

A limit relation for entropy and channel capacity per unit cost

Imre Csiszár^{1,4}, Fumio Hiai^{2,5} and Dénes Petz^{3,4}

⁴ Alfréd Rényi Institute of Mathematics,
H-1364 Budapest, POB 127, Hungary

⁵ Graduate School of Information Sciences, Tohoku University
Aoba-ku, Sendai 980-8579, Japan

Abstract: In a quantum mechanical model, Diósi, Feldmann and Kosloff arrived at a conjecture stating that the limit of the entropy of certain mixtures is the relative entropy as system size goes to infinity. The conjecture is proven in this paper for density matrices. The first proof is analytic and uses the quantum law of large numbers. The second one clarifies the relation to channel capacity per unit cost for classical-quantum channels. Both proofs lead to generalizations of the conjecture.

Key words: Shannon entropy, von Neumann entropy, relative entropy, capacity per unit cost, Holevo bound.

¹E-mail: csiszar@renyi.hu. Partially supported by the Hungarian Research Grant OTKA T068258.

²E-mail: hiai@math.is.tohoku.ac.jp. Partially supported by Grant-in-Aid for Scientific Research (B)17340043.

³E-mail: petz@math.bme.hu. Partially supported by the Hungarian Research Grant OTKA T068258.

1 Introduction

It was conjectured by Diósi, Feldmann and Kosloff in [4], based on thermodynamical considerations, that the von Neumann entropy of a quantum state equal to a mixture

$$R_n := \frac{1}{n} (\sigma \otimes \rho^{\otimes(n-1)} + \rho \otimes \sigma \otimes \rho^{\otimes(n-2)} + \dots + \rho^{\otimes(n-1)} \otimes \sigma)$$

exceeds the entropy of a component asymptotically by the Umegaki relative entropy $S(\sigma\|\rho)$, that is,

$$S(R_n) - (n-1)S(\rho) - S(\sigma) \rightarrow S(\sigma\|\rho) \quad (1)$$

as $n \rightarrow \infty$. Here ρ and σ are density matrices acting on a finite dimensional Hilbert space. Recall that $S(\sigma) = -\text{Tr } \sigma \log \sigma$ and

$$S(\sigma\|\rho) = \begin{cases} \text{Tr } \sigma(\log \sigma - \log \rho) & \text{if } \text{supp } \sigma \leq \text{supp } \rho \\ +\infty & \text{otherwise.} \end{cases}$$

Concerning the background of quantum entropy quantities, we refer to [10, 12].

Apparently no exact proof of (1) has been published even for the classical case, although for that case a heuristic proof is offered in [4].

In the paper first an analytic proof of (1) is given for the case $\text{supp } \sigma \leq \text{supp } \rho$, using an inequality between the Umegaki and the Belavkin-Staszewski relative entropies, and the weak law of large numbers in the quantum case. In the second part of the paper, it is clarified that the problem is related to the theory of classical-quantum channels. The essential observation is the fact that $S(R_n) - (n-1)S(\rho) - S(\sigma)$ in the conjecture is a Holevo quantity (classical-quantum mutual information) for a certain channel for which the relative entropy emerges as the capacity per unit cost.

The two different proofs lead to two different generalizations of the conjecture.

2 An analytic proof of the conjecture

In this section we assume that $\text{supp } \sigma \leq \text{supp } \rho$ for the support projections of σ and ρ . One can simply compute:

$$\begin{aligned} S(R_n\|\rho^{\otimes n}) &= \text{Tr}(R_n \log R_n - R_n \log \rho^{\otimes n}) \\ &= -S(R_n) - (n-1)\text{Tr } \rho \log \rho - \text{Tr } \sigma \log \rho. \end{aligned}$$

Hence the identity

$$S(R_n\|\rho^{\otimes n}) = -S(R_n) + (n-1)S(\rho) + S(\sigma\|\rho) + S(\sigma)$$

holds. It follows that the conjecture (1) is equivalent to the statement

$$S(R_n\|\rho^{\otimes n}) \rightarrow 0 \quad \text{as } n \rightarrow \infty$$

when $\text{supp } \sigma \leq \text{supp } \rho$.

Recall the Belavkin-Staszewski relative entropy

$$S_{\text{BS}}(\omega \| \rho) = \text{Tr}(\omega \log(\omega^{1/2} \rho^{-1} \omega^{1/2})) = -\text{Tr}(\rho \eta(\rho^{-1/2} \omega \rho^{-1/2}))$$

if $\text{supp } \omega \leq \text{supp } \rho$, where $\eta(t) := -t \log t$, see [1, 10]. It was proved by Hiai and Petz that

$$S(\omega \| \rho) \leq S_{\text{BS}}(\omega \| \rho), \quad (2)$$

see [6], or Proposition 7.11 in [10].

Theorem 1. *If $\text{supp } \sigma \leq \text{supp } \rho$, then $S(R_n) - (n-1)S(\rho) - S(\sigma) \rightarrow S(\sigma \| \rho)$ as $n \rightarrow \infty$.*

Proof: We want to use the quantum law of large numbers, see Proposition 1.17 in [10]. Assume that ρ and σ are $d \times d$ density matrices and we may suppose that ρ is invertible. Due to the GNS-construction with respect to the limit φ_∞ of the product states $\varphi_n(A) = \text{Tr } \rho^{\otimes n} A$ on the n -fold tensor product $M_d(\mathbb{C})^{\otimes n}$, $n \in \mathbb{N}$, all finite tensor products $M_d(\mathbb{C})^{\otimes n}$ are embedded into a von Neumann algebra \mathcal{M} acting on a Hilbert space \mathcal{H} . If γ denotes the right shift and $X := \rho^{-1/2} \sigma \rho^{-1/2}$, then R_n is written as

$$R_n = (\rho^{1/2})^{\otimes n} \left(\frac{1}{n} \sum_{i=0}^{n-1} \gamma^i(X) \right) (\rho^{1/2})^{\otimes n}.$$

By inequality (2), we get

$$\begin{aligned} 0 \leq S(R_n \| \rho^{\otimes n}) &\leq S_{\text{BS}}(R_n \| \rho^{\otimes n}) \\ &= -\text{Tr} \left(\rho^{\otimes n} \eta \left((\rho^{-1/2})^{\otimes n} R_n (\rho^{-1/2})^{\otimes n} \right) \right) \\ &= \left\langle \Omega, \eta \left(\frac{1}{n} \sum_{i=0}^{n-1} \gamma^i(X) \right) \Omega \right\rangle, \end{aligned} \quad (3)$$

where Ω is the cyclic vector in the GNS-construction.

The law of large numbers gives

$$\frac{1}{n} \sum_{i=0}^{n-1} \gamma^i(X) \rightarrow I$$

in the strong operator topology in $B(\mathcal{H})$, since $\varphi(X) = \text{Tr } \rho \rho^{-1/2} \sigma \rho^{-1/2} = 1$.

Since the continuous functional calculus preserves the strong convergence (simply due to approximation by polynomials on a compact set), we obtain

$$\eta \left(\frac{1}{n} \sum_{i=0}^{n-1} \gamma^i(X) \right) \rightarrow \eta(I) = 0 \text{ strongly.}$$

This shows that the upper bound (3) converges to 0 and the proof is complete. \square

By the same proof one can obtain that for

$$R_{m,n} := \frac{1}{n} (\sigma^{\otimes m} \otimes \rho^{\otimes(n-1)} + \rho \otimes \sigma^{\otimes m} \otimes \rho^{\otimes(n-2)} + \dots + \rho^{\otimes(n-1)} \otimes \sigma^{\otimes m}),$$

the limit relation

$$S(R_{m,n}) - (n-1)S(\rho) - mS(\sigma) \rightarrow mS(\sigma\|\rho) \quad (4)$$

holds as $n \rightarrow \infty$ when m is fixed.

In the next theorem we treat the probabilistic case in a matrix language. The proof includes the case when $\text{supp } \sigma \leq \text{supp } \rho$ is not true. Those readers who are not familiar with the quantum setting of the previous theorem are suggested to follow the arguments below.

Theorem 2. *Assume that ρ and σ are commuting density matrices. Then $S(R_n) - (n-1)S(\rho) - S(\sigma) \rightarrow S(\sigma\|\rho)$ as $n \rightarrow \infty$.*

Proof: We may assume that $\rho = \text{Diag}(\mu_1, \dots, \mu_\ell, 0, \dots, 0)$ and $\sigma = \text{Diag}(\lambda_1, \dots, \lambda_d)$ are $d \times d$ diagonal matrices, $\mu_1, \dots, \mu_\ell > 0$ and $\ell < d$. (We may consider ρ, σ in a matrix algebra of bigger size if ρ is invertible.) If $\text{supp } \sigma \leq \text{supp } \rho$, then $\lambda_{\ell+1} = \dots = \lambda_d = 0$; this will be called the regular case. When $\text{supp } \sigma \leq \text{supp } \rho$ is not true, we may assume that $\lambda_d > 0$ and we refer to the singular case.

The eigenvalues of R_n correspond to elements (i_1, \dots, i_n) of $\{1, \dots, d\}^n$:

$$\frac{1}{n} (\lambda_{i_1} \mu_{i_2} \dots \mu_{i_n} + \mu_{i_1} \lambda_{i_2} \mu_{i_3} \dots \mu_{i_n} + \dots + \mu_{i_1} \dots \mu_{i_{n-1}} \lambda_{i_n}). \quad (5)$$

We divide the eigenvalues in three different groups as follows:

- (a) A corresponds to $(i_1, \dots, i_n) \in \{1, \dots, d\}^n$ with $1 \leq i_1, \dots, i_n \leq \ell$,
- (b) B corresponds to $(i_1, \dots, i_n) \in \{1, \dots, d\}^n$ which contains exactly one d ,
- (c) C is the rest of the eigenvalues.

If the eigenvalue (5) is in group A , then it is

$$\frac{(\lambda_{i_1}/\mu_{i_1}) + \dots + (\lambda_{i_n}/\mu_{i_n})}{n} \mu_{i_1} \mu_{i_2} \dots \mu_{i_n}.$$

First we compute

$$\sum_{\kappa \in A} \eta(\kappa) = \sum_{i_1, \dots, i_n} \eta \left(\frac{(\lambda_{i_1}/\mu_{i_1}) + \dots + (\lambda_{i_n}/\mu_{i_n})}{n} \mu_{i_1} \dots \mu_{i_n} \right).$$

Below the summations are over $1 \leq i_1, \dots, i_n \leq \ell$:

$$\begin{aligned}
& \sum_{i_1, \dots, i_n} \eta \left(\frac{(\lambda_{i_1}/\mu_{i_1}) + \dots + (\lambda_{i_n}/\mu_{i_n})}{n} \mu_{i_1} \dots \mu_{i_n} \right) \\
&= - \sum_{i_1, \dots, i_n} \left(\frac{(\lambda_{i_1}/\mu_{i_1}) + \dots + (\lambda_{i_n}/\mu_{i_n})}{n} \mu_{i_1} \dots \mu_{i_n} \right) \log(\mu_{i_1} \dots \mu_{i_n}) + Q_n \\
&= -\frac{1}{n} \sum_{k=1}^n \left(\sum_{i_1, \dots, i_n} \lambda_{i_1} \mu_{i_2} \dots \mu_{i_n} \log \mu_{i_k} + \sum_{i_1, \dots, i_n} \lambda_{i_1} \mu_{i_2} \dots \mu_{i_n} \log \mu_{i_k} \right. \\
&\quad \left. + \dots + \sum_{i_1, \dots, i_n} \lambda_{i_1} \mu_{i_2} \dots \mu_{i_n} \log \mu_{i_k} \right) + Q_n \\
&= -\frac{1}{n} \sum_{k=1}^n \left((n-1) \sum_{i_k} \mu_{i_k} \log \mu_{i_k} + \sum_{i_k} \lambda_{i_k} \log \mu_{i_k} \right) + Q_n \\
&= (n-1)S(\rho) - \sum_{i=1}^{\ell} \lambda_i \log \mu_i + Q_n,
\end{aligned}$$

where

$$Q_n := \sum_{i_1, \dots, i_n} (\mu_{i_1} \dots \mu_{i_n}) \eta \left(\frac{(\lambda_{i_1}/\mu_{i_1}) + \dots + (\lambda_{i_n}/\mu_{i_n})}{n} \right).$$

Consider a probability space

$$(\Omega, \mathbb{P}) := (\{1, \dots, \ell\}^{\mathbb{N}}, (\mu_1, \dots, \mu_{\ell})^{\mathbb{N}}),$$

where $(\mu_1, \dots, \mu_{\ell})^{\mathbb{N}}$ is the product of the measure on $\{1, \dots, \ell\}$ with the distribution $(\mu_1, \dots, \mu_{\ell})$. For each $n \in \mathbb{N}$ let X_n be a random variable on Ω depending on the n th $\{1, \dots, \ell\}$ so that the value of X_n at $i \in \{1, \dots, \ell\}$ is λ_i/μ_i . Then X_1, X_2, \dots are identically distributed independent random variables and Q_n is the expectation value of

$$\eta \left(\frac{X_1 + \dots + X_n}{n} \right).$$

The strong law of large numbers says that

$$\frac{X_1 + \dots + X_n}{n} \rightarrow \mathbb{E}(X_1) = \sum_{i=1}^{\ell} \left(\frac{\lambda_i}{\mu_i} \right) \mu_i = \sum_{i=1}^{\ell} \lambda_i \text{ almost surely.}$$

Since $\eta((X_1 + \dots + X_n)/n)$ is uniformly bounded, the Lebesgue bounded convergence theorem implies that

$$Q_n \rightarrow \eta \left(\sum_{i=1}^{\ell} \lambda_i \right)$$

as $n \rightarrow \infty$.

In the regular case $\sum_{i=1}^{\ell} \lambda_i = 1$, $Q_n \rightarrow 0$ and all non-zero eigenvalues are in group A . Hence we have

$$S(R_n) - (n-1)S(\rho) - S(\sigma) = -\sum_{i=1}^{\ell} \lambda_i \log \mu_i + \sum_{i=1}^{\ell} \lambda_i \log \lambda_i + Q_n = S(\sigma \| \rho) + Q_n$$

and the statement is clear.

Next we consider the singular case, when we have

$$\sum_{\kappa \in A} \eta(\kappa) = (n-1)S(\rho) + O(1),$$

and we turn to eigenvalues in B . If the eigenvalue corresponding to $(i_1, \dots, i_n) \in \{1, \dots, d\}^n$ is in group B and $i_1 = d$, then the eigenvalue is

$$\frac{1}{n} \lambda_d \mu_{i_2} \cdots \mu_{i_n}.$$

It follows that

$$\begin{aligned} & - \sum_{i_2, \dots, i_n} \left(\frac{\lambda_d \mu_{i_2} \cdots \mu_{i_n}}{n} \right) \log \left(\frac{\lambda_d \mu_{i_2} \cdots \mu_{i_n}}{n} \right) \\ &= -\frac{\lambda_d}{n} \sum_{i_2, \dots, i_n} (\mu_{i_2} \cdots \mu_{i_n}) \log(\mu_{i_2} \cdots \mu_{i_n}) - \frac{\lambda_d}{n} \log \frac{\lambda_d}{n} \\ &= \frac{\lambda_d}{n} (n-1)S(\rho) - \frac{\lambda_d}{n} \log \frac{\lambda_d}{n}. \end{aligned}$$

When $i_2 = d, \dots, i_n = d$, we get the same quantity, so this should be multiplied with n :

$$\sum_{\kappa \in B} \eta(\kappa) = \lambda_d (n-1)S(\rho) - \lambda_d \log \frac{\lambda_d}{n}.$$

We make a lower estimate to the entropy of R_n in such a way that we compute $\sum_{\kappa} \eta(\kappa)$ when κ runs over A and B . It is clear now that

$$\begin{aligned} S(R_n) - (n-1)S(\rho) - S(\sigma) &\geq \sum_{\kappa \in A} \eta(\kappa) + \sum_{\kappa \in B} \eta(\kappa) - (n-1)S(\rho) - S(\sigma) \\ &\geq \lambda_d (n-1)S(\rho) + \lambda_d \log n + O(1) \rightarrow +\infty \end{aligned}$$

as $n \rightarrow \infty$. □

3 Interpretation as capacity

A classical-quantum channel with classical input alphabet \mathcal{X} transfers the input $x \in \mathcal{X}$ into the output $W(x) \equiv \rho_x$ which is a density matrix acting on a Hilbert space \mathcal{K} . We restrict ourselves to the case when \mathcal{X} is finite and \mathcal{K} is finite dimensional.

If a classical random variable X is chosen to be the input, with probability distribution $P = \{p(x) : x \in \mathcal{X}\}$, then the corresponding output is the quantum state $\rho_X := \sum_{x \in \mathcal{X}} p(x) \rho_x$. When a measurement is performed on the output quantum system, it gives rise to an output random variable Y which is jointly distributed with the input X . If a partition of unity $\{F_y : y \in \mathcal{X}\}$ in $B(\mathcal{K})$ describes the measurement, then

$$\text{Prob}(Y = y | X = x) = \text{Tr } \rho_x F_y \quad (x, y \in \mathcal{X}). \quad (6)$$

According to the Holevo bound, we have

$$I(X \wedge Y) := H(Y) - H(Y|X) \leq I(X, W) := S(\rho_X) - \sum_{x \in \mathcal{X}} p(x) S(\rho_x), \quad (7)$$

which is actually a simple consequence of the monotonicity of the relative entropy under state transformation [7], see also [11]. $I(X, W)$ is the so-called Holevo quantity or classical-quantum mutual information, and it satisfies the identity

$$\sum_{x \in \mathcal{X}} p(x) S(\rho_x \| \rho) = I(X, W) + S(\rho_X \| \rho), \quad (8)$$

where ρ is an arbitrary density.

The channel is used to transfer sequences from the classical alphabet; $\mathbf{x} = (x_1, x_2, \dots, x_n) \in \mathcal{X}^n$ is transferred into the quantum state $W^{\otimes n}(\mathbf{x}) = \rho_{\mathbf{x}} := \rho_{x_1} \otimes \rho_{x_2} \otimes \dots \otimes \rho_{x_n}$. A code for the channel $W^{\otimes n}$ is defined by a subset $A_n \subset \mathcal{X}^n$, which is called a codeword set. The decoder is a measurement $\{F_{\mathbf{y}} : \mathbf{y} \in \mathcal{X}^n\}$. The probability of error is $\text{Prob}(X \neq Y)$, where X is the input random variable uniformly distributed on A_n and the output random variable is determined by (6), where x and y are replaced by \mathbf{x} and \mathbf{y} .

The essential observation is the fact that $S(R_n) - (n-1)S(\rho) - S(\sigma)$ in the conjecture is a Holevo quantity in case of a channel with input sequences $(x_1, x_2, \dots, x_n) \in \{0, 1\}^n$ and outputs $\rho_{x_1} \otimes \rho_{x_2} \otimes \dots \otimes \rho_{x_n}$, where $\rho_0 = \sigma$, $\rho_1 = \rho$ and the codewords are all sequences containing exactly one 0. More generally, we shall consider Holevo quantities

$$I(A, \rho_0, \rho_1) := S\left(\frac{1}{|A|} \sum_{\mathbf{x} \in A} \rho_{\mathbf{x}}\right) - \frac{1}{|A|} \sum_{\mathbf{x} \in A} S(\rho_{\mathbf{x}}).$$

defined for any set $A \subset \{0, 1\}^n$ of binary sequences of length n .

The concept related to the conjecture we study is the channel capacity per unit cost which is defined next for simplicity only in the case where $\mathcal{X} = \{0, 1\}$, the cost of a character $0 \in \mathcal{X}$ is 1, while the cost of $1 \in \mathcal{X}$ is 0.

For a memoryless channel with a binary input alphabet $\mathcal{X} = \{0, 1\}$ and an $\varepsilon > 0$, a number $R > 0$ is called an ε -achievable rate per unit cost if for every $\delta > 0$ and for any sufficiently large T , there exists a code of length $n > T$ with at least $e^{T(R-\delta)}$ codewords such that each of the codewords contains at most T 0's and the error probability is at most ε . The largest R which is an ε -achievable per unit cost for every $\varepsilon > 0$ is the channel capacity per unit cost.

Lemma 1. For an arbitrary $A \subset \{0, 1\}^n$,

$$I(A, \rho_0, \rho_1) \leq c(A)S(\rho_0\|\rho_1)$$

holds, where

$$c(A) := \frac{1}{|A|} \sum_{\mathbf{x} \in A} |\{i : x_i = 0\}|.$$

Proof: Let $c(\mathbf{x}) := |\{i : x_i = 0\}|$ for $\mathbf{x} \in A$. Since $I(A, \rho_0, \rho_1)$ is a particular Holevo quantity $I(X, W^{\otimes n})$, we can use the identity (8) to get an upper bound

$$\frac{1}{|A|} \sum_{\mathbf{x} \in A} S(\rho_{\mathbf{x}}\|\rho_1^{\otimes n}) = \frac{1}{|A|} \sum_{\mathbf{x} \in A} c(\mathbf{x})S(\rho_0\|\rho_1) = c(A)S(\rho_0\|\rho_1)$$

for $I(A, \rho_0, \rho_1)$. □

Lemma 2. If $A \subset \{0, 1\}^n$ is a code of the channel $W^{\otimes n}$, whose probability of error (for some decoding scheme) does not exceed a given $0 < \varepsilon < 1$, then

$$(1 - \varepsilon) \log |A| - \log 2 \leq I(A, \rho_0, \rho_1).$$

Proof: The right-hand side is a bound for the classical mutual information $I(X \wedge Y) = H(Y) - H(Y|X)$, where Y is the channel output, see (7). Since the error probability $\text{Prob}(X \neq Y)$ is smaller than ε , application of the Fano inequality (see [3]) gives

$$H(X|Y) \leq \varepsilon \log |A| + \log 2.$$

Therefore

$$I(X \wedge Y) = H(X) - H(X|Y) \geq (1 - \varepsilon) \log |A| - \log 2,$$

and the proof is complete. □

The above two lemmas shows that the relative entropy $S(\rho_0\|\rho_1)$ is an upper bound for the channel capacity per unit cost of the channel $W(0) = \rho_0$ and $W(1) = \rho_1$ with a binary input alphabet. In fact, assume that $R > 0$ is an ε -achievable rate. For every $\delta > 0$ and $T > 0$ there is a code $A \subset \{0, 1\}^n$ for which we get by Lemmas 1 and 2

$$\begin{aligned} TS(\rho_0\|\rho_1) &\geq c(A)S(\rho_0\|\rho_1) \geq I(A, \rho_0, \rho_1) \\ &\geq (1 - \varepsilon) \log |A| - \log 2 \\ &\geq (1 - \varepsilon)T(R - \delta) - \log 2. \end{aligned}$$

Since T is arbitrarily large and ε, δ are arbitrarily small, $R \leq S(\rho_0\|\rho_1)$ follows. That $S(\rho_0\|\rho_1)$ equals the channel capacity per unit cost will be verified below.

Theorem 3. Let the classical-quantum channel $W : \mathcal{X} = \{0, 1\} \rightarrow B(\mathcal{K})$ be defined as $W(0) = \rho_0 \equiv \sigma$ and $W(1) = \rho_1 \equiv \rho$. Assume that $A_n \subset \{0, 1\}^n$ is chosen such that

(a) each element $\mathbf{x} = (x_1, x_2, \dots, x_n) \in A_n$ contains at most ℓ copies of 0,

(b) $\log |A_n| / \log n \rightarrow c$ as $n \rightarrow \infty$,

(c)

$$c(A_n) := \frac{1}{|A_n|} \sum_{\mathbf{x} \in A_n} |\{i : x_i = 0\}| \rightarrow c \quad \text{as } n \rightarrow \infty$$

for some real number $c > 0$ and for some natural number ℓ . If the random variable X_n has a uniform distribution on A_n , then

$$\lim_{n \rightarrow \infty} \left(S(\rho_{X_n}) - \frac{1}{|A_n|} \sum_{\mathbf{x} \in A_n} S(\rho_{\mathbf{x}}) \right) = cS(\sigma \parallel \rho).$$

The proof of the theorem is divided into lemmas. We need the direct part of the so-called quantum Stein lemma obtained in [6], see also [2, 5, 9, 12].

Lemma 3. Let ρ_0 and ρ_1 be density matrices. For every $\eta > 0$ and $0 < R < S(\rho_0 \parallel \rho_1)$, if N is sufficiently large, then there is a projection $E \in B(\mathcal{K}^{\otimes N})$ such that

$$\alpha_N[E] := \text{Tr } \rho_0^{\otimes N} (I - E) < \eta$$

and for $\beta_N[E] := \text{Tr } \rho_1^{\otimes N} E$ the estimate

$$\frac{1}{N} \log \beta_N[E] < -R$$

holds.

Note that α_N is called the error of the first kind, while β_N is the error of the second kind.

Lemma 4. Assume that $\varepsilon > 0$, $0 < R < S(\rho_0 \parallel \rho_1)$, ℓ is a positive integer and the sequences \mathbf{x} in $A_n \subset \{0, 1\}^n$ contain at most ℓ copies of 0. Let the codewords be the N -fold repetitions $\mathbf{x}^N = (\mathbf{x}, \mathbf{x}, \dots, \mathbf{x})$ of the sequences $\mathbf{x} \in A_n$. If N is the integer part of

$$\frac{1}{R} \log \frac{2n}{\varepsilon}$$

and n is large enough, then there is a decoding scheme such that the error probability is smaller than ε .

Proof: We follow the probabilistic construction in [13]. Let the codewords be the N -fold repetitions $\mathbf{x}^N = (\mathbf{x}, \mathbf{x}, \dots, \mathbf{x})$ of the sequences $\mathbf{x} \in A_n$. The corresponding output density matrices act on the Hilbert space $\mathcal{K}^{\otimes Nn} \equiv (\mathcal{K}^{\otimes n})^{\otimes N}$. We decompose this Hilbert space into an N -fold product in a different way. For each $1 \leq i \leq n$, let \mathcal{K}_i be the

tensor product of the factors $i, i + n, i + 2n, \dots, i + (N - 1)n$. So \mathcal{K} is identified with $\mathcal{K}_1 \otimes \mathcal{K}_2 \otimes \dots \otimes \mathcal{K}_n$.

For each $1 \leq i \leq n$ we perform a hypothesis testing on the Hilbert space \mathcal{K}_i . The 0-hypothesis is that the i th component of the actually chosen $\mathbf{x} \in A_n$ is 0. Based on the channel outputs at time instances $i, i + n, \dots, i + (N - 1)n$, the 0-hypothesis is tested against the alternative hypothesis that the i th component of \mathbf{x} is 1. According to the quantum Stein lemma (Lemma 3), given any $\eta > 0$ and $0 < R < S(\sigma \parallel \rho)$, for N sufficiently large, there exists a test E_i such that the probability of error of the first kind is smaller than η , while the probability of error of the second kind is smaller than e^{-NR} . The projections E_i and $I - E_i$ form a partition of unity in the Hilbert space \mathcal{K}_i , and the n -fold tensor product of these commuting projection will give a partition of unity in $\mathcal{K}^{\otimes Nn}$. Let $\mathbf{y} \in \{0, 1\}^n$ and set $F_{\mathbf{y}} := \otimes_{i=1}^n F_{y_i}$, where $F_{y_i} = E_i$ if $y_i = 0$ and $F_{y_i} = I - E_i$ if $y_i = 1$. Therefore, the result of decoding can be an arbitrary 0-1 sequence in $\{0, 1\}^n$.

The decoding scheme gives $\mathbf{y} \in \{0, 1\}^n$ in such a way that $y_i = 0$ if the tests accepted the 0-hypothesis for i and $y_i = 1$ if the alternative was accepted. The error probability should be estimated:

$$\begin{aligned} \text{Prob}(Y \neq X | X = \mathbf{x}) &= \sum_{\mathbf{y}: \mathbf{y} \neq \mathbf{x}} \text{Tr} \rho_{\mathbf{x}}^{\otimes N} F_{\mathbf{y}} = \sum_{\mathbf{y}: \mathbf{y} \neq \mathbf{x}} \prod_{i=1}^n \text{Tr} \rho_{x_i}^{\otimes N} F_{y_i} \\ &\leq \sum_{i=1}^n \sum_{\mathbf{y}: y_i \neq x_i} \prod_{j=1}^n \text{Tr} \rho_{x_j}^{\otimes N} F_{y_j} \leq \sum_{i=1}^n \text{Tr} \rho_{x_i}^{\otimes N} (I - F_{x_i}). \end{aligned}$$

If $x_i = 0$, then

$$\text{Tr} \rho_{x_i}^{\otimes N} (I - F_{x_i}) = \text{Tr} \rho_0^{\otimes N} (I - E_i) \leq \eta,$$

because it is an error of the first kind. When $x_i = 1$,

$$\text{Tr} \rho_{x_i}^{\otimes N} (I - F_{x_i}) = \text{Tr} \rho_1^{\otimes N} E_i \leq e^{-RN}$$

from the error of the second kind. It follows that $\ell\eta + ne^{-NR}$ is a bound for the error probability. The first term will be small if η is small. The second term will be small if N is large enough. If both terms are majorized by $\varepsilon/2$, then the statement of the lemma holds. We can choose n so large that N defined by the statement should be large enough. \square

Proof of Theorem 3: Since Lemma 1 gives an upper bound, that is,

$$\limsup_{n \rightarrow \infty} \left(S(\rho_{X_n}) - \frac{1}{|A_n|} \sum_{\mathbf{x} \in A_n} S(\rho_{\mathbf{x}}) \right) \leq cS(\sigma \parallel \rho),$$

it remains to prove that

$$\liminf_{n \rightarrow \infty} \left(S(\rho_{X_n}) - \frac{1}{|A_n|} \sum_{\mathbf{x} \in A_n} S(\rho_{\mathbf{x}}) \right) \geq cS(\sigma \parallel \rho).$$

Lemma 4 is about the N -times repeated input X^N and describes a decoding scheme with error probability at most ε . According to Lemma 2 we have

$$(1 - \varepsilon) \log |A_n| - 1 \leq S(\rho_{X^N}) - \frac{1}{|A|} \sum_{\mathbf{x} \in A_n} S(\rho_{\mathbf{x}^N}).$$

From the subadditivity of the entropy we have

$$S(\rho_{X^N}) \leq NS(\rho_X)$$

and

$$S(\rho_{\mathbf{x}^N}) = NS(\rho_{\mathbf{x}})$$

holds due to the additivity for product. It follows that

$$(1 - \varepsilon) \frac{\log |A_n|}{N} - \frac{1}{N} \leq S(\rho_X) - \frac{1}{|A_n|} \sum_{\mathbf{x} \in A_n} S(\rho_{\mathbf{x}}).$$

From the choice of N in Lemma 4 we have

$$R \frac{\log |A_n|}{\log n} \frac{\log n}{\log n + \log 2 - \log \varepsilon} \leq \frac{\log |A_n|}{N}$$

and the lower bound is arbitrarily close to cR . Since $R < S(\rho_0 \| \rho_1)$ was arbitrary, the proof is complete. \square

References

- [1] V.P. Belavkin and P. Staszewski, C*-algebraic generalization of relative entropy and entropy, Ann. Inst. Henri Poincaré, Sec. A **37**(1982), 51–58.
- [2] I. Bjelaković, J. Deuschel, T. Krüger, R. Seiler, R. Siegmund-Schultze and A. Szkoła, A quantum version of Sanov’s theorem, Comm. Math. Phys. **260**(2005), 659–671.
- [3] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Second edition, Wiley-Interscience, Hoboken, NJ, 2006.
- [4] L. Diósi, T. Feldmann and R. Kosloff, On the exact identity between thermodynamic and informatic entropies in a unitary model of friction, Int. J. Quantum Information, **4**(2006), 99–104.
- [5] M. Hayashi, *Quantum information. An introduction*, Springer, 2006.
- [6] F. Hiai and D. Petz, The proper formula for relative entropy and its asymptotics in quantum probability, Comm. Math. Phys. **143**(1991), 99–114.

- [7] A.S. Holevo, Some estimates for the amount of information transmittable by a quantum communication channel (in Russian), *Problemy Peredachi Informacii*, **9**(1973), 3–11.
- [8] M.A. Nielsen and I.L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000.
- [9] T. Ogawa and H. Nagaoka, Strong converse and Stein’s lemma in quantum hypothesis testing, *IEEE Tans. Inf. Theory* **46**(2000), 2428–2433.
- [10] M. Ohya and D. Petz, *Quantum Entropy and its Use*, Springer, 1993.
- [11] M. Ohya, D. Petz and N. Watanabe, On capacities of quantum channels, *Prob. Math. Stat.* **17**(1997), 179–196.
- [12] D. Petz, *Lectures on quantum information theory and quantum statistics*, book manuscript in preparation.
- [13] S. Verdu, On channel capacity per unit cost, *IEEE Trans. Inform. Theory* **36**(1990), 1019–1030.