Additive invariants on quantum channels and regularized minimum entropy*

Shmuel Friedland
Department of Mathematics, Statistics, and Computer Science
University of Illinois at Chicago
Chicago, Illinois 60607-7045, USA
E-mail: friedlan@uic.edu

May 3, 2009

Abstract

We introduce two additive invariants of output quantum channels. If the value of one these invariants is less than 1 then the logarithm of the inverse of its value is a positive lower bound for the regularized minimum entropy of an output quantum channel. We give a few examples in which one of these invariants is less than 1. We also study the special cases where the above both invariants are equal to 1.

2000 Mathematics Subject Classification. 81P68, 94A17, 94A40, 15A42,
Key words. Quantum information theory, quantum channel, minimum entropy output, regularized minimum entropy output, additivity conjecture, additive invariants.

1 Introduction

Denote by $\mathcal{S}_n(\mathbb{C})$ the Hilbert space of $n \times n$ hermitian matrices, where $\langle X, Y\rangle = \operatorname{tr} XY$. Denote by $\mathcal{S}_{n,+,1}(\mathbb{C}) \subset \mathcal{S}_{n,+}(\mathbb{C}) \subset \mathcal{S}_n(\mathbb{C})$ the convex set of positive hermitian matrices of trace one, and the cone of positive hermitian matrices respectively. A quantum channel is a completely positive linear transformation $\tau : \mathcal{S}_n(\mathbb{C}) \to \mathcal{S}_m(\mathbb{C})$:

$$\tau(X) = \sum_{i=1}^{l} A_i X A_i^*, \quad A_1, \ldots, A_l \in \mathbb{C}^{m\times n},\ X \in \mathcal{S}_n(\mathbb{C}), \tag{1.1}$$

which is trace preserving:

$$\sum_{i=1}^{l} A_i^* A_i = I_n, \tag{1.2}$$

Denote by $\tau^* : \mathcal{S}_m(\mathbb{C}) \to \mathcal{S}_n(\mathbb{C})$ the adjoint linear transformation. The *minimum* entropy output of a quantum channel τ is defined

$$\mathrm{H}(\tau) = \min_{X\in\mathcal{S}_{n,+,1}(\mathbb{C})} -\operatorname{tr}\tau(X)\log\tau(X). \tag{1.3}$$

If $\eta : \mathcal{S}_{n'}(\mathbb{C}) \to \mathcal{S}_{m'}(\mathbb{C})$ is another quantum channel, then it is well known $\tau\otimes\eta$ is a quantum channel, and

$$\mathrm{H}(\tau\otimes\eta) \le \mathrm{H}(\tau) + \mathrm{H}(\eta). \tag{1.4}$$

*This research started during author's participation in AIM workshop "Geometry and representation theory of tensors for computer science, statistics and other areas", July 21-25, 2008.

Hence the sequence $\mathrm{H}(\otimes^p\tau), p = 1, \ldots,$ is subadditive. Thus the following limit exists:

$$\mathrm{H}_r(\tau) = \lim_{p\to\infty} \frac{\mathrm{H}(\otimes^p\tau)}{p}, \tag{1.5}$$

and is called the *regularized* minimum entropy of quantum channel. Clearly, $\mathrm{H}_r(\tau) \le \mathrm{H}(\tau)$.

One of the major open problem of quantum information theory is the additivity conjecture, which claims that equality holds in (1.4). This additivity conjecture has several equivalent forms [8]. If the additivity conjecture holds then $\mathrm{H}_r(\tau) = \mathrm{H}(\tau)$, and the computation of $\mathrm{H}_r(\tau)$ is relatively simple. There are known cases where the additivity conjecture is known, see references in [7]. It is also known that the p analog of the additivity conjecture is wrong [7]. It was shown in [2] that the additivity of the entanglement of subspaces fails over the real numbers. It was recently shown by Hastings [6] that the additivity conjecture is false. Hence the computation of $\mathrm{H}_r(\tau)$ is hard. This is the standard situation in computing the entropy of Potts models in statistical physics, e.g. [5].

Let

$$\mathbf{A}(\tau) := \sum_{i=1}^{l} A_i A_i^* \in \mathcal{S}_{m,+}(\mathbb{C}). \tag{1.6}$$

Then $\log \lambda_1(\mathbf{A}(\tau)) = \log \|\mathbf{A}(\tau)\|$, where $\lambda_1(\mathbf{A})$ is the maximal eigenvalue of $\mathbf{A}(\tau)$, is the first additive invariant of quantum channels, with respect to tensor products. Let $\sigma_1(\tau) = \|\tau\| \ge \sigma_2(\tau) \ge \ldots \ge 0$ be the first and the second singular value of the linear transformation given by τ. Then $\log \sigma_1(\tau)$ is the second additive invariant. (These two invariants are incomparable in general, see §3.) The first result of this paper is

Theorem 1.1 *Let $\tau : \mathcal{S}_n(\mathbb{C}) \to \mathcal{S}_m(\mathbb{C})$ be a quantum channel. Assume that $\min(\lambda_1(\mathbf{A}(\tau)), \|\tau\|) < 1$. Then*

$$\mathrm{H}_r(\tau) \ge \max(-\log \lambda_1(\mathbf{A}(\tau)), -\log \|\tau\|). \tag{1.7}$$

In §3 section we give examples where $\min(\lambda_1(\mathbf{A}(\tau)), \sigma_1(\tau)) < 1$. τ is called a *unitary* quantum channel if in (1.1) we assume

$$A_i = t_i Q_i,\ Q_i Q_i^* = Q_i^* Q_i = I_n,\ i = 1, \ldots, l,\ \mathbf{t} = (t_1, \ldots, t_l)^\top \in \mathbb{R}^l, \mathbf{t}^\top \mathbf{t} = 1. \tag{1.8}$$

In that case $\lambda_1(\mathbf{A}(\tau)) = \sigma_1(\tau) = 1$. Note the counter example to the additivity conjecture in [6] is of this form. A quantum channel $\tau : \mathcal{S}_n(\mathbb{C}) \to \mathcal{S}_m(\mathbb{C})$ is called a *bi*-quantum channel if $m = n$ and $\tau^* : \mathcal{S}_n(\mathbb{C}) \to \mathcal{S}_n(\mathbb{C})$ is also a quantum channel. That is $\mathbf{A}(\tau) = I_n$ and it follows that $\sigma_1(\tau) = 1$. Note that a unitary quantum channel is a bi-quantum channel. The second major result of this paper is

Theorem 1.2 *Let $\tau : \mathcal{S}_n(\mathbb{C}) \to \mathcal{S}_n(\mathbb{C})$ be a bi-quantum channel. Then $\sigma_1(\tau) = 1$. Assume that $n \ge 2$ and $\sigma_2(\tau) < 1$. Then*

$$\mathrm{H}(\tau) \ge -\frac{1}{2}\log(\sigma_2(\tau)^2 + \frac{1 - \sigma_2(\tau)^2}{n}). \tag{1.9}$$

Note that (1.9) is nontrivial if $\sigma_2(\tau) < 1$. We show that the condition $\sigma_2(\tau) < 1$ holds for a generic unitary channel with $l \ge 3$.

2 Proof Theorem 1.1

Denote by $\Pi_n \subset \mathbb{R}_+^n$ the convex set of probability vectors. For $\mathbf{p} = (p_1, \ldots, p_n) \in \Pi_n$ we have

$$\mathrm{H}(\mathbf{p}) = -\sum_{i=1}^n p_i \log p_i = \sum_{i=1}^n p_i \log \frac{1}{p_i} \ge (\sum_{i=1}^n p_i) \min_{j=1,\ldots,n} \log \frac{1}{p_j} = -\log \max_{j=1,\ldots,n} p_j. \tag{2.1}$$

For $X \in \mathcal{S}_n(\mathbb{C})$ denote by $\boldsymbol{\lambda}(A) = (\lambda_1(X), \ldots, \lambda_n(X))$ the eigenvalue set of X, where $\lambda_1(A) \geq \ldots \geq \lambda_n(X)$. Then $\mathbf{u}_1, \ldots, \mathbf{u}_n$ is the corresponding orthonormal basis of $\mathbb{C}^n$ consisting of eigenvectors of X $X\mathbf{u}_i = \lambda_i(X)\mathbf{u}_i$ where $\mathbf{u}_i^*\mathbf{u}_j = \delta_{ij}$ for $i, j = 1, \ldots, n$. Ky-Fan maximal characterization is, e.g. [3],

$$\sum_{j=1}^{k} \lambda_j(X) = \max_{\mathbf{x}_1,\ldots,\mathbf{x}_k \in \mathbb{C}^n, \mathbf{x}_p^*\mathbf{x}_q = \delta_{pq}} \sum_{j=1}^{k} \mathbf{x}_j^* X \mathbf{x}_j = \sum_{j=1}^{k} \operatorname{tr}(X(\mathbf{x}_j\mathbf{x}_j^*)). \tag{2.2}$$

Hence for $\mathbf{x} \in \mathbb{C}^n, \mathbf{x}^*\mathbf{x} = 1$ we have

$$\sum_{j=1}^{k} \lambda_j(\tau(\mathbf{x}\mathbf{x}^*)) = \max_{\mathbf{y}_1,\ldots,\mathbf{y}_k \in \mathbb{C}^m, \mathbf{y}_p^*\mathbf{y}_q = \delta_{pq}} \sum_{j=1}^{k} \operatorname{tr}(\tau(\mathbf{x}\mathbf{x}^*)(\mathbf{y}_j\mathbf{y}_j^*)) = \tag{2.3}$$

$$\max_{\mathbf{y}_1,\ldots,\mathbf{y}_k \in \mathbb{C}^m, \mathbf{y}_p^*\mathbf{y}_q = \delta_{pq}} \sum_{i,j=1}^{l,k} |\mathbf{y}_j^* A_i \mathbf{x}|^2 \leq \max_{\mathbf{y}_1,\ldots,\mathbf{y}_k \in \mathbb{C}^m, \mathbf{y}_p^*\mathbf{y}_q = \delta_{pq}} \sum_{i,j=1}^{l,k} \mathbf{y}_j^* A_i A_i^* \mathbf{y}_j =$$

$$\max_{\mathbf{y}_1,\ldots,\mathbf{y}_k \in \mathbb{C}^m, \mathbf{y}_p^*\mathbf{y}_q = \delta_{pq}} \sum_{j=1}^{k} \mathbf{y}_j^* \mathbf{A}(\tau) \mathbf{y}_j = \sum_{j=1}^{k} \lambda_j(\mathbf{A}(\tau)). \tag{2.4}$$

Recall that $\sum_{j=1}^{k} \lambda_j(X)$ is a convex function on $\mathcal{S}_n(\mathbb{C})$. As the extreme points of $\mathcal{S}_{n,+,1}$ are $\mathbf{x}\mathbf{x}^*, \mathbf{x} \in \mathbb{C}^n, \mathbf{x}^*\mathbf{x} = 1$ we obtain

$$\max_{X \in \mathcal{S}_{n,+,1}} \sum_{j=1}^{k} \lambda_j(\tau(X)) \leq \sum_{j=1}^{k} \lambda_j(\mathbf{A}(\tau)), \quad k = 1, \ldots, m. \tag{2.5}$$

$X \in \mathcal{S}_{n,+,1}(\mathbb{C})$ iff $\boldsymbol{\lambda}(X) \in \Pi_n$. Hence $\mathrm{H}(X) := \mathrm{H}(\boldsymbol{\lambda}(X)) \geq -\log \lambda_1(X)$ for $X \in \mathcal{S}_{n,+,1}(\mathbb{C})$. (2.5) for $k = 1$ yields that $\mathrm{H}(\tau) \geq -\log \lambda_1(\mathbf{A}(\tau))$.

For $C \in \mathbb{R}^{m\times n}$ let $C = V\Sigma U^\top$ be the *singular value decomposition*, (SVD), of C. So $U = [\mathbf{u}_1 \ \ldots \ \mathbf{u}_n] \in \mathbb{R}^{n\times n}, V = [\mathbf{v}_1 \ \ldots \ \mathbf{v}_m] \in \mathbb{R}^{m\times m}$ be orthogonal, and $\Sigma = \operatorname{diag}(\sigma_1(A), \ldots,) \in \mathbb{R}_+^{m\times n}$, be a diagonal matrix with nonnegative diagonal entries which form a nonincreasing sequence. The positive singular values of C are the positive eigenvalues of $\sqrt{CC^\top}$ or $\sqrt{C^\top C}$. Let $\boldsymbol{\sigma}(C) = (\sigma_1(C), \sigma_2(C), \ldots, \sigma_l(C))^\top$ where $\sigma_i(C) = 0$ if $i > r = \operatorname{rank} C$. Recall that $\|C\|_F := \sqrt{\langle C, C\rangle} = \sqrt{\operatorname{tr}(CC^\top)} = \sqrt{\sum_{i=1}^{\operatorname{rank} C} \sigma_i(C)^2}$. and $\sigma_1(C) = \|C\| = \max_{\|\mathbf{u}\|=\|\mathbf{v}\|=1} |\mathbf{v}^\top(C\mathbf{u})|$. Thus, for $\mathbf{x} \in \mathbb{C}^n, \mathbf{x}^*\mathbf{x} = 1$, we have the inequality

$$\lambda_1(\tau(\mathbf{x}\mathbf{x}^*)) = \max_{\|\mathbf{y}\|=1} \operatorname{tr}((\mathbf{y}\mathbf{y}^*)\tau(\mathbf{x}\mathbf{x}^*)) = \max_{\langle \mathbf{y}\mathbf{y}^*, \mathbf{y}\mathbf{y}^*\rangle = 1} \langle \tau(\mathbf{x}\mathbf{x}^*), \mathbf{y}\mathbf{y}*\rangle \leq \sigma_1(\tau).$$

Hence

$$\max_{X \in \mathcal{S}_{n,+,1}} \lambda_1(\tau(X)) \leq \sigma_1(\tau). \tag{2.6}$$

Combine the above inequalities to deduce $\mathrm{H}(\tau) \geq \max(-\log \lambda_1(\mathbf{A}(\tau)), -\log \sigma_1(\tau))$. The properties of tensor products imply

$$\mathrm{H}(\otimes^p \tau) \geq -\log \lambda_1(\mathbf{A}(\otimes^p \tau)) = -\log \lambda_1(\otimes^p \mathbf{A}(\tau)) = -p \log \lambda_1(\mathbf{A}(\tau)),$$
$$\mathrm{H}(\otimes^p \tau) \geq -\log \sigma_1(\otimes^p \tau) = -p \log \sigma_1(\tau) = -p \log \|\tau\|$$

Hence (1.7) holds.

If $\lambda_1(\mathbf{A}(\tau)) < 1$ then the inequality $\mathrm{H}_r(\tau) \geq -\log \lambda_1(\mathbf{A}(\tau))$ can be improved [4, §4].

3 Examples

Proposition 3.1 *Let τ be a quantum channel given by (1.1). Then*

$$\lambda_1(\mathbf{A}(\tau)) \geq \frac{n}{m}, \quad \sigma_1(\tau) \geq \frac{\sqrt{n}}{\sqrt{m}}. \tag{3.1}$$

Hence, $\lambda_1(\mathbf{A}(\tau)), \sigma_1(\tau) \ge 1$ for $m \le n$. In particular, if $m \le n$ then the condition either $\lambda_1(\mathbf{A}(\tau)) = 1$ or $\sigma_1(\tau) = 1$ holds if and only if $m = n$ and τ^* is a quantum channel.

Proof. Clearly,

$$m\lambda_1(\mathbf{A}(\tau)) \ge \sum_{j=1}^{m} \lambda_j(\mathbf{A}(\tau)) = \operatorname{tr} \mathbf{A}(\tau) = \sum_{i=1}^{l} \operatorname{tr} A_i A_i^* = \sum_{i=1}^{l} \operatorname{tr} A_i^* A_i = \operatorname{tr} I_n = n.$$

Hence $\lambda_1(\mathbf{A}(\tau)) \ge \frac{n}{m}$. Clearly, if $m = n$ and $\mathbf{A}(\tau) = I_n$ then $\lambda_1(\mathbf{A}(\tau)) = 1$ and τ^* is a quantum channel. Vice versa if $m \le n$ and $\lambda_1(\mathbf{A}(\tau)) = 1$ then $m = n$. Furthermore, all eigenvalues of $\mathbf{A}(\tau)$ have to be equal to 1, i.e. $\mathbf{A}(\tau) = I_n$.

Observe that the condition that τ of the form (1.1) is a quantum channel is equivalent to the condition $\tau^*(I_m) = I_n$. As

$$\sigma_1(\tau) = \sigma_1(\tau^*) \ge \|\tau^*(\frac{1}{\sqrt{m}} I_m)\| = \frac{\sqrt{n}}{\sqrt{m}}$$

we deduce that second inequality in (3.1). Suppose that $m \le n$ and $\sigma_1(\tau) = 1$. Hence $m = n$ and $\sigma_1(\tau^*) = \|\tau^*(\frac{1}{\sqrt{n}} I_n)\| = 1$. So $\frac{1}{\sqrt{n}} I_n$ must be the left and the right singular vector of τ corresponding to the $\|\tau\|$. I.e. $\tau(I_n) = I_n$, which is equivalent to the condition that τ^* is a quantum channel. □

Example 1. A quantum channel $\tau : \mathcal{S}_1(\mathbb{C}) \to \mathcal{S}_m(\mathbb{C})$ is of the form

$$\tau(x) = \sum_{i=1}^{l} \mathbf{a}_i x \mathbf{a}_i^*, \quad \mathbf{a}_i \in \mathbb{C}^m, i = 1, \ldots, l, \ \sum_{i=1}^{l} \mathbf{a}_i^* \mathbf{a}_i = 1, \quad \mathbf{A}(\tau) = \sum_{i=1}^{l} \mathbf{a}_i \mathbf{a}_i^*. \tag{3.2}$$

Note that $\operatorname{tr} \mathbf{A}(\tau) = 1$. Hence $\lambda_1(\mathbf{A}(\tau)) < 1$, unless $\mathbf{a}_1, \ldots, \mathbf{a}_l$ are colinear. (This happens always if $m = 1$.) We claim that

$$\sigma_1(\tau) = \sqrt{\operatorname{tr} \mathbf{A}(\tau)^2}. \tag{3.3}$$

Indeed

$$\max_{|x|=1, Y \in \mathcal{S}_m(\mathbb{C}), \operatorname{tr}(Y^2)=1} |\operatorname{tr} \tau(x) Y| = \max_{Y \in \mathcal{S}_m(\mathbb{C}), \operatorname{tr}(Y^2)=1} |\operatorname{tr} \mathbf{A}(\tau) Y| = \sqrt{\operatorname{tr} \mathbf{A}(\tau)^2}.$$

Hence

$$\lambda_1(\mathbf{A}(\tau)) < \sigma_1(\tau) < 1 \text{ iff } \mathbf{a}_1, \ldots, \mathbf{a}_l \text{ are not colinear.} \tag{3.4}$$

If $\mathbf{a}_1, \ldots, \mathbf{a}_l$ are co-linear then $\lambda_1(\mathbf{A}) = \sigma_1(\mathbf{A}) = 1$. Note that in this example $\mathrm{H}(\tau) = \mathrm{H}(\mathbf{A}(\tau))$.

Example 2. A quantum channel $\tau : \mathcal{S}_n(\mathbb{C}) \to \mathcal{S}_1(\mathbb{C})$ is of the form

$$\tau(X) = \sum_{i=1}^{l} \mathbf{a}_i^* X \mathbf{a}_i, \quad \mathbf{a}_i \in \mathbb{C}^n, i = 1, \ldots, l, \ \sum_{i=1}^{l} \mathbf{a}_i \mathbf{a}_i^* = I_n, \quad \mathbf{A}(\tau) = \sum_{i=1}^{l} \mathbf{a}_i^* \mathbf{a}_i = n. \tag{3.5}$$

So $\lambda_1(\mathbf{A}(\tau)) = n \ge 1$. On the other hand

$$\sigma_1(\tau) = \max_{X \in \mathcal{S}_n(\mathbb{C}), \operatorname{tr} X^2=1, |y|=1} |\operatorname{tr}(\tau(X) y)| = \max_{X \in \mathcal{S}_n(\mathbb{C}), \operatorname{tr} X^2=1} |\operatorname{tr} X| = \sqrt{n}. \tag{3.6}$$

So for $n > 1$ $\lambda_1(\mathbf{A}(\tau)) > \sigma_1(\tau)$.

Example 3. A quantum channel of the form (1.1), where $m = n$ and (1.2) holds, is called a strongly self-adjoint if there exists a permutation π on $\{1, \ldots, l\}$ such that $A_i^* = A_{\pi(i)}$ for

$i = 1, \ldots, l$. So $\mathbf{A}(\tau) = I_n$ and $\lambda_1(\mathbf{A}(\tau)) = 1$. Note that τ is self-adjoint and $\tau(I_n) = I_n$. Since I_n is an interior point of $\mathcal{S}_{n,+}$ it follows that $\sigma_1(\tau) = 1$.

Example 4. Assume $\tau_j : \mathcal{S}_{n_j}(\mathbb{C}) \to \mathcal{S}_{m_j}(\mathbb{C}), j = 1, 2$ are two quantum channels. Consider the quantum channel $\tau = \tau_1 \otimes \tau_2$. Then

$$\log \lambda_1(\mathbf{A}(\tau)) = \log \lambda_1(\mathbf{A}(\tau_1)) + \log \lambda_1(\mathbf{A}(\tau_2)),\ \log \sigma_1(\tau) = \log \sigma_1(\tau_1) + \log \sigma_1(\tau_2).$$

Thus, it is possible to have $\lambda_1(\mathbf{A}(\tau)) < 1$ without the assumption that both τ_1 and τ_2 satisfy the same condition. Combine Example 1 and Example 3 to obtain examples of quantum channels $\tau : \mathcal{S}_n(\mathbb{C}) \to \mathcal{S}_{mn}(\mathbb{C})$, where $n, m > 1$ where $\lambda_1(\mathbf{A}(\tau)) < 1$. Similar arguments apply for $\sigma_1(\tau)$.

Example 5. Recall that if $B \in \mathbb{C}^{m\times n}$ and $C \in \mathbb{C}^{p\times q}$ then

$$B \oplus C = \left[\begin{array}{cc} B & 0_{m\times q} \\ 0_{p\times n} & C \end{array}\right] \in \mathbb{C}^{(m+p)\times(n+q)}.$$

Assume $\tau_j : \mathcal{S}_{n_j}(\mathbb{C}) \to \mathcal{S}_{m_j}(\mathbb{C}), j = 1, 2$ are two quantum channels given by $\tau_j(X_j) = \sum_{i=1}^{l_j} A_{i,j} X_j A_{i,j}^*$, where $A_{i,j} \in \mathbb{C}^{m_j\times n_j},\ i = 1, \ldots, l_j,\ j = 1, 2$. Then $\tau_1 \oplus \tau_2 : \mathcal{S}_{n_1+n_2}(\mathbb{C}) :\to \mathcal{S}_{m_1+m_2}(\mathbb{C})$ is defined as follows.

$$(\tau_1 \oplus \tau_2)(X) = \sum_{i_1=i_2=1}^{l_1,l_2} (A_{i_1,1} \oplus A_{i_2,2}) X (A_{i_1}^* \oplus A_{i_2,2}^*).$$

Clearly, $\tau_1 \oplus \tau_2$ is a quantum channel. Furthermore,

$$\mathbf{A}(\tau_1 \oplus \tau_2) = \mathbf{A}(\tau_1) \oplus \mathbf{A}(\tau_2).$$

Hence

$$\lambda_1(\mathbf{A}(\tau_1 \oplus \tau_2)) = \max(\lambda_1(\mathbf{A}(\tau_1)), \lambda_1(\mathbf{A}(\tau_2))). \tag{3.7}$$

This if $\lambda_1(\mathbf{A}(\tau_i)) < 1$ we get that $\lambda_1(\mathbf{A}(\tau_1 \oplus \tau_2) < 1$.

The formula for $\sigma_1(\tau_1 \oplus \tau_2)$ does not seems to be as simple as (3.7). By viewing $\mathcal{S}_{n_1}(\mathbb{C}) \oplus \mathcal{S}_{n_2}(\mathbb{C})$ as a subspace of $\mathcal{S}_{n_1+n_2}(\mathbb{C})$ we deduce the inequality

$$\sigma_1(\tau_1 \oplus \tau_2) \geq \max(\sigma_1(\tau_1), \sigma_1(\tau_2)).$$

Example 6. We first show how to take a neighborhood of a given quantum channel given by (1.1). View $\mathcal{A} := (A_1, \ldots, A_l)$ as a point in $(\mathbb{C}^{m\times n})^l$. Let $\mathrm{O}(\mathcal{A}) \subset (\mathbb{C}^{m\times n})^l$ be an open neighborhood of $\mathcal{A}$ such that for any $\mathcal{B} := (B_1, \ldots, B_l) \in (\mathbb{C}^{m\times n})^l$ the matrix $C(\mathcal{B}) := \sum_{i=1}^{l} B_i^* B_i$ has positive eigenvalues. Define

$$\hat{\mathcal{B}} = (\hat{B}_1, \ldots, \hat{B}_l) = (B_1 C(\mathcal{B})^{-\frac{1}{2}}, \ldots, B_l C(\mathcal{B})^{-\frac{1}{2}}) \in (\mathbb{C}^{m\times n})^l.$$

Then $\tau_{\mathcal{B}} : \mathcal{S}_n(\mathbb{C}) \to \mathcal{S}_m(\mathbb{C})$ given by

$$\tau_{\mathcal{B}}(X) = \sum_{i=1}^{l} \hat{B}_i X (\hat{B}_i)^*$$

is a quantum channel. So if $O(\mathcal{A})$ is a small neighborhood $\mathcal{A}$ then $\tau_{\mathcal{B}}$ is in the small neighborhood of τ. In particular of $\lambda_1(\mathbf{A}(\tau)) < 1$ then there exists a small neighborhood $O(\mathcal{A})$ such that $\lambda_1(\mathbf{A}(\tau_{\mathcal{B}})) < 1$ for each $\mathcal{B} \in O(\mathcal{A})$. Similar claim holds if $\sigma_1(\tau) < 1$.

4 Bi-quantum channels

Proof of Theorem 1.2. Observe first that since τ and τ^* are quantum channels if follows that $\omega := \tau^*\tau$ is a self-adjoint quantum channel on $\mathcal{S}_n(\mathbb{C})$. As ω preserves the cone of positive hermitian matrices, $\omega(I_n) = I_n$ and I_n is an interior point of $\mathcal{S}_{n,+}(\mathbb{C})$, the Krein-Milman theorem, e.g. [1], it follows that 1 is the maximal eigenvalue of ω. Hence $\sigma_1(\tau) = 1$. Observe next

$$\lambda_1(\tau(\mathbf{x}\mathbf{x}^*)) \le (\sum_{i=1}^n \lambda_i(\tau(\mathbf{x}\mathbf{x}^*))^2)^{\frac{1}{2}} = \|\tau(\mathbf{x}\mathbf{x}^*)\|.$$

We now estimate $\|\tau(\mathbf{x}\mathbf{x}^*)\|$ from above, assuming that $\|\mathbf{x}\| = 1$. Consider the singular value decomposition of τ. Here $m = n$, and assume that $U_1, \ldots, U_n, V_1, \ldots, V_n \in \mathcal{S}_n(\mathbb{C})$ are the right and left singular vectors of τ corresponding to $\sigma_1(\tau), \ldots, \sigma_n(\tau)$. Furthermore we assume that $U_1 = V_1 = \frac{1}{\sqrt{n}} I_n$. Hence

$$\sum_{i=1}^n \lambda_i(\tau(\mathbf{x}\mathbf{x}^*))^2 = \sum_{i=1}^{\operatorname{rank}\tau} \sigma_i(\tau)^2 |\operatorname{tr} U_i\mathbf{x}\mathbf{x}^*|^2 \le \sigma_1(\tau)^2 |\operatorname{tr} U_1\mathbf{x}\mathbf{x}^*|^2 + \sum_{i=2}^{\operatorname{rank}\tau} \sigma_2(\tau)^2 |\operatorname{tr} U_i\mathbf{x}\mathbf{x}^*|^2.$$

Since $\sigma_1(\tau) = 1$ and $\operatorname{tr} U_1\mathbf{x}\mathbf{x}^* = \frac{1}{\sqrt{n}} \operatorname{tr} \mathbf{x}\mathbf{x}^* = \frac{1}{\sqrt{n}}$, we deduce that

$$\sum_{i=1}^n \lambda_i(\tau(\mathbf{x}\mathbf{x}^*))^2 \le \sigma_2(\tau)^2 + \frac{1 - \sigma_2(\tau)^2}{n}. \tag{4.1}$$

So

$$\lambda_1(\tau(\mathbf{x}\mathbf{x}^*) \le \sqrt{\sigma_2(\tau)^2 + \frac{1 - \sigma_2(\tau)^2}{n}}.$$

Use the arguments of the proof of Theorem 1.1 to deduce (1.9). □

Proposition 4.1 *Let $\tau_i : \mathcal{S}_{n_i}(\mathbb{C}) \to \mathcal{S}_{n_i}(\mathbb{C})$ be a bi-quantum channel for $i = 1, 2$. Then $\tau_1 \otimes \tau_2$ is a bi-channel. Furthermore*

$$\sigma_2(\tau_1 \otimes \tau_2) = \max(\sigma_2(\tau_1), \sigma_2(\tau_2)). \tag{4.2}$$

In particular, if $\tau : \mathcal{S}_n(\mathbb{C}) \to \mathcal{S}_n(\mathbb{C})$ is a unitary channel and $\sigma_2(\tau) < 1$ then

$$\mathrm{H}(\otimes^p \tau) \ge -\frac{1}{2} \log(\sigma_2(\tau)^2 + \frac{1 - \sigma_2(\tau)^2}{n^p}). \tag{4.3}$$

Proof. Since $(\tau_1 \otimes \tau_2)^* = \tau_1^* \otimes \tau_2^*$ it follows that a tensor product of two bi-quantum channels is a bi-quantum channel. Since the singular values of $\tau_1 \otimes \tau_2$ are all possible products of of singular values of τ_1 and τ_2 we deduce (4.2). Then (4.3) is implied by Theorem 1.2. □

Lemma 4.2 *Consider a unitary channel of the form (1.1) and (1.8), where $l \ge 3$, $t_i \ne 0, i = 1, \ldots, l$, $Q_1 = I_n$, and $Q_2, \ldots, Q_l$ do not have a common nontrivial invariant subspace. Then $\sigma_2(\tau) < \sigma_1(\tau) = 1$.*

Proof. Assume that $X \in \mathcal{S}_{n,+}(\mathbb{C})$ has rank $k \in [1, n-1]$. We claim that $\operatorname{rank} \tau(X) > \operatorname{rank} X$. Recall that $X = \sum_{j=1}^k \mathbf{x}_j\mathbf{x}_j^*$, where $\mathbf{x}_1, \ldots, \mathbf{x}_k \in \mathbb{C}^n$ are nonzero orthogonal vectors. As $t_1^2, \ldots, t_k^2 > 0$ we deduce that

$$\tau(X) = t_1^2 X + \sum_{j=2}^k t_j^2 Q_j X Q_j^* \ge t_1^2 X.$$

So rank $\tau(X) \geq k$. Furthermore rank $\tau(X) = k$ if and only $Q_i\mathbf{x}_j \in \mathbf{U} := \mathrm{span}(\mathbf{x}_1, \dots, \mathbf{x}_k)$ for $i = 2, \dots, l$ and $j = 1, \dots, k$. Since $\mathbf{U}$ is not invariant under $Q_2, \dots, Q_l$ we deduce that rank $\tau(X) > k$. Clearly, if $Y \geq 0$ and rank $Y = n$ then rank $\tau(Y) = n$.

Observe next that $Q_2^*, \dots, Q_l^*$ do not have a nontrivial common invariant subspace. Indeed, if $\mathbf{V} \subset \mathbb{C}^n$ was a nontrivial common invariant of $Q_2^*, \dots, Q_l^*$, then the orthogonal complement of $\mathbf{V}$ will be a nontrivial invariant subspace of $Q_2, \dots, Q_l$, which contradicts our assumption. Hence $\tau^*(X) > \mathrm{rank}\, X$.

Let $\eta = \tau^*\tau$. Thus, rank $\eta^n(Z) = n$ for any $Z \gneq 0$, i.e., η^n maps $\mathcal{S}_{n,+}(\mathbb{C})\backslash\{0\}$ to the interior of $\mathcal{S}_{n,+}(\mathbb{C})$. By Krein-Milman theorem, i.e. [1], $1 = \lambda_1(\eta^n) > \lambda_2(\eta^n) = \sigma_2(\tau)^{2n}$. $\square$

Corollary 4.3 *Let $\tau : \mathcal{S}_n(\mathbb{C}) \to \mathcal{S}_n(\mathbb{C})$ be a generic unitary quantum channel. I.e. τ of the form (1.1) and (1.8), where $l \geq 3$, $(t_1^2, \dots, t_l^2)^\top$ is a random probability vector, and $Q_1, \dots, Q_l$ are random unitary matrices. Then $\sigma_2(\tau) < \sigma_1(\tau) = 1$.*

Proof. Let $\tau_1(X) := \tau(Q_1^* X Q_1)$. Clearly, the $l-1$ unitary matrices $Q_2Q_1^*, \dots, Q_lQ_1^*$ are $l-1$ random unitary matrices. Since $l - 1 \geq 2$ these $l-1$ matrices do not have a nontrivial common invariant subspace. Lemma 4.2 yields that $\sigma_2(\tau_1) < 1$. Clearly, $\sigma_2(\tau_1) = \sigma_2(\tau)$. $\square$

References

[1] A. Berman and R.J. Plemmons, *Nonnegative Matrices in the Matematical Sciences*, Academic Press 1979.

[2] H. Derksen, S. Friedland, G. Gour, D. Gross, L. Gurvits, A. Roy, and J. Yard, On minimum entropy output and the additivity conjecture, Notes of Quantum Information Group, American Mathematical Institute workshop "Geometry and representation theory of tensors for computer science, statistics and other areas", July 21-25, 2008.

[3] S. Friedland, Convex spectral functions, *Linear Multilin. Algebra* 9 (1981), 299-316.

[4] S.Friedland, Additive invariants on quantum channels and applications to regularized minimum entropy, arXiv:0809.0078.

[5] S. Friedland and U.N. Peled, Theory of Computation of Multidimensional Entropy with an Application to the Monomer-Dimer Problem, *Advances of Applied Math.* 34(2005), 486-522.

[6] M. B. Hastings, A counterexample to additivity of minimum output entropy, arXiv:0809.3972v2 [quant-ph].

[7] P. Hayden and A. Winter, Counterexamples to maximal p-norm multiplicativity conjecture, arXiv: 0807.4753v1 [quant-ph] 30 July, 2008.

[8] P.W. Shor, Equivalence of additivity questions in quantum information theory, *Comm. Math. Phys.* 246 (2004), 453-472, arXiv:quant-ph/030503v4, 3 July 2003.

Acknowledgement: I thank Gilad Gour for useful remarks.