



HAL
open science

Random quantum channels II: Entanglement of random subspaces, Renyi entropy estimates and additivity problems

Benoît Collins, Ion Nechita

► **To cite this version:**

Benoît Collins, Ion Nechita. Random quantum channels II: Entanglement of random subspaces, Renyi entropy estimates and additivity problems. 2009. hal-00393916v1

HAL Id: hal-00393916

<https://hal.science/hal-00393916v1>

Preprint submitted on 10 Jun 2009 (v1), last revised 14 Dec 2009 (v3)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

RANDOM QUANTUM CHANNELS II: ENTANGLEMENT OF RANDOM SUBSPACES, RÉNYI ENTROPY ESTIMATES AND ADDITIVITY PROBLEMS

BENOÎT COLLINS AND ION NECHITA

ABSTRACT. In this paper we obtain new bounds for the minimum output entropies of random quantum channels. These bounds rely on random matrix techniques arising from free probability theory. We then revisit the counterexamples developed by Hayden and Winter to get violations of the additivity equalities for minimum output Rényi entropies. We show that random channels obtained by randomly coupling the input to a qubit violate the additivity of the p -Rényi entropy. For some sequences of random quantum channels, we compute almost surely the limit of their Schatten $S_1 \rightarrow S_p$ norms.

1. INTRODUCTION

The relationship between random matrix theory and free probability theory lies in the asymptotic freeness of random matrices. Asymptotic freeness, as it was discovered by Voiculescu (see e.g. [20]), usually predicts the asymptotic pointwise behaviour of joint noncommutative moments. However in some cases it can also predict more. For example, in the case of i.i.d. GUE random matrices, it was showed by Haagerup and Thorbjørnsen [9] that even the norms have an almost sure behavior predicted by free probability theory.

Quantum information theory is the analogue of classical information theory, where classical communication protocols are replaced by quantum information protocols, known as quantum channels. Despite the apparent simplicity of some mathematical question related to information theory, their resistance to various attempts to (dis)prove them have led to the study of their statistical properties.

The Holevo conjecture is arguably the most important conjecture in quantum information theory, and the theory of random matrices has been used here with success by Hayden and Winter [12, 14] to produce counterexamples to the additivity conjecture of Rényi entropy for $p > 1$. These counterexamples are of great theoretical importance, as they depict the likely behavior of a random channel. In [10], Hastings gave a counterexample for the case $p = 1$. It is also of probabilistic nature, but uses a very different and less canonical measure.

In our previous paper [7], we introduced a graphical model that allowed us to understand more systematically the computation of expectation and covariance of random channels and their powers. In particular we studied at length the output of the Bell state under a random conjugate bi-channel and obtained the explicit asymptotic behavior of this random matrix.

In the present paper, we take the results about the output of the random conjugate bi-channel for granted and focus on the mono-channel case. After obtaining new bounds for the mono-channel, we put together the mono-channel and bi-channel bounds to obtain new counterexamples to the additivity conjectures for $p > 1$. Our new bound relies on a result obtained by one author in [6] involving Jacobi matrices and on the study of appropriate convex polyhedra.

2000 *Mathematics Subject Classification.* 15A52, 94A17, 94A40.

Key words and phrases. Random matrices, Quantum information theory, Random channel, Additivity conjecture, Schatten p -norm.

Our techniques rely on free probability theory. They allow us to understand entanglement of random spaces, in the sense that our main statement Theorem 4.1 is about the principal values of a random subspace. It does not rely on a specific choice of a measure of entanglement. Note that this subtlety is important as the papers [1, 2] imply that all Rényi entropies don't enclose enough data to fully understand entanglement.

Our paper is organized as follows. We first recall a few basics and useful results of free probability theory of random matrix theoretical flavor in Section 2. In Section 3, we describe the random quantum channel we study. Section 4 describes the behavior of the eigenvalues of the outputs of random channels. In Section 5, we use results of the previous sections and of [7] to obtain new counterexamples to the additivity conjectures.

2. A REMINDER OF FREE PROBABILITY

The following is a summary of results contained in [6], [19], [20] and [8].

2.1. Asymptotic freeness. A *non-commutative probability space* is an algebra \mathcal{A} with unit endowed with a tracial state φ . An element of \mathcal{A} is called a (non-commutative) random variable. In this paper we shall be mostly concerned with the non-commutative probability space of *random matrices* $(\mathcal{M}_n(L^{\infty-}(\Omega, \mathbb{P})), \mathbb{E}[n^{-1} \text{Tr}(\cdot)])$ (we use the standard notation $L^{\infty-}(\Omega, \mathbb{P}) = \bigcap_{p \geq 1} L^p(\Omega, \mathbb{P})$).

Let $\mathcal{A}_1, \dots, \mathcal{A}_k$ be subalgebras of \mathcal{A} having the same unit as \mathcal{A} . They are said to be *free* if for all $a_i \in \mathcal{A}_{j_i}$ ($i = 1, \dots, k$) such that $\varphi(a_i) = 0$, one has

$$\varphi(a_1 \cdots a_p) = 0$$

as soon as $j_1 \neq j_2, j_2 \neq j_3, \dots, j_{p-1} \neq j_p$. Collections S_1, S_2, \dots of random variables are said to be free if the unital subalgebras they generate are free.

Let (a_1, \dots, a_k) be a k -tuple of selfadjoint random variables and let $\mathbb{C}\langle X_1, \dots, X_k \rangle$ be the free $*$ -algebra of non commutative polynomials on \mathbb{C} generated by the k indeterminates X_1, \dots, X_k . The *joint distribution* of the family $\{a_i\}_{i=1}^k$ is the linear form

$$\begin{aligned} \mu_{(a_1, \dots, a_k)} : \mathbb{C}\langle X_1, \dots, X_k \rangle &\rightarrow \mathbb{C} \\ P &\mapsto \varphi(P(a_1, \dots, a_k)). \end{aligned}$$

Given a k -tuple (a_1, \dots, a_k) of free random variables such that the distribution of a_i is μ_{a_i} , the joint distribution $\mu_{(a_1, \dots, a_k)}$ is uniquely determined by the μ_{a_i} 's. A family $(a_1^n, \dots, a_k^n)_n$ of k -tuples of random variables is said to *converge in distribution* towards (a_1, \dots, a_k) iff for all $P \in \mathbb{C}\langle X_1, \dots, X_k \rangle$, $\mu_{(a_1^n, \dots, a_k^n)}(P)$ converges towards $\mu_{(a_1, \dots, a_k)}(P)$ as $n \rightarrow \infty$. Sequences of random variables $(a_1^n)_n, \dots, (a_k^n)_n$ are called *asymptotically free* as $n \rightarrow \infty$ iff the k -tuple $(a_1^n, \dots, a_k^n)_n$ converges in distribution towards a family of free random variables.

The following result was contained in [19] (see also [8]).

Theorem 2.1. *Let U_1, \dots, U_k, \dots be a collection of independent Haar distributed random matrices of $\mathcal{M}_n(\mathbb{C})$ and $(W_i^n)_{i \in I}$ be a set of constant matrices of $\mathcal{M}_n(\mathbb{C})$ admitting a joint limit distribution as $n \rightarrow \infty$ with respect to the state $n^{-1} \text{Tr}$. Then the family $((U_1, U_1^*), \dots, (U_k, U_k^*), \dots, (W_i))$ admits a limit distribution, and is asymptotically free with respect to $\mathbb{E}[n^{-1} \text{Tr}]$.*

2.2. Free projectors. Let us fix real numbers $0 \leq \alpha, \beta \leq 1$, and consider, for all n , a selfadjoint projector $\pi_n \in \mathcal{M}_n(\mathbb{C})$ of rank q_n such that asymptotically $q_n \sim \alpha n$ as $n \rightarrow \infty$. Let π'_n be a projector of rank q'_n such that $q'_n \sim \beta n$, and assume that it can be written under the form $U\pi U^*$ such that U is a Haar distributed unitary random matrix independent from π_n

It is a consequence of Theorem 2.1, that π_n and π'_n are asymptotically free. Therefore $\pi_n \pi'_n \pi_n$ has an empirical eigenvalues distribution converging towards a probability measure. This measure is usually denoted by $\mu_1 \boxtimes \mu_2$, where μ_1, μ_2 are the limit empirical eigenvalue distributions of the projectors π_n and π'_n respectively:

$$\mu_1 = (1 - \alpha)\delta_0 + \alpha\delta_1, \quad \mu_2 = (1 - \beta)\delta_0 + \beta\delta_1$$

In this specific case, we can compute explicitly $\mu_1 \boxtimes \mu_2$. For this purpose, we introduce two 2-variable functions which will be of great importance in what follows.

$$\begin{aligned} \varphi^+ : \{(x, y) \in [0, 1]^2\} &\rightarrow [0, 1] \\ (x, y) &\mapsto 1 - \left[\sqrt{(1-x)(1-y)} - \sqrt{xy} \right]^2 \\ \varphi^- : \{(x, y) \in [0, 1]^2\} &\rightarrow [0, 1] \\ (x, y) &\mapsto 1 - \left[\sqrt{(1-x)(1-y)} + \sqrt{xy} \right]^2 \end{aligned}$$

Let us omit the variables of φ and rewrite

$$\varphi^{+/-} = \varphi^{+/-}(\alpha, \beta) = \alpha + \beta - 2\alpha\beta \pm \sqrt{4\alpha\beta(1-\alpha)(1-\beta)}$$

It follows then from [20], Example 3.6.7, that

$$\mu_1 \boxtimes \mu_2 = [1 - \min(\alpha, \beta)]\delta_0 + [\max(\alpha + \beta - 1, 0)]\delta_1 + \frac{\sqrt{(\varphi^+ - x)(x - \varphi^-)}}{2\pi x(1-x)} 1_{[\varphi^-, \varphi^+]} dx$$

The proof relies on a technique introduced by Voiculescu to compute $\mu_1 \boxtimes \mu_2$ in general, called the S -transform. For more details, we refer the interested reader to [20]. Since we are only interested in φ^+ , we shall write from now on φ instead of φ^+ .

In the case where $\alpha + \beta < 1$, the ranges of π_n and π'_n do not (generically) overlap and $\varphi(\alpha, \beta) < 1$. The previous asymptotic freeness results imply that almost surely,

$$\liminf_n \|\pi_n \pi'_n \pi_n\|_\infty \geq \varphi(\alpha, \beta).$$

We are interested in whether we actually have

$$\lim_n \|\pi_n \pi'_n \pi_n\|_\infty = \varphi(\alpha, \beta) < 1.$$

This turns out to be true. This is an involved result whose proof we won't discuss here. We just recall the result below as a theorem, following [6] (theorem 4.15). See also [16].

Theorem 2.2. *In \mathbb{C}^n , choose at random according to the Haar measure two subspaces V_n and V'_n of respective dimensions $q_n \sim \alpha n$ and $q'_n \sim \beta n$ where $\alpha, \beta \in (0, 1)$. Let π_n (resp. π'_n) be the orthogonal projection onto V_n (resp. V'_n). Then, if $\alpha + \beta < 1$,*

$$\lim_n \|\pi_n \pi'_n \pi_n\|_\infty = \varphi(\alpha, \beta) < 1.$$

3. QUANTUM CHANNELS AND ADDITIVITY CONJECTURES

3.1. Rényi entropies and minimum output entropies. Let $\Delta_k = \{x \in \mathbb{R}_+^k \mid \sum_{i=1}^k x_i = 1\}$ be the $(k-1)$ -dimensional probability simplex. For a positive real number $p > 0$, define the *Rényi entropy of order p* of a probability vector $x \in \Delta_k$ to be

$$H^p(x) = \frac{1}{1-p} \log \sum_{i=1}^k x_i^p.$$

Since $\lim_{p \rightarrow 1} H^p(x)$ exists, we define the *Shannon entropy* of x to be this limit, namely:

$$H(x) = H^1(x) = - \sum_{i=1}^k x_i \log x_i.$$

We extend these definitions to density matrices by functional calculus:

$$H^p(\rho) = \frac{1}{1-p} \log \operatorname{Tr} \rho^p;$$

$$H(\rho) = H^1(\rho) = -\operatorname{Tr} \rho \log \rho.$$

Given a vector $x \in \mathbb{C}^n$, $\|x\| = 1$, we call P_x the rank one orthogonal projection onto the span of x . In quantum mechanics notation, $P_x = |x\rangle\langle x|$. More generally, for a subspace $V \subset \mathbb{C}^n$, we denote by P_V the orthogonal projection onto V in $\mathcal{M}_n(\mathbb{C})$.

A quantum channel is a linear completely positive trace preserving map Φ from $\mathcal{M}_n(\mathbb{C}) \rightarrow \mathcal{M}_k(\mathbb{C})$. The trace preservation condition means that density matrices are mapped to density matrices, and the complete positivity reads:

$$\forall d \geq 1, \quad \Phi \otimes \mathbf{I}_d : \mathcal{M}_{nd}(\mathbb{C}) \rightarrow \mathcal{M}_{kd}(\mathbb{C}) \text{ is a positive map.}$$

We recall that according to Stinespring theorem, a linear map $\Phi : \mathcal{M}_n(\mathbb{C}) \rightarrow \mathcal{M}_k(\mathbb{C})$ is a quantum channel if and only if there exists a finite dimensional Hilbert space $\mathcal{K} = \mathbb{C}^d$, and a partial isometry $V \in \operatorname{End}(\mathbb{C}^n, \mathbb{C}^{kd})$ (satisfying $V^*V = \mathbf{I}_n$) such that

$$(1) \quad \Phi(X) = \operatorname{Tr}_{\mathcal{K}} [VXV^*], \quad \forall X \in \mathcal{M}_n(\mathbb{C}).$$

For a quantum channel $\Phi : \mathcal{M}_n(\mathbb{C}) \rightarrow \mathcal{M}_k(\mathbb{C})$, we define its *minimum output Rényi entropy (of order p)* by

$$H_{\min}^p(\Phi) = \min_{\substack{\rho \in \mathcal{M}_n(\mathbb{C}) \\ \rho \geq 0, \operatorname{Tr} \rho = 1}} H^p(\Phi(\rho)).$$

Since the Rényi entropies are concave functions, their minima are attained on the extremal points of the set of density matrices and hence

$$H_{\min}^p(\Phi) = \min_{\substack{x \in \mathbb{C}^n \\ \|x\|=1}} H^p(\Phi(P_x)).$$

3.2. The random quantum channel model. We fix an integer k and a real number $t \in (0, 1)$. For each n , let $U_n \in \mathcal{M}_{nk}(\mathbb{C})$ be a random unitary matrix distributed according to the Haar measure, and q_n be a projection of $\mathcal{M}_{nk}(\mathbb{C})$ of trace p_n such that $p_n/(kn) \sim t$ as $n \rightarrow \infty$. To q_n we associate a non-unital matrix algebra map $\chi_n : \mathcal{M}_{p_n}(\mathbb{C}) \rightarrow \mathcal{M}_{nk}(\mathbb{C})$ satisfying $\chi_n(1) = q_n$. The choice of χ_n is unique up to unitary conjugation, and the actual choice of χ_n is irrelevant for the computations we want to perform - in the sense that any choice will yield the same results.

We study the sequence of random channels

$$\Phi_n : \mathcal{M}_{p_n}(\mathbb{C}) \rightarrow \mathcal{M}_k(\mathbb{C})$$

given by

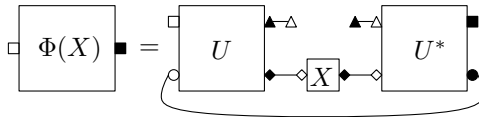
$$\Phi_n(X) = \operatorname{Tr}_n(U_n(\chi_n(X))U_n^*).$$

Remark 3.1. *In our previous paper [7], we considered exactly the same model of random quantum channels, with one small difference: the partial trace was taken with respect to \mathbb{C}^k . However, it is well-known that, when partial tracing a rank one projector, the non-zero eigenvalue of the resulting matrix do not depend on which space is traced out. Hence, from the point of view of eigenvalue statistics, the model we consider here is identical with the one in [7], Section 6.2.*

Graphically, our model amounts to Figure 1. We refer to the first paper of this series, [7] for details about this graphical notation.

We are interested in the random process given by the *set of all possible* eigenvalues of $\Phi(X)$ as $n \rightarrow \infty$. In our setup, this number is fixed.

Let V_n be the image of $U_p U^*$. This is a random vector space in $\mathbb{C}^n \otimes \mathbb{C}^k$ of dimension p_n distributed according to the uniform measure on the Haar measure on $\operatorname{Gr}_{p_n}(\mathbb{C}^{nk})$.

FIGURE 1. Diagram for $\Phi(X)$

If we can ensure that the entanglement of *every* norm one vector $x \in V_n$ in $\mathbb{C}^n \otimes \mathbb{C}^k$ is high with high probability for the uniform measure on $V_n \in \text{Gr}_{p_n}(\mathbb{C}^{nk})$, this will yield new entropy bounds. The entanglement is always a concave function of the principal values of x . We recall that for an element $x \in \mathbb{C}^n \otimes \mathbb{C}^k$ we denote $\lambda(x)$ and $\text{rk}(x)$ the singular values and rank of x , when viewed as a matrix $x \in \mathcal{M}_{n \times k}(\mathbb{C})$. In quantum information theory, these quantities are also called the *Schmidt coefficients* and the *Schmidt rank* of x respectively:

$$x = \sum_{i=1}^{\text{rk}(x)} \sqrt{\lambda_i(x)} e_i \otimes f_i,$$

where $\{e_i\}$ and $\{f_i\}$ are orthonormal families from \mathbb{C}^n and \mathbb{C}^k respectively. The strategy adopted in this paper is to describe a convex polyhedron such that, with high probability on $\text{Gr}_{p_n}(\mathbb{C}^{nk})$, for all input x , the set of eigenvalue vectors $\lambda(x)$ belong to a neighborhood on this convex set.

3.3. Known bounds. Some results are already available in order to quantify the entanglement of generic spaces in $\text{Gr}_{p_n}(\mathbb{C}^n \otimes \mathbb{C}^k)$. The best result known so far is arguably the following theorem of Hayden, Leung and Winter in [13]:

Theorem 3.2 (Hayden, Leung, Winter, [13], Theorem IV.1). *Let A and B be quantum systems of dimension d_a and d_B with $d_b \geq d_A \geq 3$. Let $0 < \alpha < \log d_A$. Then there exists a subspace $S \subset A \otimes B$ of dimension*

$$d \sim d_A d_B \frac{\Gamma \alpha^{2.5}}{(\log d_A)^{2.5}}$$

such that all states $x \in S$ have entanglement satisfying

$$H(P_x) \geq \log d_A - \alpha - \beta,$$

where $\beta = d_A / (d_B \log 2)$ and $\Gamma = 1/1753$.

To prove this result, the authors require sophisticated methods from asymptotic geometry theory. In particular, they need estimates on the covering numbers of unitary groups by balls of radius ε and results of concentration of measure. The results of concentration of measure are applied to a specific measure of entanglement (e.g. one entropy H^p), therefore the measure of entanglement does not deal directly with the behavior of the Schmidt coefficients, but rather with the behavior of a function of them.

4. CONFINING THE EIGENVALUES ALMOST SURELY

4.1. Main result. Our strategy is to describe a convex polyhedron K inside the probability simplex Δ_k with the property that, for all $\varepsilon > 0$, almost surely when n goes to infinity, all input density matrices $\rho \geq 0, \text{Tr}(\rho) = 1$, are mapped to output states $\Phi(\rho)$ whose spectra are contained $K + \varepsilon$, the ε -neighborhood of K .

For $t \in (0, 1)$, let us first define the vector $\beta^{(t)}$, where

$$\begin{aligned}\beta_1^{(t)} &= \varphi\left(\frac{1}{k}, t\right), \\ \beta_j^{(t)} &= \varphi\left(\frac{j}{k}, t\right) - \varphi\left(\frac{j-1}{k}, t\right), \quad \forall 2 \leq j \leq \lfloor k(1-t) \rfloor, \\ \beta_{\lfloor k(1-t) \rfloor + 1}^{(t)} &= 1 - \sum_{j=1}^{\lfloor k(1-t) \rfloor} \beta_j^{(t)}, \\ \beta_j^{(t)} &= 0, \quad \forall \lfloor k(1-t) \rfloor + 2 \leq j \leq k.\end{aligned}$$

One can check directly that $\beta^{(t)}$ is a probability vector and that it is a non-increasing sequence.

It turns out that the *majorization* partial order plays an important role in this situation, so let us remind here the definition and some basic properties of this relation. For two probability vectors $x, y \in \Delta_k$, we say that x is *majorized* by y (and we write $x \prec y$) if for all $j \in \{1, \dots, k\}$

$$(2) \quad s_j(x) = \sum_{i=1}^j x_i^\downarrow \leq \sum_{i=1}^j y_i^\downarrow = s_j(y),$$

where x^\downarrow and y^\downarrow are the decreasing rearrangements of x and y ; note that for $j = k$ we actually have an equality, since x and y are probability vectors. The majorization relation can also be characterized in the following way: for a probability vector y and a permutation $\sigma \in \mathcal{S}_k$, denote by $\sigma.y$ the vector obtained by permuting the coordinates of y along σ : $(\sigma.y)_i = y_{\sigma(i)}$. Then

$$x \prec y \text{ iff. } x \in S(y),$$

where $S(y)$ is the convex hull of the set $\{\sigma.y \mid \sigma \in \mathcal{S}_k\}$. Moreover, the extremal points of $S(y)$ are exactly y and its permutations $\sigma.y$.

We can now state the main result of this section:

Theorem 4.1. *Let t be a parameter in $(0, 1)$ and $\varepsilon > 0$. Let $S(\beta^{(t)}) + \varepsilon$ be the ε -ball around $S(\beta^{(t)})$ in Δ_k . Then, almost surely when $n \rightarrow \infty$, for all input density matrix ρ ,*

$$\text{spec}(\Phi(\rho)) \in S(\beta^{(t)}) + \varepsilon.$$

We split the proof of Theorem 4.1 into several lemmas. The first one is an easy consequence of the definition of the operator norm.

Lemma 4.2. *Let Q, R be two selfadjoint projections in $\mathcal{M}_n(\mathbb{C})$. Then*

$$\|QRQ\|_\infty = \max_{x \in \text{Im } Q} \text{Tr}(P_x R).$$

Proof. Since QRQ is a self adjoint operator, we have:

$$\begin{aligned}\|QRQ\|_\infty &= \sup_{\|x\| \leq 1} \langle QRQx, x \rangle = \sup_{\|x\| \leq 1} \langle RQx, Qx \rangle \\ &= \sup_{\substack{y \in \text{Im } Q \\ \|y\| \leq 1}} \langle Ry, y \rangle = \text{Tr}(P_y R).\end{aligned}$$

□

The following lemma is a reformulation of the min-max theorem:

Lemma 4.3. *Let $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_k$ be the Schmidt coefficients of a vector $x \in \mathbb{C}^{nk}$. Then, for all $1 \leq j \leq k$,*

$$s_j(x) = \lambda_1 + \lambda_2 + \dots + \lambda_j = \max_{F \in \text{Gr}_j(\mathbb{C}^k)} \text{Tr}(P_x P_{\mathbb{C}^n \otimes F}).$$

Proof. Since λ_i are the eigenvalues of $\text{Tr}_k P_x$, the min-max theorem for $\text{Tr}_k P_x$ can be stated as:

$$s_j(x) = \max_{F \in \text{Gr}_j(\mathbb{C}^k)} \text{Tr}(P_F \text{Tr}_k P_x).$$

The conditional expectation property of the partial trace implies that

$$s_j(x) = \max_{F \in \text{Gr}_j(\mathbb{C}^k)} \text{Tr}(P_x \cdot \mathbf{I}_n \otimes P_F) = \max_{F \in \text{Gr}_j(\mathbb{C}^k)} \text{Tr}(P_x \cdot P_{\mathbb{C}^n \otimes F}).$$

□

We are interested in majorization inequalities which hold uniformly for all norm one elements of a subspace V . In other words, we are interested in the quantity

$$\max_{\substack{x \in V \\ \|x\|=1}} s_j(x) = \max_{\substack{x \in V \\ \|x\|=1}} \max_{F \in \text{Gr}_j(\mathbb{C}^k)} \text{Tr}(P_x P_{\mathbb{C}^n \otimes F}).$$

Since k is a fixed parameter of our model, in order to compute the maximum over the Grassmannian, it suffices to consider only a finite number of subspaces F :

Lemma 4.4. *For all $\varepsilon > 0$, for all j , there exists a finite number of j -dimensional subspaces $F_1, \dots, F_N \in \text{Gr}_j(\mathbb{C}^k)$ such that, for all $x \in \mathbb{C}^{nk}$,*

$$\max_{i=1}^N \text{Tr}(P_x P_{\mathbb{C}^n \otimes F_i}) \leq s_j(x) \leq \max_{i=1}^N \text{Tr}(P_x P_{\mathbb{C}^n \otimes F_i}) + \varepsilon.$$

Note that in Lemma 4.4, N does depend on ε but can be chosen to be finite for any $\varepsilon > 0$.

Proof. We only need to prove the second inequality. Since the Grassmannian $\text{Gr}_j(\mathbb{C}^k)$ is compact and metric for $d(E, F) = \|P_E - P_F\|_\infty$, for all $\varepsilon > 0$ there exists a covering of $\text{Gr}_j(\mathbb{C}^k)$ by a finite number of balls of radius ε centered in F_1, \dots, F_N . Fix some $x \in \mathbb{C}^{nk}$ and consider the element $F \in \text{Gr}_j(\mathbb{C}^k)$ for which the maximum in the definition of $s_j(x)$ is attained. F is inside some ball centered at F_i and we have

$$\begin{aligned} \text{Tr}(P_x P_{\mathbb{C}^n \otimes F}) &\leq \text{Tr}(P_x P_{\mathbb{C}^n \otimes F_i}) + |\text{Tr}(P_x (P_{\mathbb{C}^n \otimes F} - P_{\mathbb{C}^n \otimes F_i}))| \\ &= \text{Tr}(P_x P_{\mathbb{C}^n \otimes F_i}) + \|P_F - P_{F_i}\|_\infty \leq \text{Tr}(P_x P_{\mathbb{C}^n \otimes F_i}) + \varepsilon, \end{aligned}$$

and the conclusion follows. □

Now we are ready to prove Theorem 4.1.

Proof of Theorem 4.1. Let $\varepsilon > 0$ and $j \in \{1, \dots, \lfloor k(1-t) \rfloor\}$. Let V be a random vector space of dimension $p_n \sim tnk$. According to Theorem 2.2, for all $i \in \{1, \dots, N\}$, almost surely when $n \rightarrow \infty$,

$$\lim_n \|P_V P_{\mathbb{C}^n \otimes F_i} P_V\|_\infty = \varphi(t, j/k).$$

For every such subspace V , one also has that

$$\max_{\substack{x \in V \\ \|x\|=1}} s_j(x) = \max_{\substack{x \in V \\ \|x\|=1}} \max_{F \in \text{Gr}_j(\mathbb{C}^k)} \text{Tr}(P_x P_{\mathbb{C}^n \otimes F}).$$

Using the compactness argument in Lemma 4.4, one can consider (at a cost of ε) only a finite number of subspaces F :

$$\max_{\substack{x \in V \\ \|x\|=1}} s_j(x) \leq \max_{i=1}^N \max_{\substack{x \in V \\ \|x\|=1}} \text{Tr}(P_x P_{\mathbb{C}^n \otimes F_i}) + \varepsilon.$$

Using Theorem 2.2 and Lemma 4.2, one has that, almost surely,

$$\limsup_n \max_{\substack{x \in V \\ \|x\|=1}} s_j(x) \leq \varphi(t, j/k) + \varepsilon.$$

Letting $\varepsilon \rightarrow 0$ concludes the proof. \square

The interest of Theorem 4.1 in comparison to Theorem 3.2 is that it does not rely specifically on one measurement of entanglement, as we are able to confine almost surely the eigenvalues in a convex set. Also, our argument relies neither on concentration inequalities nor on net estimates, as we fix k . Our Theorem 4.1 however, unlike Theorem 3.2, does not give explicit control on n . It is theoretically possible to give an explicit control on n (using techniques introduced in [16]), but this would require a considerable amount of work.

4.2. Application to Entropies. Once the eigenvalues of the output of a channel have been confined inside a fixed convex polyhedron, entropy inequalities follow easily. Indeed, the confining polyhedron is defined in terms of the majorization partial order, and thus the notion of Schur-convexity (see [4]) is crucial in what follows.

A function $f : \mathbb{R}^k \rightarrow \mathbb{R}$ is said to be Schur-convex if $x \prec y$ implies $f(x) \leq f(y)$. The Rényi entropies H^p are Schur-concave, and thus majorization relations of type $x \prec y$ imply $H^p(x) \geq H^p(y)$ for all $p \geq 1$. The reciprocal implication has been studied in [1, 2]: entropy inequalities $H^p(x) \geq H^p(y)$ (for all $p \geq 1$) characterize a weaker form of majorization called *catalytic majorization*, which has applications in LOCC protocols for the transformation of bipartite states.

For the purposes of this paper, the main corollary of Theorem 4.1 is the following

Theorem 4.5. *For a fixed parameter t , almost surely, when $n \rightarrow \infty$, for all input $\rho \in \mathcal{D}_{tnk}$,*

$$\liminf_n H_{\min}^p(\Phi_U) \geq H^p(\beta^{(t)}).$$

Proof. This follows directly from Theorem 4.1 and from the Schur-concavity of the Rényi entropies. \square

5. NEW EXAMPLES AND COUNTEREXAMPLES

Since our main result, Theorem 4.1, is valid almost surely in the limit $n \rightarrow \infty$, the limiting objects shall depend only on the (*a priori* fixed) parameters k and t . In what follows, we shall consider large values of the parameter k , we introduce the “little-o” notation $o(\cdot)$ with respect to the limit $k \rightarrow \infty$.

5.1. The conjectures. We start with the most important one, the additivity of the minimum output von Neumann entropy.

Conjecture 5.1. *For all quantum channels Φ_1 and Φ_2 , one has*

$$(3) \quad H_{\min}(\Phi_1 \otimes \Phi_2) = H_{\min}(\Phi_1) + H_{\min}(\Phi_2).$$

The previous statement can be deduced from the following, more general conjecture.

Conjecture 5.2. *For all quantum channels Φ_1 and Φ_2 , the minimum output p -Rényi entropies are additive:*

$$(4) \quad \forall p > 1, \quad H_{\min}^p(\Phi_1 \otimes \Phi_2) = H_{\min}^p(\Phi_1) + H_{\min}^p(\Phi_2).$$

Both conjectures have been disproved recently [10, 12], mainly using random matrix techniques. We refer to [11] for the theory, and to [12], [14] and also [10] for the existing counterexamples.

5.2. The Bell phenomenon. In order to provide counter examples for the additivity conjectures, one has to produce lower bounds for the minimum output entropy of single copies of the channels (and this is where Theorem 4.1 is useful) and upper bounds for the minimum output entropy of the tensor product of the quantum channels. The latter task is somewhat easier, since one has to exhibit a particular input state such that the output has low entropy.

The choice of the input state for the product channel is guided by the following observation. It is clear that if one chooses a product input state $\rho = \rho_1 \otimes \rho_2$, then the output state is still in product form, and the entropies add up:

$$H^p([\Phi_1 \otimes \Phi_2](\rho_1 \otimes \rho_2)) = H^p(\Phi_1(\rho_1) \otimes \Phi_2(\rho_2)) = H^p(\Phi_1(\rho_1)) + H^p(\Phi_2(\rho_2)).$$

Hence, such choices cannot violate the additivity of Rényi entropies. Instead, one has to look at *entangled* states, and the maximally entangled states are obvious candidates.

All our examples rely on the study of the product of conjugate channels

$$\Phi_n \otimes \bar{\Phi}_n$$

where

$$\Phi_n(X) = \text{Tr}_n(U_n X U_n^*), \quad \bar{\Phi}_n(X) = \text{Tr}_n(\bar{U}_n X \bar{U}_n^t)$$

have been introduced in subsection 3.2. Our task is to obtain a good upper bound for

$$\limsup_n H_{min}^p(\Phi_n \otimes \bar{\Phi}_n).$$

Our strategy is systematically to write

$$\limsup_n H_{min}^p(\Phi_n \otimes \bar{\Phi}_n) \leq H_{min}^p(\Phi_n \otimes \bar{\Phi}_n(E_{tnk}))$$

where E_{tnk} is the maximally entangled state over the input space $(\mathbb{C}^{tnk})^{\otimes 2}$. More precisely, E_{tnk} is the projection on the Bell vector

$$\text{Bell}_{tnk} = \frac{1}{\sqrt{tnk}} \sum_{i=1}^{tnk} e_i \otimes e_i,$$

where $\{e_i\}_{i=1}^{tnk}$ is a fixed basis of \mathbb{C}^{tnk} . Using the graphical formalism of [7], we are dealing with the diagram in Figure 2 (recall that square symbols correspond to \mathbb{C}^k , round symbols correspond to \mathbb{C}^n , diamond ones to \mathbb{C}^{tnk} and triangle-shaped symbols correspond to $\mathbb{C}^{1/t}$).

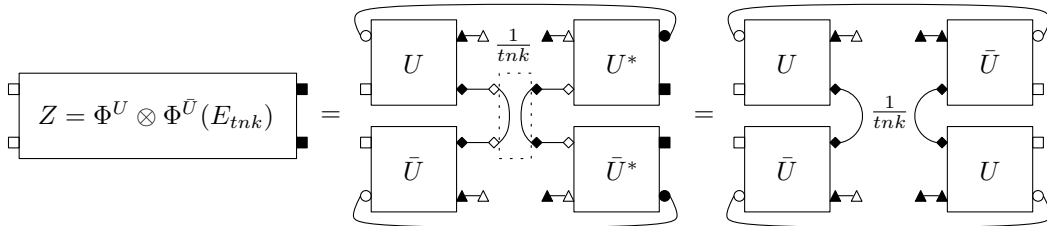


FIGURE 2. $Z_n = \Phi^U \otimes \Phi^{\bar{U}}(E_{tnk})$

The random matrix $\Phi_n \otimes \bar{\Phi}_n(E_{tnk})$ was thoroughly studied in our previous paper [7] and we recall here one of the main results of this paper:

Theorem 5.3. *Almost surely, as $n \rightarrow \infty$, the random matrix $\Phi_n \otimes \bar{\Phi}_n(\text{Bell}_{tnk}) \in \mathcal{M}_{k^2}(\mathbb{C})$ has eigenvalues*

$$\gamma^{(t)} = \left(t + \frac{1-t}{k^2}, \underbrace{\frac{1-t}{k^2}, \dots, \frac{1-t}{k^2}}_{k^2-1 \text{ times}} \right).$$

From this we deduce the following corollary, which gives an upper bound for the minimum output entropy for the product channel $\Phi \otimes \bar{\Phi}$:

Corollary 5.4. *Almost surely, as $n \rightarrow \infty$,*

$$\limsup_n H_{\min}^p(\Phi_n \otimes \bar{\Phi}_n) \leq \frac{1}{1-p} \log \left[\left(t + \frac{1-t}{k^2} \right)^p + (k^2 - 1) \left(\frac{1-t}{k^2} \right)^p \right]$$

In the case $p = 1$ the upper bound simplifies to

$$\limsup_n H_{\min}(\Phi_n \otimes \bar{\Phi}_n) \leq - \left(t + \frac{1-t}{k^2} \right) \log \left(t + \frac{1-t}{k^2} \right) - (k^2 - 1) \frac{1-t}{k^2} \log \left(\frac{1-t}{k^2} \right).$$

5.3. Macroscopic counterexamples for the Rényi entropy. In this section, we fix $t = 1/2$ and assume we that k is even, in order to avoid non-integer dimensions. A value of $1/2$ for t means that the environment to which the input of the channel is coupled is 2-dimensional, i.e. a single qubit. The main result of this section is that we obtain a violation of the Rényi entropy in that case. We believe that the examples known so far could not deal with such a simple situation.

The eigenvalue vector of the product channel is

$$\gamma = \gamma^{(1/2)} = \left(\frac{1}{2} + \frac{1}{2k^2}, \frac{1}{2k^2}, \dots, \frac{1}{2k^2} \right).$$

Since $\varphi(x, 1/2) = 1/2 + \sqrt{x(1-x)}$, the vector $\beta = \beta^{(1/2)}$ is has a particularly simple form in this case:

$$\begin{aligned} \beta_1 &= \frac{1}{2} + \frac{\sqrt{k-1}}{k}, \\ \beta_j &= \psi \left(\frac{j}{k} \right) - \psi \left(\frac{j-1}{k} \right), \quad \text{for } 2 \leq j \leq k/2, \end{aligned}$$

where the function ψ is given by $\psi(x) = \sqrt{x(1-x)}$. Note that the first eigenvalue is large (of order $1/2$) and that the others are small:

$$\beta_j \leq \frac{1}{k} \psi' \left(\frac{1}{k} \right) \leq \frac{1}{\sqrt{k}}, \quad \forall 2 \leq j \leq k/2.$$

The aim of this section is Theorem 5.5, the violation of the additivity for Rényi entropies for all $p > 1$. For the purposes of this section, the Corollary 5.4 implies that, almost surely,

$$(5) \quad \limsup_n H_{\min}^p(\Phi \otimes \bar{\Phi}) \leq \frac{p}{p-1} \log 2.$$

The main result of this section is the following theorem.

Theorem 5.5. *Almost surely as $n \rightarrow \infty$,*

$$\liminf_n H_{\min}^p(\Phi) = \liminf_n H_{\min}^p(\bar{\Phi}) \geq \frac{p}{p-1} \log 2 + o(1).$$

Hence, the additivity of the Rényi p -norms is violated for all $p > 1$.

Proof. We shall provide a lower bound for $H^p(\beta)$. Notice that the main contribution is given by the largest eigenvalue: $\beta_1^p = 2^{-p} + o(1)$. Next, we show that the contribution of the smaller eigenvalues is asymptotically zero. We consider three cases: $p > 2$, $p = 2$ and $1 < p < 2$. If $p > 2$, then

$$\sum_{j \geq 2} \beta_j^p \leq \sum_{j \geq 2} k^{-p/2} \leq k^{1-p/2} = o(1).$$

For $p = 2$, one has:

$$\begin{aligned} \sum_{j \geq 2} \beta_j^2 &= \sum_{j=2}^{k/2} \left[\psi\left(\frac{j}{k}\right) - \psi\left(\frac{j-1}{k}\right) \right]^2 \\ &\leq \sum_{j=2}^{k/2} \left[\frac{1}{k} \cdot \sup_{(j-1)/k \leq x \leq j/k} \psi'(x) \right]^2 \\ &= \sum_{j=2}^{k/2} \left[\frac{1}{k} \psi'\left(\frac{j-1}{k}\right) \right]^2 = \frac{1}{k} \sum_{j=2}^{k/2} \frac{(1-2j/k)^2}{2j(1-j/k)} = o(1). \end{aligned}$$

The case $1 < p < 2$ is the more involved:

$$\begin{aligned} \sum_{j \geq 2} \beta_j^p &= \sum_{j=2}^{k/2} \left[\psi\left(\frac{j}{k}\right) - \psi\left(\frac{j-1}{k}\right) \right]^p \\ &\leq \sum_{j=2}^{k/2} \left[\frac{1}{k} \cdot \sup_{(j-1)/k \leq x \leq j/k} \psi'(x) \right]^p \\ &= \sum_{j=2}^{k/2} \left[\frac{1}{k} \psi'\left(\frac{j-1}{k}\right) \right]^p \\ &= k^{1-p} \sum_{j=2}^{k/2} \frac{1}{k} \left[\psi'\left(\frac{j-1}{k}\right) \right]^p \\ &\leq k^{1-p} \left[\int_0^{1/2} \psi'(t)^p dt \right] = o(1). \end{aligned}$$

Hence, in all three cases, $H^p(\beta) \geq \frac{p}{p-1} \log 2 + o(1)$. This inequality and Eq. (5) provide the announced violation of the additivity conjecture for Rényi entropies.

$$H_{\min}^p(\Phi_n \otimes \bar{\Phi}_n) \leq \frac{p}{p-1} \log 2 < 2 \cdot \left[\frac{p}{p-1} \log 2 + o(1) \right] \leq 2H_{\min}^p(\Phi_n).$$

□

It is natural to wonder whether the bound $H^p(\beta^t)$ is optimal. For fixed k , this is an open question, and we believe that there is room for little improvement. However, our bounds are optimal in the sense of the corollary below. Let us fix $t \in (0, 1)$ and denote by $\Phi_{k,n}$ the random quantum channel Φ_n introduced in Section 3.2 (since k will vary in the statement below, we need to keep track of it).

Corollary 5.6. *For all $p > 1$, there exists a sequence n_k tending to infinity as k tends to infinity, such that, almost surely*

$$\lim_k H_{\min}^p(\Phi_{k,n_k} \otimes \bar{\Phi}_{k,n_k}) = \lim_k H_{\min}^p(\Phi_{k,n_k}) = \frac{p}{1-p} \log t.$$

In particular this means that we can almost surely estimate the Schatten $S_1 \rightarrow S_p$ norm of that quantum channel:

$$\lim_k \|\Phi_{k,n_k} \otimes \bar{\Phi}_{k,n_k}\|_{S_1 \rightarrow S_p} = \lim_k \|\Phi_{k,n_k}\|_{S_1 \rightarrow S_p} = t$$

Proof. For $t = 1/2$, this follows directly by a diagonal argument from Theorem 5.5 and Equation (5) together with the simple fact that the entropy increases when one takes tensor products:

$$H_{\min}^p(\Phi_{k,n_k}) \leq H_{\min}^p(\Phi_{k,n_k} \otimes \bar{\Phi}_{k,n_k}).$$

The asymptotic estimates of Theorem 5.5 are readily adapted to arbitrary $t \in (0, 1)$. As for the norm estimate, it follows from the definition of the Schatten norm and the Rényi entropy, as well as the fact that the $S_1 \rightarrow S_p$ norm is attained on density matrices. \square

It is remarkable that the norm estimate for $\|\Phi \otimes \bar{\Phi}\|_{S_1 \rightarrow S_p}$ given by $\|\Phi \otimes \bar{\Phi}(E_{tnk})\|_{S_p}$ is actually optimal. The above corollary stands as a mathematical evidence that the Bell states asymptotically maximize the $S_1 \rightarrow S_p$ norm of $\Phi \otimes \bar{\Phi}$.

The first example of ‘Rényi superadditive’ quantum channel was obtained by Holevo and Werner in [15] using a deterministic channel. However, their example violated the additivity conjecture only for $p > 4.79$. Hayden and Winter found a class of random counterexamples for the whole range of parameters $p > 1$ in [12]. Our being able to prescribe t in the counterexample of Theorem 5.5 is an improvement to the counterexamples provided in the paper [14]. Our t^{-1} corresponds to the dimension of the space R coupled to the input space and it seems that their use of Theorem 3.2 makes it necessary to have $|R|$ tend to infinity for a counterexample, whereas our counterexamples work for t fixed (and k fixed as well). Physically, this means that to obtain a counterexample, it is enough to couple randomly the input to a qubit ($k = 2$) to obtain a counterexample.

We finish this section by a computation showing that the above bounds are not good enough to obtain the violation of the additivity conjecture in the case $p = 1$. We start with the entropy of the product channel:

$$H(\gamma) = \log k + \log 2 + o(1).$$

For the case of the single channel, we need an upper bound for $H(\beta^{(1/2)})$ (recall that $h(x) = -x \log x$):

$$\begin{aligned} H(\beta) &= h(\beta_1) + \sum_{j=2}^{k/2} h(\beta_j) \\ &= \frac{\log 2}{2} + \sum_{j=2}^{k/2} h \left[\psi\left(\frac{j}{k}\right) - \psi\left(\frac{j-1}{k}\right) \right] + o(1) \\ &\leq \frac{\log 2}{2} + \sum_{j=2}^{k/2} h \left[\frac{1}{k} \cdot \sup_{(j-1)/k \leq z \leq j/k} \psi'(z) \right] + o(1) \\ &= \frac{\log 2}{2} + \sum_{j=2}^{k/2} h \left[\frac{1}{k} \psi' \left(\frac{j}{k} \right) \right] + o(1). \end{aligned}$$

Using

$$h \left[\frac{1}{k} \psi' \left(\frac{j}{k} \right) \right] = \frac{\log k}{k} \psi' \left(\frac{j}{k} \right) + \frac{1}{k} [h \circ \psi'] \left(\frac{j}{k} \right)$$

and

$$\int_0^{1/2} [h \circ \psi'](t) dt = -\frac{\log 2}{2},$$

we obtain

$$\begin{aligned} H(\beta^{(1/2)}) &\leq \frac{\log 2}{2} + \sum_{j=2}^{k/2} \frac{\log k}{k} \psi' \left(\frac{j}{k} \right) + \sum_{j=2}^{k/2} \frac{1}{k} [h \circ \psi'] \left(\frac{j}{k} \right) + o(1) \\ &= \frac{\log 2}{2} + \frac{1}{2} \log k - \frac{\log 2}{2} + o(1) \\ &= \frac{\log k}{2} + o(1). \end{aligned}$$

At the end, the entropy deficit is

$$H(\gamma) - 2H(\beta) \geq \log 2 + o(1) > 0,$$

which does not provide a violation of the minimum output von Neumann entropy.

5.4. The case $t = k^{-\alpha}$. We conclude this paper with the study of the case $t = k^{-\alpha}$, where $\alpha > 0$ is a fixed parameter. This corresponds to a larger environment size \mathbb{C}^{k^α} and, in light of Hastings' counterexample, one could have hoped that a similar violation of the additivity occurs. However, this section shows that this does not seem to be the case.

To simplify the computations, we consider only the case of the minimum output von Neumann entropy. As before, we provide estimates, when k is fixed but large, for the minimum output entropies of $\Phi \otimes \bar{\Phi}$ and Φ .

We start with the simpler case of the product channel $\Phi \otimes \bar{\Phi}$. Theorem 5.3 provides the almost sure eigenvalues of $[\Phi \otimes \bar{\Phi}](E_{tnk})$:

$$\gamma = \gamma^{(k^{-\alpha})} = \left(\frac{1}{k^\alpha} + \frac{1}{k^2} - \frac{1}{k^{\alpha+2}}, \underbrace{\frac{1}{k^2} - \frac{1}{k^{\alpha+2}}, \dots, \frac{1}{k^2} - \frac{1}{k^{\alpha+2}}}_{k^2-1 \text{ times}} \right).$$

Using the series expansion $h(1-x) = x - x^2/2 + o(x^2)$, one can compute the asymptotics for the minimum output entropy:

Proposition 5.7. *For the product channel $\Phi \otimes \bar{\Phi}$, the following upper bounds hold almost surely:*

$$(6) \quad H_{\min}(\Phi \otimes \bar{\Phi}) \leq H(\gamma) = \begin{cases} 2 \log k - \frac{(2-\alpha) \log k}{k^\alpha} + o\left(\frac{\log k}{k^\alpha}\right) & \text{if } 0 < \alpha < 2; \\ 2 \log k - \frac{2 \log 2 - 1}{k^2} + o\left(\frac{1}{k^2}\right) & \text{if } \alpha = 2; \\ 2 \log k - \frac{1}{2k^{2\alpha-2}} + o\left(\frac{1}{k^{2\alpha-2}}\right) & \text{if } \alpha > 2. \end{cases}$$

Our estimate for the single channel case is as follows:

Theorem 5.8. *For all $\alpha > 0$, the following lower bound holds true almost surely:*

$$H_{\min}(\Phi) \geq H_{\min}(\beta) = \log k - \frac{\log k}{k^\alpha} + o\left(\frac{\log k}{k^\alpha}\right).$$

For the purposes of this proof, we define $\varphi_k : [0, 1 - k^{-\alpha}] \rightarrow [0, 1]$, $\varphi_k(x) = \varphi(x, k^{-\alpha})$ and $h(x) = -x \log x$. We have

$$\begin{aligned} \frac{\partial}{\partial x} \varphi(x, y) &= 1 - 2y + \sqrt{y(1-y)} \left[\frac{\sqrt{1-x}}{\sqrt{x}} - \frac{\sqrt{x}}{\sqrt{1-x}} \right] = 1 - 2y + \sqrt{y(1-y)} g(x); \\ &= (1 - 2y) \left(1 + \frac{g(x)}{g(y)} \right), \end{aligned}$$

where the function g is defined by

$$\begin{aligned} g : (0, 1) &\rightarrow \mathbb{R} \\ x &\mapsto \frac{\sqrt{1-x}}{\sqrt{x}} - \frac{\sqrt{x}}{\sqrt{1-x}}. \end{aligned}$$

Proof. According to Theorem 4.5, for all $\varepsilon > 0$,

$$H_{\min}(\Phi) \geq H(\beta) - \varepsilon,$$

where $\beta = \beta^{(k^{-\alpha})}$ is the $k - 1$ -dimensional vector defined by

$$\begin{aligned}\beta_1 &= \varphi_k \left(\frac{1}{k} \right); \\ \beta_j &= \varphi_k \left(\frac{j}{k} \right) - \varphi_k \left(\frac{j-1}{k} \right) = \frac{1}{k} \varphi'_k \left(\frac{\xi_j}{k} \right), \quad \forall 2 \leq j \leq k-1.\end{aligned}$$

Our purpose in what follows is to provide a “good” estimate for $H(\beta)$. We start by rescaling the eigenvalues: $H(\beta) = \log k + \frac{1}{k} H(k\beta)$. In this way, we can focus on the “entropy defect” $\log k - H(\beta)$ and reduce our problem to showing that

$$(7) \quad \frac{k^{\alpha-1}}{\log k} H(k\beta) = \frac{k^{\alpha-1}}{\log k} \sum_{j=1}^{k-1} h(k\beta_j) \xrightarrow[k \rightarrow \infty]{} -1,$$

The next step in our asymptotic computation is to replace the unknown points ξ_j by simpler estimates of the type j/k . Notice that the largest eigenvalue β_1 is of order k^{-1} . By the continuity of the function h , there exists a constant $C > 0$ such that $|h(k\beta_j)| \leq C$ and thus, individual terms in the sum (7) have no asymptotic contribution. It is clear that the function $x \mapsto \varphi'_k(x)$ is decreasing at fixed k and since the entropy function h is increasing for $x \in (0, e^{-1})$ and decreasing for $x \geq e^{-1}$, we can bound $h(\varphi'_k(\xi_j/k))$ by $h(\varphi'_k(j/k))$, and we reduce our problem to showing that

$$(8) \quad \frac{k^{\alpha-1}}{\log k} \sum_{j=1}^{k-1} h \left(\varphi'_k \left(\frac{j}{k} \right) \right) \xrightarrow[k \rightarrow \infty]{} -1,$$

or, equivalently,

$$\frac{k^{\alpha-1}}{\log k} \sum_{j=1}^{\lfloor k/2 \rfloor} h \left(\varphi'_k \left(\frac{j}{k} \right) \right) + h \left(\varphi'_k \left(1 - \frac{j}{k} \right) \right) \xrightarrow[k \rightarrow \infty]{} -1.$$

Now,

$$\begin{aligned}h \left[(1-2y) \left(1 + \frac{g(x)}{g(y)} \right) \right] + h \left[(1-2y) \left(1 - \frac{g(x)}{g(y)} \right) \right] &= \\ = 2h(1-2y) + (1-2y) \left[h \left(1 + \frac{g(x)}{g(y)} \right) + h \left(1 - \frac{g(x)}{g(y)} \right) \right].\end{aligned}$$

The term $2h(1-2y) = 2h(1-2k^{-\alpha}) \sim 4k^{-\alpha}$ has no asymptotic contribution and, using $h(1+t) + h(1-t) = -t^2 + O(t^4)$, we are left with computing the limit of the main contribution

$$\frac{k^{\alpha-1}}{\log k} \sum_{j=1}^{\lfloor k/2 \rfloor} -\frac{g(j/k)^2}{g(y)^2} \sim \frac{k^{\alpha-1}}{\log k} \sum_{j=1}^{\lfloor k/2 \rfloor} -g(j/k)^2 k^{-\alpha}.$$

Finally,

$$\frac{1}{k \log k} \sum_{j=1}^{\lfloor k/2 \rfloor} -g(j/k)^2 = \frac{1}{\log k} \sum_{j=1}^{\lfloor k/2 \rfloor} \frac{1}{j} \frac{(1-2j/k)^2}{1-j/k} \sim -\frac{\log(k/2)}{\log k} \xrightarrow[k \rightarrow \infty]{} -1.$$

The error term

$$\frac{k^{\alpha-1}}{\log k} \sum_{j=1}^{\lfloor k/2 \rfloor} -\frac{g(j/k)^4}{g(y)^4} \sim \frac{k^{\alpha-1}}{\log k} \sum_{j=1}^{\lfloor k/2 \rfloor} -g(j/k)^4 k^{-2\alpha} \sim \frac{1}{k^{\alpha+1} \log k} \sum_{j=1}^{\lfloor k/2 \rfloor} \frac{1}{j^2} \frac{(1-2j/k)^4}{(1-j/k)^2}$$

converges to zero. In conclusion, we have shown that Equation (7) holds and we deduce that

$$H(\beta) = \log k - \frac{\log k}{k^\alpha} + o \left(\frac{\log k}{k^\alpha} \right).$$

□

For this type of random quantum channels, we believe that this asymptotic bound is the best known so far. However, it does not yield a violation of the Holevo additivity conjecture.

In addition to the rigorous estimates obtained in this section, we made numerical experiments for various values of t and k based on the bounds given by Corollary 5.4 and Theorem 4.5. They did not yield examples violating the additivity for $p = 1$. From this, we conclude that either our random quantum channel model does not violate the Holevo additivity conjecture with high probability, or that our bounds of Corollary 5.4 and/or Theorem 4.5 can be improved.

ACKNOWLEDGMENTS

This paper was completed while one author (B.C.) was visiting the university of Tokyo and then the university of Wrocław and he thanks these two institutions for providing him with a very fruitful working environment. I.N. thanks Guillaume Aubrun for useful discussions.

B.C. was partly funded by ANR GranMa and ANR Galoisint. The research of both authors was supported in part by NSERC grants including grant RGPIN/341303-2007.

REFERENCES

- [1] Aubrun, G. and Nechita, I. *Catalytic majorization and l_p norms*. Comm. Math. Phys. 278 (2008), no. 1, 133–144.
- [2] Aubrun, G. and Nechita, I. *Stochastic domination for iterated convolutions and catalytic majorization*. To appear in Ann. Inst. H. Poincaré Probab. Statist.
- [3] Bengtsson, I., Życzkowski, K. *Geometry of quantum states. An introduction to quantum entanglement*. Cambridge University Press, Cambridge, 2006. xii+466 pp.
- [4] R. Bhatia, *Matrix Analysis*. Graduate Texts in Mathematics, 169. Springer-Verlag, New York, 1997.
- [5] Braunstein, S. L. *Geometry of quantum inference*. Phys. Lett. A 219 (1996), no. 3-4, 169–174.
- [6] Collins, B. *Product of random projections, Jacobi ensembles and universality problems arising from free probability* Probab. Theory Related Fields, 133(3):315344, 2005.
- [7] Collins, B. and Nechita, I. *Random quantum channels I: Graphical calculus and the Bell state phenomenon*. arXiv/0905.2313.
- [8] Collins, B. and Śniady, P. *Integration with respect to the Haar measure on unitary, orthogonal and symplectic group*. Comm. Math. Phys. 264 (2006), no. 3, 773–795.
- [9] Haagerup, U. and Thorbjørnsen, S. *A new application of random matrices: $\text{Ext}(C_{\text{red}}^*(F_2))$ is not a group*. Ann. of Math. (2) 162 (2005), no. 2, 711–775.
- [10] Hastings, M.B. *A Counterexample to Additivity of Minimum Output Entropy* arXiv/0809.3972v3, Nature Physics 5, 255 (2009)
- [11] Hayashi, M. *Quantum information. An introduction*. Springer-Verlag, Berlin, 2006.
- [12] Hayden, P. *The maximal p -norm multiplicativity conjecture is false* arXiv/0707.3291v1
- [13] Hayden, P., Leung, D. and Winter A. *Aspects of generic entanglement* Comm. Math. Phys. 265 (2006), 95–117.
- [14] Hayden, P. and Winter A. *Counterexamples to the maximal p -norm multiplicativity conjecture for all $p > 1$* . Comm. Math. Phys. 284 (2008), no. 1, 263–280.
- [15] Werner R. and Hoelvo, A. *Counterexample to an additivity conjecture for output purity of quantum channels*. Journal of Mathematical Physics 43, 4353–4357, 2002.
- [16] Ledoux, M. *Differential operators and spectral distributions of invariant ensembles from the classical orthogonal polynomials part I: the continuous case*. Elect. Journal in Probability 9, 177–208 (2004)
- [17] Nechita, I. *Asymptotics of random density matrices*. Ann. Henri Poincaré 8 (2007), no. 8, 1521–1538.
- [18] Nica, A and Speicher, R. *Lectures on the combinatorics of free probability*, volume 335 of London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 2006.
- [19] Voiculescu, D.V. *A strengthened asymptotic freeness result for random matrices with applications to free entropy* Internat. Math. Res. Notices, (1):4163, 1998.
- [20] Voiculescu, D.V., Dykema, K.J. and Nica, A. *Free random variables*, AMS (1992).
- [21] Życzkowski, K., Sommers, H.-J. *Induced measures in the space of mixed quantum states*. J. Phys. A 34 (2001), no. 35, 7111–7125.

DÉPARTEMENT DE MATHÉMATIQUE ET STATISTIQUE, UNIVERSITÉ D'OTTAWA, 585 KING EDWARD,
OTTAWA, ON, K1N6N5 CANADA AND CNRS, INSTITUT CAMILLE JORDAN UNIVERSITÉ LYON 1, 43 Bd
DU 11 NOVEMBRE 1918, 69622 VILLEURBANNE, FRANCE

E-mail address: `bcollins@uottawa.ca`

INSTITUT CAMILLE JORDAN UNIVERSITÉ LYON 1, 43 Bd DU 11 NOVEMBRE 1918, 69622 VILLEUR-
BANNE, FRANCE

E-mail address: `nechita@math.univ-lyon1.fr`