

8-10-2016

Universal recoverability in quantum information

Marius Junge
University of Illinois Urbana-Champaign

Renato Renner
ETH Zürich

David Sutter
ETH Zürich

Mark M. Wilde
Louisiana State University

Andreas Winter
Universitat Autònoma de Barcelona

Follow this and additional works at: https://digitalcommons.lsu.edu/physics_astronomy_pubs

Recommended Citation

Junge, M., Renner, R., Sutter, D., Wilde, M., & Winter, A. (2016). Universal recoverability in quantum information. *IEEE International Symposium on Information Theory - Proceedings, 2016-August*, 2494-2498. <https://doi.org/10.1109/ISIT.2016.7541748>

This Conference Proceeding is brought to you for free and open access by the Department of Physics & Astronomy at LSU Digital Commons. It has been accepted for inclusion in Faculty Publications by an authorized administrator of LSU Digital Commons. For more information, please contact ir@lsu.edu.



Conference Paper

Universal recoverability in quantum information

Author(s):

Junge, Marius; Renner, Renato; Sutter, David; Wilde, Mark M.; Winter, Andreas

Publication Date:

2016

Permanent Link:

<https://doi.org/10.3929/ethz-b-000120060> →

Originally published in:

<http://doi.org/10.1109/ISIT.2016.7541748> →

Rights / License:

[In Copyright - Non-Commercial Use Permitted](#) →

This page was generated automatically upon download from the [ETH Zurich Research Collection](#). For more information please consult the [Terms of use](#).

Universal recoverability in quantum information

Marius Junge*, Renato Renner†, David Sutter‡, Mark M. Wilde‡, and Andreas Winter§

*Department of Mathematics, University of Illinois at Urbana-Champaign, Illinois 61801-2975, USA

†Institute for Theoretical Physics, ETH Zurich, Switzerland

‡Hearne Institute for Theoretical Physics, Department of Physics and Astronomy,

Center for Computation and Technology, Louisiana State University, Baton Rouge, Louisiana 70803, USA

§ICREA & Física Teòrica: Informació i Fenòmens Quàntics, Universitat Autònoma de Barcelona, ES-08193 Bellaterra (Barcelona), Spain

Abstract—The quantum relative entropy is well known to obey a monotonicity property (i.e., it does not increase under the action of a quantum channel). Here we present several refinements of this entropy inequality, some of which have a physical interpretation in terms of recovery from the action of the channel. The recovery channel given here is explicit and universal, depending only on the channel and one of the arguments to the relative entropy.

I. INTRODUCTION

The quantum relative entropy is a fundamental measure of distinguishability in quantum information theory [1], finding an operational interpretation in the context of quantum hypothesis testing [2], [3]. Let $\mathcal{L}(\mathcal{H})$ denote the set of linear operators acting on a finite-dimensional Hilbert space \mathcal{H} , $\mathcal{L}_+(\mathcal{H})$ the set of positive semi-definite operators, and let $\mathcal{D}(\mathcal{H})$ denote the set of density operators (positive semi-definite with unit trace). The quantum relative entropy is defined as the following function of $\rho \in \mathcal{D}(\mathcal{H})$ and $\sigma \in \mathcal{L}_+(\mathcal{H})$:

$$D(\rho\|\sigma) \equiv \begin{cases} \text{Tr}\{\rho[\log \rho - \log \sigma]\} & \text{if } \text{supp}(\rho) \subseteq \text{supp}(\sigma) \\ +\infty & \text{else} \end{cases}$$

where \log denotes the natural logarithm here and throughout for convenience. One of the main properties that $D(\rho\|\sigma)$ obeys is known as monotonicity [4], [5]. Let $\mathcal{N} : \mathcal{L}(\mathcal{H}) \rightarrow \mathcal{L}(\mathcal{H}')$ be a quantum channel (a completely positive, trace-preserving map), where \mathcal{H}' is finite-dimensional. Then the following monotonicity inequality holds [4], [5]

$$D(\rho\|\sigma) \geq D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)). \quad (1)$$

The equality conditions for this entropy inequality are that $D(\rho\|\sigma) = D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma))$ if and only if there exists a recovery channel \mathcal{R} , depending only on σ and \mathcal{N} , such that $\rho = (\mathcal{R} \circ \mathcal{N})(\rho)$ and $\sigma = (\mathcal{R} \circ \mathcal{N})(\sigma)$ [6], [7].

The main purpose of this paper is to present several further refinements of the entropy inequality in (1), recently reported in [8] and [9] (see also the earlier contributions on this topic in [10], [11] and the more recent one in [12]). One of the refinements can be summarized informally as follows: if the decrease in quantum relative entropy between two quantum states after a quantum channel is relatively small, then it is possible to perform a recovery channel, such that we can perfectly recover one state while approximately recovering the other. This can be interpreted as quantifying how well one can

reverse the action of a quantum channel. Throughout, we take ρ , σ , and \mathcal{N} as given in the following definition:

Definition 1: Let $\rho \in \mathcal{D}(\mathcal{H})$ and $\sigma \in \mathcal{L}_+(\mathcal{H})$, such that $\text{supp}(\rho) \subseteq \text{supp}(\sigma)$. Let $\mathcal{N} : \mathcal{L}(\mathcal{H}) \rightarrow \mathcal{L}(\mathcal{H}')$ be a quantum channel.

The formal statement of the main theorem is as follows:

Theorem 2: Given ρ , σ , and \mathcal{N} as in Definition 1, there exists an explicit recovery channel $\mathcal{R} : \mathcal{L}(\mathcal{H}') \rightarrow \mathcal{L}(\mathcal{H})$, depending only on σ and \mathcal{N} , such that

$$D(\rho\|\sigma) \geq D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) - \log F(\rho, (\mathcal{R} \circ \mathcal{N})(\rho)). \quad (2)$$

The fact that \mathcal{R} satisfies (2) for all $\rho \in \mathcal{D}(\mathcal{H})$ implies that

$$\sigma = (\mathcal{R} \circ \mathcal{N})(\sigma). \quad (3)$$

Given that the quantum fidelity $F(\omega, \tau) \equiv \|\sqrt{\omega}\sqrt{\tau}\|_1^2$ [13] takes values between zero and one for density operators ω and τ , we can immediately conclude that

$$-\log F(\rho, (\mathcal{R} \circ \mathcal{N})(\rho)) \geq 0, \quad (4)$$

so that the above theorem implies (1) as a consequence. Furthermore, the recovery channel satisfying (2) has the property that it perfectly recovers σ from $\mathcal{N}(\sigma)$ (satisfying (3)), a fact which we prove later and which makes (2) non-trivial.

The proof for Theorem 2 relies on the method of complex interpolation [14], [15] and the notion of a Rényi generalization of a relative entropy difference [16]. We review this background before going through the proof. We also present another lower bound for the relative entropy difference $D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma))$ and give two upper bounds for special cases, which were previously reported in [9], [11]. One of the consequences of Theorem 2 is to provide physically meaningful improvements to many well known quantum entropy inequalities, such as strong subadditivity [17], joint convexity of quantum relative entropy, and concavity of conditional quantum entropy. These are discussed in [8], [11] and improve upon the results in [18], [19].

II. BACKGROUND

The proof of Theorem 2 given here requires some mathematical background. So we first begin by defining the Schatten norms and several of their properties. We then review some essential results from complex analysis, that lead to a complex interpolation theorem known as the Stein–Hirschman interpolation theorem [20], [14].

A. Schatten Norms and Duality

An important technical tool in the proof given here is the Schatten p -norm of an operator A , defined as

$$\|A\|_p \equiv [\text{Tr} \{|A|^p\}]^{1/p}, \quad (5)$$

where $A \in \mathcal{L}(\mathcal{H})$, $|A| \equiv \sqrt{A^\dagger A}$, and $p \geq 1$. $\|A\|_p$ is equal to the p -norm of the singular values of A . That is, if $\sigma_i(A)$ is the vector of singular values of A , then

$$\|A\|_p = \left[\sum_i \sigma_i(A)^p \right]^{1/p}. \quad (6)$$

The convention is for $\|A\|_\infty$ to be defined as the largest singular value of A because $\|A\|_p$ converges to this in the limit as $p \rightarrow \infty$. In the proof of Theorem 2, we repeatedly use the fact that $\|A\|_p$ is unitarily invariant. That is, $\|A\|_p$ is invariant with respect to linear isometries, in the sense that $\|A\|_p = \|UAV^\dagger\|_p$, where $U, V \in \mathcal{L}(\mathcal{H}, \mathcal{H}')$ are linear isometries satisfying $U^\dagger U = I_{\mathcal{H}}$ and $V^\dagger V = I_{\mathcal{H}'}$. From these norms, one can define information measures relating quantum states and channels, with the one used here known as a Rényi generalization of a relative entropy difference [21], [16].

Throughout we adopt the common convention and define $f(A)$ for a function f and a positive semi-definite operator A as follows: $f(A) \equiv \sum_{i:\lambda_i \neq 0} f(\lambda_i) |i\rangle\langle i|$, where $A = \sum_i \lambda_i |i\rangle\langle i|$ is a spectral decomposition of A . We denote the support of A by $\text{supp}(A)$, and we let Π_A denote the projection onto the support of A .

B. Complex Analysis

We now review a few concepts from complex analysis [22]. We will not prove these results in detail, but the purpose instead is to recall them, and the interested reader can follow references to books on complex analysis for details of proofs. The culmination of the development is the Stein–Hirschman complex interpolation theorem (Theorem 5).

The well known maximum modulus principle [22] has an extension to an unbounded strip in \mathbb{C} , which we call the *maximum modulus principle on a strip*. Let S denote the standard strip in \mathbb{C} , \bar{S} its closure, and $\partial\bar{S}$ its boundary:

$$S \equiv \{z \in \mathbb{C} : 0 < \text{Re}\{z\} < 1\}, \quad (7)$$

$$\bar{S} \equiv \{z \in \mathbb{C} : 0 \leq \text{Re}\{z\} \leq 1\}, \quad (8)$$

$$\partial\bar{S} \equiv \{z \in \mathbb{C} : \text{Re}\{z\} = 0 \vee \text{Re}\{z\} = 1\}. \quad (9)$$

Let $f : \bar{S} \rightarrow \mathbb{C}$ be bounded on \bar{S} , holomorphic on S , and continuous on $\partial\bar{S}$. Then the supremum of $|f|$ is attained on $\partial\bar{S}$. That is, $\sup_{z \in \bar{S}} |f(z)| = \sup_{z \in \partial\bar{S}} |f(z)|$.

The maximum modulus principle on a strip implies a result known as the Hadamard three-lines theorem:

Theorem 3 (Hadamard Three-Lines): Let $f : \bar{S} \rightarrow \mathbb{C}$ be a function that is bounded on \bar{S} , holomorphic on S , and continuous on the boundary $\partial\bar{S}$. Let $\theta \in (0, 1)$ and $M(\theta) \equiv \sup_{t \in \mathbb{R}} |f(\theta + it)|$. Then $\log M(\theta)$ is a convex function on $[0, 1]$, implying that

$$\log M(\theta) \leq (1 - \theta) \log M(0) + \theta \log M(1). \quad (10)$$

There is a strengthening of the Hadamard three-lines theorem due to Hirschman [20], which in fact implies the Hadamard three-lines theorem:

Theorem 4 (Hirschman): Let $f(z) : \bar{S} \rightarrow \mathbb{C}$ be a function that is bounded on \bar{S} , holomorphic on S , and continuous on the boundary $\partial\bar{S}$. Then for $\theta \in (0, 1)$, the following holds

$$\log |f(\theta)| \leq \int_{-\infty}^{\infty} dt \left(\alpha_\theta(t) \log [|f(it)|^{1-\theta}] + \beta_\theta(t) \log [|f(1+it)|^\theta] \right), \quad (11)$$

where

$$\alpha_\theta(t) \equiv \frac{\sin(\pi\theta)}{2(1-\theta) [\cosh(\pi t) - \cos(\pi\theta)]}, \quad (12)$$

$$\beta_\theta(t) \equiv \frac{\sin(\pi\theta)}{2\theta [\cosh(\pi t) + \cos(\pi\theta)]}. \quad (13)$$

For a fixed $\theta \in (0, 1)$, $\alpha_\theta(t), \beta_\theta(t) \geq 0$ for all $t \in \mathbb{R}$ and

$$\int_{-\infty}^{\infty} dt \alpha_\theta(t) = \int_{-\infty}^{\infty} dt \beta_\theta(t) = 1, \quad (14)$$

(see, e.g., [22, Exercise 1.3.8]) so that $\alpha_\theta(t)$ and $\beta_\theta(t)$ can be interpreted as probability density functions. Furthermore,

$$\lim_{\theta \searrow 0} \beta_\theta(t) = \frac{\pi}{2} [\cosh(\pi t) + 1]^{-1} \equiv \beta_0(t), \quad (15)$$

where β_0 is also a probability density function on \mathbb{R} . With these observations, we can see that Hirschman's theorem implies the Hadamard three-lines theorem, given that an expectation can never exceed a supremum.

C. Complex Interpolation of Schatten Norms

We can extend much of the development above to operator-valued functions, which is needed to prove Theorem 2. Let $G : \mathbb{C} \rightarrow \mathcal{L}(\mathcal{H})$ be an operator-valued function. We say that $G(z)$ is holomorphic if every function mapping z to a matrix entry is holomorphic. For our purposes in what follows, we are interested in operator-valued functions of the form A^z , where A is a positive semi-definite operator. In this case, we apply the aforementioned convention and take $A^z = \sum_{i:\lambda_i \neq 0} \lambda_i^z |i\rangle\langle i|$, where $A = \sum_i \lambda_i |i\rangle\langle i|$ is an eigendecomposition of A with $\lambda_i \geq 0$ for all i . Given that x^z , with $x > 0$, is holomorphic, combined with the closure properties of holomorphic functions, we can conclude that A^z is holomorphic if A is positive semi-definite.

We can now state a version of the Hirschman theorem which applies to operator-valued functions and allows for bounding their Schatten norms [14]. The proof is standard and recalled in [8]. This theorem is one of the main technical tools that we need to establish Theorem 2.

Theorem 5 (Stein–Hirschman): Let $G : \bar{S} \rightarrow L(\mathcal{H})$ be an operator-valued function that is bounded on \bar{S} , holomorphic on S , and continuous on the boundary $\partial\bar{S}$. Let $\theta \in (0, 1)$ and define p_θ by

$$\frac{1}{p_\theta} = \frac{1-\theta}{p_0} + \frac{\theta}{p_1}, \quad (16)$$

where $p_0, p_1 \in [1, \infty]$. Then the following bound holds

$$\log \|G(\theta)\|_{p_\theta} \leq \int_{-\infty}^{\infty} dt \alpha_\theta(t) \log \left[\|G(it)\|_{p_0}^{1-\theta} \right] + \int_{-\infty}^{\infty} dt \beta_\theta(t) \log \left[\|G(1+it)\|_{p_1}^\theta \right], \quad (17)$$

where $\alpha_\theta(t)$ and $\beta_\theta(t)$ are defined in (12)–(13).

III. PETZ RECOVERY MAP

The recovery channel appearing in the lower bound of Theorem 2 has an explicit form and is constructed from a map known as the Petz recovery map [6], [7], which is defined as follows:

Definition 6: Let $\sigma \in \mathcal{L}_+(\mathcal{H})$, and let $\mathcal{N} : \mathcal{L}(\mathcal{H}) \rightarrow \mathcal{L}(\mathcal{H}')$ be a quantum channel. The Petz recovery map $\mathcal{P}_{\sigma, \mathcal{N}} : \mathcal{L}(\mathcal{H}') \rightarrow \mathcal{L}(\mathcal{H})$ is a completely positive, trace-non-increasing linear map defined as follows for $Q \in \mathcal{L}(\mathcal{H}')$:

$$\mathcal{P}_{\sigma, \mathcal{N}}(Q) \equiv \sigma^{1/2} \mathcal{N}^\dagger \left([\mathcal{N}(\sigma)]^{-1/2} Q [\mathcal{N}(\sigma)]^{-1/2} \right) \sigma^{1/2}. \quad (18)$$

The Petz recovery map $\mathcal{P}_{\sigma, \mathcal{N}}$ is linear, and it is completely positive because it is equal to a serial concatenation of three completely positive maps: $Q \rightarrow [\mathcal{N}(\sigma)]^{-1/2} Q [\mathcal{N}(\sigma)]^{-1/2}$, $Q \rightarrow \mathcal{N}^\dagger(Q)$, and $M \rightarrow \sigma^{1/2} M \sigma^{1/2}$ for $M \in \mathcal{L}(\mathcal{H})$. It is trace-non-increasing because the following holds for $Q \in \mathcal{L}_+(\mathcal{H}')$:

$$\begin{aligned} & \text{Tr}\{\mathcal{P}_{\sigma, \mathcal{N}}(Q)\} \\ &= \text{Tr} \left\{ \sigma \mathcal{N}^\dagger \left([\mathcal{N}(\sigma)]^{-1/2} Q [\mathcal{N}(\sigma)]^{-1/2} \right) \right\} \end{aligned} \quad (19)$$

$$= \text{Tr} \left\{ \mathcal{N}(\sigma) [\mathcal{N}(\sigma)]^{-1/2} Q [\mathcal{N}(\sigma)]^{-1/2} \right\} \quad (20)$$

$$= \text{Tr}\{\Pi_{\mathcal{N}(\sigma)} Q\} \leq \text{Tr}\{Q\}. \quad (21)$$

We can also define a partial isometric map $\mathcal{U}_{\sigma, t}$ as

$$\mathcal{U}_{\sigma, t}(M) \equiv \sigma^{it} M \sigma^{-it}. \quad (22)$$

Since $\sigma^{it} \sigma^{-it} = \Pi_\sigma$ (with Π_σ the support projection of σ),

$$\mathcal{U}_{\sigma, t}(\sigma) = \sigma, \quad (23)$$

so that this isometric map does not have any effect when σ is input. In the case that σ is positive definite, $\mathcal{U}_{\sigma, t}$ is a unitary channel. We can define a rotated or “swiveled” Petz map [11], [9], which plays an important role in the construction of a recovery channel satisfying the lower bound in Theorem 2.

Definition 7 (Rotated Petz Map): Let $\sigma \in \mathcal{L}_+(\mathcal{H})$, and let $\mathcal{N} : \mathcal{L}(\mathcal{H}) \rightarrow \mathcal{L}(\mathcal{H}')$ be a quantum channel. A rotated Petz map is defined for $Q \in \mathcal{L}(\mathcal{H}')$ as

$$\mathcal{R}_{\sigma, \mathcal{N}}^t(Q) \equiv (\mathcal{U}_{\sigma, -t} \circ \mathcal{P}_{\sigma, \mathcal{N}} \circ \mathcal{U}_{\mathcal{N}(\sigma), t})(Q). \quad (24)$$

The following is a consequence of some basic algebra and [23, Lemma 2] (see [24, Proposition 12.3.1]):

Proposition 8 (Perfect Recovery): Let $\sigma \in \mathcal{L}_+(\mathcal{H})$, and let $\mathcal{N} : \mathcal{L}(\mathcal{H}) \rightarrow \mathcal{L}(\mathcal{H}')$ be a quantum channel. A rotated Petz map $\mathcal{R}_{\sigma, \mathcal{N}}^t$ perfectly recovers σ from $\mathcal{N}(\sigma)$:

$$\mathcal{R}_{\sigma, \mathcal{N}}^t(\mathcal{N}(\sigma)) = \sigma. \quad (25)$$

IV. RÉNYI INFORMATION MEASURE

Given ρ , σ , and \mathcal{N} as in Definition 1, we define a Rényi information measure known as a Rényi generalization of a relative entropy difference [16]:

$$\begin{aligned} & \tilde{\Delta}_\alpha(\rho, \sigma, \mathcal{N}) \equiv \\ & \frac{2\alpha}{\alpha-1} \log \left\| \left([\mathcal{N}(\rho)]^{\frac{1-\alpha}{2\alpha}} [\mathcal{N}(\sigma)]^{\frac{\alpha-1}{2\alpha}} \otimes I_E \right) U \sigma^{\frac{1-\alpha}{2\alpha}} \rho^{\frac{1}{2}} \right\|_{2\alpha}, \end{aligned}$$

where $\alpha \in (0, 1) \cup (1, \infty)$ and $U : \mathcal{H} \rightarrow \mathcal{H}' \otimes \mathcal{H}_E$ is an isometric extension of the channel \mathcal{N} . That is, U is a linear isometry satisfying $\text{Tr}_E\{U(\cdot)U^\dagger\} = \mathcal{N}(\cdot)$ and $U^\dagger U = I_{\mathcal{H}}$. Recall that all isometric extensions of a channel are related by an isometry acting on the environment system E [24], so that the definition above is invariant under any such choice. The adjoint \mathcal{N}^\dagger of a channel is given in terms of an isometric extension U as $\mathcal{N}^\dagger(\cdot) = U^\dagger((\cdot) \otimes I_E)U$ [24, Prop. 5.2.1].

The following lemma is one of the main reasons that $\tilde{\Delta}_\alpha(\rho, \sigma, \mathcal{N})$ generalizes a relative entropy difference.

Lemma 9 ([16], [11]): The following limit holds for ρ , σ , and \mathcal{N} as given in Definition 1:

$$\lim_{\alpha \rightarrow 1} \tilde{\Delta}_\alpha(\rho, \sigma, \mathcal{N}) = D(\rho \parallel \sigma) - D(\mathcal{N}(\rho) \parallel \mathcal{N}(\sigma)). \quad (26)$$

V. PROOF OF THE RECOVERABILITY THEOREM

This section presents the proof of Theorem 2. In fact, we prove a stronger statement, which implies Theorem 2 for a particular recovery channel that we discuss below.

Theorem 10: Let ρ , σ , and \mathcal{N} be as in Definition 1. Then

$$\begin{aligned} & D(\rho \parallel \sigma) - D(\mathcal{N}(\rho) \parallel \mathcal{N}(\sigma)) \geq \\ & - \int_{-\infty}^{\infty} dt \beta_0(t) \log \left[F \left(\rho, (\mathcal{R}_{\sigma, \mathcal{N}}^{t/2} \circ \mathcal{N})(\rho) \right) \right], \end{aligned} \quad (27)$$

where $\beta_0(t) = \frac{\pi}{2} [\cosh(\pi t) + 1]^{-1}$ is a probability density function for $t \in \mathbb{R}$ and $\mathcal{R}_{\sigma, \mathcal{N}}^{t/2}$ is a rotated Petz recovery map.

Proof: We can prove this result by employing Theorem 5. Let $U : \mathcal{H} \rightarrow \mathcal{H}' \otimes \mathcal{H}_E$ be an isometric extension of the channel \mathcal{N} . Pick

$$G(z) \equiv \left([\mathcal{N}(\rho)]^{z/2} [\mathcal{N}(\sigma)]^{-z/2} \otimes I_E \right) U \sigma^{z/2} \rho^{1/2}, \quad (28)$$

for $z \in \bar{\mathbb{S}}$, $p_0 = 2$, $p_1 = 1$, and $\theta \in (0, 1)$, which fixes $p_\theta = \frac{2}{1+\theta}$. The operator valued-function $G(z)$ satisfies the conditions needed to apply Theorem 5. For the choices above,

$$\|G(\theta)\|_{\frac{2}{(1+\theta)}} = \left\| \left([\mathcal{N}(\rho)]^{\frac{\theta}{2}} [\mathcal{N}(\sigma)]^{-\frac{\theta}{2}} \otimes I_E \right) U \sigma^{\frac{\theta}{2}} \rho^{\frac{1}{2}} \right\|_{\frac{2}{(1+\theta)}},$$

$$\begin{aligned} \|G(it)\|_2 &= \left\| \left([\mathcal{N}(\rho)]^{it/2} [\mathcal{N}(\sigma)]^{-it/2} \otimes I_E \right) U \sigma^{it} \rho^{1/2} \right\|_2 \\ &\leq \left\| \rho^{1/2} \right\|_2 = 1, \end{aligned} \quad (29)$$

$$\begin{aligned} & \|G(1+it)\|_1 \\ &= \left\| \left([\mathcal{N}(\rho)]^{\frac{1+it}{2}} [\mathcal{N}(\sigma)]^{-\frac{1+it}{2}} \otimes I_E \right) U \sigma^{\frac{1+it}{2}} \rho^{\frac{1}{2}} \right\|_1 \\ &= \sqrt{F}(\rho, (\mathcal{U}_{\sigma, -t/2} \circ \mathcal{P}_{\sigma, \mathcal{N}} \circ \mathcal{U}_{\mathcal{N}(\sigma), t/2})(\mathcal{N}(\rho))) \\ &= \sqrt{F}(\rho, (\mathcal{R}_{\sigma, \mathcal{N}}^{t/2} \circ \mathcal{N})(\rho)). \end{aligned} \quad (30)$$

Then we can apply Theorem 5 to conclude that

$$\begin{aligned} & \log \left\| \left([\mathcal{N}(\rho)]^{\theta/2} [\mathcal{N}(\sigma)]^{-\theta/2} \otimes I_E \right) U \sigma^{\theta/2} \rho^{1/2} \right\|_{2/(1+\theta)} \\ & \leq \int_{-\infty}^{\infty} dt \beta_{\theta}(t) \log \left[F \left(\rho, (\mathcal{R}_{\sigma, \mathcal{N}}^{t/2} \circ \mathcal{N})(\rho) \right)^{\theta/2} \right]. \end{aligned} \quad (31)$$

Letting $\theta = (1 - \alpha) / \alpha$, we see that this is the same as

$$\begin{aligned} & \tilde{\Delta}_{\alpha}(\rho, \sigma, \mathcal{N}) \geq \\ & - \int_{-\infty}^{\infty} dt \beta_{(1-\alpha)/\alpha}(t) \log \left[F \left(\rho, (\mathcal{R}_{\sigma, \mathcal{N}}^{t/2} \circ \mathcal{N})(\rho) \right) \right]. \end{aligned} \quad (32)$$

Since the inequality in (31) holds for all $\theta \in (0, 1)$ and thus (32) holds for all $\alpha \in (1/2, 1)$, we can take the limit as $\alpha \nearrow 1$ and apply (26) and the dominated convergence theorem to conclude that (27) holds. ■

With the theorem above in hand, Theorem 2 follows as a consequence by taking $\mathcal{R}_{\sigma, \mathcal{N}}$ to be as follows:

$$\mathcal{R}_{\sigma, \mathcal{N}}(Q) \equiv \int_{-\infty}^{\infty} dt \beta_0(t) \mathcal{R}_{\sigma, \mathcal{N}}^{t/2}(Q) + \text{Tr}\{(I - \Pi_{\mathcal{N}(\sigma)})Q\}\omega, \quad (33)$$

where $Q \in \mathcal{L}(\mathcal{H}')$ and $\omega \in \mathcal{D}(\mathcal{H})$. This is because

$$\begin{aligned} & - \int_{-\infty}^{\infty} dt \beta_0(t) \log \left[F \left(\rho, (\mathcal{R}_{\sigma, \mathcal{N}}^{t/2} \circ \mathcal{N})(\rho) \right) \right] \\ & \geq - \log \left[F \left(\rho, \left(\int_{-\infty}^{\infty} dt \beta_0(t) \mathcal{R}_{\sigma, \mathcal{N}}^{t/2} \circ \mathcal{N} \right) (\rho) \right) \right] \\ & \geq - \log [F(\rho, (\mathcal{R}_{\sigma, \mathcal{N}} \circ \mathcal{N})(\rho))], \end{aligned} \quad (34)$$

where the first inequality is due to the concavity of both the logarithm and the fidelity, and the second inequality follows from the assumption that $\text{supp}(\rho) \subseteq \text{supp}(\sigma)$ and the operator monotonicity of the square root function.

The extra term $\text{Tr}\{(I - \Pi_{\mathcal{N}(\sigma)})Q\}\omega$ is needed to ensure that $\mathcal{R}_{\sigma, \mathcal{N}}$ is trace-preserving. Setting $\hat{\Pi}_{\mathcal{N}(\sigma)} \equiv I - \Pi_{\mathcal{N}(\sigma)}$, trace preservation follows because

$$\begin{aligned} \text{Tr}\{\mathcal{R}_{\sigma, \mathcal{N}}(Q)\} &= \int_{-\infty}^{\infty} dt \beta_0(t) \text{Tr}\{\mathcal{R}_{\sigma, \mathcal{N}}^{t/2}(Q)\} + \text{Tr}\{Q\} \\ &= \int_{-\infty}^{\infty} dt \beta_0(t) \text{Tr}\{\Pi_{\mathcal{N}(\sigma)}Q\} + \text{Tr}\{\hat{\Pi}_{\mathcal{N}(\sigma)}Q\} \\ &= \text{Tr}\{\Pi_{\mathcal{N}(\sigma)}Q\} + \text{Tr}\{\hat{\Pi}_{\mathcal{N}(\sigma)}Q\} = \text{Tr}\{Q\}. \end{aligned} \quad (35)$$

Observe that this recovery channel has the ‘‘perfect recovery of σ ’’ property mentioned in (3), which follows from Proposition 8 and the particular form in (33).

VI. EQUALITY CONDITIONS

As a corollary of Theorem 10, we obtain equality conditions for the monotonicity of quantum relative entropy:

Corollary 11 (Equality Conditions): Let ρ , σ , and \mathcal{N} be as given in Definition 1. Then $D(\rho\|\sigma) = D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma))$ if and only if all rotated Petz recovery maps perfectly recover ρ from $\mathcal{N}(\rho)$: $\forall t \in \mathbb{R} : (\mathcal{R}_{\sigma, \mathcal{N}}^t \circ \mathcal{N})(\rho) = \rho$.

Proof: Recall from Proposition 8 that, independent of the conditions in the statement of the corollary, we always have

that $(\mathcal{R}_{\sigma, \mathcal{N}}^t \circ \mathcal{N})(\sigma) = \sigma$ for all $t \in \mathbb{R}$. We start by proving the ‘‘only if’’ part. Suppose that $\forall t \in \mathbb{R} : (\mathcal{R}_{\sigma, \mathcal{N}}^t \circ \mathcal{N})(\rho) = \rho$. Then for a particular $t \in \mathbb{R}$, monotonicity implies that

$$\begin{aligned} D(\rho\|\sigma) &\geq D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) \\ D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) &\geq D((\mathcal{R}_{\sigma, \mathcal{N}}^t \circ \mathcal{N})(\rho)\|(\mathcal{R}_{\sigma, \mathcal{N}}^t \circ \mathcal{N})(\sigma)) \\ &= D(\rho\|\sigma), \end{aligned} \quad (36)$$

which in turn imply that $D(\rho\|\sigma) = D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma))$. We now prove the ‘‘if part’’ of the theorem. Suppose that $D(\rho\|\sigma) = D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma))$. By Theorem 10, we can conclude that

$$\int_{-\infty}^{\infty} dt \beta_0(t) \left[-\log \left[F \left(\rho, (\mathcal{R}_{\sigma, \mathcal{N}}^{t/2} \circ \mathcal{N})(\rho) \right) \right] \right] = 0. \quad (38)$$

Since $\beta_0(t)$ is a positive definite function for all $t \in \mathbb{R}$, $-\log F \geq 0$, the recovery maps $\mathcal{R}_{\sigma, \mathcal{N}}^{t/2}$ are continuous in t and so is the fidelity, we can conclude that

$$-\log \left[F \left(\rho, (\mathcal{R}_{\sigma, \mathcal{N}}^{t/2} \circ \mathcal{N})(\rho) \right) \right] = 0 \quad (39)$$

for all $t \in \mathbb{R}$, which is the same as $F(\rho, (\mathcal{R}_{\sigma, \mathcal{N}}^{t/2} \circ \mathcal{N})(\rho)) = 1$ for all $t \in \mathbb{R}$. Then $(\mathcal{R}_{\sigma, \mathcal{N}}^t \circ \mathcal{N})(\rho) = \rho$ follows. ■

VII. OTHER BOUNDS

In this section, we present other bounds for the relative entropy difference $D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma))$, one of which is a direct consequence of Theorem 5 and [11, Theorem 4] and two others which were previously reported in [9, Remark 12]. The first bound we present is an upper bound, and to have an interpretation in terms of recoverability, we need to take ρ , σ , and \mathcal{N} as given in the following definition:

Definition 12: Let $\rho_{SE'}$ be a positive definite density operator and let $\sigma_{SE'}$ be a positive definite operator, each acting on a finite-dimensional tensor-product Hilbert space $\mathcal{H}_S \otimes \mathcal{H}_{E'}$. Let \mathcal{N} be a quantum channel given as follows: $\mathcal{N}(\theta_{SE'}) = \text{Tr}_E\{U_{SE' \rightarrow BE} \theta_{SE'} U_{SE' \rightarrow BE}^\dagger\}$, where $U_{SE' \rightarrow BE}$ is a unitary operator taking $\mathcal{H}_S \otimes \mathcal{H}_{E'}$ to an isomorphic finite-dimensional tensor-product Hilbert space $\mathcal{H}_B \otimes \mathcal{H}_E$, such that $\mathcal{N}(\rho)$ and $\mathcal{N}(\sigma)$ are each positive definite and act on \mathcal{H}_B .

Following the proof of Theorem 10, we pick

$$G(z) \equiv \left([\mathcal{N}(\rho)]^{-z/2} [\mathcal{N}(\sigma)]^{z/2} \otimes I_E \right) U \sigma^{-z/2} \rho^{1/2}, \quad (40)$$

$p_0 = 2, p_1 = \infty$, apply Theorem 5, and arrive at the following:

Theorem 13: For ρ , σ , and \mathcal{N} as given in Definition 12, the following inequality holds

$$\begin{aligned} D(\rho\|\sigma) - D(\mathcal{N}(\rho)\|\mathcal{N}(\sigma)) &\leq \int_{-\infty}^{\infty} dt \beta_0(t) D_{\max} \left(\rho \left\| \mathcal{P}_{\sigma, \mathcal{N}}^{t/2}(\mathcal{N}(\rho)) \right. \right), \end{aligned} \quad (41)$$

where $D_{\max}(\omega\|\tau) \equiv 2 \log \left\| \omega^{1/2} \tau^{-1/2} \right\|_{\infty}$ [25].

However, we note that there is an improvement of this bound, which is found as follows. There is an alternate Rényi generalization of a relative entropy difference [16], defined as

$$\begin{aligned} \Delta_{\alpha}(\rho, \sigma, \mathcal{N}) &\equiv \\ & \frac{2}{\alpha - 1} \log \left\| \left([\mathcal{N}(\rho)]^{\frac{1-\alpha}{2}} [\mathcal{N}(\sigma)]^{\frac{\alpha-1}{2}} \otimes I_E \right) U \sigma^{\frac{1-\alpha}{2}} \rho^{\frac{1}{2}} \right\|_2, \end{aligned}$$

where $\alpha \in (0, 1) \cup (1, \infty)$ and $U : \mathcal{H} \rightarrow \mathcal{H}' \otimes \mathcal{H}_E$ is an isometric extension of the channel \mathcal{N} . It has the property that $\lim_{\alpha \rightarrow 1} \Delta_\alpha(\rho, \sigma, \mathcal{N}) = D(\rho \parallel \sigma) - D(\mathcal{N}(\rho) \parallel \mathcal{N}(\sigma))$ [16], [9]. Following the proof of Theorem 10, we pick

$$G(z) \equiv \left([\mathcal{N}(\rho)]^{-z/2} [\mathcal{N}(\sigma)]^{z/2} \otimes I_E \right) U \sigma^{-z/2} \rho^{(1+z)/2},$$

$p_0 = 2, p_1 = 2$, apply Theorem 5, and arrive at the following: *Theorem 14 (Remark 12 of [9]):* For ρ, σ , and \mathcal{N} as given in Definition 12, the following inequality holds

$$\begin{aligned} D(\rho \parallel \sigma) - D(\mathcal{N}(\rho) \parallel \mathcal{N}(\sigma)) \\ \leq \int_{-\infty}^{\infty} dt \beta_0(t) D_2\left(\rho \parallel \mathcal{P}_{\sigma, \mathcal{N}}^{t/2}(\mathcal{N}(\rho))\right), \end{aligned} \quad (42)$$

where $D_2(\omega \parallel \tau) \equiv \log \text{Tr}\{\omega^2 \tau^{-1}\}$.

This bound is stronger than that in Theorem 13 because $D_2(\omega \parallel \tau) \leq D_{\max}(\omega \parallel \tau)$. This inequality follows because

$$D_2(\omega \parallel \tau) = \log \text{Tr}\{\omega \omega^{1/2} \tau^{-1} \omega^{1/2}\} \quad (43)$$

$$\leq \log \max_{\gamma} \text{Tr}\{\gamma \omega^{1/2} \tau^{-1} \omega^{1/2}\} \quad (44)$$

$$= \log \left\| \omega^{1/2} \tau^{-1} \omega^{1/2} \right\|_{\infty} \quad (45)$$

$$= D_{\max}(\omega \parallel \tau), \quad (46)$$

where the optimization in the second line is over all density operators γ and the second-to-last equality follows from a variational characterization of the infinity norm.

Following the proof of Theorem 10, we pick

$$G(z) \equiv \left([\mathcal{N}(\rho)]^{z/2} [\mathcal{N}(\sigma)]^{-z/2} \otimes I_E \right) U \sigma^{z/2} \rho^{(1-z)/2},$$

$p_0 = 2, p_1 = 2$, apply Theorem 5, and arrive at the following: *Theorem 15 (Remark 12 of [9]):* For ρ, σ , and \mathcal{N} as given in Definition 1, the following inequality holds

$$\begin{aligned} D(\rho \parallel \sigma) - D(\mathcal{N}(\rho) \parallel \mathcal{N}(\sigma)) \\ \geq \int_{-\infty}^{\infty} dt \beta_0(t) D_0\left(\rho \parallel \mathcal{P}_{\sigma, \mathcal{N}}^{t/2}(\mathcal{N}(\rho))\right), \end{aligned} \quad (47)$$

where $D_0(\omega \parallel \tau) \equiv -\log \text{Tr}\{\Pi_{\omega} \tau\}$.

VIII. CONCLUSION

We have presented several refinements of the monotonicity of quantum relative entropy. In all cases, these have an interpretation in terms of recoverability. An open question is to refine the lower and upper bounds further, perhaps with different measures or other recovery maps. Note that stronger bounds are possible in the classical case [26].

Acknowledgements—We thank O. Fawzi, R. Frank, E. Lieb, V. Scholz, M. Tomamichel, and T. Vidick for helpful discussions. MJ was supported by NSF DMS 1501103 and NSF-DMS 1201886. RR and DS acknowledge support by the European Research Council (ERC) via grant No. 258932, by the Swiss National Science Foundation (SNSF) via the National Centre of Competence in Research ‘‘QSIT’’, and by the European Commission via the project ‘‘RAQUEL’’. MMW acknowledges the NSF under Award No. CCF-1350397 and

DARPA Quiness through award W31P4Q-12-1-0019. AWs work was supported by the EU (STREP RAQUEL), the ERC (AdG IRQUAT), the Spanish MINECO (grant FIS2013-40627-P) with the support of FEDER funds, as well as by the Generalitat de Catalunya CIRIT, project 2014-SGR-966.

REFERENCES

- [1] H. Umegaki, ‘‘Conditional expectations in an operator algebra IV,’’ *Kodai Math. Sem. Rep.*, vol. 14, no. 2, pp. 59–85, 1962.
- [2] F. Hiai and D. Petz, ‘‘The proper formula for relative entropy and its asymptotics in quantum probability,’’ *Communications in Mathematical Physics*, vol. 143, no. 1, pp. 99–114, December 1991.
- [3] T. Ogawa and H. Nagaoka, ‘‘Strong converse and Stein’s lemma in quantum hypothesis testing,’’ *IEEE Transactions on Information Theory*, vol. 46, no. 7, pp. 2428–2433, November 2000, arXiv:quant-ph/9906090.
- [4] G. Lindblad, ‘‘Completely positive maps and entropy inequalities,’’ *Comm. Math. Phys.*, vol. 40, no. 2, pp. 147–151, June 1975.
- [5] A. Uhlmann, ‘‘Relative entropy and the Wigner-Yanase-Dyson-Lieb concavity in an interpolation theory,’’ *Communications in Mathematical Physics*, vol. 54, no. 1, pp. 21–32, 1977.
- [6] D. Petz, ‘‘Sufficient subalgebras and the relative entropy of states of a von Neumann algebra,’’ *Communications in Mathematical Physics*, vol. 105, no. 1, pp. 123–131, March 1986.
- [7] —, ‘‘Sufficiency of channels over von Neumann algebras,’’ *Quarterly Journal of Mathematics*, vol. 39, no. 1, pp. 97–108, 1988.
- [8] M. Junge, R. Renner, D. Sutter, M. M. Wilde, and A. Winter, ‘‘Universal recovery from a decrease of quantum relative entropy,’’ September 2015, arXiv:1509.07127.
- [9] F. Dupuis and M. M. Wilde, ‘‘Swiveled Rényi entropies,’’ June 2015, arXiv:1506.00981.
- [10] M. Berta, M. Lemm, and M. M. Wilde, ‘‘Monotonicity of quantum relative entropy and recoverability,’’ *Quantum Information and Computation*, vol. 15, no. 15 & 16, pp. 1333–1354, November 2015, arXiv:1412.4067.
- [11] M. M. Wilde, ‘‘Recoverability in quantum information theory,’’ *Proc. Royal Soc. A*, vol. 471, no. 2182, p. 20150338, October 2015.
- [12] D. Sutter, M. Tomamichel, and A. W. Harrow, ‘‘Strengthened monotonicity of relative entropy via pinched Petz recovery map,’’ July 2015, arXiv:1507.00303.
- [13] A. Uhlmann, ‘‘The ‘‘transition probability’’ in the state space of a *-algebra,’’ *Rep. Math. Phys.*, vol. 9, no. 2, pp. 273–279, 1976.
- [14] E. M. Stein, ‘‘Interpolation of linear operators,’’ *Trans. American Mathematical Society*, vol. 83, no. 2, pp. 482–492, November 1956.
- [15] J. Bergh and J. Löfström, *Interpolation Spaces*. Springer-Verlag Berlin Heidelberg, 1976.
- [16] K. P. Seshadreesan, M. Berta, and M. M. Wilde, ‘‘Rényi squashed entanglement, discord, and relative entropy differences,’’ *Journal of Physics A*, vol. 48, no. 39, p. 395303, September 2015.
- [17] E. H. Lieb and M. B. Ruskai, ‘‘Proof of the strong subadditivity of quantum-mechanical entropy,’’ *Journal of Mathematical Physics*, vol. 14, pp. 1938–1941, 1973.
- [18] O. Fawzi and R. Renner, ‘‘Quantum conditional mutual information and approximate Markov chains,’’ *Communications in Mathematical Physics*, vol. 340, no. 2, pp. 575–611, December 2015, arXiv:1410.0664.
- [19] D. Sutter, O. Fawzi, and R. Renner, ‘‘Universal recovery map for approximate Markov chains,’’ *Accepted for publication in Proceedings of the Royal Society A*, April 2015, arXiv:1504.07251.
- [20] I. I. Hirschman, ‘‘A convexity theorem for certain groups of transformations,’’ *Journal d’Analyse Mathématique*, vol. 2, no. 2, pp. 209–218, December 1952.
- [21] M. Berta, K. Seshadreesan, and M. M. Wilde, ‘‘Rényi generalizations of the conditional quantum mutual information,’’ *Journal of Mathematical Physics*, vol. 56, no. 2, p. 022205, February 2015, arXiv:1403.6102.
- [22] L. Grafakos, *Classical Fourier Analysis*, 2nd ed. Springer, 2008.
- [23] A. Jencova, ‘‘Reversibility conditions for quantum operations,’’ *Reviews in Mathematical Physics*, vol. 24, no. 7, p. 1250016, August 2012.
- [24] M. M. Wilde, *From Classical to Quantum Shannon Theory*, 2015, arXiv:1106.1445v6.
- [25] N. Datta, ‘‘Min- and max-relative entropies and a new entanglement monotone,’’ *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2816–2826, June 2009, arXiv:0803.2770.
- [26] K. Li and A. Winter, ‘‘Squashed entanglement, k -extendibility, quantum Markov chains, and recovery maps,’’ 2014, arXiv:1410.4184.