Recoverability of quantum channels via hypothesis testing

Anna Jenčová[1]

Abstract

A quantum channel is sufficient with respect to a set of input states if it can be reversed on this set. In the approximate version, the input states can be recovered within an error bounded by the decrease of the relative entropy under the channel. Using a new integral representation of the relative entropy in Frenkel (Integral formula for quantum relative entropy implies data processing inequality, Quantum **7**, 1102 (2023)), we present an easy proof of a characterization of sufficient quantum channels and recoverability by preservation of optimal success probabilities in hypothesis testing problems, equivalently, by preservation of L_1-distance.

Keywords Quantum channels · Quantum relative entropy · Data processing inequality · Hypothesis testing

Mathematics Subject Classification 81R15 · 94A17 · 46L53 · 62B05

1 Introduction

One of the fundamental properties of quantum relative entropy is monotonicity under quantum channels, or the data processing inequality (DPI):

$$D(\Phi(\rho)\|\Phi(\sigma)) \leq D(\rho\|\sigma) \qquad (1)$$

for any pair of quantum states ρ, σ and any completely positive trace preserving map, [32, 52]. The DPI implies other important quantum entropic inequalities, such as the Holevo bound [18], strong subadditivity of von Neumann entropy (SSA) [31] or the joint convexity of relative entropy. In fact, SSA, joint convexity and DPI are all equivalent, see [44] and the proof of DPI in [32] is based on the SSA.

✉ Anna Jenčová
jenca@mat.savba.sk

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

The question when the data processing inequality becomes an equality for a completely positive map and a pair of states was first answered by Petz [38, 39], who proved that, provided the relative entropy $D(\rho \| \sigma)$ is finite, equality occurs if and only if the two states can be fully recovered. This means that there exists a channel Ψ such that $\Psi \circ \Phi(\rho) = \rho$ and $\Psi \circ \Phi(\sigma) = \sigma$. In this case, we say that the channel Φ is sufficient with respect to the pair of states $\{\rho, \sigma\}$, in analogy with the classical notion of a statistic sufficient with respect to a family of probability distributions. Moreover, Petz proved that there exists a universal recovery channel Φ_σ, such that $\Phi_\sigma \circ \Phi(\sigma) = \sigma$ and we have $\Phi_\sigma \circ \Phi(\rho) = \rho$ if and only if the channel Φ is sufficient with respect to $\{\rho, \sigma\}$.

Sufficiency, or sometimes called reversibility, of channels was studied in a number of subsequent works and several characterizations and applications were found, [17, 20, 24, 25, 33, 35, 46]. In particular, equality conditions for various forms of DPI were studied, e.g. [27, 30, 44], and their relation to sufficiency were examined for other information theoretic or statistical quantities, such as different versions of quantum f-divergences [15, 16], quantum Rényi relative entropies [15, 21–23], Holevo quantity [45], Fisher information and L_1-distance [20].

An approximate version of sufficiency, called (approximate) recoverability is a much stronger result stating that if the decrease in the relative entropy is small, there exists a channel that recovers σ perfectly while ρ is recovered up to a small error. First result of this form was proved in the work of Fawzi and Renner [8], who considered approximate quantum Markov chains. This was soon extended to more general channels [28, 48, 49, 53] and a variety of quantities such as f-divergences [4, 5], optimized f-divergences [11] and Fisher information [12]. An important result in this context is existence of an universal recovery channel Φ_σ^u depending only on the state σ such that [28]

$$D(\rho \| \sigma) - D(\Phi(\rho) \| \Phi(\sigma)) \geq -2 \log F(\rho, \Phi_\sigma^u \circ \Phi(\rho)) \geq \| \rho - \Phi_\sigma^u \circ \Phi(\rho) \|_1^2,$$

here $\| \cdot \|_1$ denotes the trace norm and $F(\rho, \sigma) = \| \rho^{1/2} \sigma^{1/2} \|_1$ is the fidelity. See also [6, 7, 11] for the respective results for normal states of von Neumann algebras.

In the simplest setting of quantum hypothesis testing, the null hypothesis $H_0 = \sigma$ is tested against the alternative $H_1 = \rho$. The tests are represented by operators $0 \leq M \leq I$, with the interpretation that $\text{Tr}\,[\omega M]$ is the probability of rejecting the hypothesis if the true state is ω. For the test represented by M, the Bayes error probability for $\lambda \in [0, 1]$ is expressed as

$$P_e(\lambda, \rho, \sigma, M) = \lambda \text{Tr}\,[\sigma M] + (1 - \lambda) \text{Tr}\,[\rho (I - M)]$$

and the test is Bayes optimal for λ if this error probability is minimal over all possible tests. It is quite clear that if we replace the states by $\Phi(\sigma)$ and $\Phi(\rho)$, the achievable error probabilities cannot be decreased. It is a natural question when the optimal error probabilities are preserved under Φ, which is equivalent to preservation of the L_1-norm:

$$\| \rho - s\sigma \|_1 = \| \Phi(\rho) - s\Phi(\sigma) \|_1, \qquad \forall s. \qquad (2)$$

In classical statistics, the theorem of Pfanzagl [40, 47] states that if the achievable error probabilities for a pair of probability measures $\{P_0, P_1\}$ do not increase after transformation by a statistic T, then T must be sufficient with respect to $\{P_0, P_1\}$. The corresponding result for quantum channels was investigated in [20, 26], and in [34] where more general risk functions for decision problems were considered. The equivalent question of preservation of the L_1-distance, with applications to error correction, was studied in [2, 50]. In all these works, additional conditions were needed, such as the equalities have to be assumed either for larger sets of states with a special structure, or for any number of copies of ρ and σ. The case when ρ and σ commute, or the channel Φ has commutative range, was solved in [20].

Many of the results on recoverability of channels rely on an integral representation of the relative entropies or other quantities in question such as f-divergences. These formulas are based on integral representation of operator convex functions. Recently, a new integral formula for the relative entropy of positive semidefinite matrices was proved in [9]. This formula can be easily extended to infinite dimensional Hilbert spaces and rewritten in terms of the optimal Bayes error probabilities. We use this formula for simple proofs of a characterization of recoverability of quantum channels by preserving hypothesis testing error probabilities, or equivalently L_1-distances, without any additional assumptions needed in the previous works.

2 Preliminaries

Throughout this paper, $\mathcal{H}$ is a Hilbert space and we denote by $\mathcal{T}(\mathcal{H})$ the set of operators with finite trace and by $\mathcal{S}(\mathcal{H})$ the set of states (density operators) on $\mathcal{H}$, that is, positive operators of trace 1. For a self-adjoint operator $A \in B(\mathcal{H})$, $A_\pm$ denotes the positive/negative part of A and for $A \geq 0$, we denote the projection onto the support of A by $\mathrm{supp}(A)$. The L_1-distance in $\mathcal{T}(\mathcal{H})$ is defined as

$$\|S\|_1 := \sup_{\|A\| \leq 1} \mathrm{Tr}\,[AS] = \mathrm{Tr}\,|S|, \qquad S \in \mathcal{T}(\mathcal{H}).$$

If $S \in \mathcal{T}(\mathcal{H})$ is self-adjoint, then we have

$$\mathrm{Tr}\,[S_+] = \sup_{0 \leq M \leq I} \mathrm{Tr}\,[MS], \quad \mathrm{Tr}\,[S_-] = -\inf_{0 \leq M \leq I} \mathrm{Tr}\,[MS]$$

and $\mathrm{Tr}\,[S_\pm] = \frac{1}{2}(\|S\|_1 \pm \mathrm{Tr}\,[S])$.

A quantum channel Φ is a completely positive trace preserving map $\mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$. The adjoint of Φ is the map $\Phi^* : B(\mathcal{K}) \to B(\mathcal{H})$, defined by

$$\mathrm{Tr}\,[\Phi^*(A)\rho] = \mathrm{Tr}\,[A\Phi(\rho)], \qquad A \in B(\mathcal{H}),\ \rho \in \mathcal{S}(\mathcal{H}).$$

It is easily seen that Φ^* is completely positive and unital.

For positive operators $\rho, \sigma \in \mathcal{T}(\mathcal{H})$, the quantum relative entropy is defined as

$$D(\rho\|\sigma) = \begin{cases} \text{Tr}\left[\rho(\log(\rho) - \log(\sigma))\right], & \text{supp}(\rho) \leq \text{supp}(\sigma) \\ \infty, & \text{otherwise.} \end{cases}$$

Relative entropy satisfies the data processing inequality (1) which holds for any pair of states ρ, σ and any quantum channel $\Phi : \mathcal{T}(\mathcal{H}) \rightarrow \mathcal{T}(\mathcal{K})$.

2.1 Quantum hypothesis testing and L_1-distance

In the problem of hypothesis testing, the task is to test the hypothesis $H_0 = \sigma$ against the alternative $H_1 = \rho$. Any test is represented by an effect on $\mathcal{H}$, that is, an operator $0 \leq M \leq I$, corresponding to rejecting the hypothesis. For a test M, the error probabilities are

$$\alpha(M) = \text{Tr}\left[\sigma M\right], \qquad \beta(M) = \text{Tr}\left[\rho(I - M)\right].$$

For $\lambda \in (0, 1)$, we define the Bayes optimal test as the minimizer of

$$P_e(\lambda, \sigma, \rho, M) := \lambda\alpha(M) + (1 - \lambda)\beta(M) = (1 - \lambda)(1 - \text{Tr}\left[(\rho - s\sigma)M\right]),$$
$$s = \frac{\lambda}{1 - \lambda}.$$

The proof of the following description of the Bayes optimal tests can be found in [26].

Lemma 1 (Quantum Neyman-Pearson) *Let ρ, σ be states, $\lambda \in (0, 1)$ and put $s = \frac{\lambda}{1-\lambda}$. A test M is a Bayes optimal test for λ, σ, ρ if and only if*

$$M = P_{s,+} + X_s, \qquad 0 \leq X_s \leq P_{s,0},$$

where $P_{s,\pm} = \text{supp}((\rho - s\sigma)_\pm)$ and $P_{s,0} = I - P_{s,+} - P_{s,-}$. The optimal error probability is then

$$P_e(\lambda, \sigma, \rho) := \max_M P_e(\lambda, \sigma, \rho, M) = (1 - \lambda)(1 - \text{Tr}\left[(\rho - s\sigma)_+\right])$$
$$= (1 - \lambda)(s - \text{Tr}\left[(\rho - s\sigma)_-\right])$$
$$= \frac{1}{2}(1 - (1 - \lambda)\|\rho - s\sigma\|_1).$$

It is easily seen that the error probabilities and the related quantities in the above lemma are monotone under channels, in particular,

$$P_e(\lambda, \Phi(\sigma), \Phi(\rho)) \geq P_e(\lambda, \sigma, \rho),$$
$$\|\Phi(\rho) - s\Phi(\sigma)\|_1 \leq \|\rho - s\sigma\|_1,$$
$$\text{Tr}\left[(\Phi(\rho) - s\Phi(\sigma))_-\right] \leq \text{Tr}\left[(\rho - s\sigma)_-\right].$$

In fact, monotonicity holds if Φ is a positive trace preserving map, so complete positivity is not needed.

2.2 Integral formula for the relative entropy

The following new integral representation of the relative entropy was proved by Frenkel in [9], in the case $\dim(\mathcal{H}) < \infty$.

Theorem 1 *Let ρ, σ be positive operators in $\mathcal{T}(\mathcal{H})$. Then*

$$D(\rho\|\sigma) = \mathrm{Tr}\,[\rho - \sigma] + \int_{-\infty}^{\infty} \frac{dt}{|t|(1-t)^2}\,\mathrm{Tr}\,[((1-t)\rho + t\sigma)_-].$$

Proof By [9, Theorem 6], the equality holds if $\dim(\mathcal{H}) < \infty$. We will now prove that it can be extended to the case when $\dim(\mathcal{H}) = \infty$. Assume first that $\mathrm{supp}(\rho) \le \mathrm{supp}(\sigma)$, so that we may assume that σ is faithful and $\mathcal{H}$ is separable by restriction to the support of σ. We will use a standard limiting argument to extend the finite dimensional result to the separable case.

Let P_n be an increasing sequence of finite rank projections such that $\vee_n P_n = I$. Put $\rho_n = P_n \rho P_n$, $\sigma_n = P_n \sigma P_n$. Then restricted to the finite dimensional space $P_n \mathcal{H}$, ρ_n and σ_n are positive semidefinite operators with $\mathrm{supp}(\rho_n) \le \mathrm{supp}(\sigma_n)$. Moreover, $\lim_n \mathrm{Tr}\,[\rho_n] = \mathrm{Tr}\,[\rho]$, $\lim_n \mathrm{Tr}\,[\sigma_n] = \mathrm{Tr}\,[\sigma]$ and by [14, Theorem 4.5] we have $D(\rho\|\sigma) = \lim_n D(\rho_n\|\sigma_n)$.

For $t \in \mathbb{R}$ and $n \in \mathbb{N}$, put

$$f_n(t) := \mathrm{Tr}\,[((1-t)\rho_n - t\sigma_n)_-], \qquad f(t) := \mathrm{Tr}\,[((1-t)\rho - t\sigma)_-].$$

Then

$$f_n(t) = \mathrm{Tr}\,[(t\sigma_n - (1-t)\rho_n)_+] = \sup_{0 \le M_n \le P_n} \mathrm{Tr}\,[M_n(t\sigma - (1-t)\rho)]$$

$$\le \sup_{0 \le M_{n+1} \le P_{n+1}} \mathrm{Tr}\,[M_{n+1}(t\sigma - (1-t)\rho)] = \mathrm{Tr}\,[((1-t)\rho_{n+1} - t\sigma_{n+1})_-]$$

$$= f_{n+1}(t),$$

where the inequality follows from $0 \le M_n \le P_n \le P_{n+1}$. Furthermore, since $P_n \to I$ in the strong operator topology, we have using [13, Theorem 1] that

$$\|P_n((1-t)\rho - t\sigma)P_n\|_1 \to \|(1-t)\rho - t\sigma\|_1.$$

It follows that

$$f_n(t) = \tfrac{1}{2}(\|(1-t)\rho_n - t\sigma_n\|_1 - \mathrm{Tr}\,[(1-t)\rho_n - t\sigma_n])$$

$$\to \tfrac{1}{2}(\|(1-t)\rho - t\sigma\|_1 - \mathrm{Tr}\,[(1-t)\rho - t\sigma))$$

$$= f(t).$$

Hence f_n is an increasing sequence of positive integrable functions converging pointwise to f. Since the integral formula holds in finite dimensions, we see using the Lebesgue monotone convergence theorem that

$$D(\rho\|\sigma) = \lim_n D(\rho_n\|\sigma_n) = \lim_n \left(\text{Tr}\left[\rho_n - \sigma_n\right] + \int_{-\infty}^{\infty} \frac{dt}{|t|(1-t)^2} f_n(t) \right)$$

$$= \text{Tr}\left[\rho - \sigma\right] + \int_{-\infty}^{\infty} \frac{dt}{|t|(1-t)^2} f(t).$$

If $\text{supp}(\rho) \not\leq \text{supp}(\sigma)$, then there is some projection Q such that $\text{Tr}\left[\sigma Q\right] = 0$ and $c := \text{Tr}\left[\rho Q\right] > 0$. Then for any $t > 1$ we have

$$\text{Tr}\left[((1-t)\rho - t\sigma)_-\right] \geq \text{Tr}\left[Q(t\sigma - (1-t)\rho)\right] = (t-1)c$$

and hence

$$\int_{-\infty}^{\infty} \frac{dt}{|t|(t-1)^2} \text{Tr}\left[((1-t)\rho - t\sigma)_-\right] \geq c \int_1^{\infty} \frac{dt}{t(t-1)} = \infty.$$

In this case we also have $D(\rho\|\sigma) = \infty$ by definition. $\qquad\square$

The integral formula leads to an easy proof of the fact that DPI for the relative entropy holds for all positive trace preserving maps. This fact was first proved in [36], using interpolation techniques.

For our purposes, the following form of the integral formula will be useful.

Corollary 1 *Let $\rho, \sigma \in \mathcal{S}(\mathcal{H})$. Then for any $\lambda, \mu \geq 0$ such that $\mu\sigma \leq \rho \leq \lambda\sigma$, we have*

$$D(\rho\|\sigma) = \int_{\mu}^{\lambda} \frac{ds}{s} \text{Tr}\left[(\rho - s\sigma)_-\right] + \log(\lambda) + 1 - \lambda.$$

Proof Since $((1-t)\rho + t\sigma)_- = 0$ for $t \in [0, 1]$, the integral splits into two parts, integrating over $t \leq 0$ and $t \geq 1$. For the first integral, since $1 - t > 0$, we have $((1-t)\rho + t\sigma)_- = (1-t)(\rho - \frac{t}{t-1}\sigma)_-$ and

$$\int_{-\infty}^{0} \frac{dt}{-t(1-t)^2} \text{Tr}\left[(1-t)\rho + t\sigma\right]_- = \int_{-\infty}^{0} \frac{dt}{t(t-1)} \text{Tr}\left[(\rho - \frac{t}{t-1}\sigma)_-\right]$$

$$= \int_0^1 \frac{ds}{s} \text{Tr}\left[(\rho - s\sigma)_-\right]$$

$$= \int_{\mu}^1 \frac{ds}{s} \text{Tr}\left[(\rho - s\sigma)_-\right].$$

For $t \geq 1$, we use $((1-t)\rho + t\sigma)_- = ((t-1)\rho - t\sigma)_+ = (t-1)(\rho - \frac{t}{t-1}\sigma)_+$ and inserting into the integral, we obtain

$$\int_1^\infty \frac{dt}{t(t-1)^2} \mathrm{Tr}\left[((1-t)\rho + t\sigma)_-\right] = \int_1^\infty \frac{ds}{s} \mathrm{Tr}\left[(\rho - s\sigma)_+\right]$$

$$= \int_1^\lambda \frac{ds}{s} \mathrm{Tr}\left[(\rho - s\sigma)_+\right].$$

The proof is finished by using the equality $\mathrm{Tr}\left[(\rho - s\sigma)_+\right] = 1 - s + \mathrm{Tr}\left[(\rho - s\sigma)_-\right]$.

□

Remark 1 The smallest value of λ in the above expression is related to the quantum max-relative entropy defined as

$$D_{\max}(\rho\|\sigma) := \log\min\{\lambda, \ \rho \leq \lambda\sigma\}.$$

Similarly, the largest value of μ is $e^{-D_{\max}(\sigma\|\rho)}$. An important related quantity is the Hilbert projective metric [3]

$$D_\Omega(\rho\|\sigma) := D_{\max}(\rho\|\sigma) + D_{\max}(\sigma\|\rho).$$

See [41–43] for more details and interpretations in the context of quantum information theory. Note also that we may always put $\mu = 0$ and if $\dim(\mathcal{H}) < \infty$, then the condition that $\rho \leq \lambda\sigma$ for some $\lambda > 0$ is equivalent to $\mathrm{supp}(\rho) \leq \mathrm{supp}(\sigma)$, so it holds whenever $D(\rho\|\sigma)$ is finite. In infinite dimensions, this condition is much more restrictive.

2.3 Sufficiency and recoverability for quantum channels

The following definition first appeared in [39] and can be seen as a quantum generalization of the classical notion of a sufficient statistic.

Definition 1 We say that a channel $\Phi : B(\mathcal{H}) \to B(\mathcal{K})$ is sufficient with respect to a set of states $\mathcal{S} \subseteq \mathcal{S}(\mathcal{H})$ if there exists a channel $\Psi : B(\mathcal{K}) \to B(\mathcal{H})$ such that

$$\Psi \circ \Phi(\rho) = \rho, \qquad \forall \rho \in \mathcal{S}.$$

For a state $\sigma \in \mathcal{S}(\mathcal{H})$, we define an inner product $\langle \cdot, \cdot \rangle_\sigma$ in $B(\mathrm{supp}(\sigma))$ by

$$\langle A, B \rangle_\sigma := \mathrm{Tr}\left[A^*\sigma^{1/2}B\sigma^{1/2}\right], \qquad A, B \in B(\mathrm{supp}(\sigma)).$$

It was proved in [39] that the (unique) linear map $\Phi_\sigma : \mathcal{T}(\mathrm{supp}(\Phi(\sigma))) \to \mathcal{T}(\mathrm{supp}(\sigma))$ determined by

$$\langle \Phi^*(B), A \rangle_\sigma = \langle B, \Phi_\sigma^*(A) \rangle_{\Phi(\sigma)}, \qquad A \in B(\mathrm{supp}(\sigma)), B \in B(\mathrm{supp}(\Phi(\sigma)))$$

is a channel, called the Petz dual of Φ with respect to σ (or the Petz recovery map). Note that we always have $\Phi_\sigma \circ \Phi(\sigma) = \sigma$ and as it was further proved in [39], if

both σ and $\Phi(\sigma)$ are faithful, then Φ is sufficient with respect to $\mathcal{S}$ if and only if $\Phi_\sigma \circ \Phi(\rho) = \rho$ for all $\rho \in \mathcal{S}$, so that Φ_σ is a universal recovery channel.

Remark 2 If $\dim(\mathcal{H}) < \infty$, we obtain the familiar form of the Petz recovery channel:

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

We also define

$$\Phi_{\sigma,t}(\cdot) = \sigma^{-it} \Phi_\sigma(\Phi(\sigma)^{it} \cdot \Phi(\sigma)^{-it}) \sigma^{it}, \qquad t \in \mathbb{R}$$

and

$$\Phi_{\sigma,\mu}(\cdot) = \int_{-\infty}^{\infty} \Phi_{\sigma,t}(\cdot) d\mu(t),$$

for a probability measure μ on $\mathbb{R}$. Clearly, all these maps are channels $\mathcal{T}(\text{supp}(\Phi(\sigma))) \to \mathcal{T}(\text{supp}(\sigma))$ that recover the state σ.

Theorem 2 *Assume that $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ are such that $D(\rho\|\sigma) < \infty$. Then the following are equivalent.*

   (i) Φ is sufficient with respect to $\{\rho, \sigma\}$;
   (ii) $D(\Phi(\rho)\|\Phi(\sigma)) = D(\rho\|\sigma)$;
  (iii) $\Phi_{\sigma,t} \circ \Phi(\rho) = \rho$, for some $t \in \mathbb{R}$;
  (iv) $\Phi_{\sigma,t} \circ \Phi(\rho) = \rho$, for all $t \in \mathbb{R}$;
   (v) $\Phi_{\sigma,\mu} \circ \Phi(\rho) = \rho$ for some probability measure μ.

Proof In finite dimensions the proof follows from [53, Theorem 3.3]. The proof in the general case will be given in the Appendix.   □

The following is an approximate version of sufficiency of channels, called recoverability of Φ.

Theorem 3 [28] *Let $\sigma \in \mathcal{S}(\mathcal{H})$. Then for any channel $\Phi : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ there exists a channel $\Phi_\sigma^u : \mathcal{T}(\mathcal{K}) \to \mathcal{T}(\mathcal{H})$ such that $\Phi_\sigma^u \circ \Phi(\sigma) = \sigma$ and for any $\rho \in \mathcal{S}(\mathcal{H})$ we have*

$$D(\rho\|\sigma) \geq D(\Phi(\rho)\|\Phi(\sigma)) - 2\log F(\rho, \Phi_\sigma^u \circ \Phi(\rho))$$

$$\geq D(\Phi(\rho)\|\Phi(\sigma)) + \frac{1}{4}\|\rho - \Phi_\sigma^u \circ \Phi(\rho)\|_1^2.$$

In the above theorem, $F(\rho_0, \rho_1)$ is the fidelity

$$F(\rho_0, \rho_1) = \|\rho_0^{1/2} \rho_1^{1/2}\|_1.$$

The second inequality in Theorem 3 is obtained using the inequality $-\log(x) \geq 1 - x$ for $x \in (0, 1)$ and the Fuchs-van de Graaf inequality, [10].

The universal recovery channel Φ_σ^u can be chosen as

$$\Phi_\sigma^u(\cdot) = \Phi_{\sigma,\beta_0}(P \cdot P) + \text{Tr}\,[(I - P)\cdot], \tag{3}$$

here $P = \text{supp}(\Phi(\sigma))$ and β_0 is the probability density function

$$\beta_0(t) = \frac{\pi}{\cosh(2\pi t) + 1}.$$

Note that if $\text{supp}(\rho) \leq \text{supp}(\sigma)$, then $\text{supp}(\Phi(\rho)) \leq \text{supp}(\Phi(\sigma))$, so that $\Phi_\sigma^u(\Phi(\rho)) = \Phi_{\sigma,\beta_0}(\Phi(\rho))$ and the statement in this case follows by [28, Theorem 2.1]. If $\text{supp}(\rho) \not\leq \text{supp}(\sigma)$, then $D(\rho\|\sigma) = \infty$ and the inequality holds trivially.

3 Sufficiency and recoverability by hypothesis testing

The characterization in Theorem 2 and the integral formula in Corollary 1 now give an easy proof of characterization of sufficiency and recoverability by quantities related to hypothesis testing. Note that here we do not have to make any further assumptions about the states.

Theorem 4 *Let* $\Phi : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ *be a channel and let* $\rho, \sigma \in \mathcal{S}(\mathcal{H})$. *Then the following are equivalent.*

(i) $P_e(\lambda, \Phi(\rho), \Phi(\sigma)) = P_e(\lambda, \rho, \sigma)$, *for all* $\lambda \in [0, 1]$;
(ii) $\|\Phi(\rho) - s\Phi(\sigma)\|_1 = \|\rho - s\sigma\|_1$, *for all* $s \geq 0$;
(iii) $\text{Tr}\,[(\Phi(\rho) - s\Phi(\sigma))_+] = \text{Tr}\,[(\rho - s\sigma)_+]$, *for all* $s \geq 0$;
(iv) $\text{Tr}\,[(\Phi(\rho) - s\Phi(\sigma))_-] = \text{Tr}\,[(\rho - s\sigma)_-]$, *for all* $s \geq 0$;
(v) Φ *is sufficient with respect to* $\{\rho, \sigma\}$.

Proof The equivalences between (i)-(iv) are clear from Lemma 1. Assume that (iv) holds. Suppose first that $\rho \leq \lambda\sigma$ for some $\lambda > 0$. Then also $\Phi(\rho) \leq \lambda\Phi(\sigma)$ and we have by Corollary 1

$$D(\Phi(\rho)\|\Phi(\sigma)) = \int_0^\lambda \frac{ds}{s}\text{Tr}\,[(\Phi(\rho) - s\Phi(\sigma))_-] + \log(\lambda) + 1 - \lambda$$

$$= \int_0^\lambda \frac{ds}{s}\text{Tr}\,[(\rho - s\sigma)_-] + \log(\lambda) + 1 - \lambda = D(\rho\|\sigma).$$

By Theorem 2, this implies (v). In the general case, let $\sigma_0 = \frac{1}{2}(\rho + \sigma)$, then $\rho \leq 2\sigma_0$ and it is easily seen that the equality (ii) implies a similar equality with σ replaced by σ_0. It follows that Φ is sufficient with respect to $\{\rho, \sigma_0\}$, which implies (v). The implication (v) $\implies$ (ii) follows from monotonicity of the L_1-distance. $\square$

We are now interested in a similar result for recoverability. Assume first that there is a channel $\Lambda : \mathcal{T}(\mathcal{K}) \to \mathcal{T}(\mathcal{H})$ such that $\Lambda \circ \Phi(\sigma) = \sigma$ and $\|\Lambda \circ \Phi(\rho) - \rho\|_1 \leq \epsilon$. We then have

$$\|\rho - s\sigma\|_1 = \|\rho - \Lambda \circ \Phi(\rho) + \Lambda \circ \Phi(\rho) - s\Lambda \circ \Phi(\sigma)\|_1 \leq \|\Phi(\rho) - s\Phi(\sigma)\|_1 + \epsilon. \tag{4}$$

Using Lemma 1, we see that the resulting inequality in (4) is equivalent to any of the following inequalities

$$\text{Tr}\,[(\Phi(\rho) - s\Phi(\sigma))_+] \geq \text{Tr}\,[(\rho - s\sigma)_+] - \frac{\epsilon}{2}, \qquad s \geq 0 \tag{5}$$

$$\text{Tr}\,[(\Phi(\rho) - s\Phi(\sigma))_-] \geq \text{Tr}\,[(\rho - s\sigma)_-] - \frac{\epsilon}{2}, \qquad s \geq 0 \tag{6}$$

$$P_e(\lambda, \Phi(\sigma), \Phi(\rho)) \leq P_e(\lambda, \sigma, \rho) + \frac{1 - \lambda}{2}\epsilon, \qquad \lambda \in [0, 1]. \tag{7}$$

The following result gives the converse statement. Note that here we will need the assumption that the Hilbert projective metric $D_\Omega(\rho\|\sigma)$ is finite, equivalently, that $\mu\sigma \leq \rho \leq \lambda\sigma$ for some $\mu, \lambda > 0$ (see Remark 1), to get a nontrivial result.

Theorem 5 *Let $\rho, \sigma \in \mathcal{S}(\mathcal{H})$ and let $\Phi : \mathcal{T}(\mathcal{H}) \to \mathcal{T}(\mathcal{K})$ be a quantum channel. If*

$$\|\Phi(\rho) - s\Phi(\sigma)\|_1 \geq \|\rho - s\sigma\|_1 - \epsilon, \qquad \forall s \geq 0$$

holds for some $\epsilon \geq 0$, then there exists a channel $\Lambda : \mathcal{T}(\mathcal{K}) \to \mathcal{T}(\mathcal{H})$ such that $\Lambda \circ \Phi(\sigma) = \sigma$ and

$$\|\Lambda \circ \Phi(\rho) - \rho\|_1 \leq \sqrt{2\epsilon}\, D_\Omega(\rho\|\sigma)^{1/2}.$$

Moreover, we may take $\Lambda = \Phi_\sigma^u$ as in (3).

Proof The statement is trivial if $D_\Omega(\rho\|\sigma) = \infty$, so assume that $\mu\sigma \leq \rho \leq \lambda\sigma$ for $\mu, \lambda > 0$, $\mu = e^{-D_{\max}(\sigma\|\rho)}$ and $\lambda = e^{D_{\max}(\rho\|\sigma)}$. Then also $\mu\Phi(\sigma) \leq \Phi(\rho) \leq \lambda\Phi(\sigma)$. By the assumptions, inequality (6) holds. Using Corollary 1, we get

$$D(\rho\|\sigma) - D(\Phi(\rho)\|\Phi(\sigma)) = \int_\mu^\lambda \frac{ds}{s}\left(\text{Tr}\,[(\rho - s\sigma)_-] - \text{Tr}\,[(\Phi(\rho) - s\Phi(\sigma))_-]\right)$$

$$\leq \frac{\epsilon}{2}\int_\mu^\lambda \frac{1}{s}ds = \frac{\epsilon}{2}\big(\log(\lambda) - \log(\mu)\big) = \frac{\epsilon}{2}D_\Omega(\rho\|\sigma).$$

The statement now follows by Theorem 3. $\qquad\qquad\square$

Remark 3 The recoverability result can be also formulated in the setting of comparison of statistical experiments, which is an extension of the classical theory of Blackwell [1], Törgersen [51] and Le Cam [29]. A (quantum) statistical experiment is any parametrized family of (quantum) states. For two experiments $\mathcal{E}$ and $\mathcal{E}_0$ with the same parameter set (not necessarily living on the same Hilbert space), we say that $\mathcal{E}_0$ is $(2, \epsilon)$-deficient with respect to $\mathcal{E}$ if the error probabilities of testing problems involving elements of $\mathcal{E}_0$ are up to ϵ not worse than those of corresponding testing problems for $\mathcal{E}$. See [19] for a more precise definition. In particular, for $\mathcal{E}_0 = \{\rho_0, \sigma_0\}$ and $\mathcal{E} = \{\rho, \sigma\}$, this amounts to the condition

$$P_e(\lambda, \rho_0, \sigma_0) \leq P_e(\lambda, \rho, \sigma) + \epsilon, \qquad \forall \lambda \in [0, 1].$$

Using Lemma 1, we see that this is equivalent to any of the inequalities

$$\|\rho_0 - s\sigma_0\|_1 \geq \|\rho - s\sigma\|_1 - 2\epsilon(1+s), \qquad s \geq 0$$
$$\text{Tr}\left[(\rho_0 - s\sigma_0)_+\right] \geq \text{Tr}\left[(\rho - s\sigma)_+\right] - \epsilon(1+s), \qquad s \geq 0$$
$$\text{Tr}\left[(\rho_0 - s\sigma_0)_-\right] \geq \text{Tr}\left[(\rho - s\sigma)_-\right] - \epsilon(1+s), \qquad s \geq 0.$$

It is easily seen that this is true if there is some channel Λ such that $\|\Lambda(\rho_0) - \rho\|_1 \leq \epsilon$ and $\|\Lambda(\sigma_0) - \sigma\|_1 \leq \epsilon$. In the classical case the converse holds, but in the quantum case this is not true. We can obtain some form of the converse statement if $\rho_0 = \Phi(\rho)$ and $\sigma_0 = \Phi(\sigma)$, in a similar way as in Theorem 5.

A Appendix: Proof of Theorem 2

The implication (i) $\implies$ (ii) follows by the data processing inequality (1), (ii) $\implies$ (iii) (with $t = 0$) was proved in [24, 39]. The implications (iii) $\implies$ (i) and (iv) $\implies$ (v) $\implies$ (i) are easy, so the only thing left to prove is (i) $\implies$ (iv).

By the assumption $D(\rho\|\sigma) < \infty$, we have that $\text{supp}(\rho) \leq \text{supp}(\sigma)$ and also $\text{supp}(\Phi(\rho)) \leq \text{supp}(\Phi(\sigma))$. We may therefore assume that both σ and $\Phi(\sigma)$ are faithful, by restriction to the respective supports.

With this assumption, we will also need to recall some further properties of sufficient channels from [24, 39]. Let us denote by u_t and v_t the Connes cocycles

$$u_t = \rho^{it}\sigma^{-it}, \quad v_t = \Phi(\rho)^{it}\Phi(\sigma)^{-it}, \qquad t \in \mathbb{R},$$

then u_t and v_t are one-parameter families of isometries satisfying the conditions

$$\sigma^{is}u_t\sigma^{-is} = u_s^*u_{t+s}, \quad \Phi(\sigma)^{is}v_t\Phi(\sigma)^{-is} = v_s^*v_{t+s}, \qquad s, t \in \mathbb{R}.$$

By the results of [24, 39], we can see that if Φ is sufficient with respect to $\{\rho, \sigma\}$, then u_t is in the multiplicative domain of the unital completely positive map Φ_σ^* and similarly v_t is in the multiplicative domain of Φ^*, see [37, Theorem 3.18] for the definition and properties of multiplicative domains. Moreover, $\Phi^*(v_t) = u_t$ and $\Phi_\sigma^*(u_t) = v_t$. It follows that for any $s, t \in \mathbb{R}$,

$$\Phi^*(\Phi(\sigma)^{it}v_s\Phi(\sigma)^{-it}) = \Phi^*(v_t^*v_{s+t}) = u_t^*u_{s+t} = \sigma^{it}u_s\sigma^{-it}$$

and similarly $\Phi_\sigma^*(\sigma^{it}u_s\sigma^{-it}) = \Phi(\sigma)^{it}v_s\Phi(\sigma)^{-it}$. Let now $A \in B(\mathcal{H})$, we have for all $s, t \in \mathbb{R}$,

$$\langle \sigma^{it}u_sA^*\sigma^{-it}, \sigma^{it}u_s\sigma^{-it} \rangle_\sigma = \langle u_sA^*, u_s \rangle_\sigma = \text{Tr}\,[A\rho^{is}\sigma^{1/2-is}\rho_s^{is}\sigma^{1/2-is}]$$

and the analytic continuation to $s = -\frac{1}{2}i$ of the last expression becomes $\text{Tr}\,[A\rho]$. On the other hand, using the above properties of the cocycles and of multiplicative

domains, we get by the definition of the Petz dual

$$
\begin{aligned}
\langle\, \sigma^{it} u_s A^* \sigma^{-it}, \sigma^{it} u_s \sigma^{-it} \,\rangle_\sigma \\
&= \langle\, \sigma^{it} u_s A^* \sigma^{-it}, \Phi^*(\Phi(\sigma)^{it} v_s \Phi(\sigma)^{-it}) \,\rangle_\sigma \\
&= \langle\, \Phi_\sigma^*(\sigma^{it} u_s A^* \sigma^{-it}), \Phi(\sigma)^{it} v_s \Phi(\sigma)^{-it} \,\rangle_{\Phi(\sigma)} \\
&= \langle\, \Phi(\sigma)^{it} v_s \Phi(\sigma)^{-it} \Phi_\sigma^*(\sigma^{it} A^* \sigma^{-it}), \Phi(\sigma)^{it} v_s \Phi(\sigma)^{-it} \,\rangle_{\Phi(\sigma)} \\
&= \mathrm{Tr}\,[\Phi_{t,\sigma}^*(A)\Phi(\rho)^{is}\Phi(\sigma)^{1/2-is}\Phi(\rho)^{is}\Phi(\sigma)^{1/2-is}],
\end{aligned}
$$

here the analytic continuation to $s = -\frac{1}{2}i$ equals

$$
\mathrm{Tr}\,[\Phi_{t,\sigma}^*(A)\Phi(\rho)] = \mathrm{Tr}\,[A\Phi_{t,\sigma}(\Phi(\rho))].
$$

Since A and t were arbitrary, this finishes the proof of (i) $\implies$ (iv).

Data availability Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Conflict of interest The author declares that there is no conflict of interest.

References

1. Blackwell, D.: Equivalent comparisons of experiments. Ann. Math. Stat. **24**(2), 265–272 (1953). https://doi.org/10.1214/aoms/1177729032
2. Blume-Kohout, R., Ng, H.K., Poulin, D., Viola, L.: Information-preserving structures: a general framework for quantum zero-error information. Phys. Rev. A **82**(6), 062306 (2010). https://doi.org/10.1103/PhysRevA.82.062306
3. Bushell, P.J.: Hilbert's metric and positive contraction mappings in a Banach space. Arch. Ration. Mech. Anal. **52**, 330–338 (1973). https://doi.org/10.1007/BF00247467
4. Carlen, E.A., Vershynina, A.: Recovery and the data processing inequality for quasi-entropies. IEEE Trans. Inf. Theory **64**(10), 6929–6938 (2018). https://doi.org/10.1109/TIT.2018.2812038

5. Carlen, E.A., Vershynina, A.: Recovery map stability for the data processing inequality. J. Phys. A Math. Theor. **53**(3), 035204 (2020). https://doi.org/10.1088/1751-8121/ab5ab7

6. Faulkner, T., Hollands, S.: Approximate recoverability and relative entropy II: 2-positive channels of general von Neumann algebras. Lett. Math. Phys. **112**(2), 26 (2022). https://doi.org/10.1007/s11005-022-01510-9

7. Faulkner, T., Hollands, S., Swingle, B., Wang, Y.: Approximate recovery and relative entropy I: General von Neumann subalgebras. Commun. Math. Phys. **389**(1), 349–397 (2022). https://doi.org/10.1007/s00220-021-04143-6

8. Fawzi, O., Renner, R.: Quantum conditional mutual information and approximate Markov chains. Commun. Math. Phys. **340**(2), 575–611 (2015). https://doi.org/10.1007/s00220-015-2466-x

9. Frenkel, P.E.: Integral formula for quantum relative entropy implies data processing inequality. Quantum **7**, 1102 (2023)

10. Fuchs, C.A., Van De Graaf, J.: Cryptographic distinguishability measures for quantum-mechanical states. IEEE Trans. Inf. Theory **45**(4), 1216–1227 (1999). https://doi.org/10.1109/18.761271

11. Gao, L., Wilde, M.M.: Recoverability for optimized quantum f-divergences. J. Phys. A Math. Theor. **54**(38), 385302 (2021). https://doi.org/10.1088/1751-8121/ac1dc2

12. Gao, L., Li, H., Marvian, I., Rouzé, C.: Sufficient statistic and recoverability via Quantum Fisher Information metrics. arXiv:2302.02341 (2023)

13. Grümm, H.: Two theorems about C_p. Rep. Math. Phys. **4**(3), 211–215 (1973). https://doi.org/10.1016/0034-4877(73)90026-8

14. Hiai, F.: Quantum f-divergences in von Neumann algebras. I. Standard f-divergences. J. Math. Phys. **59**(10), 102202 (2018)

15. Hiai, F.: Quantum f-Divergences in von Neumann Algebras: Reversibility of Quantum Operations. Mathematical Physics Studies, Springer, Singapore (2021). https://doi.org/10.1007/978-981-33-4199-9

16. Hiai, F., Mosonyi, M.: Different quantum f-divergences and the reversibility of quantum operations. Rev. Math. Phys. **29**(07), 1750023 (2017). https://doi.org/10.1142/S0129055X17500234

17. Hiai, F., Mosonyi, M., Petz, D., Bény, C.: Quantum f-divergences and error correction. Rev. Math. Phys. **23**(07), 691–747 (2011). https://doi.org/10.1142/S0129055X11004412

18. Holevo, A.S.: Bounds for the quantity of information transmitted by a quantum communication channel. Problemy Peredachi Informatsii **9**(3), 3–11 (1973)

19. Jenčová, A.: Comparison of quantum binary experiments. Rep. Math. Phys. **70**(2), 237–249 (2012). https://doi.org/10.1016/S0034-4877(12)60043-3

20. Jenčová, A.: Reversibility conditions for quantum operations. Rev. Math. Phys. **24**(07), 1250016 (2012). https://doi.org/10.1142/S0129055X1250016X

21. Jenčová, A.: Preservation of a quantum Rényi relative entropy implies existence of a recovery map. J. Phys. A **50**, 085303 (2017). https://doi.org/10.1088/1751-8121/aa5661

22. Jenčová, A.: Rényi relative entropies and noncommutative L_p-spaces. Ann. Henri Poincaré **19**, 2513–2542 (2018). https://doi.org/10.1007/s00023-018-0683-5

23. Jenčová, A.: Rényi relative entropies and noncommutative L_p-spaces II. Ann. Henri Poincaré **22**, 3235–3254 (2021). https://doi.org/10.1007/s00023-021-01074-9

24. Jenčová, A., Petz, D.: Sufficiency in quantum statistical inference: a survey with examples. Infin. Dimens. Anal. Quantum Probab. Relat. Top. **9**(03), 331–351 (2006). https://doi.org/10.1142/S0219025706002408

25. Jenčová, A., Petz, D.: Sufficiency in quantum statistical inference. Commun. Math. Phys. **263**, 259–276 (2006). https://doi.org/10.1007/s00220-005-1510-7

26. Jenčová, A.: Quantum hypothesis testing and sufficient subalgebras. Lett. Math. Phys. **93**, 15–27 (2010). https://doi.org/10.1007/s11005-010-0398-0

27. Jenčová, A., Ruskai, M.B.: A unified treatment of convexity of relative entropy and related trace functions, with conditions for equality. Rev. Math. Phys. **22**, 1099–1121 (2010)

28. Junge, M., Renner, R., Sutter, D., Wilde, M.M., Winter, A.: Universal recovery maps and approximate sufficiency of quantum relative entropy. Ann. Henri Poincaré **19**(10), 2955–2978 (2018). https://doi.org/10.1007/s00023-018-0716-0

29. Le Cam, L.: Sufficiency and approximate sufficiency. Ann. Math. Stat. **35**(4), 1419–1455 (1964). https://doi.org/10.1214/aoms/1177700372

30. Leditzky, F., Rouzé, C., Datta, N.: Data processing for the sandwiched Rényi divergence: a condition for equality. Lett. Math. Phys. **107**(1), 61–80 (2017). https://doi.org/10.1007/s11005-016-0896-9

31. Lieb, E.H., Ruskai, M.B.: Proof of the strong subadditivity of quantum-mechanical entropy. Les rencontres physiciens-mathématiciens de Strasbourg-RCP25 **19**, 36–55 (1973). https://doi.org/10.1063/1.1666274

32. Lindblad, G.: Completely positive maps and entropy inequalities. Commun. Math. Phys. **40**, 147–151 (1975). https://doi.org/10.1007/BF01609396

33. Łuczak, A.: Quantum sufficiency in the operator algebra framework. Int. J. Theor. Phys. **53**(10), 3423–3433 (2014). https://doi.org/10.1007/s10773-013-1747-4

34. Łuczak, A.: On a general concept of sufficiency in von Neumann algebras. Probab. Math. Stat. **35**, 313–324 (2015)

35. Mosonyi, M., Petz, D.: Structure of sufficient quantum coarse-grainings. Lett. Math. Phys. **68**, 19–30 (2004). https://doi.org/10.1007/s11005-004-4072-2

36. Müller-Hermes, A., Reeb, D.: Monotonicity of the quantum relative entropy under positive maps. Ann. Henri Poincaré **18**, 1777–1788 (2017). https://doi.org/10.1007/s00023-017-0550-9

37. Paulsen, V.: Completely Bounded Maps and Operator Algebras. Cambridge University Press, Cambridge (2002)

38. Petz, D.: Sufficient subalgebras and the relative entropy of states of a von Neumann algebra. Commun. Math. Phys. **105**(1), 123–131 (1986). https://doi.org/10.1007/BF01212345

39. Petz, D.: Sufficiency of channels over von Neumann algebras. Q. J. Math. **39**(1), 97–108 (1988). https://doi.org/10.1093/qmath/39.1.97

40. Pfanzagl, J.: A characterization of sufficiency by power functions. Metrika **21**(1), 197–199 (1974). https://doi.org/10.1007/BF01893900

41. Reeb, D., Kastoryano, M.J., Wolf, M.M.: Hilbert's projective metric in quantum information theory. J. Math. Phys. **52**(8), 082201 (2011). https://doi.org/10.1063/1.3615729

42. Regula, B.: Probabilistic transformations of quantum resources. Phys. Rev. Lett. **128**(11), 110505 (2022). https://doi.org/10.1103/PhysRevLett.128.110505

43. Regula, B., Lami, L., Wilde, M.M.: Postselected quantum hypothesis testing (2022). arXiv:2209.10550

44. Ruskai, M.B.: Inequalities for quantum entropy: a review with conditions for equality. J. Math. Phys. **43**(9), 4358–4375 (2002). https://doi.org/10.1063/1.1497701

45. Shirokov, M.E.: Reversibility conditions for quantum channels and their applications. Sbornik Mathematics **204**(8), 1215 (2013). https://doi.org/10.1070/SM2013v204n08ABEH004337

46. Shirokov, M.E.: Reversibility of a quantum channel: general conditions and their applications to bosonic linear channels. J. Math. Phys. **54**(11), 112201 (2013). https://doi.org/10.1063/1.4827436

47. Strasser, H.: Mathematical Theory of Statistics. Walter de Gruyter, Berlin (1985). https://doi.org/10.1515/9783110850826

48. Sutter, D., Tomamichel, M., Harrow, A.W.: Strengthened monotonicity of relative entropy via pinched Petz recovery map. IEEE Trans. Inf. Theory **62**(5), 2907–2913 (2016). https://doi.org/10.1109/TIT.2016.2545680

49. Sutter, D., Berta, M., Tomamichel, M.: Multivariate trace inequalities. Commun. Math. Phys. **352**, 37–58 (2017). https://doi.org/10.1007/s00220-016-2778-5

50. Ticozzi, F., Viola, L.: Quantum information encoding, protection, and correction from trace-norm isometries. Phys. Rev. A **81**(3), 032313 (2010). https://doi.org/10.1103/PhysRevA.81.032313

51. Törgersen, E.: Comparison of Statistical Experiments. Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge (1991). https://doi.org/10.1017/CBO9780511666353

52. Uhlmann, A.: Relative entropy and the Wigner-Yanase-Dyson-Lieb concavity in an interpolation theory. Commun. Math. Phys. **54**, 21–32 (1977). https://doi.org/10.1007/BF01609834

53. Wilde, M.M.: Recoverability in quantum information theory. Proc. R. Soc. A Math. Phys. Eng. Sci. **471**(2182), 20150338 (2015). https://doi.org/10.1098/rspa.2015.0338