

Article

Eigenvalue and Entropy Statistics for Products of Conjugate Random Quantum Channels

Benoît Collins^{1,2} and Ion Nechita^{1,*}

¹ Department of Mathematics and Statistics, University of Ottawa, ON, Canada

² CNRS, Institut Camille Jordan, Université Lyon 1, France

* Author to whom correspondence should be addressed; E-Mail: inechita@uottawa.ca;
Tel.: +1 613 562 5800 x 2082; Fax: +1 613 562 5776.

Received: 4 May 2010; in revised form: 17 June 2010 / Accepted: 18 June 2010 /

Published: 23 June 2010

Abstract: Using the graphical calculus and integration techniques introduced by the authors, we study the statistical properties of outputs of products of random quantum channels for entangled inputs. In particular, we revisit and generalize models of relevance for the recent counterexamples to the minimum output entropy additivity problems. Our main result is a classification of regimes for which the von Neumann entropy is lower on average than the elementary bounds that can be obtained with linear algebra techniques.

Keywords: random quantum channels; weingarten calculus; minimum output entropy; von neumann entropy; additivity problem

1. Introduction

As in classical computer science, randomized proofs and constructions are ubiquitous in quantum information. Since quantum mechanics is non commutative, the random objects of study are matrices. Therefore, quantum information theory provides a rich source of random matrix problems.

One of the most important classes of problems in the mathematical aspects of quantum information theory is the study of data transmission through noisy quantum channels. A famous conjecture reduced the calculation of the channel capacity for classical data to the question of the additivity of Minimum channel Output Entropy. The conjecture was stated in 1999 by King and Ruskai [1] and shown to be equivalent to the additivity of the Holevo capacity (and to other quantities of interest) by Shor [2]. For

a long time, no counterexamples were available and additivity was proven to hold in many cases. A stronger, L^p version of this question was also available and relevant to operator algebra and operator space theory. This version was disproved by Hayden and Winter in 2007, for all $p > 1$ [3]. The original conjecture, regarding von Neumann entropies, was disproved by Hastings in 2008 [4]. His very innovative argument exploited the idea of tubular neighborhoods so as to considerably refine available estimates on random quantum channels. However, constructive, non-random counterexamples to any of these conjectures are still elusive.

The random counterexamples to the various forms of the additivity conjecture rely on bounds on the Minimum Output Entropies (MOE) for single and product channels that follow mainly from two important ideas. Let Φ be a random quantum channel between matrix spaces such that the dimensions of the input and output spaces are large enough. The first key idea is that, with high probability, the Minimum Output Entropy of Φ is almost maximal: all output states are highly mixed. On the other hand, if one considers the product channel $\Phi \otimes \bar{\Phi}$ (where $\bar{\Phi}$ is obtained by replacing the Stinespring unitary U defining the channel by its conjugate), then if one takes a maximally entangled (or Bell) state as an input, the output density matrix has *always* a large eigenvalue. This second important fact was observed by Winter, and it implies that the output state in question has low entropy, allowing for a violation of additivity.

Our work addresses bounds for conjugate product channels, and improves them in several cases. We provide a complete spectral description of the output of product channels when the input is maximally entangled. In [5] and [6], we have studied situations when the channels are conjugate ($\Phi \otimes \bar{\Phi}$) or independent ($\Phi \otimes \Psi$) in two different asymptotic regimes.

In this work, after recalling the aforementioned results and reviewing the techniques used in deriving them, we consider more general models of random quantum channels, from two different perspectives. We first generalize the linear scaling asymptotic regime to include the situations where the dimension of the input space is different from the dimension of the output of a quantum channel; however, all three parameters (the respective dimensions of the input, output and ancilla spaces) scale linearly. Then we move beyond the linear regime, considering situations where the dimensions of the output space and of the ancilla space scale in a non-linear fashion. Motivated by the search of improved bounds one may use in the study of additivity questions, we compute asymptotic expressions for the von Neumann entropies of output matrices for the models under consideration.

The paper is organized as follows: in Section 2, we first review the tools available to study moments of outputs of random quantum channels. These techniques were introduced in [7,8] and [5] and their first applications to quantum information theory were developed in [5,6] and [9]. In Section 3, we generalize the results of [6] to the case where the relative dimensions of the input and the output are different. In Section 4, we generalize the setting of [6] to the case where the relative dimensions of the input space and the ancilla space have relative polynomial growth. This is motivated by the recent results of [10], where the authors consider the case $k \sim n^{1/2}$ (n being the dimension of the input/output space and k being the dimension of the ancilla space). We show that depending on the growth, different results occur and that the case where the ancilla space and the input space have the same dimension has a potential for yielding a bigger violation for the additivity of the entropy. Finally, in Section 5, we use these results to provide new bounds for von Neumann entropy of the output of product random quantum channels.

2. Studying Moments of Outputs of Random Quantum Channels: Techniques and First Examples

In this section, we recall, for the convenience of the reader and for the sake of being self-contained, techniques to compute the eigenvalue distribution of random quantum channels, as well as a few results obtained recently with these techniques.

The techniques rely on Weingarten calculus (subsection 2.1) and on a graphical model (subsection 2.2). Then, in subsections 2.4 and 2.5, we recall two applications of these techniques.

2.1. Weingarten calculus

In this section, we recall a few facts about the Weingarten calculus, useful to evaluate averages with respect to the Haar measure on the unitary group.

Definition 2.1. The unitary Weingarten function $\text{Wg}(n, \sigma)$ is a function of a dimension parameter n and of a permutation σ in the symmetric group $\mathcal{S}_p$ on p elements, defined as the pseudo-inverse of the function $\sigma \mapsto n^{\#\sigma}$ under the convolution for the symmetric group ($\#\sigma$ denotes the number of cycles of the permutation σ).

Note that the function $\sigma \mapsto n^{\#\sigma}$ is invertible for $n \geq p$, (to see that it is invertible for n large enough, observe that it behaves like $n^p \delta_e$ as $n \rightarrow \infty$). In this case, we can replace the pseudo-inverse by the inverse. We refer to [8] for historical references and further details. We shall use the shorthand notation $\text{Wg}(\sigma) = \text{Wg}(n, \sigma)$ when the dimension parameter n is obvious.

The following theorem relates integrals with respect to the Haar measure on the unitary group (n) and the Weingarten function Wg . (see for example [11]):

Theorem 2.2. Let n be a positive integer and $(i_1, \dots, i_p)$, $(i'_1, \dots, i'_p)$, $(j_1, \dots, j_p)$, $(j'_1, \dots, j'_p)$ be p -tuples of positive integers from $\{1, 2, \dots, n\}$. Then

$$\int_{(n)} U_{i_1 j_1} \cdots U_{i_p j_p} \overline{U_{i'_1 j'_1}} \cdots \overline{U_{i'_p j'_p}} dU = \sum_{\sigma, \tau \in \mathcal{S}_p} \delta_{i_1 i'_{\sigma(1)}} \cdots \delta_{i_p i'_{\sigma(p)}} \delta_{j_1 j'_{\tau(1)}} \cdots \delta_{j_p j'_{\tau(p)}} \text{Wg}(n, \tau \sigma^{-1}) \quad (1)$$

If $p \neq p'$ then

$$\int_{(n)} U_{i_1 j_1} \cdots U_{i_p j_p} \overline{U_{i'_1 j'_1}} \cdots \overline{U_{i'_{p'} j'_{p'}}} dU = 0 \quad (2)$$

We are interested in the values of the Weingarten function in the limit $n \rightarrow \infty$. The following result encloses all the data we need for our computations about the asymptotics of the Wg function; see [11] for a proof.

Theorem 2.3. For a permutation $\sigma \in \mathcal{S}_p$, let $\text{Cycles}(\sigma)$ denote the set of cycles of σ . Then

$$\text{Wg}(n, \sigma) = (-1)^{n - \#\sigma} \prod_{c \in \text{Cycles}(\sigma)} \text{Wg}(n, c) (1 + O(n^{-2})) \quad (3)$$

and

$$\text{Wg}(n, (1, \dots, d)) = (-1)^{d-1} c_{d-1} \prod_{-d+1 \leq j \leq d-1} (n-j)^{-1} \quad (4)$$

where $c_i = \frac{(2i)!}{(i+1)!i!}$ is the i -th Catalan number.

The Catalan numbers and Wg are related to the Moebius function on the lattice of non-crossing partitions, as follows:

$$\text{Wg}(n, \sigma) = n^{-(p+|\sigma|)} (\text{Mob}(\sigma) + O(n^{-2})) \quad (5)$$

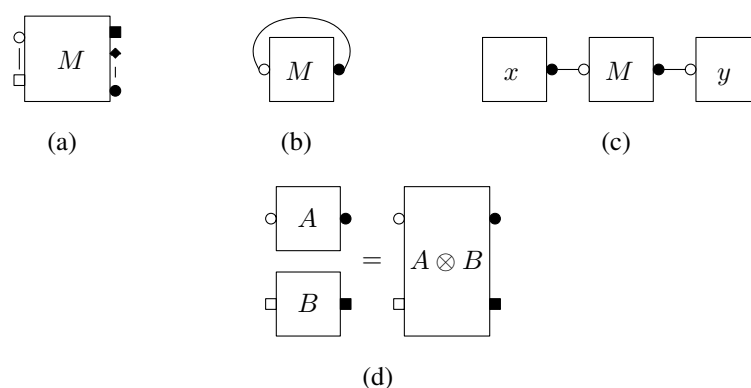
where $|\sigma| = p - \#\sigma$ is the *length* of σ , i.e., the minimal number of transpositions that multiply to σ . We refer to [8] for details about the function Mob.

2.2. Planar expansion

The purpose of the graphical calculus introduced in [5] is to yield an effective method to evaluate the expectation of random tensors with respect to the Haar measure on a unitary group. In graphical language, a tensor corresponds to a *box*, and an appropriate Hilbertian structure yields a correspondence between boxes and tensors. However, the calculus yielding expectations only relies on diagrammatic operations.

Each box B is represented as a rectangle with decorations on its boundary. The decorations are either white or black, and belong to $S(B) \sqcup S^*(B)$. Figure 1 depicts an example of boxes and diagrams.

Figure 1. Basic diagrams and axioms: (a) diagram for a general tensor M ; (b) trace of a $(1, 1)$ -tensor (matrix) M ; (c) Scalar product $\langle y | M | x \rangle$; (d) tensor product of two diagrams. The round, square and diamond-shaped labels correspond to pairs of dual finite dimensional complex Hilbert spaces.



It is possible to construct new boxes out of old ones by formal algebraic operations such as sums or products. We call *diagram* a picture consisting in boxes and wires according to the following rule: a wire may link a white decoration in $S(B)$ to its black counterpart in $S^*(B)$. A diagram can be turned into a box by choosing an orientation and a starting point.

Regarding the Hilbertian structure, wires correspond to tensor contractions. There exists an involution for boxes and diagrams. It is antilinear and it turns a decoration in $S(B)$ into its counterpart in $S^*(B)$. Our conventions are close to those of [12,13]. They should be familiar to the reader acquainted with

existing graphical calculus of various types (planar algebra theory, Feynman diagrams theory, traced category theory). Our notations are designed to fit well to the problem of computing expectations, as shown in the next section. In Figure 2(b), 2(c) and 2(d) we depict the trace of a matrix, multiplication of tensors and the tensor product operation. For details, we refer to [5].

The main application of our calculus is to compute expectation of diagrams where some boxes represent random matrices (e.g., Haar distributed or Gaussian). For this, we need a concept of *removal* of boxes U and $\bar{U}$. A removal r is a way to pair decorations of the U and $\bar{U}$ boxes appearing in a diagram. It therefore consists in a pairing α of the white decorations of U boxes with the white decorations of $\bar{U}$ boxes, together with a pairing β between the black decorations of U boxes and the black decorations of $\bar{U}$ boxes. Assuming that $\mathcal{D}$ contains p boxes of type U and that the boxes U (resp. $\bar{U}$) are labeled from 1 to p , then $r = (\alpha, \beta)$ where α, β are permutations of $\mathcal{S}_p$.

Given a removal $r \in \text{Rem}(\mathcal{D})$, we construct a new diagram $\mathcal{D}_r$ associated to r , which has the important property that it no longer contains boxes of type U or $\bar{U}$. One starts by erasing the boxes U and $\bar{U}$ but keeps the decorations attached to them. Assuming that one has labeled the erased boxes U and $\bar{U}$ with integers from $\{1, \dots, p\}$, one connects *all* the (inner parts of the) *white* decorations of the i -th erased U box with the corresponding (inner parts of the) *white* decorations of the $\alpha(i)$ -th erased $\bar{U}$ box. In a similar manner, one uses the permutation β to connect black decorations.

In [5], we proved the following result:

Theorem 2.4. *The following holds true:*

$$\mathbb{E}_U(\mathcal{D}) = \sum_{r=(\alpha,\beta) \in \text{Rem}_U(\mathcal{D})} \mathcal{D}_r \text{Wg}(n, \alpha\beta^{-1})$$

2.3. Wishart matrices, Marchenko-Pastur distributions and their entropy

We recall the definition of a *free Poisson* (or Marchenko-Pastur) random variable [14]. For $c > 0$, the probability measure

$$\pi_c = \max(1 - c, 0)\delta_0 + \frac{\sqrt{4c - (x - 1 - c)^2}}{2\pi x} \mathbf{1}_{[1+c-2\sqrt{c}, 1+c+2\sqrt{c}]}(x) dx$$

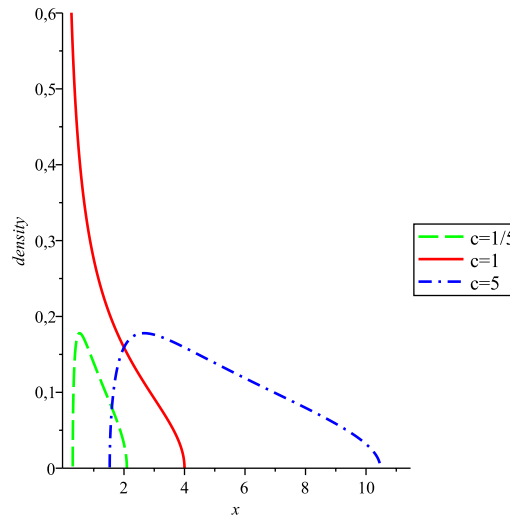
is called a free Poisson measure of parameter c . The plots of the densities for these measures are plotted in Figure 2.

The free Poisson distribution arises in random matrix theory as the almost sure limit of the eigenvalue counting distribution for Wishart matrices, *i.e.*, matrices $X_n X_n^*$ where X_n is an $n \times \lfloor cn \rfloor$ matrix whose entries are i.i.d. standard complex Gaussian random variables of variance $1/n$.

From a combinatorial perspective, the free Poisson distribution π_c has the nice property that all its *free* cumulants are equal to c . Hence, the free moment-cumulant formula (see [15], Lecture 11, pp. 173) reads

$$\int x^p d\pi_c(x) = \sum_{\sigma \in NC(p)} c^{\#\sigma} \quad (6)$$

Figure 2. Densities for the Marchenko-Pastur measures of parameters $c = 1/5$, $c = 1$ and $c = 5$. For $c = 1/5$, only the absolutely continuous part of the measure was plotted; $\pi_{1/5}$ has a Dirac mass of $4/5$ at $x = 0$ which is not represented.



where $\#\sigma$ denotes the number of blocks of the non-crossing partition σ . From the moment formula, one can obtain the value of the following integral, useful in the computation of von Neumann entropies [16]:

$$\int x \log x \, d\pi_c(x) = \begin{cases} \frac{1}{2} + c \log c & \text{if } c \geq 1 \\ \frac{c^2}{2} & \text{if } 0 < c < 1 \end{cases} \quad (7)$$

2.4. Application 1: Fixed ancilla space

The counterexamples to the additivity conjecture obtained so far arise from the random choice of a quantum channel from the ensemble

$$\Phi : \mathcal{M}_m() \rightarrow \mathcal{M}_n() \quad (8)$$

given by $\Phi(X) = \text{Tr}_k[U(X \otimes |0\rangle\langle 0|)U^*]$, where $U \in (nk)$ is a random unitary matrix and $|0\rangle\langle 0|$ is an ancilla rank-one projector. The counterexamples rely on the idea of using a tensor product of conjugate channels $\Phi \otimes \bar{\Phi}$ and, more precisely, the output of this channel when the input is the Bell state $(\{e_1, \dots, e_m\})$ is some fixed basis of m :

$$E_m = \frac{1}{m} \sum_{i,j=1}^m |e_i\rangle\langle e_j| \otimes |e_i\rangle\langle e_j| \quad (9)$$

In the regime where $m = tnk$ with n and k integers and $t \in (0, 1)$ a fixed parameter, we gave in [5] a complete spectral description of the (random) density matrix $[\Phi \otimes \bar{\Phi}](E_{tnk})$. The following result improves on the previously known bound of Winter, $\lambda_1 \geq t$:

Theorem 2.5. *Almost surely, as $n \rightarrow \infty$, the k^2 non-zero eigenvalues of the random matrix $[\Phi \otimes \bar{\Phi}](E_{tnk}) \in \mathcal{M}_{n^2}()$ converge towards the deterministic probability vector*

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

In the particular case $\Phi : \mathcal{M}_n() \rightarrow \mathcal{M}_n()$, corresponding to $kt = 1$, the eigenvalues are $\frac{1}{k} + \frac{1}{k^2} - \frac{1}{k^3}$, with multiplicity one and $\frac{1}{k^2} - \frac{1}{k^3}$, with multiplicity $k^2 - 1$. Not only the value of the largest eigenvalue is improved from $\frac{1}{k}$ to $\frac{1}{k} + \frac{1}{k^2} - \frac{1}{k^3}$, but the lower eigenvalues are also computed.

A better understanding of the spectrum of the output matrix for the product channel yields immediately better bounds for the Minimum Output Entropy of $\Phi \otimes \bar{\Phi}$. Applications of this result are twofold. First, it allows for violations of additivity of Rényi entropies, for all $p > 1$, just by using a qubit as an ancilla state for the input ($t = 1/2$). Second, the improvements on the bound for the entropy of the product channel can yield better minimum values of k needed to obtain violations of additivity for $p = 1$ (see [17,18]).

2.5. Application 2: Ancilla and input space of linear dimensions

Theorem 2.5 is highly non-intuitive: it is not clear why the small eigenvalues should all behave in the same way. Moreover, there was numerical evidence [3] that the spectrum should not be flat beyond the second eigenvalue. This raises the question of what happens when the ancilla space is not of fixed dimension, but rather of dimension comparable to the input space.

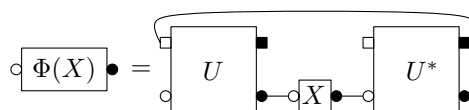
The study of such asymptotic regimes was initiated in [6]. After stating the main result obtained in that paper, we shall generalize in Section 3 the setting, allowing for the dimension of the input space to vary linearly with the dimension of the output.

In [6], Section 6.3, we considered random quantum channels $\Phi : \mathcal{M}_n() \rightarrow \mathcal{M}_n()$ obtained from random Haar unitary matrices $U \in (nk)$ via the Stinespring representation

$$\Phi(X) = \text{Tr}_k [U(X \otimes P_k)U^*] \quad (10)$$

where $P_k \in \mathcal{M}_k()$ is a non-random rank-one projector (pure state) and both n and k grow to infinity at a constant ratio $k/n \rightarrow c > 0$. The diagram for such a channel is represented in Figure 3.

Figure 3. Diagram for a quantum channel with equal input and output spaces. The state P_k of the ancilla space is omitted, since it has no role to play in the computations. Round labels attached to boxes correspond to input/output spaces n and square symbols correspond to ancilla spaces k .



For the regime where both n and k grow to infinity at a constant ratio c , the main result of [6] is as follows.

Theorem 2.6. Consider a pair of conjugate random quantum channels $\Phi, \bar{\Phi}$ in the regime where $n, k \rightarrow \infty$, $k \sim cn$. The eigenvalues $\lambda_1 \geq \dots \geq \lambda_{n^2}$ of the random matrix $Z_n = [\Phi \otimes \bar{\Phi}](E_n)$ are such that:

- The first eigenvalue satisfies $cn\lambda_1 \rightarrow 1$ (in probability).
- The distribution $\frac{1}{n^2-1} \sum_{i=2}^{n^2} \delta_{c^2 n^2 \lambda_i}$ converges a.s. to a free Poisson distribution of parameter c^2 .

Here we see that a new phenomenon of two different convergence rates for eigenvalues appears. This is due to the fact that the $U - \bar{U}$ model for the product channel contains the “conjugation” symmetry. Instead of considering a channel and its complex conjugate, we looked in [6] at two independent quantum channels, taken from the same ensemble.

Theorem 2.7. In the regime $k \sim cn$, $n \rightarrow \infty$, let $Z_n = [\Phi \otimes \Psi](E_n)$ be the output of the product of two independent quantum channels Φ and Ψ , when the input is a maximally entangled state E_n . Then, almost surely, the distribution of the rescaled output matrix $c^2 n^2 Z_n$ converges towards a free Poisson of parameter c^2 .

A striking feature of this asymptotic regime is that the von Neumann entropies of the $U - V$ and $U - \bar{U}$ models are almost the same. It is then natural to ask whether the $U - \bar{U}$ symmetry is in fact needed to obtain violations of the additivity. Indeed, it seems that the largest eigenvalue for the output of the product channel does not play a big role in the bounds for the entropy. Having counterexamples with independent channels will be an important step to a better understanding of additivity violations. Possible violations with independent channels would be generic, as opposed to conjugate-channels violations which are not. Also, these considerations give concrete hope that larger violations of additivity could be achieved.

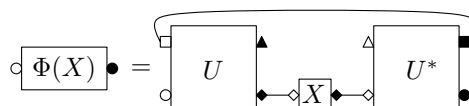
3. Generalized Linear Setting—Input and Output Spaces of Different Dimension

In this section, we generalize the model of quantum channels we have considered, by allowing input and output spaces of different dimensions. We consider random quantum channels $\Phi : \mathcal{M}_m() \rightarrow \mathcal{M}_n()$ defined by

$$\Phi(X) = \text{Tr}_k [U(X \otimes P_l)U^*] \quad (11)$$

where $l = nk/m$ and P_l is a deterministic rank-one projector in $\mathcal{M}_l()$; we tacitly assume that l is an integer. All three dimensions m, n and k grow to infinity, at constant ratios: $m/n \rightarrow b$ and $k/n \rightarrow c$, with $b, c \in (0, \infty)$ fixed constants. The generalized diagram corresponding to Φ is depicted in Figure 4.

Figure 4. Diagram for a quantum channel with different input and output spaces. Round labels attached to boxes correspond to output spaces n , square symbols correspond to ancilla spaces k and diamonds correspond to input spaces m . The rank-one projector P_l is omitted.

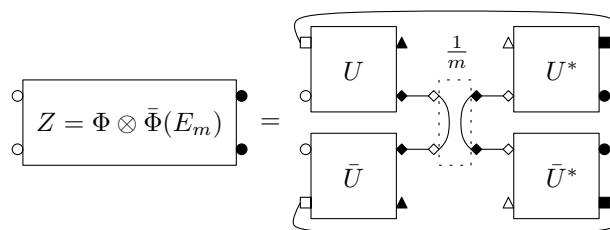


When presented with the maximally entangled (or Bell state) $E_m \in \mathcal{M}_{m^2}()$ as an input, the product conjugate channel $\Phi \otimes \bar{\Phi}$ produces a random density matrix

$$Z = [\Phi \otimes \bar{\Phi}](E_m) \in \mathcal{M}_{n^2}() \quad (12)$$

The remaining of this section is dedicated to the study of the random matrix Z , depicted in Figure 5. The analysis of the spectrum of Z follows closely corresponding results in [6], Section 6.3, which is a specialization of this section, in the case $m = n$ (i.e., $b = 1$). The spectral properties of the output random matrix Z are summarized in Theorem 3.4, the main result of this section. The reader is invited to compare the conclusions of Theorems 2.6 and 3.4.

Figure 5. Diagram for the output of a product of two conjugate channels, when the input is the maximally entangled state. The complex Hilbert spaces associated to labels are as follows: $\circ \bullet \rightsquigarrow^n$, $\square \blacksquare \rightsquigarrow^k$, $\diamond \blacklozenge \rightsquigarrow^m$ and $\triangle \blacktriangle \rightsquigarrow^l$.



The first step of our analysis of the output matrix is the computation of the asymptotic moments.

Proposition 3.1. Consider a sequence of random quantum channels Φ_n where $m, n, k \rightarrow \infty$, $m/n \rightarrow b$ and $k/n \rightarrow c$. The asymptotic moments of the output matrix $Z = [\Phi \otimes \bar{\Phi}](E_m)$ are given by:

$$\begin{aligned} \text{Tr}(Z) &= 1; \\ \mathbb{E} \text{Tr} \left[\left(\frac{c}{b} n Z \right)^2 \right] &= 1 + \frac{1}{b^2} + \frac{c^2}{b^2} + o(1) \\ \mathbb{E} \text{Tr} \left[\left(\frac{c}{b} n Z \right)^p \right] &= 1 + o(1), \quad \forall p \geq 3 \end{aligned}$$

Proof. The starting point of the proof is the following exact formula for the moments of the random matrix Z , obtained from the graph expansion technique detailed in [5]:

$$\mathbb{E}[\text{Tr}(Z^p)] = \sum_{\alpha, \beta \in \mathcal{S}_{2p}} k^{\# \alpha} n^{\#(\alpha \gamma^{-1})} m^{\#(\beta \delta) - p} \text{Wg}(\alpha \beta^{-1}) \quad (13)$$

where the permutations $\gamma, \delta \in \mathcal{S}_{2p}$ are defined as follows. We relabel the index set $\{1, 2, \dots, 2p\}$ as $\{p^B, \dots, 1^B, 1^T, 2^T, \dots, p^T\}$ in order to make precise the association of indices with blocks corresponding to the “top” channel Φ ($1^T, \dots, p^T$) and blocks corresponding to the “bottom” channel $\bar{\Phi}$ ($1^B, \dots, p^B$). With this notation, we define the permutations

$$\gamma(i^T) = (i-1)^T, \quad \gamma(i^B) = (i+1)^B \quad \text{and} \quad \delta(i^T) = i^B, \quad \delta(i^B) = i^T \quad (14)$$

Using the asymptotic expressions for the dimensions $m \sim bn$, $k \sim cn$ and for the Weingarten function (see Theorem 2.3)

$$\text{Wg}(\alpha \beta^{-1}) \sim (nk)^{-2p - |\alpha \beta^{-1}|} \text{Mob}(\alpha \beta^{-1}) \sim c^{-2p - |\alpha \beta^{-1}|} n^{-4p - 2|\alpha \beta^{-1}|} \text{Mob}(\alpha \beta^{-1}) \quad (15)$$

equation (13) becomes

$$\mathbb{E}[\text{Tr}(Z^p)] \sim \sum_{\alpha, \beta \in \mathcal{S}_{2p}} c^{-(|\alpha|+|\alpha\beta^{-1}|)} b^{p-|\beta\delta|} n^{-f(\alpha, \beta)} \text{Mob}(\alpha\beta^{-1}) \quad (16)$$

where the function $f(\alpha, \beta)$ is given by

$$f(\alpha, \beta) = |\alpha| + |\alpha\gamma^{-1}| + |\beta\delta| + 2|\alpha\beta^{-1}| - p \quad (17)$$

In order to find the dominating terms in the sums (13) or (16), one has to minimize the quantity $f(\alpha, \beta)$ over the permutation group $\mathcal{S}_{2p}$. This has been done in the proof of Theorem 6.8 of [6]:

- for $p = 1$, $f(\alpha, \beta) \geq 0$, with equality iff. $\alpha = \beta = \text{id}$;
- for $p = 2$, $f(\alpha, \beta) \geq p$, with equality iff. $\alpha = \beta \in \{\text{id}, \delta, \gamma\}$;
- for $p \geq 3$, $f(\alpha, \beta) \geq p$, with equality iff. $\alpha = \beta = \delta$.

One concludes now by plugging the optimal values for the permutations α and β into equation (16).

Theorem 3.1 only gives a partial description of the spectrum of the random matrix Z ; from the moment information one can deduce that there are some eigenvalues on the scale n^{-1} and that the rest of the spectrum is distributed on lower scales, such as n^{-2} . Obtaining information on the lower scale eigenvalues by brute force via the moment method is a difficult task, since their asymptotic contribution is negligible with respect to the contribution of the eigenvalue(s) on the scale n^{-1} . The trick we use to obtain information about the smaller eigenvalues is inspired by Hayden and Winter's proof of the existence of a *large* eigenvalue. Their proof contains, as a byproduct, some information on the eigenvector for the large eigenvalue. We introduce the orthogonal projection $Q = I - E$, where $E = E_n$ is the maximally entangled state on a product of two copies of the output space $n \otimes n$. Using the $(\text{rank } n^2 - 1)$ projector Q , we shall obtain some information on the smallest $n^2 - 1$ eigenvalues of the random output matrix Z , by analyzing the “compressed” matrix QZQ (which, in a suitable basis, corresponds to considering the $(1, 1)$ minor of Q).

Proposition 3.2. *Almost surely, the matrix $c^2 n^2 QZQ$ converges in distribution, to a free Poisson (or Marchenko-Pastur) law of parameter c^2 .*

Remark 3.3. By ‘almost surely’, we mean with probability one, in any probability space on which the whole sequence (indexed by the input dimension) of random quantum channels is defined. In this paper, we supply no proofs of almost sure convergence results, as they require further -not so enlightening- technicalities. We refer the interested reader to the appendix of [6] for details. Let us just mention that the proofs rely on the Borel-Cantelli lemma. More precisely, one proves that the covariance of any moment behaves as $O(n^{-2})$ as the dimension goes to infinity. The fact that $O(n^{-2})$ is summable over n makes it possible to use the Borel-Cantelli lemma.

To prove this result, one can use the arguments of Theorem 6.9 from [6] *mutatis mutandis*. The method of moments is employed by computing the moments of the random matrix $c^2 n^2 QZQ$ and showing that they converge to the corresponding moments of the free Poisson distribution of parameter c^2 :

$$\lim_{n \rightarrow \infty} \frac{1}{n^2} \mathbb{E}[\text{Tr}(c^2 n^2 QZQ)^p] = \int x^p d\pi_{c^2}(x) \quad (18)$$

The reader can note that the parameter b (describing the size of the entangled input) has no influence on the lower part of the spectrum. It only appears in the expression of the largest eigenvalue of Z , as stated in the following Theorem, which is the main result of this section.

Theorem 3.4. *Consider a pair of conjugate random quantum channels $\Phi, \bar{\Phi}$ in the regime where $m, n, k \rightarrow \infty$, $m \sim bn$ and $k \sim cn$. The eigenvalues $\lambda_1 \geq \dots \geq \lambda_{n^2}$ of the random matrix $Z_n = [\Phi \otimes \bar{\Phi}](E_m)$ are such that:*

- *The first eigenvalue satisfies $(c/b)n\lambda_1 \rightarrow 1$ in probability.*
- *The distribution $\frac{1}{n^2-1} \sum_{i=2}^{n^2} \delta_{c^2 n^2 \lambda_i}$ converges almost surely to a free Poisson distribution of parameter c^2 .*

The proof of this result combines Theorems 3.1, 3.2 and Cauchy's interlacing theorem ([19], Corollary III.1.5).

Remark 3.5. *The almost sure convergence argument described in Remark 3.3 does not extend to the first item of Theorem 3.4, as the covariances tend to zero but are not summable.*

4. Non-linear Output Dimension

In this section we generalize the “linear” model of [6] in a different direction than we did in Section 3. We shall consider random quantum channels $\Phi : \mathcal{M}_n() \rightarrow \mathcal{M}_n()$ defined by the Stinespring representation (10), where the dimension of the ancilla space k scales with n in a non-linear fashion:

$$k \sim cn^d, \quad \text{when } n \rightarrow \infty \quad (19)$$

Here, $c > 0$ and $d \geq 0$ are two real parameters of the model. As before, we are interested in the spectral properties of the random matrix $Z = [\Phi \otimes \bar{\Phi}](E_n)$, where E_n is the rank-one projection on the maximally entangled state in the input space of the product channel, ${}^n \otimes {}^n$.

Before performing a detailed analysis of the spectrum of Z , let us make some observations on the role of the parameters c and d , as well as on several particular cases already treated in the literature. Generally, in such models, the parameter c will play the role of a *scaling* parameter in the limiting spectral distribution. This phenomenon can be observed in [20], Theorem 5 or in [6], Theorem 6.11. On the other hand, the exponent parameter d will have a more *qualitative* role to play, as it will decide the type of behavior of the spectrum of the random matrix Z .

Several particular cases of this very general model of random quantum channels have already been studied in the literature. In [5], we studied the case where the dimension k of the ancillary system is fixed, which corresponds in our setting to the case $d = 0$ (hence $k = c$). It has been shown (Section 2.4, Theorem 2.5) that in this situation, the random matrix Z has one large eigenvalue ($\lambda_1 = k^{-1} + k^{-2} - k^{-3}$) and that the rest of the spectrum is “flat”: $\lambda_2 = \dots = \lambda_{k^2} = k^{-2} - k^{-3}$. In [6], the case $d = 1$ was investigated; this corresponds to a coupling with an ancilla space of dimension k which scales as $k \sim cn$. The situation was rather different in this case: one large eigenvalue of size $(cn)^{-1}$ was observed, and the lower spectrum was not flat, having a free Poisson π_{c^2} shape. As a final remark, note that the model under study here is different than the one in Section 3, where inputs of arbitrary size were considered.

The main result of this section is the following theorem, which classifies the spectral behavior of the output random matrix Z in terms of the parameter d .

Proposition 4.1. *The asymptotic moments of the random output matrix $Z = [\Phi \otimes \bar{\Phi}](E_n)$ are given by:*

1. *If $d = 0$ (see [5]):*

$$\mathbb{E}[\text{Tr}(Z^p)] = \left(\frac{1}{c} + \frac{1}{c^2} - \frac{1}{c^3}\right)^p + (c^2 - 1) \left(\frac{1}{c^2} - \frac{1}{c^3}\right)^p + o(1) \quad \forall p \geq 2 \quad (20)$$

2. *If $d \in (0, 1)$:*

$$\begin{aligned} \mathbb{E}[\text{Tr}(Z^p)] &\sim 2c^{-2}n^{-2d} \sim 2k^{-2} & \text{if } p = 2 \\ \mathbb{E}[\text{Tr}(Z^p)] &\sim c^{-p}n^{-dp} \sim k^{-p} & \forall p \geq 3 \end{aligned} \quad (21)$$

3. *If $d = 1$ (see [6]):*

$$\begin{aligned} \mathbb{E}[\text{Tr}(Z^p)] &\sim (1 + 2c^{-2})n^{-2} & \text{if } p = 2 \\ \mathbb{E}[\text{Tr}(Z^p)] &\sim c^{-p}n^{-dp} \sim k^{-p} & \forall p \geq 3 \end{aligned} \quad (22)$$

4. *If $d \in (1, 2)$:*

$$\begin{aligned} \mathbb{E}[\text{Tr}(Z^p)] &\sim n^{-(2p-2)} & \text{if } p < \frac{2}{2-d} \\ \mathbb{E}[\text{Tr}(Z^p)] &\sim (1 + c^{-p})n^{-dp} \sim (1 + c^{-p})n^{-(2p-2)} & \text{if } p = \frac{2}{2-d} \\ \mathbb{E}[\text{Tr}(Z^p)] &\sim c^{-p}n^{-dp} \sim k^{-p} & \text{if } p > \frac{2}{2-d} \end{aligned} \quad (23)$$

5. *If $d \geq 2$:*

$$\mathbb{E}[\text{Tr}(Z^p)] \sim n^{-(2p-2)} \quad \forall p \geq 2 \quad (24)$$

Proof. The starting point of the proof is the following exact moment formula, obtained via the graphical calculus introduced in [5] and the Weingarten formula:

$$\mathbb{E}[\text{Tr}(Z^p)] = \sum_{\alpha, \beta \in \mathcal{S}_{2p}} k^{\#\alpha} n^{\#(\alpha\gamma^{-1}) + \#(\beta\delta) - p} \text{Wg}(\alpha\beta^{-1}) \quad (25)$$

After using the asymptotic expression for the ancillary dimension $k \sim cn^d$ and the Weingarten function

$$\begin{aligned} \text{Wg}(\alpha\beta^{-1}) &\sim (nk)^{-2p - |\alpha\beta^{-1}|} \text{Mob}(\alpha\beta^{-1}) \\ &\sim c^{-2p - |\alpha\beta^{-1}|} n^{-(d+1)(2p + |\alpha\beta^{-1}|)} \text{Mob}(\alpha\beta^{-1}) \end{aligned} \quad (26)$$

we obtain the following expression (which holds if the right-hand-side is non-zero):

$$\mathbb{E}[\text{Tr}(Z^p)] \sim \sum_{\alpha, \beta \in \mathcal{S}_{2p}} c^{-(|\alpha| + |\alpha\beta^{-1}|)} n^{-S(\alpha, \beta)} \text{Mob}(\alpha\beta^{-1}) \quad (27)$$

where $S(\alpha, \beta)$ is the exponent of n in the preceding sum:

$$S(\alpha, \beta) = d|\alpha| + |\alpha\gamma^{-1}| + |\beta\delta| + (d+1)|\alpha\beta^{-1}| - p \quad (28)$$

In this proof, since the permutation δ is a product of disjoint transpositions, thus an involution, we shall use the fact that $|\alpha\delta| = |\alpha\delta^{-1}| = |\alpha^{-1}\delta|$. In order to find the dominating terms in the sum (27), one has to minimize the quantity $S(\alpha, \beta)$ over $\mathcal{S}_{2p}^2$. The solution to this problem is obtained in three steps. First, using the following triangular inequalities:

$$\begin{aligned} |\alpha| + |\alpha\beta^{-1}| &\geq |\beta|, \\ |\alpha\gamma^{-1}| + |\alpha\beta^{-1}| &\geq |\beta\gamma^{-1}| \end{aligned} \quad (29)$$

we obtain that

$$S(\alpha, \beta) \geq d|\beta| + |\beta\gamma^{-1}| + |\beta\delta| - p =: S_1(\beta) \quad (30)$$

where the inequality can be saturated if, e.g., $\alpha = \beta$. The minimization problem for the S_1 function, although much simpler than the two-variable problem for S , can be further simplified by replacing the two-cycle permutation γ with the full-cycle:

$$\text{minimize} \quad S_2(\beta) = d|\beta| + |\beta\tilde{\gamma}^{-1}| + |\beta\delta| - p \quad (31)$$

where $\tilde{\gamma} = (p^T \dots 2^T \ 1^T \ 1^B \ 2^B \dots p^B)$. Since the permutation δ is an element of the geodesic $\text{id} \rightarrow \tilde{\gamma}$, the solution for the S_2 minimization problem is easy to find using one or more of the following inequalities:

$$\begin{aligned} |\beta| &\geq 0; \\ |\beta| + |\beta\tilde{\gamma}^{-1}| &\geq |\tilde{\gamma}| = 2p - 1 \\ |\beta\delta| + |\beta\tilde{\gamma}^{-1}| &\geq |\delta\tilde{\gamma}^{-1}| = p - 1 \end{aligned} \quad (32)$$

The solution for the S_2 problem, in terms of the value of the parameter d , is summarized in Table 1.

Table 1. Solution to the S_2 minimization problem of equation (31).

d	Minorant for $S_2(\beta)$	Equality cases
0	-1	$\{\delta \rightarrow \tilde{\gamma}\}$
$(0, 2)$	$dp - 1$	δ
2	$2p - 1$	$\{\text{id} \rightarrow \delta\}$
$(2, \infty)$	$2p - 1$	id

Next, we move towards finding the minimum of $S_1(\beta)$, defined in equation (30). The permutations γ and $\tilde{\gamma}$ are at distance one:

$$\gamma = \tilde{\gamma} \cdot (1^B \ p^T) \quad (33)$$

hence the same holds for $\beta\gamma^{-1}$ and $\beta\tilde{\gamma}^{-1}$. We have thus $S_1(\beta) = S_2(\beta) \pm 1$ and, even more precisely,

$$S_1(\beta) = \begin{cases} S_2(\beta) - 1 & \text{if } 1^B \text{ and } p^T \text{ are in the same block of } \beta\tilde{\gamma}^{-1} \\ S_2(\beta) + 1 & \text{otherwise} \end{cases} \quad (34)$$

In the same manner that is was argued in [6], p^T and 1^B belong to the same block of $\beta\tilde{\gamma}^{-1}$ if and only if $\beta \leq \gamma$ (the permutations being compared with the partial order relation on the corresponding non-crossing partitions). Analyzing the different equality cases in Table 1 and using the fact that the unique element of the geodesic set $\{\text{id} \rightarrow \delta\}$ which is smaller than γ is $\beta = \text{id}$, we conclude that, for $d \geq 2$, $S_1(\beta) \geq 2p - 2$, with equality iff. $\beta = \text{id}$. The case $d \in [0, 2)$ is more intricate, since one cannot have $S_1(\beta) = S_2(\beta) - 1$ and saturate at the same time the lower bound for S_2 .

For $d = 0$, it was shown in [5] that $S_1(\beta) \geq 0$, with equality iff $\beta \in \{\delta, \gamma\}$. Choose $d \in (0, 1]$ and consider $\beta \in \mathcal{S}_{2p}$ such that $S_1(\beta) = S_2(\beta) - 1$. Then, since $\beta \leq \gamma$, one has $|\beta\delta| \geq p$ and thus

$$\begin{aligned} S_1(\beta) &= S_2(\beta) - 1 = d|\beta| + |\beta\gamma^{-1}| + |\beta\delta| - p - 1 \\ &= d(|\beta| + |\beta\gamma^{-1}|) + (1 - d)|\beta\gamma^{-1}| + |\beta\delta| - p - 1 \\ &\geq d(2p - 1) + (1 - d) + p - p - 1 = d(2p - 2) \end{aligned} \quad (35)$$

We conclude that, for $d \in (0, 1]$, $p \geq 3$ and β such that $S_1(\beta) = S_2(\beta) - 1$, $S_1(\beta) > S_1(\delta) = dp$. Thus, for $d \in (0, 1]$ and $p \geq 3$, the minimum dp is attained only at the point $\beta = \delta$. For $p = 2$, an exhaustive search in S_4 reveals that, for $d \in (0, 1)$, $S_1(\beta) \geq dp$, with equality iff $\beta = \delta, \gamma$, and, for $d = 1$, $S_1(\beta) \geq p$, with equality iff $\beta = \text{id}, \delta, \gamma$.

In the case $d \in (1, 2)$, the situation is different. We shall consider three cases:

1. $\beta \notin \{\text{id} \rightarrow \tilde{\gamma}\}$. Since β is not a geodesic permutation, we have that $|\beta| + |\beta\tilde{\gamma}^{-1}| \geq 2p + 1$, $|\beta| + |\beta\delta| \geq p + 2$, $|\beta| \geq 1$ and $|\beta\delta| \geq 1$. It follows that

$$\begin{aligned} S_1(\beta) &\geq S_2(\beta) - 1 \geq |\beta| + |\beta\tilde{\gamma}^{-1}| + (d - 1)(|\beta| + |\beta\delta|) + (2 - d)|\beta\delta| - p - 1 \\ &\geq 2p + 1 + (d - 1)(p + 2) + (2 - d) - p - 1 = dp + d > dp = S_1(\delta) \end{aligned} \quad (36)$$

2. $\beta \in \{\text{id} \rightarrow \gamma\}$. In this situation, $S_1(\beta) = S_2(\beta) - 1$ and thus (we use the fact that $|\beta\delta| \geq p$ in this case)

$$\begin{aligned} S_1(\beta) &= S_2(\beta) - 1 \geq |\beta| + |\beta\tilde{\gamma}^{-1}| + (d - 1)|\beta| + |\beta\delta| - p - 1 \\ &\geq 2p - 1 + 0 + p - p - 1 \geq 2p - 2 = S_1(\text{id}) \end{aligned} \quad (37)$$

with equality iff. $\beta = \text{id}$.

3. $\beta \in \{\text{id} \rightarrow \tilde{\gamma}\}$, $\beta \notin \{\text{id} \rightarrow \gamma\}$. In this situation, $S_1(\beta) = S_2(\beta) + 1$ and thus

$$\begin{aligned} S_1(\beta) &= S_2(\beta) + 1 \geq |\beta| + |\beta\tilde{\gamma}^{-1}| + (d - 1)(|\beta| + |\beta\delta|) + (2 - d)|\beta\delta| - p + 1 \\ &\geq 2p - 1 + (d - 1)p + (d - 2)0 - p + 1 \geq dp = S_1(\delta) \end{aligned} \quad (38)$$

with equality iff. $\beta = \delta$.

Analyzing the three cases, we conclude that if $p \leq 2/(2 - d)$, we have $S_1(\beta) \geq 2p - 2$, otherwise $S_1(\beta) \geq dp$, the unique minimizers being respectively $\beta = \text{id}$, $\beta = \delta$ and $\beta \in \{\text{id}, \delta\}$ for the interface case $p = 2/(2 - d)$. The answer to the S_1 minimization problem is summarized in Table 2.

In order to solve the initial problem for the two-variable function $S(\alpha, \beta)$, one needs to notice that, for a fixed value of β , the only possibility to saturate the inequalities (29) at the same time is $\alpha = \beta$. Since,

Table 2. Solution to the S_1 minimization problem of equation (30).

d	Minorant for $S_1(\beta)$	Equality cases
0	0	$\{\delta \rightarrow \gamma\}$
$(0, 1)$ ($p = 2$)	$2d$	δ, γ
1 ($p = 2$)	2	id, δ, γ
$(0, 1]$ ($p \geq 3$)	dp	δ
$(1, 2)$ ($p < \frac{2}{2-d}$)	$2p - 2$	id
$(1, 2)$ ($p = \frac{2}{2-d}$)	$2p - 2 = dp$	id, δ
$(1, 2)$ ($p > \frac{2}{2-d}$)	dp	δ
$[2, \infty)$	$2p - 2$	id

for $d > 0$, both these inequalities are used to go from S to S_1 , we conclude that for strictly positive d , the solution for the S minimization problem can be found in Table 2, with $\alpha = \beta$. The solution for $d = 0$ has been entirely described in [5]. One concludes by replacing the values for the minimizing permutations into equation (27).

In the cases $d = 0$ and $d \geq 2$, the behavior of the eigenvalues can be easily deduced from the moment information, since one can identify in the formulas the moments of some probability distribution. In the case $d = 0$, as it was argued in [5], the largest eigenvalue of Z converges to $\frac{1}{c} + \frac{1}{c^2} - \frac{1}{c^3}$ and the $k^2 - 1$ others converge to $\frac{1}{c^2} - \frac{1}{c^3}$. Such a behavior is typical for the model we study, with a spectrum containing one large eigenvalue and $k^2 - 1$ (or $n^2 - 1$) identical smaller eigenvalues. The case $d \geq 2$ is somehow atypical: all the n^2 eigenvalues behave like n^{-2} . This is due to the fact that the “large” eigenvalue, which usually behaves as k^{-1} has no contribution asymptotically. We summarize these facts in the following proposition.

Proposition 4.2. *In the regime $d = 0$ (which corresponds to considering a fixed ancilla dimension $k = c$), the eigenvalues of the random matrix Z are such that, almost surely, in the limit $n \rightarrow \infty$,*

$$\lambda_1 \rightarrow \frac{1}{c} + \frac{1}{c^2} - \frac{1}{c^3} \quad \text{and} \quad \lambda_2, \dots, \lambda_{k^2} \rightarrow \frac{1}{c^2} - \frac{1}{c^3} \quad (39)$$

In the regime $d \geq 2$, the (rescaled) empirical spectral distribution of Z converges to the Dirac mass at 1, δ_1 :

$$\lim_{n \rightarrow \infty} \frac{1}{n^2} \sum_{i=1}^{n^2} \delta_{n^2 \lambda_i} = \delta_1 \quad (40)$$

As in Section 3, in order to understand fully the eigenvalues of the random matrix Z , we need to understand the lower part of the spectrum, in the remaining cases $d \in (0, 1)$ and $d \in (1, 2)$ (the case $d = 1$ being treated in [6]). This is done by “pinching” the matrix Z by the projector $Q = I - E_n$, orthogonal to the maximally entangled state E_n .

Proposition 4.3. *The matrix $k^2 Q Z Q$ converges, in moments, to the Dirac mass at I , δ_1 .*

Proof. We follow the idea of the proof of Theorem 6.10 in [6], compute the moments of the rank k^2 matrix $k^2 Q Z Q$, and show that they converge to the corresponding moments of the limit law:

$$\lim_{n \rightarrow \infty} \frac{1}{k^2} \mathbb{E}[\text{Tr}(k^2 Q Z Q)^p] = 1 \quad (41)$$

After replacing $Q = I - E$ and developing the product, we get

$$\begin{aligned} \frac{1}{k^2} \mathbb{E}[\text{Tr}(k^2 Q Z Q)^p] &= k^{2p-2} \mathbb{E}[\text{Tr}(I - E) Z (I - E) Z \cdots (I - E) Z] \\ &= c^{2p} n^{2p-2} \sum_{f \in \mathcal{F}_p} (-1)^{|f^{-1}(E)|} n^{-|f^{-1}(E)|} \mathbb{E}[\text{Tr} f(1) Z f(2) Z \cdots f(p) Z] \end{aligned} \quad (42)$$

where $\mathcal{F}$ is a set of the 2^p choice functions $f : \{1, 2, \dots, p\} \rightarrow \{I, E\}$. The factor $n^{-|f^{-1}(E)|}$ is due to the normalization of the Bell states $E = E_n$. The moment $\mathbb{E}[\text{Tr} f(1) Z f(2) Z \cdots f(p) Z]$ is computed via the graphical Weingarten calculus:

$$\mathbb{E}[\text{Tr} f(1) Z f(2) Z \cdots f(p) Z] = \sum_{\alpha, \beta \in \mathcal{S}_{2p}} k^{\#\alpha} n^{\#(\alpha \hat{f}^{-1}) + \#(\beta \delta) - p} \text{Wg}(\alpha \beta^{-1}) \quad (43)$$

where $\hat{f} \in \mathcal{S}_{2p}$ is the permutation associated to the choice function $f \in \mathcal{F}_p$ describing the way f connects the different instances of the channel (the arithmetic operations of indices i should be understood modulo p):

$$\begin{aligned} i^T &\xrightarrow{\hat{f}} \begin{cases} (i-1)^T & \text{if } f(i) = I \\ i^B & \text{if } f(i) = E \end{cases} \\ i^B &\xrightarrow{\hat{f}} \begin{cases} (i+1)^B & \text{if } f(i+1) = I \\ i^T & \text{if } f(i+1) = E \end{cases} \end{aligned}$$

Exactly as in the proof of Theorem 6.10 from [5], one has to understand the possible cancellations of high powers in n . In order to do this, we rewrite the non-asymptotic equation (42) as

$$\frac{1}{k^2} \mathbb{E}[\text{Tr}(k^2 Q Z Q)^p] = \sum_{\alpha, \beta \in \mathcal{S}_{2p}} k^{4p - |\alpha| - 2} n^{3p - |\beta \delta|} \text{Wg}(\alpha \beta^{-1}) \sum_{f \in \mathcal{F}_p} (-1)^{|f^{-1}(E)|} n^{-(|f^{-1}(E)| + |\alpha \hat{f}^{-1}|)}. \quad (44)$$

As in [5], we can show that for all permutations $\alpha \in \mathcal{V}$, the sum over all choices $f \in \mathcal{F}_p$ is exactly zero, where

$$\begin{aligned} \mathcal{V} &= \{\sigma \in \mathcal{S}_{2p} \mid \exists i \in \{1, \dots, p\} \text{ s.t. } \sigma(i^T) = i^B \text{ or } \sigma(i^B) = i^T\} \\ &= \{\sigma \in \mathcal{S}_{2p} \mid \sigma \delta \text{ has at least one fixed point}\} \end{aligned} \quad (45)$$

Hence,

$$\frac{1}{k^2} \mathbb{E}[\text{Tr}(k^2 Q Z Q)^p] \sim \sum_{f \in \mathcal{F}_p, \alpha, \beta \in \mathcal{S}_{2p}, \alpha \notin \mathcal{V}} (-1)^{|f^{-1}(E)|} c^{2p-2-(|\alpha|+|\alpha \beta^{-1}|)} n^{-S(\alpha, \beta, f)} \text{Mob}(\alpha \beta^{-1}) \quad (46)$$

where

$$S(\alpha, \beta, f) = |\beta\delta| + d|\alpha| + (d+1)|\alpha\beta^{-1}| + |f^{-1}(E)| + |\alpha\hat{f}^{-1}| - p(2d+1) + 2d \quad (47)$$

Since $\alpha \notin \mathcal{V}$, $\alpha\delta$ has no fixed point, and hence $|\alpha\delta| \geq p$. Using the facts that $|\alpha\beta^{-1}| + |\beta\delta| \geq |\alpha\delta|$, $|\alpha\beta^{-1}| \geq 0$ and $|\alpha| + |\alpha\hat{f}^{-1}| \geq |\hat{f}|$, we obtain that

$$S(\alpha, \beta, f) \geq |f^{-1}(E)| + d|\hat{f}| + (1-d)|\alpha\hat{f}^{-1}| - 2dp + 2d,$$

with equality if and only if $\alpha = \beta \in \{\text{id} \rightarrow \hat{f}\}$.

The number of cycles of $\hat{f}$ is easily shown to be:

$$\#\hat{f} = \begin{cases} 2 & \text{if } f \equiv \text{I}, \\ |f^{-1}(E)| & \text{otherwise} \end{cases} \quad (48)$$

hence, $|f^{-1}(E)| + d|\hat{f}| \geq 2dp - 2d$, with equality iff $f \equiv \text{I}$. We can conclude that $S(\alpha, \beta, f) \geq 0$, with equality if and only if $\alpha = \beta = \hat{\text{I}} = \gamma$. Replacing these values in equation (46), we obtain the announced result.

Using Cauchy's interlacing theorem ([19], Corollary III.1.5) for the eigenvalues of QZQ and those of Z , we obtain the complete description of the spectrum of the random output matrix.

Theorem 4.4. *In the regime $k \sim cn^d$, with $d \in (0, 1)$, the eigenvalues $\lambda_1 \geq \dots \geq \lambda_{n^2}$ of $Z = [\Phi \otimes \bar{\Phi}](E_n)$ satisfy:*

- In probability, $k\lambda_1 \rightarrow 1$.
- Almost surely, $\frac{1}{k^2-1} \sum_{i=2}^{k^2} \delta_{k^2\lambda_i}$ converges in distribution to the Dirac mass at 1, δ_1 .
- The remaining $n^2 - k^2$ eigenvalues are null: $\lambda_{k^2+1} = \dots = \lambda_{n^2} = 0$.

We finally treat the regime $d \in (1, 2)$, stating the results and underlining the (small) differences between the proofs in this case and the proofs of Proposition 4.3 and, respectively, of Theorem 4.4.

Proposition 4.5. *In the regime $d \in (1, 2)$, the matrix n^2QZQ converges, in moments, to the Dirac mass at 1, δ_1 .*

Proof. As in the proof of Proposition 4.3, we obtain

$$\frac{1}{n^2} \mathbb{E}[\text{Tr}(n^2QZQ)^p] \sim \sum_{f \in \mathcal{F}_p, \alpha, \beta \in \mathcal{S}_{2p}, \alpha \notin \mathcal{V}} (-1)^{|f^{-1}(E)|} c^{-(|\alpha| + |\alpha\beta^{-1}|)} n^{-S(\alpha, \beta, f)} \text{Mob}(\alpha\beta^{-1}) \quad (49)$$

where

$$S(\alpha, \beta, f) = |\beta\delta| + d|\alpha| + (d+1)|\alpha\beta^{-1}| + |f^{-1}(E)| + |\alpha\hat{f}^{-1}| - 3p + 2 \quad (50)$$

Using the same arguments as before, we obtain that

$$S(\alpha, \beta, f) \geq |f^{-1}(E)| + |\hat{f}| + (d-1)|\alpha| - 2p + 2,$$

with equality if and only if $\alpha = \beta \in \{\text{id} \rightarrow \hat{f}\}$.

Counting the number of cycles of $\hat{f}$, we have that $|f^{-1}(E)| + |\hat{f}| \geq 2p - 2$, with equality iff $f \equiv \text{I}$. We conclude that $S(\alpha, \beta, f) \geq 0$, with equality if and only if $\alpha = \beta = \text{id}$. The result follows by plugging the minimizing values into the asymptotic expression (49).

Theorem 4.6. *In the regime $k \sim cn^d$, with $d \in (1, 2)$, the eigenvalues $\lambda_1 \geq \dots \geq \lambda_{n^2}$ of $Z = [\Phi \otimes \bar{\Phi}](E_n)$ satisfy:*

- *In probability, $k\lambda_1 \rightarrow 1$.*
- *Almost surely, $\frac{1}{n^2-1} \sum_{i=2}^{n^2} \delta_{n^2\lambda_i}$ converges in distribution to the Dirac mass at 1, δ_1 .*

5. Asymptotics of the Von Neumann Entropy

Using the moment information and the behavior of the lower part of the spectrum deduced in Section 4, we now analyze the von Neumann entropy of the random output matrix Z :

$$H(Z) = - \sum_{i=1}^{n^2} \lambda_i \log \lambda_i \quad (51)$$

In the physical literature, the idea of using conjugate quantum channels to tackle important questions, such as the additivity of the minimum output entropy for quantum channels, dates back to the work of A. Winter and P. Hayden [3]. To bound the entropy of Z , they use the following fact, coming from linear algebra, which is independent of the random model used: the largest eigenvalue of Z is larger than the inverse of the dimension of the ancilla space, $\lambda_1 \geq 1/k$. This bound (which is actually a bound on the operator norm of Z) yields the following bound on the von Neumann entropy:

$$H(Z) \leq 2 \log k - \frac{\log k}{k} + \frac{1}{k} \quad (52)$$

One of the main applications of the results in this paper is the fact that our exact spectral information yield better upper bounds for the von Neumann entropy in some specific cases.

Theorem 5.1. *The asymptotic von Neumann entropy of the random output matrix $Z = [\Phi \otimes \bar{\Phi}](E_n)$ is given by:*

1. *If $d = 0$ ($k = c$ is an integer):*

$$H(Z) = - \left(\frac{1}{c} + \frac{1}{c^2} - \frac{1}{c^3} \right) \log \left(\frac{1}{c} + \frac{1}{c^2} - \frac{1}{c^3} \right) - (c^2 - 1) \left(\frac{1}{c^2} - \frac{1}{c^3} \right) \log \left(\frac{1}{c^2} - \frac{1}{c^3} \right) + o(1) \quad (53)$$

2. *If $d \in (0, 1)$:*

$$H(Z) = 2 \log k + o(1) \quad (54)$$

3. *If $d = 1$ (see [6]):*

$$H(Z) = \begin{cases} 2 \log k - \frac{c^2}{2} + o(1) & \text{if } 0 < c < 1, \\ 2 \log n - \frac{1}{2c^2} + o(1) & \text{if } c \geq 1 \end{cases} \quad (55)$$

4. *If $d \in (1, 2)$:*

$$H(Z) = 2 \log n + o(1) \quad (56)$$

5. If $d \geq 2$:

$$H(Z) = 2 \log n + o(1) \quad (57)$$

One can make the following very instructive observations about the above theorem. First, notice that in all cases where $d > 0$, the main contribution to the von Neumann entropy is given by the lower part of the spectrum, and not by the main eigenvalue. This is in contrast with the case of the p -Rényi entropies ($p > 0$), where the largest eigenvalue gives the main contribution [3].

Another important point concerns the fixed dimension case $d = 0$ and the linear case, $d = 1$, $k \sim cn$. In these regimes, the entropy defect $2 \log(k \wedge n) - H(Z)$ is macroscopic (53),(55). This improves considerably the naive bound (52) and may provide more insight into the question of additivity of minimal output entropies, as argued in [4,10,21]. However, Hastings' techniques [4], as well as the recent developments of Aubrun, Szarek and Werner [10] do not seem to apply to this linear regime. Studying additivity violations in the linear regime and using the bounds in Theorem 5.1 to provide larger violations remain interesting open problems.

Acknowledgements

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

References

1. King, C.; Ruskai, M.-B. Minimal entropy of states emerging from noisy quantum channels. *IEEE Trans. Inf. Theory* **2001**, *47*, 192–209.
2. Shor, P. Equivalence of additivity questions in quantum information theory. *Comm. Math. Phys.* **2004**, *246*, 453–472.
3. Hayden, P.; Winter, A. Counterexamples to the maximal p -norm multiplicativity conjecture for all $p > 1$. *Comm. Math. Phys.* **2008**, *284*, 263–280.
4. Hastings, M.B. Superadditivity of communication capacity using entangled inputs. *Nat. Phys.* **2009**, *5*, 255–257.
5. Collins, B.; Nechita, I. Random quantum channels I: Graphical calculus and the bell state phenomenon. *Comm. Math. Phys.* **2010**, *297*, 345–370.
6. Collins, B.; Nechita, I. Gaussianization and eigenvalue statistics for random quantum channels (III). 2009, arXiv:0910.1768. arXiv.org e-Print archive. available at: <http://arxiv.org/abs/0910.1768> (accessed 18 June 2010).
7. Collins, B. Product of random projections, Jacobi ensembles and universality problems arising from free probability. *Probab. Theory Relat. Fields* **2005**, *133*, 315–344.
8. Collins, B.; Śniady, P. Integration with respect to the Haar measure on unitary, orthogonal and symplectic group. *Comm. Math. Phys.* **2006**, *264*, 773–795.
9. Collins, B.; Nechita, I.; Życzkowski, K. Random graph states, maximal flow and Fuss-Catalan distributions. *J. Phys. A: Math. Theor.* **2010**, *43*, 275303.

10. Aubrun, G.; Szarek, S.; Werner, E. Hastings' additivity counterexample via Dvoretzky's theorem. 2010, arXiv:1003.4925. arXiv.org e-Print archive. available at: <http://arxiv4.library.cornell.edu/abs/1003.4925> (accessed 18 June 2010)
11. Collins, B. Moments and cumulants of polynomial random variables on unitary groups, the Itzykson-Zuber integral and free probability. *Int. Math. Res. Not.* **2003**, *17*, 953–982.
12. Coecke, B. Kindergarten quantum mechanics—lecture notes. *Quantum Theory: Reconsideration Found.* **2006**, *3*, 81–98.
13. Jones, V.F.R. Planar algebras, I. 1999, arXiv:math/9909027v1. arXiv.org e-Print archive. available at: <http://arxiv.org/abs/math/9909027v1> (accessed 18 June 2010).
14. Marchenko, V.A.; Pastur, L.A. The distribution of eigenvalues in certain sets of random matrices. *Mat. Sb.* **1967**, *72*, 507–536; *Math. USSR Sb.* **1967**, *1*, 457–483.
15. Nica, A.; Speicher, R. Lectures on the combinatorics of free probability. In *London Mathematical Society Lecture Note Series NO. 135*; Cambridge University Press: Cambridge, UK, 2006.
16. Page, D.N. Average entropy of a subsystem. *Phys. Rev. Lett.* **1993**, *71*, 1291–1294.
17. Fukuda, M.; King, C.; Moser, D. Comments on hastings' additivity counterexamples. 2009, arXiv:0905.3697. arXiv.org e-Print archive. available at: <http://arxiv.org/abs/0905.3697> (accessed 18 June 2010).
18. Fukuda, M.; King, C. Entanglement of random subspaces via the Hastings bound. 2009, arXiv:0907.5446. arXiv.org e-Print archive. available at: <http://arxiv.org/abs/0907.5446> (accessed 18 June 2010).
19. Bhatia, R. *Matrix Analysis (Graduate Texts in Mathematics)*; Springer-Verlag: New York, NY, USA, 1997.
20. Nechita, I. Asymptotics of random density matrices. *Ann. Henri Poincaré* **2007**, *8*, 1521–1538.
21. Collins, B.; Nechita, I. Random quantum channels II: Entanglement of random subspaces, Rényi entropy estimates and additivity problems. 2009, arXiv:0906.1877. arXiv.org e-Print archive. available at: <http://arxiv.org/abs/0906.1877> (accessed 18 June 2010).