Preservation of a quantum Rényi relative entropy implies existence of a recovery map

2017 J. Phys. A: Math. Theor. 50 085303

(http://iopscience.iop.org/1751-8121/50/8/085303)

IOP Publishing Journal of Physics A: Mathematical and Theoretical
J. Phys. A: Math. Theor. **50** (2017) 085303 (12pp) doi:10.1088/1751-8121/aa5661

Preservation of a quantum Rényi relative entropy implies existence of a recovery map

Anna Jenčová

Mathematical Institute, Slovak Academy of Sciences, Štefánikova 49, 814 73 Bratislava, Slovakia

E-mail: jenca@mat.savba.sk

Received 19 May 2016, revised 19 December 2016
Accepted for publication 3 January 2017
Published 18 January 2017

CrossMark

Abstract

It is known that a necessary and sufficient condition for equality in the data processing inequality (DPI) for the quantum relative entropy is the existence of a recovery map. We show that equality in DPI for a sandwiched Rényi relative α-entropy with $\alpha > 1$ is also equivalent to this property. For the proof, we use an interpolating family of L_p-norms with respect to a state.

Keywords: data processing inequality, sandwiched Rényi entropy, quantum channels, recovery map

1. Introduction

One of the key notions of quantum information theory is that of a relative entropy, or divergence, which can be seen as a measure of information-theoretic difference between quantum states. A fundamental property of a relative entropy D is the data processing inequality (DPI)

$$D(\Phi(\rho)\|\Phi(\sigma)) \leqslant D(\rho\|\sigma), \tag{1}$$

which holds for any pair of quantum states $\{\rho, \sigma\}$ and any quantum channel Φ. This property expresses the fact that a physical transformation, represented by the channel Φ, cannot increase distinguishability of states. It is clear that if there is a quantum channel Ψ such that

$$\Psi \circ \Phi(\sigma) = \sigma \text{ and } \Psi \circ \Phi(\rho) = \rho,$$

then equality in DPI holds. Such a channel Ψ, if it exists, is called a recovery map for the triple (Φ, ρ, σ). The aim of the present work is to prove the opposite implication, in the case that D is a quantum version of the Rényi relative entropy.

One of the most important quantum relative entropies is the Umegaki relative entropy [47], which has an operational significance as a distinguishability measure on quantum states [16, 32] and is related to many other entropic quantities. For two states ρ and σ, it is defined as

$$D_1(\rho\|\sigma) = \operatorname{Tr}\rho(\log(\rho) - \log(\sigma)),$$

if the support $\operatorname{supp}(\rho)$ of ρ is contained in $\operatorname{supp}(\sigma)$ and is infinite otherwise. Data processing inequality for D_1 was proved in [24, 36, 46], recently also for positive trace-preserving maps [29]. See also [41] for a discussion including some related inequalities and equality conditions.

For $\alpha \in (0,1) \cup (1,\infty)$, the standard quantum version of the Rényi relative α-entropy is defined by [34]

$$D_\alpha(\rho\|\sigma) = \begin{cases} \frac{1}{\alpha - 1}\log(\operatorname{Tr}\rho^\alpha\sigma^{1-\alpha}) & \text{if } \alpha \in (0,1) \text{ or } \operatorname{supp}(\rho) \subseteq \operatorname{supp}(\sigma) \\ \infty & \text{otherwise.} \end{cases}$$

This quantity can be derived from quantum *f*-divergences, or quasi-entropies, defined in [36] and is a straightforward generalization of the classical family of Rényi relative α-entropies [40]. The values for $\alpha = 0, 1, \infty$ can be obtained by taking limits, in particular, $\lim_{\alpha\to 1} D_\alpha = D_1$, the Umegaki relative entropy. The Rényi relative α-entropy satisfies DPI for $\alpha \in [0,2]$, see [15, 36]. For $\alpha \in (0,1)$, the relative α-entropies appear in error exponents [1, 11, 14, 31] and as cutoff rates [25] in quantum hypothesis testing.

It was an important observation by Petz that if Φ is a quantum channel and ρ, σ are states such that $D_1(\rho\|\sigma)$ is finite, then the equality

$$D_1(\Phi(\rho)\|\Phi(\sigma)) = D_1(\rho\|\sigma)$$

is equivalent to existence of a recovery map for (Φ, ρ, σ). This was first proved in [37] in the general framework of von Neumann algebras, in the case that Φ is a restriction to a subalgebra. In [38], this result was extended to subsets of states and any channel Φ. Here the Umegaki relative entropy was replaced by transition probability, which is closely related to the Rényi relative entropy $D_{1/2}$, but the proof, using integral representations of operator convex functions, can be easily extended to D_α for all $\alpha \in (0,2)$, see [15, 18, 19].

In analogy with the classical notion of a sufficient statistic [9], in particular its characterization as a statistical isomorphism (see e.g. [44]), Petz in [38] called a channel Φ sufficient with respect to $\{\rho,\sigma\}$ if there is a recovery map for (Φ,ρ,σ). The fundamental result of [37] is thus a quantum generalization of the well-known characterization of classical sufficient statistics in terms of the Kullback–Leibler divergence, [22].

Sufficiency of channels, sometimes also called reversibility, and its equivalent characterizations were subsequently studied by several authors. On one hand, the characterization by equality in DPI was extended to a large class of quantum divergences, such as *f*-divergences, Fisher information and some distinguishability measures related to quantum hypothesis testing, [15, 17]. On the other hand, it was proved that sufficiency is equivalent to a certain factorization structure of both the channel and the involved states, [18, 19, 28]. See [15] for a review of quantum *f*-divergences and conditions for sufficiency, and [13, 17] for some extensions and further results. Moreover, sufficiency has been studied also in the framework of quantum extension of Blackwell's comparison of statistical experiments [3] and in the setting of bosonic channels [42].

The theory of sufficient channels proved useful for finding equality conditions in some quantum theoretic inequalities, most notably for characterization of the quantum Markov property by equality in strong subadditivity of von Neumann entropy, [12, 18]. Further, equality conditions were obtained for Holevo quantity and related entropic inequalities, [42, 43] and for convexity of some f-divergences, as well as in some related Minkowski inequalities, [20]. See also [33] for applications to secret sharing schemes.

Recently, another quantum version of Rényi relative entropy was introduced in [48] and independently in [30]. It is the so-called sandwiched Rényi relative α-entropy, defined for $\alpha > 0, \alpha \neq 1$ as

$$\tilde{D}_\alpha(\rho\|\sigma) = \begin{cases} \frac{1}{\alpha - 1} \log \mathrm{Tr}\left[\left(\sigma^{\frac{1-\alpha}{2\alpha}}\rho\sigma^{\frac{1-\alpha}{2\alpha}}\right)^\alpha\right] & \text{if } \mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma) \\ \infty & \text{otherwise} \end{cases}$$

Again, the values for $\alpha = 0, 1, \infty$ are obtained by taking limits, [7, 30, 48] and we have $\tilde{D}_1 = D_1$ and $\tilde{D}_\infty = D_{\max}$, where

$$D_{\max}(\rho\|\sigma) = \log \inf\{\lambda > 0, \rho \leqslant \lambda\sigma\} \quad (2)$$

is the max-relative entropy, introduced in [5]. Moreover, $\tilde{D}_\alpha$ satisfies DPI for $\alpha \in [1/2, \infty]$, [2, 10, 30, 48]. For $\alpha > 1$ the sandwiched Rényi relative entropies $\tilde{D}_\alpha$ have an operational interpretation as strong converse exponents in quantum hypothesis testing [27], quantum channel discrimination [4] and classical-quantum channel coding [26].

It is a natural question, mentioned also in [27] and [8], whether equality in DPI for $\tilde{D}_\alpha$ characterizes sufficiency. An algebraic equality condition for $\alpha \in (1/2, 1) \cup (1, \infty)$ was proved in the recent paper [23] and applications to Rényi versions of Araki–Lieb inequalities and entanglement measures were found, but the question whether this implies existence of a recovery map remained open. Partial results for a larger family of α-z-Rényi entropies were also obtained in [13], under some restrictions on the triple (Φ, ρ, σ).

In the present work, we answer this question in the affirmative for $\alpha > 1$ and any triple (Φ, ρ, σ) where Φ is a completely positive (or 2-positive) trace preserving map and $\mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma)$. Since the sandwiched Rényi relative entropies do not belong to the family of f-divergences, the techniques used e.g. in [15] cannot be applied to this case. We will use a method based on an interpolating family of L_p-norms, close to the approach introduced in [2]. The complex interpolation method can also be utilized to extend the definition of $\tilde{D}_\alpha$ to infinite dimensions, as will be done in a subsequent paper.

2. Preliminaries

Throughout the paper, we will restrict to finite dimensional Hilbert spaces. For a Hilbert space $\mathcal{H}$, we denote the algebra of bounded linear operators on $\mathcal{H}$ by $B(\mathcal{H})$ and the cone of positive operators by $B(\mathcal{H})^+$. States on $B(\mathcal{H})$ are identified with positive operators with unit trace, the set of all states will be denoted by $\mathfrak{S}(\mathcal{H})$. For $X \in B(\mathcal{H})^+$, $\mathrm{supp}(X)$ denotes the support of X.

For $p \geqslant 1$, the Schatten p-norm in $B(\mathcal{H})$ is introduced as

$$\|X\|_p = \left(\mathrm{Tr}\,|X|^p\right)^{1/p}, \qquad X \in B(\mathcal{H})$$

and we put $\|\cdot\|_\infty = \|\cdot\|$, the operator norm. The space $B(\mathcal{H})$ equipped with the norm $\|\cdot\|_2$ becomes a Hilbert space, with respect to the Hilbert–Schmidt inner product

$$\langle X, Y\rangle = \mathrm{Tr}\,X^*Y, \qquad X, Y \in B(\mathcal{H}).$$

If $\mathcal{K}$ is another Hilbert space and $\Phi : B(\mathcal{H}) \to B(\mathcal{K})$ is a linear map, its adjoint with respect to the Hilbert–Schmidt inner product will be denoted by Φ^*. The map Φ is trace-preserving if $\mathrm{Tr}\,\Phi(X) = \mathrm{Tr}\,X$ for all $X \in B(\mathcal{H})$ and unital if $\Phi(I) = I$. Further, Φ is positive if $\Phi(B(\mathcal{H})^+) \subseteq B(\mathcal{K})^+$and n-positive if $\mathrm{id}_n \otimes \Phi$ is positive, where id_n is the identity map on $B(\mathbb{C}^n)$.

Φ is completely positive if it is n-positive for all $n \in \mathbb{N}$. A completely positive trace-preserving map is called a quantum channel.

We will also need the notion of a conditional expectation on $B(\mathcal{H})$, which is defined as a positive unital map E onto a subalgebra $\mathcal{F} \subseteq B(\mathcal{H})$, with the property

$$E(AXB) = AE(X)B, \qquad \forall A, B \in \mathcal{F}, X \in B(\mathcal{H}), \tag{3}$$

see e.g. [34, 39]. Note that any conditional expectation is completely positive and $E^2 = E$.

2.1. Non-commutative L_p-spaces with respect to a state

The use of complex interpolation method appears in the study of the sandwiched Rényi relative entropies in the work by Beigi, [2]. For our results, we use an interpolating family of L_p-norms with respect to a state $\sigma \in \mathfrak{S}(\mathcal{H})$, which are closely related but not the same as those introduced in [2], see remark 1 below. In a more general setting of von Neumann algebras, the corresponding L_p-spaces were introduced in [45, 50] and are contained in a larger family of interpolation L_p-spaces defined in [21].

For $1 \leqslant p \leqslant \infty$ and $1/p + 1/q = 1$, let $L_{p,\sigma}(\mathcal{H})$ denote the linear space of operators $Y \in B(\mathcal{H})$, such that $Y = \sigma^{1/2q} X \sigma^{1/2q}$ for some $X \in B(\mathcal{H})$, equipped with the norm

$$\|Y\|_{p,\sigma} = \|X\|_p.$$

It is clear that for any p, $L_{p,\sigma}(\mathcal{H})$ coincides with the subspace $L_\sigma(\mathcal{H})$ of operators whose support and range lie in $\mathrm{supp}(\sigma)$, which can be identified with $B(\mathrm{supp}(\sigma))$. We will use this identification without further notice below, so that for example we will write σ^z for the operator $(\sigma|_{\mathrm{supp}(\sigma)})^z \oplus 0$ for any $z \in \mathbb{C}$. In this way, we may write

$$\|Y\|_{p,\sigma} = \|\sigma^{\frac{1-p}{2p}} Y \sigma^{\frac{1-p}{2p}}\|_p, \qquad Y \in L_\sigma(\mathcal{H}). \tag{4}$$

It follows from the properties of Schatten p-norms that this indeed defines a norm. For $p = 1$, the norm $\|\cdot\|_{1,\sigma}$ is just $\|\cdot\|_1$ restricted to $L_\sigma(\mathcal{H})$ and for $p = \infty$,

$$\|Y\|_{\infty,\sigma} = \|\sigma^{-1/2} Y \sigma^{-1/2}\|. \tag{5}$$

Note also that if $\rho \in \mathfrak{S}(\mathcal{H})$, then $\rho \in L_\sigma(\mathcal{H})$ if and only if $\rho \leqslant \lambda\sigma$ for some $\lambda > 0$ and in this case

$$\|\rho\|_{\infty,\sigma} = \inf\{\lambda > 0, \rho \leqslant \lambda\sigma\} = 2^{D_{\max}(\rho\|\sigma)}.$$

For $Z, Y \in L_\sigma(\mathcal{H})$, we define

$$\langle Z, Y\rangle_\sigma = \mathrm{Tr}\, Z\sigma^{-1/2} Y \sigma^{-1/2}.$$

Let $1 \leqslant p \leqslant \infty$ and $1/p + 1/q = 1$, then

$$\langle Z, Y\rangle_\sigma = \mathrm{Tr}\left(\sigma^{\frac{1-q}{2q}} Z \sigma^{\frac{1-q}{2q}}\right)\left(\sigma^{\frac{1-p}{2p}} Y \sigma^{\frac{1-p}{2p}}\right).$$

By duality of the corresponding Schatten norms, the following duality holds:

$$\|Y\|_{p,\sigma} = \sup_{\|Z\|_{q,\sigma} \leqslant 1} |\langle Z, Y\rangle_\sigma|. \tag{6}$$

Using remark 1 below, this can be also obtained from [2]. The space $L_{2,\sigma}(\mathcal{H})$ is a Hilbert space with respect to the inner product

$$(Y_1, Y_2) \mapsto \langle Y_1^*, Y_2\rangle_\sigma.$$

Remark 1. Let us denote the norm in [2] by $\|\cdot\|_{p,\sigma,B}$, then it is easy to see that for $Y \in L_\sigma(\mathcal{H})$,

$$\|Y\|_{p,\sigma} = \|\sigma^{-1/2} Y \sigma^{-1/2}\|_{p,\sigma,B}$$

and one can switch the results in [2] to our setting by means of the map $\Gamma_\sigma : X \mapsto \sigma^{1/2} X \sigma^{1/2}$ and its inverse. We often use this relation to our advantage, but our definition seems preferable for the present work, since it leads to simpler expressions. For example, the sandwiched Rényi relative entropy is obtained directly as logarithm of the norm and the Petz recovery map is the adjoint with respect to the inner product $\langle\cdot,\cdot\rangle_\sigma$ (see (10) and (11) below).

On the other hand, it was proved in [21, 50] that the spaces $L_{p,\sigma}(\mathcal{H})$ can be obtained by the complex interpolation method and most of the results of this and the next section can be obtained from these works. Nevertheless, in order not to go into unnecessary technicalities, we prefer to give direct proofs or use the relation to [2]. Let us also remark that this family of norms was studied also in [35], where further results can be found.

We next define certain operator valued analytic functions on the stripe $S = \{z \in \mathbb{C}, 0 \leqslant \mathrm{Re}(z) \leqslant 1\}$ which will be useful for evaluation of the norm $\|\cdot\|_{p,\sigma}$. So let $Y \in L_\sigma(\mathcal{H})$ and $1 < p < \infty$. Let $X := \sigma^{-1/2q} Y \sigma^{-1/2q}$ and let $X = U|X|$ be the polar decomposition. We will denote

$$f_{Y,p}(z) = \|Y\|_{p,\sigma}^{1-zp} \sigma^{(1-z)/2} U|X|^{zp} \sigma^{(1-z)/2}, \qquad z \in S. \tag{7}$$

Then $f_{Y,p}$ is a bounded continuous function $S \to L_\sigma(\mathcal{H})$, holomorphic in the interior and $f_{Y,p}(1/p) = Y$. Moreover, we have

$$f_{Y,p}(\mathrm{i}t) = \|Y\|_{p,\sigma}^{1-\mathrm{i}tp} \sigma^{1/2} \big(\sigma^{-\mathrm{i}t/2} U|X|^{\mathrm{i}tp} \sigma^{-\mathrm{i}t/2}\big) \sigma^{1/2}$$

and by (5),

$$\|f_{Y,p}(\mathrm{i}t)\|_{\infty,\sigma} = \|Y\|_{p,\sigma} \|\sigma^{-\mathrm{i}t/2} U|X|^{\mathrm{i}tp} \sigma^{-\mathrm{i}t/2}\| = \|Y\|_{p,\sigma}, \quad t \in \mathbb{R}. \tag{8}$$

Similarly, for all $t \in \mathbb{R}$,

$$\|f_{Y,p}(1+\mathrm{i}t)\|_1 = \|Y\|_{p,\sigma}^{1-p} \|\sigma^{-\mathrm{i}t/2} U|X|^{p+p\mathrm{i}t} \sigma^{-\mathrm{i}t/2}\|_1 = \|Y\|_{p,\sigma}, \tag{9}$$

the last equality is obtained from the fact that $\|\cdot\|_1$ is unitarily invariant. The following lemma will be needed in the sequel. Note also that the inequality part follows directly from the version of Hadamard three lines theorem proved in [2].

Lemma 2. *Let $h : S \to L_\sigma(\mathcal{H})$ be a bounded continuous function, holomorphic in the interior of S. Then for any $\theta \in [0, 1]$, we have*

$$\|h(\theta)\|_{1/\theta,\sigma} \leqslant \max\{\sup_t \|h(\mathrm{i}t)\|_{\infty,\sigma}, \sup_t \|h(1+\mathrm{i}t)\|_1\}.$$

Moreover, if equality is attained at some $\theta \in (0, 1)$, then it holds for all $\theta \in [0, 1]$.

Proof. Let $\theta \in (0, 1)$. By the duality (6), there is some Z in the unit ball of $L_{1/(1-\theta),\sigma}(\mathcal{H})$ such that $\|h(\theta)\|_{1/\theta,\sigma} = \langle Z, h(\theta)\rangle_\sigma$. Consider the corresponding function $f_{Z,1/(1-\theta)}$, so that $f_{Z,1/(1-\theta)}(1-\theta) = Z$ and by (8) and (9), we have for all $t \in \mathbb{R}$,

$$\|f_{Z,1/(1-\theta)}(\mathrm{i}t)\|_{\infty,\sigma} = \|f_{Z,1/(1-\theta)}(1+\mathrm{i}t)\|_1 = \|Z\|_{1/(1-\theta),\sigma} = 1.$$

Put $H(z) := \langle f_{Z,1/(1-\theta)}(1-z), h(z)\rangle_\sigma$, $z \in S$, then $H : S \to \mathbb{C}$ is bounded, continuous and holomorphic in the interior of S. We have for $t \in \mathbb{R}$,

$$|H(\mathrm{i}t)| \leqslant \|f_{Z,1/(1-\theta)}(1-\mathrm{i}t)\|_1 \|h(\mathrm{i}t)\|_{\infty,\sigma} = \|h(\mathrm{i}t)\|_{\infty,\sigma}$$

and

$$|H(1+\mathrm{i}t)| \leqslant \|f_{Z,1/(1-\theta)}(-\mathrm{i}t)\|_{\infty,\sigma} \|h(1+\mathrm{i}t)\|_1 = \|h(1+\mathrm{i}t)\|_1.$$

Let $M := \max\{\sup_t \|h(\mathrm{i}t)\|_{\infty,\sigma}, \sup_t \|h(1+\mathrm{i}t)\|_1\}$, then it follows by the Hadamard three lines theorem that $|H(z)| \leqslant M$ for all $z \in S$. The inequality part of the statement now follows by $\|h(\theta)\|_{1/\theta,\sigma} = H(\theta)$.

If equality is attained at θ, then by the maximum modulus principle, H must be a constant, so that $H(z) = M$ for all $z \in S$. For any $\lambda \in [0, 1]$ we then have

$$\begin{aligned} M &= H(\lambda) \leqslant \|f_{Z,1/(1-\theta)}(1-\lambda)\|_{1/(1-\lambda),\sigma} \|h(\lambda)\|_{1/\lambda,\sigma} \\ &\leqslant \|h(\lambda)\|_{1/\lambda,\sigma} \leqslant M, \end{aligned}$$

where the last two inequalities follow by the first part of the proof. □

2.2. Positive trace-preserving maps and their duals

Let $\mathcal{K}$ be a finite dimensional Hilbert space and let $\Phi : B(\mathcal{H}) \to B(\mathcal{K})$ be a positive trace-preserving map, then its adjoint Φ^* is a unital positive map. Let $\sigma \in \mathfrak{S}(\mathcal{H})$, let $P \in B(\mathcal{H})$ be the projection onto $\mathrm{supp}(\sigma)$ and $Q \in B(\mathcal{K})$ the projection onto $\mathrm{supp}(\Phi(\sigma))$. Then

$$0 = \mathrm{Tr}\,\Phi(\sigma)Q^\perp = \mathrm{Tr}\,\sigma\Phi^*(Q^\perp),$$

where $Q^\perp = I - Q$, so that $\Phi^*(Q^\perp) \leqslant P^\perp$. Let X be a positive element in $L_\sigma(\mathcal{H})$, then

$$\mathrm{Tr}\,\Phi(X)Q^\perp = \mathrm{Tr}\,X\Phi^*(Q^\perp) = 0,$$

so that $\mathrm{supp}(\Phi(X)) \subseteq \mathrm{supp}(\Phi(\sigma))$. Since $L_\sigma(\mathcal{H})$ is generated by positive elements, it follows that Φ maps $L_\sigma(\mathcal{H})$ into $L_{\Phi(\sigma)}(\mathcal{K})$. The following result is easily obtained by remark 1 and the proof of theorem 6 in [2]. Note that as observed in [29], only positivity of Φ is used in this proof.

Proposition 3. *Φ defines a contraction $L_{p,\sigma}(\mathcal{H}) \to L_{p,\Phi(\sigma)}(\mathcal{K})$ for all $1 \leqslant p \leqslant \infty$.*

Let Φ_σ denote the adjoint of Φ with respect to $\langle\cdot,\cdot\rangle_\sigma$, that is, $\Phi_\sigma : L_{\Phi(\sigma)}(\mathcal{K}) \to L_\sigma(\mathcal{H})$ satisfies

$$\langle \Phi_\sigma(X), Y\rangle_\sigma = \langle X, \Phi(Y)\rangle_{\Phi(\sigma)}, \qquad X \in L_{\Phi(\sigma)}(\mathcal{K}), Y \in L_\sigma(\mathcal{H}). \tag{10}$$

It is easy to see that

$$\Phi_\sigma(X) = \sigma^{1/2}\Phi^*(\Phi(\sigma)^{-1/2}X\Phi(\sigma)^{-1/2})\sigma^{1/2}. \tag{11}$$

Note that this is precisely the (adjoint of) the dual map of Φ^* as defined by Petz [38]. Note also that Φ_σ is trace-preserving, positive and $\Phi_\sigma(\Phi(\sigma)) = \sigma$, so that proposition 3 implies that Φ_σ is a contraction $L_{p,\Phi(\sigma)}(\mathcal{K}) \to L_{p,\sigma}(\mathcal{H})$ for any p. Moreover, for any $n \in \mathbb{N}$, Φ_σ is n-positive if and only if Φ is.

2.3. Quantum channels and sufficiency

Let $\Phi : B(\mathcal{H}) \to B(\mathcal{K})$ be a quantum channel and let $\sigma \in \mathfrak{S}(\mathcal{H})$. The next result shows that the channel Φ_σ defines a universal recovery map for Φ and σ. For this reason, Φ_σ is sometimes called the Petz recovery map.

Theorem 4. *Reference [38] Let* $\Phi : B(\mathcal{H}) \to B(\mathcal{K})$ *be a quantum channel and let* $\rho, \sigma \in \mathfrak{S}(\mathcal{H})$ *be such that* $\mathrm{supp}(\rho) \subseteq \mathrm{supp}(\sigma)$*. Then* Φ *is sufficient with respect to* $\{\rho, \sigma\}$ *if and only if* $\Phi_\sigma \circ \Phi(\rho) = \rho$*.*

By restriction to $\mathrm{supp}(\sigma)$, we may assume that σ is invertible. In this case, $\Omega := \Phi_\sigma \circ \Phi$ is a channel on $B(\mathcal{H})$ and all states $\rho \in \mathfrak{S}(\mathcal{H})$ such that Φ is sufficient with respect to $\{\rho, \sigma\}$ are precisely all invariant states of Ω. Note that by (11), σ is an invertible invariant state of Ω. The following results are known.

Theorem 5. *Let* $\Omega : B(\mathcal{H}) \to B(\mathcal{H})$ *be a channel such that* $\Omega(\sigma) = \sigma$ *for some invertible* $\sigma \in \mathfrak{S}(\mathcal{H})$*. Then there are Hilbert spaces* $\mathcal{H}_n^L$*,* $\mathcal{H}_n^R$ *and a unitary operator* $U : \mathcal{H} \to \bigoplus_n \mathcal{H}_n^L \otimes \mathcal{H}_n^R$*, such that*

(*i*) *the set* $\mathcal{F}_{\Omega^*}$ *of fixed points of* Ω^* *has the form*

$$\mathcal{F}_{\Omega^*} = U^* \left(\bigoplus_n B(\mathcal{H}_n^L) \otimes I_{\mathcal{H}_n^R} \right) U.$$

(*ii*) *the set* $\mathcal{F}_\Omega$ *of fixed points of* Ω *has the form*

$$\mathcal{F}_\Omega = U^* \left(\bigoplus_n B(\mathcal{H}_n^L) \otimes \sigma_n^R \right) U,$$

for some invertible $\sigma_n^R \in \mathfrak{S}(\mathcal{H}_n^R)$*.*

Proof. Part (i) is quite standard. It is proved e.g. in [39, example 9.4] that $\mathcal{F}_{\Omega^*}$ is a subalgebra and the sequence $\frac{1}{n}\sum_{k=0}^{n-1}(\Omega^*)^k$, where $(\Omega^*)^k$ denotes the k-fold composition $\Omega^* \circ \cdots \circ \Omega^*$, converges to a conditional expectation E onto $\mathcal{F}_{\Omega^*}$. Since any subalgebra in $B(\mathcal{H})$ is isomorphic to a direct sum of full matrix algebras, it must have the stated form.

The proof of part (ii) can be found in [49]. We give another proof of (ii) using some arguments of [12], which is perhaps more straightforward.

Note that the conditional expectation E satisfies $E^*(\sigma) = \sigma$ and $\Omega^* \circ E = E \circ \Omega^* = E$. Let now $Y \in \mathcal{F}_\Omega$. Then $\Omega^k(Y) = Y$ for any $k \in \mathbb{N}$, so that $E^*(Y) = Y$. Conversely, let $E^*(Y) = Y$, then

$$\Omega(Y) = \Omega(E^*(Y)) = (E \circ \Omega^*)^*(Y) = E^*(Y) = Y.$$

We have proved that $\mathcal{F}_\Omega = \mathcal{F}_{E^*}$.

Let $P_n : \mathcal{H} \to \mathcal{H}_n^L \otimes \mathcal{H}_n^R$ be orthogonal projections, then $Q_n := U^* P_n U$ are central projections in $\mathcal{F}_{\Omega^*} = \mathcal{F}_E$, the range of E. Therefore, we must have for all $X \in B(\mathcal{H})$,

$$\begin{aligned} E(X) &= \sum_{m,n} E(Q_m X Q_n) = \sum_{m,n} Q_m E(Q_m X Q_n) Q_n \\ &= \sum_{m,n} Q_n E(Q_m X Q_n) Q_n = \sum_n Q_n E(Q_n X Q_n) Q_n, \end{aligned}$$

where we used the property (3) in the second and in the last equality. Further, by the same property, we have for any $X_n \in B(\mathcal{H}_n^L)$, $Y_n \in B(\mathcal{H}_n^R)$

$$\begin{aligned} E(U^*(X_n \otimes Y_n)U) &= U^*(X_n \otimes I_{\mathcal{H}_n^R}) U E(U^*(I_{\mathcal{H}_n^L} \otimes Y_n)U) \\ &= E(U^*(I_{\mathcal{H}_n^L} \otimes Y_n)U) U^*(X_n \otimes I_{\mathcal{H}_n^R}) U \end{aligned}$$

so that $E(U^*(I_{\mathcal{H}_n^L}\otimes Y_n)U)$ lies in the center of $U^*(B(\mathcal{H}_n^L)\otimes I_{\mathcal{H}_n^R})U$ and therefore is a multiple of Q_n. It follows that there is some linear functional ψ_n on $B(\mathcal{H}_n^R)$ such that

$$E(U^*(I_{\mathcal{H}_n^L}\otimes Y_n)U)=\psi_n(Y_n)Q_n.$$

Since E is positive and unital, ψ_n must be such as well and there must be some $\sigma_n^R\in\mathfrak{S}(\mathcal{H}_n^R)$, such that $\psi_n(Y_n)=\mathrm{Tr}\,[\sigma_n^R Y_n]$, $Y_n\in B(\mathcal{H}_n^R)$. Let us denote $\phi_{\sigma_n^R}:Y_n\mapsto\mathrm{Tr}\,[\sigma_n^R Y_n]I_{\mathcal{H}_n^R}$, $Y_n\in B(\mathcal{H}_n^R)$. It follows that

$$E=U^*\left(\sum_n(\mathrm{id}_{B(\mathcal{H}_n^L)}\otimes\phi_{\sigma_n^R})(P_nU\cdot U^*P_n)\right)U$$

and

$$E^*=U^*\left(\sum_n(\mathrm{id}_{B(\mathcal{H}_n^L)}\otimes\phi^*_{\sigma_n^R})(P_nU\cdot U^*P_n)\right)U.$$

It is now clear that $\mathcal{F}_\Omega=\mathcal{F}_{E^*}$ has the form as in (ii), with σ_n^R as above. Since $\sigma\in\mathcal{F}_\Omega$ is invertible, σ_n^R must be invertible as well, for all n. $\square$

As a consequence, we obtain a following characterization of sufficient channels. Similar results were already obtained in [28] and [18].

Corollary 6. *Let $\Phi:B(\mathcal{H})\to B(\mathcal{K})$ be a channel and let $\sigma\in\mathfrak{S}(\mathcal{H})$ be invertible. Then there is a unitary U and factorizations*

$$U\mathcal{H}=\bigoplus_n\mathcal{H}_n^L\otimes\mathcal{H}_n^R,\qquad U\sigma U^*=\bigoplus_n A_n^L\otimes\sigma_n^R,$$

where $A_n^L\in B(\mathcal{H}_n^L)^+$ and $\sigma_n^R\in\mathfrak{S}(\mathcal{H}_n^R)$ are invertible, such that for any $\rho\in\mathfrak{S}(\mathcal{H})$, Φ is sufficient with respect to $\{\rho,\sigma\}$ if and only if

$$U\rho U^*=\bigoplus_n B_n^L\otimes\sigma_n^R$$

for some $B_n^L\in B(\mathcal{H}_n^L)^+$.

Proof. Follows by theorems 4 and 5 applied to the channel $\Omega=\Phi_\sigma\circ\Phi$. $\square$

3. The main result

Let $\rho,\sigma\in\mathfrak{S}(\mathcal{H})$. It is easy to see that for $\alpha>1$ we may define the sandwiched Rényi relative entropies by

$$\tilde{D}_\alpha(\rho\|\sigma)=\begin{cases}\dfrac{\alpha}{\alpha-1}\log\|\rho\|_{\alpha,\sigma} & \text{if}\rho\in L_{\alpha,\sigma}(\mathcal{H})\\ \infty & \text{otherwise}\end{cases}$$

Similarly as in [2, 29], the data processing inequality for $\tilde{D}_\alpha$, $\alpha>1$ and for any positive trace-preserving map Φ is an obvious consequence of proposition 3. Assume now that Φ is a channel. It is clear that if Φ is sufficient with respect to $\{\rho,\sigma\}$, then equality in DPI must be attained. We will show that the converse is also true.

Theorem 7. *Let $\Phi : B(\mathcal{H}) \to B(\mathcal{K})$ be a channel and let $1 < \alpha < \infty$. Let $\rho, \sigma \in \mathfrak{S}(\mathcal{H})$ be such that* $\operatorname{supp}(\rho) \subseteq \operatorname{supp}(\sigma)$*. Then Φ is sufficient with respect to $\{\rho, \sigma\}$ if and only if*

$$\tilde{D}_\alpha(\Phi(\rho)\|\Phi(\sigma)) = \tilde{D}_\alpha(\rho\|\sigma).$$

The proof is based on the following lemmas. We assume below that $\rho, \sigma \in \mathfrak{S}(\mathcal{H})$ and $\operatorname{supp}(\rho) \subseteq \operatorname{supp}(\sigma)$.

Lemma 8. *Let $\Phi : B(\mathcal{H}) \to B(\mathcal{K})$ be a positive trace-preserving map. Then $\tilde{D}_2(\Phi(\rho)\|\Phi(\sigma)) = \tilde{D}_2(\rho\|\sigma)$ if and only if $\Phi_\sigma \circ \Phi(\rho) = \rho$.*

Proof. Assume that the first equality holds. Then since $L_{2,\sigma}(\mathcal{H})$ and $L_{2,\Phi(\sigma)}(\mathcal{K})$ are Hilbert spaces and $\Phi_\sigma \circ \Phi$ is a contraction,

$$\|\rho\|_{2,\sigma}^2 = \|\Phi(\rho)\|_{2,\Phi(\sigma)}^2 = \langle \Phi(\rho), \Phi(\rho)\rangle_{\Phi(\sigma)} = \langle \Phi_\sigma \circ \Phi(\rho), \rho\rangle_\sigma \leqslant \|\rho\|_{2,\sigma}^2.$$

By the equality condition in Schwarz inequality, it follows that we must have $\Phi_\sigma \circ \Phi(\rho) = \rho$. □

Lemma 9. *Let $\Phi : B(\mathcal{H}) \to B(\mathcal{K})$ be a positive trace-preserving map and let $p > 1$. Let $Y \in L_\sigma(\mathcal{H})$ be such that $\|\Phi(Y)\|_{p,\Phi(\sigma)} = \|Y\|_{p,\sigma}$ and let $f_{Y,p}$ be as in (7). Then*

$$\|\Phi(f_{Y,p}(\theta))\|_{1/\theta,\Phi(\sigma)} = \|f_{Y,p}(\theta)\|_{1/\theta,\sigma}, \qquad \forall\ \theta \in (0, 1).$$

Proof. The function $\Phi \circ f_{Y,p} : S \to L_{\Phi(\sigma)}(\mathcal{K})$ is bounded, continuous, holomorphic in the interior of S and $\Phi \circ f_{Y,p}(1/p) = \Phi(Y)$. Using lemma 2, proposition 3 and the equalities (8) and (9), we obtain

$$\begin{aligned}
\|\Phi(Y)\|_{p,\Phi(\sigma)} &\leqslant \max\{\sup_{t\in\mathbb{R}}\|\Phi(f_{Y,p}(\mathrm{i}t))\|_{\infty,\Phi(\sigma)}, \sup_{t\in\mathbb{R}}\|\Phi(f_{Y,p}(1+\mathrm{i}t))\|_1\} \\
&\leqslant \max\{\sup_{t\in\mathbb{R}}\|f_{Y,p}(\mathrm{i}t)\|_{\infty,\sigma}, \sup_{t\in\mathbb{R}}\|f_{Y,p}(1+\mathrm{i}t)\|_1\} \\
&= \|Y\|_{p,\sigma} = \|\Phi(Y)\|_{p,\Phi(\sigma)}.
\end{aligned}$$

The statement now follows by the equality part in lemma 2. □

Proof of theorem 7. Put $p := \alpha$, $1/p + 1/q = 1$. Assume that the equality holds, that is, $\|\Phi(\rho)\|_{p,\Phi(\sigma)} = \|\rho\|_{p,\sigma}$. By putting $\theta = 1/2$ in lemma 9, we obtain that

$$\|\Phi(f_{\rho,p}(1/2))\|_{2,\Phi(\sigma)} = \|f_{\rho,p}(1/2)\|_{2,\sigma}.$$

Let $X = \sigma^{-1/2q}\rho\sigma^{-1/2q}$, so that $f_{\rho,p}(1/2) = \|\rho\|_{p,\sigma}^{1-p/2}\sigma^{1/4}X^{p/2}\sigma^{1/4}$, and put

$$\tau = (\operatorname{Tr}\sigma^{1/4}X^{p/2}\sigma^{1/4})^{-1}\sigma^{1/4}X^{p/2}\sigma^{1/4}.$$

Then $\tau \in \mathfrak{S}(\mathcal{H})$ and since τ is a constant multiple of $f_{\rho,p}(1/2)$, we have $\|\Phi(\tau)\|_{2,\Phi(\sigma)} = \|\tau\|_{2,\sigma}$. By lemma 8, this implies that Φ is sufficient with respect to $\{\tau, \sigma\}$. Let

$$U\mathcal{H} = \bigoplus_n \mathcal{H}_n^L \otimes \mathcal{H}_n^R, \qquad U\sigma U^* = \bigoplus_n A_n^L \otimes \sigma_n^R$$

be a factorization as in corollary 6, then $U\tau U^* = \bigoplus_n B_n^L \otimes \sigma_n^R$ for some $B_n^L \in B(\mathcal{H}_n^L)^+$. This entails that

$$UXU^* = \bigoplus_n C_n^L \otimes (\sigma_n^R)^{1/p}$$

for some suitable $C_n^L \in B(\mathcal{H}_n^L)^+$, and consequently $\rho = \sigma^{1/2q} X \sigma^{1/2q}$ has a factorization of the form required in corollary 6. Hence Φ is sufficient with respect to $\{\rho, \sigma\}$. □

4. Concluding remarks

We have proved that equality in DPI for $\tilde{D}_\alpha$ implies sufficiency for $\alpha > 1$, but it is still not clear whether this is true for $\alpha \in (1/2, 1)$, where DPI holds and the methods based on non-commutative L_p-norms can no longer be used. Note that the value $\alpha = 1/2$ is excluded since it is known that equality does not imply sufficiency in this case, [27].

An algebraic equality condition for the range $\alpha \in (1/2, 1) \cup (1, \infty)$ was obtained in the recent paper [23]. For $\alpha = 2$, this algebraic condition is just as in our lemma 8, but the proof in [23] requires the map to be completely positive. We also remark that, as already observed in [6], this algebraic condition can be obtained in the L_p-space framework for all $\alpha > 1$ assuming only positivity of Φ, using the fact that the spaces are uniformly convex and hence the norm of any element is attained at a unique point of the dual unit sphere. A similar uniqueness lies also at the core of the proof in [23].

As a final remark, note that for the main result, it is not necessary that Φ is completely positive. Indeed, the only place where more than positivity of Φ is required is the proof of theorem 5, but a closer look at the proof of [39, example 9.4] shows that it would be enough to assume that the map Ω^* is a Schwarz map, that is, satisfying the inequality

$$\Omega^*(X^*X) \geqslant \Omega^*(X^*)\,\Omega^*(X), \qquad \forall X \in B(\mathcal{H}).$$

This holds if both Φ and Φ_σ are adjoints of a Schwarz map, which is true for all $\sigma \in \mathfrak{S}(\mathcal{H})$ if and only if Φ is 2-positive, [17, proposition 2].

Acknowledgments

The research started from discussions with N Datta and M M Wilde during the BIRS workshop 'Beyond IID in Information Theory', held in July 2015 in Banff, Canada. I am grateful to these colleagues for turning my attention to this problem and for useful discussions at the workshop and afterwards. I am also indebted to the anonymous referees, whose valuable remarks and suggestions helped to improve the paper. The support from the grant No. VEGA 2/0069/16 is acknowledged as well.

References

[1] Audenaert K M R, Nussbaum M, Szkola A and Verstraete F 2008 Asymptotic error rates in quantum hypothesis testing *Commun. Math. Phys.* **279** 251–83
[2] Beigi S 2013 Sandwiched Rényi divergence satisfies data processing inequality *J. Math. Phys.* **54** 122202
[3] Buscemi F 2012 Comparison of quantum statistical models: equivalent conditions for sufficiency *Commun. Math. Phys.* **310** 625–47
[4] Cooney T, Mosonyi M and Wilde M M 2016 Strong converse exponents for a quantum channel discrimination problem and quantum-feedback-assisted communication *Commun. Math. Phys.* **344** 797–829

[5] Datta N 2009 Min- and max-relative entropies and a new entanglement monotone *IEEE Trans. Inf. Theory* **55** 2816–26
[6] Datta N, Jenčová A and Wilde M M 2015 Equality conditions for the sandwiched Rényi relative entropy (unpublished notes)
[7] Datta N and Leditzky F 2014 A limit of the quantum Rényi divergence *J. Phys. A: Math. Theor.* **47** 045304
[8] Datta N and Wilde M M 2015 Quantum Markov chains, sufficiency of quantum channels, and Rényi information measures *J. Phys. A: Math. Theor.* **48** 505301
[9] Fisher R A 1922 On the mathematical foundations of theoretical statistics *Phil. Trans. R. Soc.* A **222** 309–68
[10] Frank R L and Lieb E H 2013 Monotonicity of a relative Rényi entropy *J. Math. Phys.* **54** 122201
[11] Hayashi M 2007 Error exponent in asymmetric quantum hypothesis testing and its application to classical-quantum channel coding *Phys. Rev. A* **76** 062301
[12] Hayden P, Jozsa R, Petz D and Winter A 2004 Structure of states which satisfy strong subadditivity of quantum entropy with equality *Commun. Math. Phys.* **246** 359–74
[13] Hiai F and Mosonyi M 2016 Different quantum *f*-divergences and the reversibility of quantum operations (arXiv:1604.03089)
[14] Hiai F, Mosonyi M and Ogawa T 2008 Error exponents in hypothesis testing for correlated states on a spin chain *J. Math. Phys.* **49** 032112
[15] Hiai F, Mosonyi M, Petz D and Beny C 2011 Quantum f-divergences and error correction *Rev. Math. Phys.* **23** 691–747
[16] Hiai F and Petz D 1991 The proper formula for relative entropy and its asymptotics in quantum probability *Commun. Math. Phys.* **143** 99–114
[17] Jenčová A 2012 Reversibility conditions for quantum operations *Rev. Math. Phys.* **24** 1250016
[18] Jenčová A and Petz D 2006 Sufficiency in quantum statistical inference *Commun. Math. Phys.* **263** 259–76
[19] Jenčová A and Petz D 2006 Sufficiency in quantum statistical inference. A survey with examples *Infinite Dimens. Anal. Quantum Prob. Relat. Top.* **9** 331–51
[20] Jenčová A and Ruskai M B 2010 A unified treatment of convexity of relative entropy and related trace functions, with conditions for equality *Rev. Math. Phys.* **22** 1099–121
[21] Kosaki H 1984 Applications of the complex interpolation method to a von Neumann algebra: non-commutative L_p-spaces *J. Funct. Anal.* **56** 26–78
[22] Kullback S and Leibler R A 1951 On information and sufficiency *Ann. Math. Stat.* **22** 78–86
[23] Leditzky F, Rouzé C and Datta N 2016 Data processing for the sandwiched Rényi divergence: a condition for equality *Lett. Math. Phys.* (doi:10.1007/s11005-016-0896-9)
[24] Lindblad G 1975 Completely positive maps and entropy inequalities *Commun. Math. Phys.* **40** 147–51
[25] Mosonyi M and Hiai F 2011 On the quantum Rényi relative entropies and related capacity formulas *IEEE Trans. Inf. Theory* **57** 2474–87
[26] Mosonyi M and Ogawa T 2014 Strong converse exponent for classical-quantum channel coding (arXiv:1409.3562)
[27] Mosonyi M and Ogawa T 2015 Quantum hypothesis testing and the operational interpretation of the quantum Rényi relative entropies *Commun. Math. Phys.* **334** 1617–48
[28] Mosonyi M and Petz D 2004 Structure of sufficient quantum coarse-grainings *Lett. Math. Phys.* **68** 19–30
[29] Müller-Hermes A and Reeb D 2015 Monotonicity of the quantum relative entropy under positive maps (arXiv:1512.06117)
[30] Müller-Lennert M, Dupuis F, Szehr O, Fehr S and Tomamichel M 2013 On quantum Rényi entropies: a new generalization and some properties *J. Math. Phys.* **54** 122203
[31] Nagaoka H 2006 The converse part of the theorem for quantum Hoeffding bound (arxiv:quant-ph/0611289)
[32] Ogawa T and Nagaoka H 2000 Strong converse and Steins lemma in quantum hypothesis testing *IEEE Trans. Inf. Theory* **46** 2428–33
[33] Ogawa T, Sasaki A, Iwamoto M and Yamamoto H 2005 Quantum secret sharing schemes and reversibility of quantum operations *Phys. Rev.* A **72** 032318
[34] Ohya M and Petz D 1993 *Quantum Entropy and its Use* (Heidelberg: Springer)

[35] Olkiewicz R and Zegarlinski B 1999 Hypercontractivity in noncommutative L_p spaces *J. Funct. Anal.* **161** 246–85
[36] Petz D 1984 Quasi-entropies for finite quantum systems *Rep. Math. Phys.* **23** 57–65
[37] Petz D 1986 Sufficient subalgebras and the relative entropy of states of a von Neumann algebra *Commun. Math. Phys.* **105** 123–31
[38] Petz D 1988 Sufficiency of channels over von Neumann algebras *Q. J. Math. Oxford* **39** 97–108
[39] Petz D 2008 *Quantum Information Theory and Quantum Statistics* (Berlin: Springer)
[40] Rényi A 1961 On measures of information and entropy *Proc. Symp. on Mathematical Statistics Probability* (Berkeley, CA: University of California Press) p 547561
[41] Ruskai M B 2002 Inequalities for quantum entropy: a review with conditions for equality *J. Math. Phys.* **43** 4358–75
[42] Shirokov M E 2013 Reversibility of a quantum channel: general conditions and their applications to Bosonic linear channels *J. Math. Phys.* **54** 112201
[43] Shirokov M E 2014 On equalities in two entropic inequalities *Sb. Math.* **205** 1045–68
[44] Strasser H 1985 *Mathematical Theory of Statistics* ed C B de Gruyter (Berlin: Springer)
[45] Trunov N V 1979 A noncommutative analogue of the space L_p *Izv. VUZ Mat.* **23** 69–77
[46] Uhlmann A 1977 Relative entropy and Wigner–Yanase–Dyson–Lieb concavity in an interpolation theory *Commun. Math. Phys.* **54** 21–32
[47] Umegaki H 1962 Conditional expectation in an operator algebra, IV: entropy and information *Kodai Math. Sem. Rep.* **14** 59–85
[48] Wilde M M, Winter A and Yang D 2014 Strong converse for the classical capacity of entanglement-breaking and Hadamard channels via a sandwiched Rényi relative entropy *Commun. Math. Phys.* **331** 593–622
[49] Wolf M M 2012 Quantum channels and operations—guided tour. Preprint at www-m5.ma.tum.de/foswiki/pub/M5/Allgemeines/MichaelWolf/QChannelLecture.pdf
[50] Zolotarev A A 1982 L_P-spaces with respect to a state on a von Neumann algebra, and interpolation *Izv. VUZ Mat.* **26** 36–43