(A|C)_\rho. \tag{51}$$

We then substitute the corresponding dual entropies according to Theorem 3, which yields the desired inequalities upon appropriate new parametrization. $\qquad\square$

We note that the fully classical (commutative) case of all these inequalities is trivial except for the second inequalities in (47) and (48), which were proven before by one of the authors[21] (Lemma 6). Other special cases of these inequalities are also well known and have operational significance. For example, (48) for $\alpha = \infty$ states that $\widetilde{H}_\infty^\uparrow(A|B)_\rho \leq \widetilde{H}_2^\downarrow(A|B)_\rho$, which relates the conditional min-entropy in (19) to the conditional collision entropy in (20). To understand this inequality more operationally we rewrite the conditional min-entropy as its dual semi-definite program,[24]

$$\widetilde{H}_\infty^\uparrow(A|B)_\rho = \inf_{\Lambda_{B\to A'}} -\log\left(|A| \cdot F(\Phi_{AA'}, \Lambda_{B\to A'}[\rho_{AB}])\right), \tag{52}$$

where A' is a copy of A, the infimum is over all quantum channels $\Lambda_{B\to A'}$, $|A|$ denotes the dimension of A, and $\Phi_{AA'}$ is the maximally entangled state on AA'. Now, the above inequality becomes apparent since the conditional collision entropy can be written as[10]

$$\widetilde{H}_2^\downarrow(A|B)_\rho = -\log\left(|A| \cdot F(\Phi_{AA'}, \Lambda_{B\to A'}^{\text{pg}}[\rho_{AB}])\right), \tag{53}$$

where $\Lambda_{B\to A'}^{\text{pg}}$ denotes the pretty good recovery map of Barnum and Knill.[5] Also, (46) for $\alpha = \frac{1}{2}$ yields $\widetilde{H}_{\frac{1}{2}}^\uparrow(A|B)_\rho \leq H_0^\uparrow(A|B)_\rho$, which relates the quantum conditional max-entropy in (21) to the quantum conditional generalization of the Hartley entropy in (22).

We believe that the sandwich relations (46)–(49) for α close to 1 will prove useful in applications in quantum information theory as they allow to switch between different definitions of the conditional Rényi entropy.

V. ENTROPIC UNCERTAINTY RELATIONS

A series of papers[9,40] culminating in Ref. 12 established a general technique to derive uncertainty relations for quantum conditional entropies based on two main ingredients: (1) a duality relation, and (2) a data-processing inequality for the underlying divergence. It is evident that all our definitions of conditional Rényi entropies fit the framework of Ref. 12, which then immediately yields the following entropic uncertainty relations:

Corollary 5. Let $\rho_{ABC} \in \mathcal{S}(ABC)$ and let $\{M_x\}_x$ and $\{N_y\}_y$ be two positive operator-valued measures. We define the overlap $c := \max_{x,y} \left\| \sqrt{M_x}\sqrt{N_y} \right\|$ and consider the post-measurement states

$$\rho_{XB} := \bigoplus_x \mathrm{Tr}_{AC}\left\{ M_x \rho_{ABC} \right\} \quad and \quad \rho_{YC} := \bigoplus_y \mathrm{Tr}_{AB}\left\{ N_y \rho_{ABC} \right\}. \tag{54}$$

Then, the following relations hold:

$$H_\alpha^\downarrow(X|B)_\rho + H_\beta^\downarrow(Y|C)_\rho \geq \log\frac{1}{c}, \qquad for \qquad \alpha, \beta \in [0, 2],\ \alpha + \beta = 2, \tag{55}$$

$$\widetilde{H}_\alpha^\uparrow(X|B)_\rho + \widetilde{H}_\beta^\uparrow(Y|C)_\rho \geq \log\frac{1}{c}, \qquad for \qquad \alpha, \beta \in \left[\frac{1}{2}, \infty\right],\ \frac{1}{\alpha} + \frac{1}{\beta} = 2, \tag{56}$$

$$H_\alpha^\uparrow(X|B)_\rho + \widetilde{H}_\beta^\downarrow(Y|C)_\rho \geq \log\frac{1}{c}, \qquad for \qquad \alpha \in [0, 2],\ \beta \in \left[\frac{1}{2}, \infty\right],\ \alpha \cdot \beta = 1. \tag{57}$$

We want to point out that the first and second inequalities were first shown in Refs. 12 and 31, respectively; the third inequality is novel. To verify it, we apply Theorem 1 of Ref. 12 to $H_\alpha^\uparrow(X|B)_\rho$ and note that $H_\alpha^\uparrow(X|B)_\rho$ has the required form. Furthermore, it is already pointed out in Ref. 12 that the underlying divergence, $D_\alpha(\rho\|\sigma)$ for $\alpha \in [0, 2]$, satisfies the required properties for the application of their theorem. As such, comparing (57) to the corresponding duality relation (44), we see that in order to derive the uncertainty relation we need to restrict to $\alpha \in [0, 2]$ to be in the regime where data-processing holds.

It is noteworthy that even for the case of classical side information (if the systems B and C are classical), the three relations are genuinely different. The first inequality bounds the sum of two ↓-entropies, the second the sum of two ↑-entropies, and the third inequality the sum of a ↓- and an ↑-entropy. Let us further specialize these inequalities for the case where both B and C are trivial. It was already noted in Ref. 31 that (56) specializes to the well-known Maassen-Uffink relation.[26] We have

$$H_\alpha(X)_\rho + H_\beta(Z)_\rho \geq \log\frac{1}{c} \quad for \quad \alpha, \beta \in \left[\frac{1}{2}, \infty\right],\ \frac{1}{\alpha} + \frac{1}{\beta} = 2, \tag{58}$$

evaluated for the marginals of the states in (54). It is also easy to verify that (55) and (57) specialize to strictly weaker uncertainty relations when B and C are trivial.

APPENDIX: HÖLDER INEQUALITIES

We prove the following Hölder and reverse Hölder inequalities for traces of operators.

Lemma 6. Let A, $B \geq 0$ and let $p > 0$, $q \in \mathbb{R}$ such that $\frac{1}{p} + \frac{1}{q} = 1$. Then, the following Hölder and reverse Hölder inequalities hold:

$$\text{Tr}\{AB\} \leq \left(\text{Tr}\{A^p\}\right)^{\frac{1}{p}} \left(\text{Tr}\{B^q\}\right)^{\frac{1}{q}} \qquad \text{if } p > 1\,, \tag{A1}$$

$$\text{Tr}\{AB\} \geq \left(\text{Tr}\{A^p\}\right)^{\frac{1}{p}} \left(\text{Tr}\{B^q\}\right)^{\frac{1}{q}} \qquad \text{if } p < 1 \text{ and } B \gg A\,. \tag{A2}$$

Here, B^q is evaluated on the support of B by convention.

The first statement also immediately follows from a Hölder inequality for unitarily invariant norms (the trace norm in this case), e.g., in Corollary IV.2.6 of Ref. 11. However, we believe that the following reduction of the proof to the commutative case is noteworthy.

Proof. For commuting A and B, the above result immediately follows from the corresponding classical Hölder and reverse Hölder inequalities. Now, let $\mathcal{M}$ be a pinching in the eigenbasis of B. Since $\mathcal{M}[A]$ commutes with B, we have

$$\text{Tr}\{AB\} = \text{Tr}\{\mathcal{M}[A]B\} \leq \left(\text{Tr}\left\{\left(\mathcal{M}[A]\right)^p\right\}\right)^{\frac{1}{p}} \left(\text{Tr}\{B^q\}\right)^{\frac{1}{q}} \qquad \text{if } p > 1, \tag{A3}$$

$$\text{Tr}\{AB\} = \text{Tr}\{\mathcal{M}[A]B\} \geq \left(\text{Tr}\left\{\left(\mathcal{M}[A]\right)^p\right\}\right)^{\frac{1}{p}} \left(\text{Tr}\{B^q\}\right)^{\frac{1}{q}} \qquad \text{if } p < 1\,. \tag{A4}$$

under the respective constraints. Now, note that for $p > 1$, we have $\|\mathcal{M}[A]\|_p \leq \|A\|_p$ by the pinching inequality for the Schatten p-norm (Eq. (IV.52) of Ref. 11) and (A1) follows. On the other hand, for $p < 1$, we use Theorem V.2.1 of Ref. 11, which implies that $\left(\mathcal{M}[A]\right)^p \geq \mathcal{M}[A^p]$. This yields (A2) and concludes the proof. $\qquad\square$

[1] H. Araki, "On an inequality of Lieb and Thirring," Lett. Math. Phys. **19**(2), 167–170 (1990).

[2] S. Arimoto, "Information measures and capacity of order for discrete memoryless channels," in *Topics in Information Theory*, ser. Colloq. Math. Soc. J. Bolyai 16, edited by I. Csiszar and P. Elias (Amsterdam, Holland, 1977), pp. 41–52.

[3] K. M. R. Audenaert, "On the Araki-Lieb-Thirring inequality," Int. J. Inf. Syst. Sci. **4**(1), 78–83 (2008); e-print arXiv:math/0701129.

[4] K. M. R. Audenaert and N. Datta, "α-z-relative Renyi entropies," preprint arXiv:1310.7178 (2013).

[5] H. Barnum and E. Knill, "Reversing quantum dynamics with near-optimal quantum and classical fidelity," J. Math. Phys. **43**(5), 2097 (2002).

[6] S. Beigi, "Sandwiched Rényi divergence satisfies data processing inequality," J. Math. Phys. **54**(12), 122202 (2013).

[7] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized privacy amplification," IEEE Trans. Inf. Theory **41**(6), 1915–1923 (1995).

[8] M. Berta, "Single-shot quantum state merging," Master's thesis (ETH Zurich, 2008); e-print arXiv:0912.4495.

[9] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, "The uncertainty principle in the presence of quantum memory," Nat. Phys. **6**(9), 659–662 (2010).

[10] M. Berta, P. J. Coles, and S. Wehner, "An equality between entanglement and uncertainty," preprint arXiv:1302.5902 (2013).

[11] R. Bhatia, *Matrix Analysis*, Graduate Texts in Mathematics (Springer, 1997).

[12] P. J. Coles, R. Colbeck, L. Yu, and M. Zwolak, "Uncertainty relations from simple entropic properties," Phys. Rev. Lett. **108**(21), 210405 (2012).

[13] I. Csiszár, "Generalized cutoff rates and Renyi's information measures," IEEE Trans. Inf. Theory **41**(1), 26–34 (1995).

[14] N. Datta and F. Leditzky, "A limit of the quantum Renyi divergence," preprint arXiv:1308.5961 (2013).

[15] R. L. Frank and E. H. Lieb, "Monotonicity of a relative Rényi entropy," J. Math. Phys. **54**(12), 122201 (2013).

[16] R. G. Gallager, "Source coding with side information and universal coding," in *Proceedings of the IEEE ISIT* (IEEE, Ronneby, Sweden, 1979), Vol. 21.

[17] M. K. Gupta and M. M. Wilde, "Multiplicativity of completely bounded p-norms implies a strong converse for entanglement-assisted capacity," preprint arXiv:1310.7028 (2013).

[18] R. V. L. Hartley, "Transmission of information," Bell Syst. Tech. J. **7**(3), 535–563 (1928).

[19] M. Hayashi, "Exponential decreasing rate of leaked information in universal random privacy amplification," IEEE Trans. Inf. Theory **57**(6), 3989–4001 (2011).

[20] M. Hayashi, "Large deviation analysis for quantum security via smoothing of Renyi entropy of order 2," preprint arXiv:1202.0322 (2012).

[21] M. Hayashi, "Security analysis of epsilon-almost dual universal2 hash functions," preprint arXiv:1309.1596 (2013).

[22] M. Hayashi, "Tight exponential analysis of universally composable privacy amplification and its applications," IEEE Trans. Inf. Theory **59**(11), 7728–7746 (2013).

[23] M. Iwamoto and J. Shikata, "Information theoretic security for encryption based on conditional Renyi entropies," (2013), see http://eprint.iacr.org/2013/440.

[24] R. König, R. Renner, and C. Schaffner, "The operational meaning of min- and max-entropy," IEEE Trans. Inf. Theory **55**(9), 4337–4347 (2009).

[25] E. H. Lieb and W. E. Thirring, "Inequalities for the moments of the eigenvalues of the Schrödinger Hamiltonian and their relation to Sobolev inequalities," in *The Stability of Matter: From Atoms to Stars* (Springer, Berlin, Heidelberg, 2005), Chap. III, pp. 205–239.

[26] H. Maassen and J. Uffink, "Generalized entropic uncertainty relations," Phys. Rev. Lett. **60**(12), 1103–1106 (1988).

[27] M. Mosonyi, "Rényi divergences and the classical capacity of finite compound channels," preprint arXiv:1310.7525 (2013).

[28] M. Mosonyi and F. Hiai, "On the quantum Rényi relative entropies and related capacity formulas," IEEE Trans. Inf. Theory **57**(4), 2474–2487 (2011).

[29] M. Mosonyi and T. Ogawa, "Quantum hypothesis testing and the operational interpretation of the quantum Renyi relative entropies," preprint arXiv:1309.3228 (2013).

[30] M. Müller-Lennert, "Quantum relative Rényi entropies," Master thesis (ETH Zurich, 2013).

[31] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel, "On quantum Rényi entropies: A new generalization and some properties," J. Math. Phys. **54**(12), 122203 (2013).

[32] H. Nagaoka, "The converse part of the theorem for quantum Hoeffding bound," preprint arXiv:quant-ph/0611289 (2006).

[33] We use the convention that $\frac{1}{\infty} = 0$ and $0 \cdot \infty = 1$.

[34] T. Ogawa and M. Hayashi, "On error exponents in quantum hypothesis testing," IEEE Trans. Inf. Theory **50**(6), 1368–1372 (2004).

[35] R. Renner, "Security of quantum key distribution," Ph.D. thesis (ETH Zurich, 2005); e-print arXiv:quant-ph/0512258.

[36] A. Rényi, "On measures of information and entropy," in *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability* (University of California Press, Berkeley, 1961), pp. 547–561.

[37] N. Sharma and N. A. Warsi, "Fundamental bound on the reliability of quantum information transmission," Phys. Rev. Lett. **110**(8), 080501 (2013).

[38] M. Tomamichel, "Smooth entropies—A tutorial: With focus on applications in cryptography," (2012), see http://2012.qcrypt.net/docs/slides/Marco.pdf.

[39] M. Tomamichel, R. Colbeck, and R. Renner, "A fully quantum asymptotic equipartition property," IEEE Trans. Inf. Theory **55**(12), 5840–5847 (2009).

[40] M. Tomamichel and R. Renner, "Uncertainty relation for smooth entropies," Phys. Rev. Lett. **106**(11), 110506 (2011).

[41] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, "Leftover hashing against quantum side information," IEEE Trans. Inf. Theory **57**(8), 5524–5535 (2011).

[42] M. M. Wilde, A. Winter, and D. Yang, "Strong converse for the classical capacity of entanglement-breaking and Hadamard channels," Communications in Mathematical Physics **331**(2), 593–622 (2014).

[43] H. Yagi, "Finite blocklength bounds for multiple access channels with correlated sources," in *Proceedings of the IEEE ISITA* (IEEE, 2012), pp. 377–381.