

RANDOM QUANTUM CHANNELS I: GRAPHICAL CALCULUS AND THE BELL STATE PHENOMENON

BENOÎT COLLINS AND ION NECHITA

ABSTRACT. This paper is the first of a series where we study quantum channels from the random matrix point of view. We develop a graphical tool that allows us to compute the expected moments of the output of a random quantum channel.

As an application, we study variations of random matrix models introduced by Hayden [7], and show that their eigenvalues converge almost surely.

In particular we obtain for some models sharp improvements on the value of the largest eigenvalue, and this is shown in a further work to have new applications to minimal output entropy inequalities.

1. INTRODUCTION, MOTIVATION & PLAN

The theory of random matrices is a field of its own, but whenever it comes to applications, the driving idea is almost always that although it is very difficult to exhibit matrices having specified properties, a suitably chosen random matrix will have very similar properties as the original matrix with a high probability. This idea has been used successfully for example in operator algebra with the theory of free probability.

In 2007 for the first time, a similar leitmotiv was used with success by Hayden in [7] and Hayden-Winter in [9] to disprove the Rényi entropy additivity conjecture for a wide class of parameters p . A proof for the most important case $p = 1$ was even announced by Hastings in [6] with probabilistic arguments of different nature. This is arguably the most important conjecture in quantum information theory, and the random matrix models introduced by Hayden and their modifications due to Hastings seemed very new from our random matrix points of view.

This paper is therefore an attempt to understand these matrix models with random matrix techniques. For this purpose, we introduce a formalism that is very close to that of planar algebras of Jones [10], and we suggest that the language of quantum gates and planar algebras should be considered as very closely related to each other.

Our paper is organized as follows. In Section 2.1 we recall known facts about integration over unitary groups and their large dimension asymptotics. This is nowadays known as Weingarten calculus. In Section 3, we introduce a graphical model to represent (random) matrices arising in random quantum calculus. Section 4 gives a theoretical method for computing expectations with our graphical model and in the last two sections we give explicit applications of these techniques to random quantum channels. More precisely, in Section 5 we investigate tensor products of two independent quantum channels and in Section 6 we look at a product of a random channel Φ^U with the channel $\Phi^{\overline{U}}$ defined by the conjugate unitary \overline{U} .

Limit theorems presented in this paper are just a sample of what we can be accomplished with the calculus developed in Section 4. New results will be given in the forthcoming papers [3, 4].

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

Key words and phrases. Random matrices, Weingarten calculus, Quantum information theory, Random quantum channel.

2. BACKGROUND ON WEINGARTEN CALCULUS AND QUANTUM CHANNELS

2.1. Weingarten calculus. This section contains some basic material on unitary integration and Weingarten calculus. A more complete exposition of these matters can be found in [2, 5]. We start with the definition of the Weingarten function.

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 . It is the 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).*

Notice that the function $\sigma \mapsto n^{\#\sigma}$ is invertible as n is large, as it behaves like $n^p \delta_e$ as $n \rightarrow \infty$. If $n < p$ the function is not invertible any more, but we can keep this definition by taking the pseudo inverse and the theorems below will still hold true (we refer to [5] 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 function Wg is used to compute integrals with respect to the Haar measure on the unitary group (we shall denote by $\mathcal{U}(n)$ the unitary group acting on an n -dimensional Hilbert space). The first theorem is as follows:

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

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

If $p \neq p'$ then

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

Since we shall perform integration over large unitary groups, 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 [2] 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*

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

and

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

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

A shorthand for this theorem is the introduction of a function Mob on the symmetric group, invariant under conjugation and multiplicative over the cycles, satisfying for any permutation $\sigma \in \mathcal{S}_p$:

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

where $|\sigma| = p - \#\sigma$ is the *length* of σ , i.e. the minimal number of transpositions that multiply to σ . We refer to [5] for details about the function Mob . We finish this section by

a well known lemma which we will use several times towards the end of the paper. This result is contained in [12].

Lemma 2.4. *The function $d(\sigma, \tau) = |\sigma^{-1}\tau|$ is an integer valued distance on \mathcal{S}_p . Besides, it has the following properties:*

- the diameter of \mathcal{S}_p is $p - 1$;
- $d(\cdot, \cdot)$ is left and right translation invariant;
- for three permutations $\sigma_1, \sigma_2, \tau \in \mathcal{S}_p$, the quantity $d(\tau, \sigma_1) + d(\tau, \sigma_2)$ has the same parity as $d(\sigma_1, \sigma_2)$;
- the set of geodesic points between the identity permutation id and some permutation $\sigma \in \mathcal{S}_p$ is in bijection with the set of non-crossing partitions smaller than π , where the partition π encodes the cycle structure of σ . Moreover, the preceding bijection preserves the lattice structure.

We end this section by the following definition which generalizes the trace function. For some matrices $A_1, A_2, \dots, A_p \in \mathcal{M}_n(\mathbb{C})$ and some permutation $\sigma \in \mathcal{S}_p$, we define

$$\text{Tr}_\sigma(A_1, \dots, A_p) = \prod_{\substack{c \in \text{Cycles}(\sigma) \\ c = (i_1 i_2 \dots i_k)}} \text{Tr}(A_{i_1} A_{i_2} \dots A_{i_k}).$$

We also put $\text{Tr}_\sigma(A) = \text{Tr}_\sigma(A, A, \dots, A)$.

2.2. Quantum channels. In Quantum Information Theory, a *quantum channel* is the most general transformation of a quantum system. Quantum channels generalize the unitary evolution of isolated quantum systems to *open quantum systems*. Mathematically, we recall that a quantum channel is a linear completely positive trace preserving map Φ from $\mathcal{M}_n(\mathbb{C})$ to itself. The trace preservation condition is necessary since quantum channels should map density matrices to density matrices. The complete positivity condition can be stated as

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

The following two characterizations of quantum channels turn out to be very useful.

Proposition 2.5. *A linear map $\Phi : \mathcal{M}_n(\mathbb{C}) \rightarrow \mathcal{M}_n(\mathbb{C})$ is a quantum channel if and only if one of the following two equivalent conditions holds.*

- (1) (**Stinespring dilation**) *There exists a finite dimensional Hilbert space $\mathcal{K} = \mathbb{C}^d$, a density matrix $Y \in \mathcal{M}_d(\mathbb{C})$ and an unitary operation $U \in \mathcal{U}(nd)$ such that*
- (6)
$$\Phi(X) = \Phi^{U,Y}(X) = \text{Tr}_{\mathcal{K}}[U(X \otimes Y)U^*], \quad \forall X \in \mathcal{M}_n(\mathbb{C}).$$
- (2) (**Kraus decomposition**) *There exists an integer k and matrices $L_1, \dots, L_k \in \mathcal{M}_n(\mathbb{C})$ such that*

$$\Phi(X) = \sum_{i=1}^k L_i X L_i^*, \quad \forall X \in \mathcal{M}_n(\mathbb{C}).$$

and

$$\sum_{i=1}^k L_i^* L_i = \text{I}_n.$$

It can be shown that the dimension of the ancilla space in the Stinespring dilation theorem can be chosen $d = \dim \mathcal{K} = n^2$ and that the state Y can always be considered to be a rank one projector. A similar result holds for the number of Kraus operators: one can always find a decomposition with $k = n^2$ operators.

In the final two sections of the paper we study a model of *random quantum channels* originating from the Stinespring dilation formula (6). We shall be interested in the spectral

properties of the elements in the image of such random channels. Quantum channels will be the main field of application of the graphical calculus we develop in the next two sections, our aim being the treatment of some additivity problems in quantum information theory.

3. GRAPHICAL MODEL

In this section, we lay out the foundation for the graphical calculus we shall develop later. We introduce a graphical formalism for representing tensors and tensor contractions that is adapted to quantum information theory. We start at an abstract level, with a purely diagrammatic axiomatization and then we study the Hilbert representations, where graph-theoretic objects shall be associated with concrete elements of Hilbert spaces.

3.1. Diagrams and tensors.

Diagrams, boxes, decorations and wires. Our starting point is a set \tilde{S} endowed with an involution without fixed point $*$. The set \tilde{S} splits as $S \sqcup S^*$ according to the involution. Elements of \tilde{S} are called *decorations*.

A *diagram* is a collection of decorated *boxes* and possibly *wires* (or strings) connecting the boxes along their decorations according to rules which we shall specify. In terms of graph theory, a diagram is an unoriented (multi-)graph whose vertices are boxes, and whose edges are strings. Each vertex comes with a (possibly empty) n -tuple of indices (or decorations or labels) in \tilde{S}^n . The number n of decorations may depend on the vertex. We say that two diagrams are isomorphic if they are isomorphic as multi-graphs with labeled vertices.

A box is an elementary diagram from which we can construct more elaborate diagrams by putting boxes together and possibly wiring them together. Each box B of a diagram has attached to it a collection of $n(B)$ decorations in $\tilde{S}^{n(B)}$. The union of the decorations attached to a box B is denoted by $S(B) \sqcup S^*(B)$.

Graphically, boxes are represented by rectangles with symbols corresponding to the decorations attached to them (see Figure 1). We take the convention that decorations in S^* are represented by empty (or white) symbols and decorations in S by full (or black) symbols. Each decoration is thought as having potentially up to two *attachment points*. An *inner* one (which is attached to the box it belongs to) and an *outer* one, which we shall allow to be attached to a string later on.

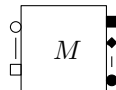


FIGURE 1. A box M

Constructing new diagrams out of old ones. Given a family of existing diagrams (e.g. boxes) there exists several ways of creating new diagrams.

- (1) One can put diagrams together, i.e. take their disjoint union (when it comes to taking representations in Hilbert spaces, this operation will amount to tensoring). One diagram can be viewed as a box. This amounts to specifying an order between the boxes.
- (2) Given a diagram A and a complex number x , one can create a new diagram $A' = xA$.
- (3) Given two boxes A, B having the same n -tuples of decorations, one can define $A + B$. This axiom and the previous one (together with evident relations such as $A + A = 2A$ which we don't enumerate in detail) endow the set of identically decorated diagrams with a structure of a complex vector space.

- (4) One can add *wires* to an existing diagram (or between two diagrams that have been put together). A wire is allowed between the outer attachment of two decorations only if the decorations have the same shape and different shadings. Such a wire can be created if and only if the two candidate decorations have their outer attachments unoccupied.
- (5) There exists an anti-linear *involution* on the diagrams, denoted by $*$. This operation does nothing on the wires. On the boxes, it reverts the shading of the decorations. The involution $*$ is conjugate linear.

Hilbert structure. We shall now consider a concrete representation of the diagrams introduced above as tensors in Hilbert spaces. We start by assuming that the set S of full (or black) decorations corresponds to a collection of finite dimensional Hilbert spaces $S = \{V_1, V_2, \dots\}$. An important fact that will be useful later is that each Hilbert space V_i comes equipped with an orthonormal basis $\{e_1, e_2, \dots, e_{\dim V_i}\}$. Our aim is to define a $*$ -linear map T between the diagrams and tensors in products of Hilbert spaces in the above class and their duals. By duality, white decorations correspond to dual spaces $S^* = \{V_1^*, V_2^*, \dots\}$. With these conventions, boxes can be seen as tensors whose legs belong to the vector spaces corresponding to its decorations. In a diagram, symbols of the same shape denote isomorphic spaces, but the converse may be false. A particular space V_i (or V_i^*) can appear several times in a box. The reader acquainted with quantum mechanics might think of white shapes as corresponding to ‘bras’ and black shapes corresponding to ‘kets’, but we shall get back to quantum mechanical notions later.

To a box B we therefore associate a tensor

$$(7) \quad T_B \in \left[\bigotimes_{i \in S(B)} V_i \right] \otimes \left[\bigotimes_{j \in S^*(B)} V_j^* \right].$$

Using the canonical duality between tensors and linear applications, T_B can also be seen as a linear map

$$T_B : \bigotimes_{j \in S^*(B)} V_j \rightarrow \bigotimes_{i \in S(B)} V_i,$$

We use freely partial duality results, and for example, an element of $V \otimes W^*$ can as well be seen as an element of $\mathcal{L}(W, V)$ or $\mathcal{L}(V^*, W^*)$.

Equation (7) defines the map T from the collection of boxes to the collection of vectors in Hilbert spaces obtained by tensoring finitely many copies of $V_i, i \in S(B) \cup S^*(B)$. This map is denoted by

$$T : B \mapsto T_B$$

and we now explain how we can extend it to all diagrams. A *wire* connecting two decorations of the same shape (corresponding to some Hilbert space V) is associated with the identity map (or tensor) $I : V \rightarrow V$. Together with our duality axiom, it also corresponds to a canonical tensor contraction (or trace)

$$C : V^* \otimes V \rightarrow \mathbb{C}.$$

We denote the set of wires in a diagram \mathcal{D} by $\mathcal{C}(\mathcal{D})$.

With this notation, a diagram \mathcal{D} is associated with the tensor T obtained by applying all the contractions (“wires”) to the product of tensors represented by the boxes. One is left with a tensor

$$T_{\mathcal{D}} = \left[\prod_{C \in \mathcal{C}(\mathcal{D})} C \right] \left(\bigotimes_{B \text{ box of } \mathcal{D}} T_B \right).$$

This is well defined (provided that one specifies one total order on the boxes): the order of the factors in the product does not matter, since wires act on different spaces. For a

box B , we denote by $FS(B) \subset S(B)$ the subset of black decorations which have no wires attached (we call such a decoration *free*). $FS^*(B)$ is defined in the same manner for white decorations (dual spaces). With this notation, the tensor $T_{\mathcal{D}}$ associated to a diagram \mathcal{D} can be seen in two ways: as an element of a Hilbert space

$$T_{\mathcal{D}} \in \left[\bigotimes_{j \in \bigcup_B FS^*(B)} V_j^* \right] \otimes \left[\bigotimes_{i \in \bigcup_B FS(B)} V_i \right],$$

or, equivalently, as a linear map

$$T_{\mathcal{D}} : \bigotimes_{j \in \bigcup_B FS^*(B)} V_j \rightarrow \bigotimes_{i \in \bigcup_B FS(B)} V_i.$$

We need two further axioms to ensure that we are indeed dealing with acceptable Hilbert representations.

- (1) A diagram such that all outer attachments of its decorations are occupied by wires corresponds canonically to an element in \mathbb{C} . In addition, a trivial box with a given decoration of type i closed on itself by a wire into a loop takes a value in \mathbb{N} . This value is called the dimension of V_i .
- (2) Given a diagram \mathcal{D} , if it is canonically paired to its dual \mathcal{D}^* by strings, the result lies in \mathbb{R}^+ .

Special diagrams. To make our calculus useful, we need to introduce a few special diagrams (equivalently, boxes) satisfying some specific axioms.

- (1) **The trivial box.** A wire connecting two identically shaped decorations of different shading corresponds to the identity map $I : V \rightarrow V$. We shall call this box the *trivial* or the identity box.



FIGURE 2. Trivial box

It satisfies the following identity axiom:

$$\bullet \text{---} \circ \bullet \text{---} \circ = \bullet \text{---} \circ$$

FIGURE 3. Trivial axiom

- (2) **Bras and kets.** The simplest boxes one can consider are vectors and linear forms. Following the quantum mechanics ‘bra’ and ‘ket’ vocabulary, vectors, or $(1, 0)$ -tensors have no white decorations and only one black decoration, whereas linear forms (or $(0, 1)$ -tensors) have one white label and no black labels. Since our Hilbert spaces come equipped with fixed basis, we introduce some special notation for the ket $|e_1\rangle = e_1$ and the bra $\langle e_1| = \langle e_1, \cdot \rangle$ corresponding to the first vector, as in Figure 4 (the choice of the first element of the basis being of course arbitrary).

$$\bullet = \boxed{e_1} \bullet \quad \circ = \circ \boxed{e_1}$$

FIGURE 4. Fixed ket and bra

- (3) **The Bell state.** Since each space $V \in S$ comes equipped with a particular fixed basis $\{e_i\}_{i=1}^{\dim V}$, we can define the *bra Bell state* as the tensor (it is in fact a linear form)

$$\text{Bell}_V^* = \sum_{i=1}^{\dim V} e_i^* \otimes e_i^*,$$

and its ket counterpart (which is a vector in $V \otimes V$)

$$\text{Bell}_V = \sum_{i=1}^{\dim V} e_i \otimes e_i.$$

This notation is needed in the sense that Bell states are not canonical and are not well defined from the sole data of V . They rely on some additional real structure of the vector space V which can be encoded by the data of an explicit basis. Bell states are represented in Figure 5(a). They satisfy the graphical axiom in Figure 5(b). Bell states play a central role in our formalism; we shall see later that they allow us to define the *transposition* of a box and even to consider wires connecting identical decorations.

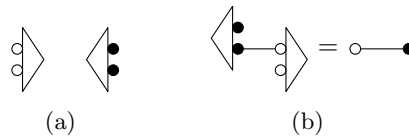


FIGURE 5. Bell states and axiom

- (4) **Unitary boxes.** Boxes associated to unitary matrices U satisfy the graphical axiom depicted in Figure 6 which corresponds to the identities $UU^* = U^*U = I$.



FIGURE 6. Unitary axioms

3.2. **Examples.** Let us now look at some simple diagrams which illustrate this formalism.

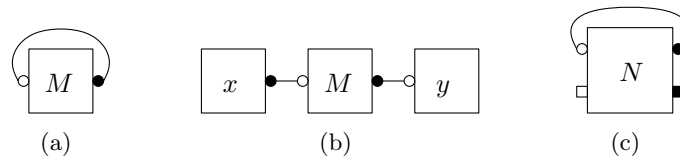


FIGURE 7. Some simple diagrams

Suppose that each diagram in Figure 7 comes equipped with two vector spaces V_1 and V_2 which we shall represent respectively by circle and square shaped symbols. In the first diagram, M is a tensor (or a matrix, depending on which point of view we adopt) $M \in V_1^* \otimes V_1$, and the wire applies the contraction $V_1^* \otimes V_1 \rightarrow \mathbb{C}$ to M . The result of the diagram \mathcal{D}_a is thus $T_{\mathcal{D}_a} = \text{Tr}(M) \in \mathbb{C}$. In the second diagram, again there are no free decorations, hence the result is the complex number $T_{\mathcal{D}_b} = \langle y, Mx \rangle$. Finally, in the third example, N is a $(2, 2)$ tensor or a linear application $N \in \mathcal{L}(V_1 \otimes V_2, V_1 \otimes V_2)$. When one applies to the tensor N the contraction of the couple (V_1, V_1^*) , the result is the partial trace of N over the space V_1 : $T_{\mathcal{D}_c} = \text{Tr}_{V_1}(N) \in \mathcal{L}(V_2, V_2)$.

Bell states allow us to introduce the *transposition* operation for a tensor (or a box) as follows. We define transposition for a matrix M (or a tensor $M \in V^* \otimes V$) and we extend it in a trivial way to more general situations. Graphically, the box corresponding to the transposed tensor M^t is defined in Figure 8(a); it consists in connecting an appropriate Bell state to each decoration of the box. Note however that this operation is different from

the involution $*$ applied to the same box. Moreover, Bell states allow for wires connecting identical shaped symbols of the same color, as in Figure 8(b). Such non-canonical tensor contractions ($V \otimes V \rightarrow \mathbb{C}$ or $V^* \otimes V^* \rightarrow \mathbb{C}$) are shorthand graphical notations for the corresponding diagram containing a Bell state, and we shall use them quite often in what follows.

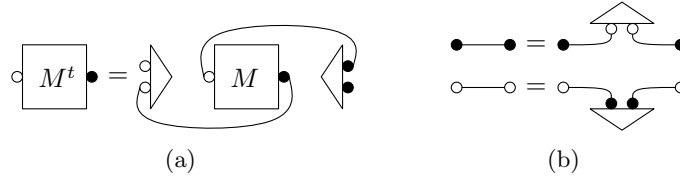


FIGURE 8. Bell states and transposition

Also, for reasons which shall be clear later, we shall sometimes make substitution $\overline{M} = (M^*)^t$. Finally, by grouping two Bell states together, one obtains the (non-canonical) tensor E (Figure 9), called “the maximal entangled state”. It corresponds to the tensor

$$E = \sum_{i=1}^{\dim V} \sum_{j=1}^{\dim V} e_i^* \otimes e_i^* \otimes e_j \otimes e_j \in V^* \otimes V^* \otimes V \otimes V.$$

The reader with background in quantum information will notice that the maximally entangled state we just defined is *not normalized* in order to be a density matrix. The reader with background in planar algebra theory will recognize a multiple of the Jones projection.

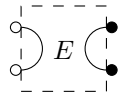


FIGURE 9. The maximal entangled state E

The diagram in Figure 10 is of crucial importance in what follows. It corresponds to a quantum channel in its Stinespring representation (see Eq. (6)). Round shaped inputs and outputs correspond to the Hilbert space \mathcal{H} and squares correspond to the “environment” \mathcal{K} . We shall study such diagrams with random interaction unitaries U in Sections 5 and 6.

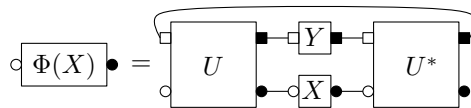


FIGURE 10. Diagram for a quantum channel in its Stinespring form

3.3. Comments on other existing graphical calculi. The above formalism is the one that seemed the most compatible with Weingarten calculus. Here, we comment about already existing graphical formalisms, in the hope that this section will serve as a dictionary for the reader acquainted to one of the calculi below.

Our calculus is mainly inspired by Bob Coecke’s *Kindergarten Quantum Mechanics* [1]. However we choose not to orient the strings; rather, we separate with color (black/white) the vector spaces and their duals, therefore there is only one possible pairing. A common feature of the two calculi is the central place occupied in the formalisms by Bell states.

V.F.R. Jones's theory of planar algebras [10] is also connected to our graphical calculus. One of our diagrammatic axioms is the existence of a Bell state. This is very closely related to the axioms of Temperley Lieb algebras and the diagrammatic for a Jones projection. Most of our calculus could take place in Jones' *bipartite graph planar algebra*.

4. PLANAR EXPANSION

In this section, we consider diagrams that may contain random matrices. This is where probability theory comes into play; we focus on the case where the random elements appearing in the diagrams are random unitary Haar-distributed on some finite dimensional unitary group.

Our task is to compute expectation values $\mathbb{E}(\mathcal{D})$ of diagrams \mathcal{D} containing boxes associated with random unitary operations. We shall write $\mathbb{E}(\mathcal{D})$ as a weighted sum of some diagrams obtained from \mathcal{D} that do not contain anymore random tensors.

4.1. Expectation of a diagram containing random independent unitary matrices. Suppose we have a diagram \mathcal{D} that has boxes of two types: either boxes of type U , U^* , \bar{U} or U^t where U is a unitary random variables in a fixed space of type $\text{End}(\otimes_{i \in I} V_i)$, distributed according to the Haar measure on the unitary group $\mathcal{U}(n)$ on this space, or other boxes which are independent (as classical random variables) from U (this includes deterministic boxes or tensors). We shall now present an algorithm for computing the expectation of such a diagram with respect to the probability law of U . Before describing the algorithm, let us note that if a diagram contains several *independent* Haar unitary matrices, one can recursively apply the algorithm to compute the expectation over all the random unitary matrices appearing in the diagram.

The first step in our algorithm is to ensure that \mathcal{D} contains only boxes of type U and \bar{U} . This can be done by using the transposition transformation via Bell states, and replacing U^t boxes by U boxes with the opposite shading of the decorations and U^* boxes by \bar{U} boxes.

Next, we introduce a concept of *removal* of boxes U and \bar{U} . A removal r is a procedure which transforms a diagram \mathcal{D} into a new diagram \mathcal{D}_r which does not contain neither U nor \bar{U} boxes. In other words, r is a way to remove random unitaries U from a diagram \mathcal{D} . The set of all admissible removal procedures for a diagram \mathcal{D} will be denoted by $\text{Rem}(\mathcal{D})$.

We now move on to describe removal procedures and how they operate on diagrams. First of all, a removal is not possible if the number of boxes U in \mathcal{D} is different from the number of boxes \bar{U} . In such a case, the set $\text{Rem}(\mathcal{D})$ will be defined to be empty. This rule is the diagrammatic equivalent of Eq. (2) from Theorem 2.2.

Assuming that the number of U boxes and \bar{U} boxes is the same, a removal r is a way to pair decorations of the U and \bar{U} boxes appearing in a diagram. More precisely, r is the data of 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} . We proceed in the following way: 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. A diagrammatic explanation of the above algorithm is described in Figure 11.

We are now ready to state the main result of this section.

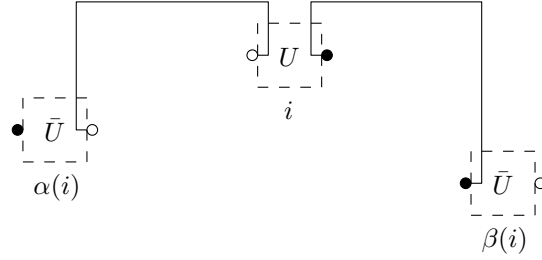


FIGURE 11. Removal: elimination of boxes and pairing of decorations

Theorem 4.1. *The following holds true:*

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

Proof. This is just Weingarten calculus of Theorem 2.2 applied to our graphical conventions. \square

When more than one independent unitary matrices U, V, \dots are present in a diagram, we proceed by induction over each independent matrix: we successively remove U, V, \dots . One can check directly that the order of the induction does not change the final result. This is compatible with the probabilistic property of the expectation, $\mathbb{E}_{U,V}(\mathcal{D}) = \mathbb{E}_V(\mathbb{E}_U(\mathcal{D}))$.

Theorem 4.1 might just look as a reformulation of known results, but without this graphical method, obtaining the main results of this paper is extremely cumbersome and very counterintuitive.

Let us now comment on the first step of our removal algorithm, replacing U^* boxes with \bar{U} boxes. The purpose of such a substitution is purely practical: later in the removal procedure, we pair decorations of *the same color*. If we should have decided to work with U and U^* boxes, one should always pair decorations of different colors, and this can turn out to be rather cumbersome when doing combinatorics. On the other hand, each time we replace a U^* box by a \bar{U} box, we introduce two more Bell states into our diagram (see Figure 8); although we decided not to display such states and rather to allow wires connecting decorations of the same color, this operation increases in some sense the “complexity” of the diagram.

In the next sub-section we present a warm-up toy example of Theorem 4.1. Further applications of the above theorem will be considered in a forthcoming paper [4], where problems from free probability theory will be treated using similar techniques.

4.2. First example: partial tracing a randomly rotated matrix. As a first application of the graphical formalism, we consider the following problem. Let $X \in \mathcal{M}_{nk}(\mathbb{C})$ be a deterministic matrix. In a manner similar to random quantum channels, we define, for a fixed integer parameter $k \geq 1$, the random matrix

$$Y = \text{Tr}_k[UXU^*] \in \mathcal{M}_n(\mathbb{C}),$$

where $U \in \mathcal{U}(nk)$ is a Haar distributed random unitary matrix. Notice that we are considering here non-normalized traces. Using our graphical formalism, we shall compute the moments of Y , $\mathbb{E}[\text{Tr}(Y^p)]$ for all $p \geq 1$. After replacing U^* boxes with \bar{U} , one gets the diagram in Figure 12, where round decorations correspond to \mathbb{C}^n and square ones to \mathbb{C}^k . Note that in Figure 12 there are p groups “ $UX\bar{U}$ ” wired together.

By Theorem 4.1, the expectation (with respect to the Haar measure of the unitary group $\mathcal{U}(nk)$) of this diagram is a weighted sum (with Weingarten weights) of diagrams \mathcal{D}_r obtained after the removal of U and \bar{U} boxes. Such diagrams \mathcal{D}_r contain only X blocks

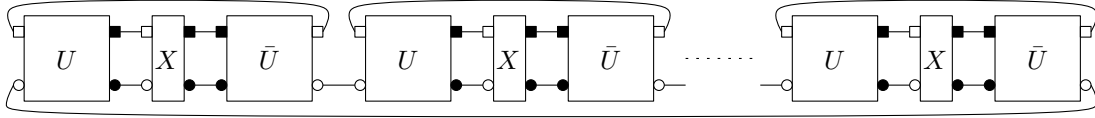


FIGURE 12. The diagram for $\text{Tr}(Y^p)$

and loops of different types. Let us compute the value of a diagram \mathcal{D}_r , where the removal is given by $r = (\alpha, \beta) \in \mathcal{S}_p^2$.

Suppose we number the boxes from 1 to p and the permutations α connects the white decorations and β the black decorations. The point here is that the permutation α will be responsible for the loops appearing in \mathcal{D}_r , whereas β will connect X boxes. We start by counting the number of loops in \mathcal{D}_r . Loops are of two types, the ones containing the top, square decorations (a loop of this type has a value of k) and the ones that come from the bottom, round decorations, each with a value of n . Since the top decorations are already connected (in the original diagram \mathcal{D}) by the identity permutation, the number of loops of the first type is given by the number of cycles of α , $\#\alpha$; they give a total contribution of $k^{\#\alpha}$. Loops corresponding to round decorations are initially connected by the cycle

$$(8) \quad \gamma = (n \ n - 1 \ \dots \ 3 \ 2 \ 1) \in \mathcal{S}_p.$$

Hence, the number of such loops is $\#(\gamma^{-1}\alpha)$ and they give a total contribution of $n^{\#(\gamma^{-1}\alpha)}$. In conclusion, the total contribution of loops is $k^{\#\alpha}n^{\#(\gamma^{-1}\alpha)}$. The contribution of the X boxes is straightforward to compute, since these boxes are connected only by β . After the removal we get $\#\beta$ connected components of powers of X , and the total contribution is $\text{Tr}_\beta(X)$.

Putting all this factors together, we obtain the following proposition:

Proposition 4.2. *The mean p -th moment of the random matrix $Y = \text{Tr}_k[UXU^*]$ is given by*

$$(9) \quad \mathbb{E}[\text{Tr}(Y^p)] = \sum_{\alpha, \beta \in \mathcal{S}_p} k^{\#\alpha} n^{\#(\gamma^{-1}\alpha)} \text{Tr}_\beta(X) \text{Wg}(\alpha\beta^{-1}).$$

In the particular case where X is a rank one projector, one has $\text{Tr}_\beta(X) = 1$ for all permutations β and since

$$\sum_{\sigma \in \mathcal{S}_p} \text{Wg}(nk, \sigma) = \left(\prod_{j=0}^{p-1} (nk + j) \right)^{-1},$$

one obtains the following simplification:

$$(10) \quad \mathbb{E}[\text{Tr}(Y^p)] = \left(\prod_{j=0}^{p-1} (nk + j) \right)^{-1} \sum_{\alpha \in \mathcal{S}_p} k^{\#\alpha} n^{\#(\gamma^{-1}\alpha)}.$$

We will discuss at length the simplifications that occur when dealing with rank one projectors in the forthcoming paper [4].

5. TENSOR PRODUCTS OF INDEPENDENT RANDOM QUANTUM CHANNELS

In the present section and in the next one, we consider two different models of tensor products of random quantum channels. In both cases, we first fix an interesting input state X_{12} (the Bell state) and investigate the random matrix

$$[\Phi_1 \otimes \Phi_2](X_{12}).$$

Our two models correspond to the choice of two different random pairs (Φ_1, Φ_2) . In both models, the channels Φ_1, Φ_2 are defined by random unitary matrices U_1, U_2 via the Stinespring representation introduced in Eq. (6).

The difference between the two cases lies in the correlation between the random matrices U_1 and U_2 . In the first model, interaction unitaries $U_{1,2}$ are *independent* Haar distributed random matrices. The second model, which is more involved, deals with the case where U_1 is distributed according to the Haar measure and $U_2 = \overline{U_1}$. This choice introduces an interesting symmetry into the problem and such a construction has become classical in quantum information theory [7, 6]. Asymptotic results in this case shed light on the interesting phenomenon that the output of the product channel has one “large” eigenvalue. We call this phenomenon the *Bell state phenomenon*. In order to simplify the notation, we shall assume that Y_1 and Y_2 are rank-one projectors and that $n_1 = n_2 = n$, $k_1 = k_2 = k$.

Before looking in detail at the two models of interest, let us make one brief comment on the choice of the input state of the channels. It is clear that if one chooses an input state which factorizes $X_{12} = X_1 \otimes X_2$, then

$$[\Phi_1 \otimes \Phi_2](X_{12}) = \Phi_1(X_1) \otimes \Phi_2(X_2),$$

and there is no correlation (classical or quantum) between the channels. In order to avoid such trivial situations, one has to choose an input state which is *entangled*. An obvious choice (given that $n_1 = n_2 = n$) is to take $X_{12} = E_n$, the n -dimensional Bell state (or the maximally entangled state), and we shall use this state in what follows.

The first model, although new, does not bring strikingly new results from the random matrix point of view. We treat it here as an illustration of what our calculus can allow to compute, and as a point of comparison with the second model.

Independent interaction unitaries. In the remaining of this section, we consider two *independent* realizations $U_1 = U$ and $U_2 = V$ of Haar-distributed unitary random matrices on $\mathcal{U}(nk)$. For both channels the state of the environment is a rank-one projector and we are interested in the $n^2 \times n^2$ random matrix

$$Z = [\Phi^U \otimes \Phi^V](E_n),$$

where E_n is the maximal entangled Bell state (notice the $1/n$ normalization)

$$E_n = \frac{1}{n} \sum_{i,j=1}^n |e_i\rangle\langle e_j| \otimes |e_i\rangle\langle e_j|.$$

The diagram associated with the $(2,2)$ tensor Z is drawn in the Figure 13; we chose to represent by squares decorations corresponding to \mathbb{C}^k and by circles decorations corresponding to \mathbb{C}^n .

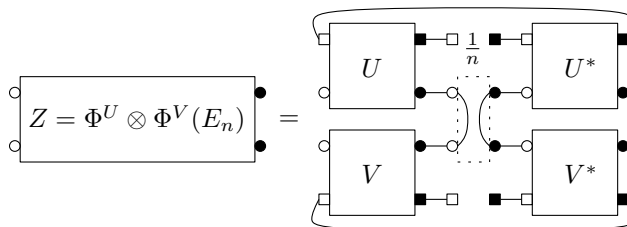


FIGURE 13. $Z = \Phi^U \otimes \Phi^V(E_n)$

As usual, we are interested in computing the moments $\mathbb{E}[\text{Tr}(Z^p)]$ for all $p \geq 1$ using the graphical method. We start by replacing U^* (resp. V^*) blocks by \overline{U} (resp. \overline{V}) blocks. An important point here is that there are two type of blocks corresponding to the independent random unitary matrices U and V (when computing the p -th moment of Z ,

there are p blocks of each type). This has two important consequences: when expanding the diagram in order to compute the expectation of the trace, one can only pair U blocks with \overline{U} blocks and V blocks with \overline{V} blocks; “cross-pairings” between U blocks and V blocks are not allowed by the expansion algorithm. This algorithm proceeds iteratively, first by removing, say, the U blocks (the V blocks being treated as constants) and then by removing the V blocks. Hence “cross-pairings” cannot occur. The second consequence of the presence of two independent Haar unitary matrices is that in the final expression for the expectation of the diagram, there will be two Weingarten weights, one for each independent unitary integration.

Lemma 5.1. *The following holds true (γ is the cycle permutation defined in Eq. (8))*

$$(11) \quad \mathbb{E}[\text{Tr}(Z^p)] = \sum_{\alpha_U, \beta_U, \alpha_V, \beta_V \in \mathcal{S}_p} k^{\#\alpha_U + \#\alpha_V} n^{\#(\gamma^{-1}\alpha_U) + \#(\gamma^{-1}\alpha_V) + \#(\beta_U^{-1}\beta_V) - p} \text{Wg}(\alpha_U \beta_U^{-1}) \text{Wg}(\alpha_V \beta_V^{-1}).$$

Proof. As it has already been stated, the expectation with respect to both unitary matrices U and V can be seen as the result of two removal procedures, and hence the Weingarten sum shall be indexed by a pair of removals (r_U, r_V) . In other words, the Weingarten sum shall be indexed by 2 pairs of permutations, one for each type of block; we shall denote them by $\alpha_U, \beta_U, \alpha_V, \beta_V \in \mathcal{S}_p$. The four permutations are responsible for pairing blocks in the following way ($1 \leq i \leq p$):

- (1) the white decorations of the i -th U -block are paired with the white decorations of the $\alpha_U(i)$ -th \overline{U} block;
- (2) the black decorations of the i -th U -block are paired with the black decorations of the $\beta_U(i)$ -th \overline{U} block;
- (3) the white decorations of the i -th V -block are paired with the white decorations of the $\alpha_V(i)$ -th \overline{V} block;
- (4) the black decorations of the i -th V -block are paired with the black decorations of the $\beta_V(i)$ -th \overline{V} block.

The diagram associated with $\text{Tr}(Z^p)$ contains, aside from the random unitary blocks, deterministic bras \square and kets \blacksquare . However, these boxes have a trivial contribution of 1 to the final result. Hence, the result of the graph expansion is a (sum over a) collection of loops, multiplied by some scalar factor. The different contributions of a quadruple $(\alpha_U, \beta_U, \alpha_V, \beta_V) \in \mathcal{S}_p^4$ are given by (recall that circles correspond to n -dimensional spaces and squares correspond to k -dimensional spaces):

- (1) “ $\square U$ ”-loops: $k^{\#\alpha_U}$;
- (2) “ $\square V$ ”-loops: $k^{\#\alpha_V}$;
- (3) “ $\circ U$ ”-loops: $n^{\#(\gamma^{-1}\alpha_U)}$;
- (4) “ $\circ V$ ”-loops: $n^{\#(\gamma^{-1}\alpha_V)}$;
- (5) “ $\blacksquare U$ ”-loops: none;
- (6) “ $\blacksquare V$ ”-loops: none;
- (7) “ $\bullet U, V$ ”-loops: $n^{\#(\beta_U^{-1}\beta_V)}$;
- (8) normalization factors $1/n$ from the Bell matrices E_n : n^{-p} ;
- (9) Weingarten weights for the U -matrices: $\text{Wg}(\alpha_U \beta_U^{-1})$;
- (10) Weingarten weights for the V -matrices: $\text{Wg}(\alpha_V \beta_V^{-1})$.

Adding all these contributions, we obtain the announced exact closed-form expression. \square

Asymptotics. The preceding expression is intractable at fixed n and k , so we study two asymptotic regimes:

- (I) n fixed, $k \rightarrow \infty$;
- (II) k fixed, $n \rightarrow \infty$;

At this stage, before looking into each particular asymptotic regime, we can make an important observation. Notice that in the preceding expression, aside from the factor $n^{\#(\beta_U^{-1}\beta_V)}$, the general term of the sum factorizes into a “ (α_U, β_U) ” part and a “ (α_V, β_V) ” part. This was to be expected, since the coupling between the two channels is realized by the input state E_n which has a contribution of $n^{\#(\beta_U^{-1}\beta_V)-p}$. Let us also note that a third interesting asymptotic regime, $n, k \rightarrow \infty$, $k/n \rightarrow c > 0$ will be studied using the same methods in a forthcoming paper.

Theorem 5.2. *In the first regime, n fixed, $k \rightarrow \infty$, the output of the tensor product of the channels, for large values of k , is close to the chaotic state*

$$\rho_* = \frac{I_{n^2}}{n^2}.$$

In the second regime, k fixed, $n \rightarrow \infty$, the asymptotic eigenvalues of Z are $1/k^2$ with multiplicity k^2 and 0 with multiplicity $n^2 - k^2$.

Proof. Using the standard asymptotics for the Weingarten functions

$$\begin{aligned} \text{Wg}(\alpha_U \beta_U^{-1}) &\stackrel{k \rightarrow \infty}{\sim} (nk)^{-p-|\alpha_U \beta_U^{-1}|} \text{Mob}(\alpha_U \beta_U^{-1}) \text{ and} \\ \text{Wg}(\alpha_V \beta_V^{-1}) &\stackrel{k \rightarrow \infty}{\sim} (nk)^{-p-|\alpha_V \beta_V^{-1}|} \text{Mob}(\alpha_V \beta_V^{-1}), \end{aligned}$$

the power of k appearing in a general $(\alpha_U, \beta_U, \alpha_V, \beta_V)$ term is

$$k^{p-|\alpha_U|+p-|\alpha_V|-p-|\alpha_U \beta_U^{-1}|-p-|\alpha_V \beta_V^{-1}|} = k^{-(|\alpha_U|+|\alpha_V|+|\alpha_U \beta_U^{-1}|+|\alpha_V \beta_V^{-1}|)}.$$

It is obvious that all the terms converge to zero, except the one with $\alpha_U = \beta_U = \alpha_V = \beta_V = \text{id}$. Using $\text{Mob}(\text{id}) = 1$, we conclude that

$$\lim_{k \rightarrow \infty} \mathbb{E}[\text{Tr}(Z^p)] = n^{2-2p}.$$

One can restate this in terms of the empirical eigenvalue distribution of the $n^2 \times n^2$ matrix Z :

$$\mu_Z = \frac{1}{n^2} \sum_{i=1}^{n^2} \delta_{\lambda_i(Z)} \xrightarrow[k \rightarrow \infty]{} \delta_{1/n^2}.$$

In other words, the output of the tensor product of the channels, for large values of k , is close to the chaotic state

$$\rho_* = \frac{I_{n^2}}{n^2}.$$

As for the second regime, using similar considerations, we obtain

$$\lim_{n \rightarrow \infty} \mathbb{E}[\text{Tr}(Z^p)] = k^{2-2p}.$$

□

Note that both regimes presented here are trivial to some extent. We could prove at only a small additional cost that the convergence of the eigenvalues is actually almost sure. See the next section for the technique of proof, a direct adaptation of the Borel-Cantelli lemma.

Finally, we want to emphasize that the asymptotic behavior of the output in the second regime changes drastically when considering the conjugate case, and that this fact will have very important consequences in the theory of quantum information.

6. TENSOR PRODUCTS OF CONJUGATE RANDOM QUANTUM CHANNELS

We have seen that tensor products of independent random channels have an eigenvalue behavior close to the single channel case (see [11] for the treatment of the single channel case) - despite the fact that the input state is maximally entangled. In this section, we consider the case where $U_1 = U, U_2 = \bar{U}$ and $U \in \mathcal{U}(nk)$ is a Haar uniform random unitary matrix. Tensor products of channels of this type are now classical in the literature (see [7, 6]). One of the reasons why channels of this particular form receive such attention is that one can show that the product channel has a “trivial large eigenvalue” of order $1/k$. We shall provide a graphical proof of this fact later, in Lemma 6.6.

Again, we are interested in the moments of the random matrix $Z = \Phi^U \otimes \Phi^{\bar{U}}(E_n)$, depicted in the Figure 14.

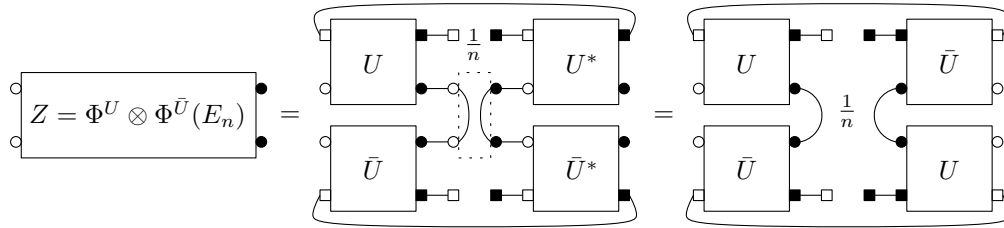


FIGURE 14. $Z = \Phi^U \otimes \Phi^{\bar{U}}(E_n)$

This time calculations are more complicated, because only one unitary matrix appears in the product channel. This means that in the removal algorithm, one can pair boxes from Φ^U with boxes from $\Phi^{\bar{U}}$ thus obtaining more complicated patterns. Another consequence of the fact that we use only one random unitary matrix is that the Weingarten sums are indexed by only one pair of permutations $(\alpha, \beta) \in \mathcal{S}_{2p}^2$.

In order to count the loops obtained after the graph expansion, we label the U and the \bar{U} boxes in the following manner: $1^T, 2^T, \dots, p^T$ for the U boxes of the first channel (T as “top”) and $1^B, 2^B, \dots, p^B$ for the U boxes of the second channel (B as “bottom”). We shall also order the labels as $\{1^T, 2^T, \dots, p^T, 1^B, 2^B, \dots, p^B\} \simeq \{1, \dots, 2p\}$. A removal $r = (\alpha, \beta) \in \mathcal{S}_{2p}^2$ of the random (U and \bar{U}) boxes connects the decorations in the following way:

- (1) the white decorations of the i -th U -block are paired with the white decorations of the $\alpha(i)$ -th \bar{U} block;
- (2) the black decorations of the i -th U -block are paired with the black decorations of the $\beta(i)$ -th \bar{U} block.

Next, we introduce two fixed permutations $\gamma, \delta \in \mathcal{S}_{2p}$ which will be useful in counting the loops. The permutation γ represents the initial wiring of the \circ decorations (before the graph expansion) and δ accounts for the wires between the \bullet decorations (which come from E_n). More precisely, for all i ,

$$(12) \quad \gamma(i^T) = (i - 1)^T, \quad \gamma(i^B) = (i + 1)^B, \quad \text{and} \quad \delta(i^T) = i^B, \quad \delta(i^B) = i^T.$$

We are now ready to compute the average moments of the random matrix Z .

Lemma 6.1. *The following holds true*

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

Proof. With the notations introduced above, we can now count the contributions for each individual pairing (α, β) :

- (1) “ \square ”-loops: $k^{\#\alpha}$;

- (2) “○”-loops: $n^{\#(\alpha\gamma^{-1})}$;
- (3) “■”-loops: none;
- (4) “●”-loops: $n^{\#(\beta\delta^{-1})} = n^{\#(\beta\delta)}$ (notice that δ is an involution);
- (5) normalization factors $1/n$ from the E_n matrices: n^{-p} ;
- (6) Weingarten weights for the U -matrices: $\text{Wg}(\alpha\beta^{-1})$.

Adding up all the above contributions, we obtain the claimed formula. \square

In the rest of the section, we shall focus on the asymptotic regime n fixed, $k \rightarrow \infty$, and in the next section we shall look into the more interesting case k fixed, $n \rightarrow \infty$.

Before stating the asymptotic result, let us make two preliminary remarks. In the case of the conjugate product channel, since only one unitary matrix appears in the diagrams, there is a notable difference concerning the asymptotics of the Weingarten function:

$$\text{Wg}(\alpha\beta^{-1}) \sim (nk)^{-2p-|\alpha\beta^{-1}|} \text{Mob}(\alpha\beta^{-1}).$$

One can easily compute the following quantities involving the permutations γ and δ which will be useful later, when doing asymptotics: $|\gamma| = 2p - 2$, $|\delta| = p$, $|\gamma\delta| = p$.

Proposition 6.2. *In the asymptotic regime where n is fixed and $k \rightarrow \infty$, the random matrix Z converges to the chaotic state*

$$\rho_* = \frac{\mathbf{I}_{n^2}}{n^2}.$$

Proof. Computing the asymptotic trace for large k gives

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

Minimizing the power of k above gives $|\alpha| + |\alpha\beta^{-1}| \geq 0$, with equality iff $\alpha = \beta = \text{id}$, hence

$$\lim_{k \rightarrow \infty} \mathbb{E}[\text{Tr}(Z^p)] = n^{2-2p},$$

and the conclusion is the same as in the case of two independent quantum channels: the output Z is asymptotically close to the chaotic state ρ_* . \square

6.1. Conjugate channels, the Bell phenomenon. We are left with studying the most interesting regime, k fixed and $n \rightarrow \infty$. Our main result is as follows:

Theorem 6.3. *In the regime of k fixed, $n \rightarrow \infty$, the eigenvalues of the matrix Z converge almost surely towards:*

- $\frac{1}{k} + \frac{1}{k^2} - \frac{1}{k^3}$, with multiplicity one;
- $\frac{1}{k^2} - \frac{1}{k^3}$, with multiplicity $k^2 - 1$;
- 0, with multiplicity $n^2 - k^2$.

Note that it follows from the Stinespring theorem that Z has at most k^2 non-zero eigenvalues. Therefore a moment approach is possible for the proof.

We start with a technical Lemma about the structure of geodesics between the specific permutations γ and δ introduced in Equation (12).

Lemma 6.4. *For $1 \leq i \leq p$, let τ_i be the transposition $(i^T, (i-1)^B)$. Then the permutations α on the geodesic $\gamma \rightarrow \alpha \rightarrow \delta$ are indexed by subsets $A \subseteq \{1, \dots, p\}$: $\alpha = \gamma \prod_{i \in A} \tau_i$. Moreover, for such a permutation, we have*

$$|\alpha| = \begin{cases} 2p - 2 & \text{if } A = \emptyset, \\ 2p - |A| & \text{if } A \neq \emptyset. \end{cases}$$

Proof. If $A = \emptyset$, then $|\alpha| = |\gamma| = 2p - 2$. Otherwise, after computing the action of α

$$\alpha(i^T) = \begin{cases} i^B & \text{if } i \in A, \\ (i-1)^T & \text{if } i \notin A; \end{cases}$$

$$\alpha(i^B) = \begin{cases} i^T & \text{if } (i+1) \in A, \\ (i+1)^B & \text{if } (i+1) \notin A; \end{cases}$$

it is easy to see that each element i of A spans a cycle of α and thus $|\alpha| = 2p - \#\alpha = 2p - |A|$. \square

We split this proof of Theorem 6.3 in two steps: first we prove the convergence in expectation, and then we prove the almost sure convergence.

Proof of the convergence in expectation. Using the same asymptotic formula as in the previous section (this time for large n), the quantity one wants to minimize in this case is

$$|\alpha\gamma^{-1}| + |\beta\delta| + |\alpha\beta^{-1}| = |\gamma^{-1}\alpha| + |\alpha^{-1}\beta| + |\beta^{-1}\delta| \geq |\gamma^{-1}\delta| = p.$$

Equality is attained when $\gamma \rightarrow \alpha \rightarrow \beta \rightarrow \delta$ is a geodesic in \mathcal{S}_{2p} . Using this observation, we obtain

$$\mathbb{E}[\text{Tr}(Z^p)] \sim \sum_{\gamma \rightarrow \alpha \rightarrow \beta \rightarrow \delta} k^{-(|\alpha|+|\alpha\beta^{-1}|)} \text{Mob}(\alpha\beta^{-1}).$$

It turns out that we can compute exactly the last sum as follows. First, notice that the geodesic condition $\gamma \rightarrow \alpha \rightarrow \beta \rightarrow \delta$ can be restated as $\text{id} \rightarrow \gamma^{-1}\alpha \rightarrow \gamma^{-1}\beta \rightarrow \gamma^{-1}\delta$. But $\gamma^{-1}\delta$ is a product of p transpositions with disjoint support: $\gamma^{-1}\delta = \prod_{i=1}^p \tau_i$, where τ_i is the transposition $(i^T, (i-1)^B)$ for all $1 \leq i \leq p$. As in Lemma 6.4, permutations on a geodesic between id and $\gamma^{-1}\delta$ are parameterized by subsets of $\{1, \dots, p\}$ as follows. Permutations $\gamma^{-1}\alpha$ and $\gamma^{-1}\beta$ lie on a geodesic between id and $\gamma^{-1}\delta$ (i.e. $\text{id} \rightarrow \gamma^{-1}\alpha \rightarrow \gamma^{-1}\beta \rightarrow \gamma^{-1}\delta$) if and only if there exist two subsets $\emptyset \subseteq A \subseteq B \subseteq \{1, 2, \dots, p\}$ such that

$$\gamma^{-1}\alpha = \prod_{i \in A} \tau_i,$$

$$\gamma^{-1}\beta = \prod_{i \in B} \tau_i.$$

For two such permutations, it is obvious that $|\alpha^{-1}\beta| = |(\gamma^{-1}\alpha)^{-1}\gamma^{-1}\beta| = |B \setminus A|$. In order to compute $|\alpha|$, we rely on Lemma 6.4.

Since $\alpha^{-1}\beta$ is a product of $|B \setminus A|$ transpositions of disjoint support, it follows by [5] that $\text{Mob}(\alpha^{-1}\beta) = (-1)^{|B \setminus A|}$ and we are left with the following expression:

$$\mathbb{E}[\text{Tr}(Z^p)] \sim \sum_B k^{-(2p-2+|B|)} (-1)^{|B|} + \sum_{\emptyset \neq A \subseteq B} k^{-(2p-|A|+|B \setminus A|)} (-1)^{|B \setminus A|}.$$

Using the multinomial identities

$$\sum_{\emptyset \subseteq A \subseteq \{1, \dots, p\}} x^{|A|} = (1+x)^p \quad \text{and}$$

$$\sum_{\emptyset \subseteq A \subseteq B \subseteq \{1, \dots, p\}} x^{|A|} y^{|B \setminus A|} = (1+x+y)^p,$$

we obtain the asymptotic traces of the output matrix Z :

$$\mathbb{E}[\text{Tr}(Z^p)] \sim \left(\frac{1}{k} + \frac{1}{k^2} - \frac{1}{k^3} \right)^p + (k^2 - 1) \left(\frac{1}{k^2} - \frac{1}{k^3} \right)^p.$$

We conclude that the matrix Z has, asymptotically, the following eigenvalues:

- $\frac{1}{k} + \frac{1}{k^2} - \frac{1}{k^3}$, with multiplicity one;

- $\frac{1}{k^2} - \frac{1}{k^3}$, with multiplicity $k^2 - 1$;
- 0, with multiplicity $n^2 - k^2$.

□

Next we move on to the proof of almost sure convergence. We would like to mention about the proof below that we believe that it should be possible to prove that

$$\mathbb{E} \left[(\text{Tr}(Z^p) - \mathbb{E} \text{Tr}(Z^p))^2 \right] = O(n^{-2})$$

simply by observing that the function

$$U \rightarrow \text{Tr}(Z^p)$$

is Lipschitz on the unitary group and by applying a Gromov-Milman type concentration measure argument. We refer to [8] for an exposition of such techniques. The authors acknowledge that this approach might be slightly less cumbersome in the specific case of this proof. However, we chose to keep our proof of a combinatorial nature for the sake of coherence.

Proof of the almost sure convergence. It is a standard technique in probability theory that in order to show the almost-sure convergence of the eigenvalues of Z to their respective limits, it suffices for the covariance series to converge, for all values of p :

$$\sum_{n=1}^{\infty} \mathbb{E} \left[(\text{Tr}(Z^p) - \mathbb{E} \text{Tr}(Z^p))^2 \right] < \infty.$$

Indeed, this inequality together with the Borel-Cantelli lemma imply that almost surely as $n \rightarrow \infty$,

$$\text{Tr}(Z^p) \rightarrow \mathbb{E} \text{Tr}(Z^p)$$

The two ingredients which make the proof work are the following. The first one is the fact that the error one makes when approximating the Weingarten function with its dominating term is of the order -2 :

$$\text{Wg}(\alpha) = (nk)^{-(p+|\alpha|)} (\text{Mob}(\alpha) + O((nk)^{-2})).$$

This follows from Theorem 2.3 and the definition of Mob below. The second ingredient is contained in the geodesic inequality $|\gamma^{-1}\alpha| + |\alpha^{-1}\beta| + |\beta^{-1}\delta| \geq |\gamma^{-1}\delta| = p$. Earlier, we have completely described the set of couples (α, β) which saturate the equality. It turns out that one can say more on the values of the function $(\alpha, \beta) \mapsto E(\alpha, \beta) = |\gamma^{-1}\alpha| + |\alpha^{-1}\beta| + |\beta^{-1}\delta| - p$, as follows. Applying Lemma 2.4 two times, it is clear that the values taken by $E(\alpha, \beta)$ are all even, $E(\alpha, \beta) \neq 1$ and thus

$$\begin{aligned} \mathbb{E}[\text{Tr}(Z^p)] &= \sum_{\alpha, \beta \in \mathcal{S}_{2p}} k^{\#\alpha} n^{\#(\alpha\gamma^{-1}) + \#(\beta\delta) - p} \text{Wg}(\alpha\beta^{-1}) \\ &= \sum_{\gamma \rightarrow \alpha \rightarrow \beta \rightarrow \delta} k^{-(|\alpha| + |\alpha\beta^{-1}|)} \text{Mob}(\alpha\beta^{-1}) + O\left(\frac{1}{n^2}\right). \end{aligned}$$

We start by computing the easiest term of the covariance, namely

$$\mathbb{E}[\text{Tr}(Z^p)]^2 = \sum_{\substack{\gamma \rightarrow \alpha_1 \rightarrow \beta_1 \rightarrow \delta \\ \gamma \rightarrow \alpha_2 \rightarrow \beta_2 \rightarrow \delta}} k^{-(|\alpha_1| + |\alpha_1\beta_1^{-1}| + |\alpha_2| + |\alpha_2\beta_2^{-1}|)} \text{Mob}(\alpha_1\beta_1^{-1}) \text{Mob}(\alpha_2\beta_2^{-1}) + O\left(\frac{1}{n^2}\right).$$

The second term $\mathbb{E}[\text{Tr}(Z^p)^2]$ is more difficult to estimate and one needs to introduce the permutations $\bar{\gamma}, \bar{\delta} \in \mathcal{S}_{4p}$:

$$\begin{aligned} \bar{\gamma} &= (1^T 2^T \cdots p^T) ((p+1)^T (p+2)^T \cdots (2p)^T) (1^B 2^B \cdots p^B) ((p+1)^B (p+2)^B \cdots (2p)^B); \\ \bar{\delta} &= (1^T 1^B) (2^T 2^B) \cdots (p^T p^B) ((p+1)^T (p+1)^B) \cdots ((2p)^T (2p)^B). \end{aligned}$$

With this notation, we have

$$\begin{aligned} \mathbb{E}[\text{Tr}(Z^p)^2] &= \sum_{\alpha, \beta \in \mathcal{S}_{4p}} k^{\#\alpha} n^{\#(\alpha\bar{\gamma}^{-1}) + \#(\beta\bar{\delta}) - p} \text{Wg}(\alpha\beta^{-1}) = \\ &= \sum_{\alpha, \beta \in \mathcal{S}_{4p}} k^{-(|\alpha| + |\alpha\beta^{-1}|)} n^{2p - (|\bar{\gamma}^{-1}\alpha| + |\alpha^{-1}\beta| + |\beta^{-1}\bar{\delta}|)} \text{Mob}(\alpha\beta^{-1}) + O\left(\frac{1}{n^2}\right). \end{aligned}$$

One can easily show that $|\bar{\gamma}^{-1}\alpha| + |\alpha^{-1}\beta| + |\beta^{-1}\bar{\delta}| \geq |\bar{\gamma}^{-1}\bar{\delta}| = 2p$. Since both $\bar{\gamma}$ and $\bar{\delta}$ leave invariant the sets $\{1^{T,B}, 2^{T,B}, \dots, p^{T,B}\}$ and $\{(p+1)^{T,B}, (p+2)^{T,B}, \dots, 2p^{T,B}\}$, geodesic couples (α, β) are obtained as direct sums

$$\begin{aligned} \alpha &= \alpha_1 \oplus \alpha_2, \\ \beta &= \beta_1 \oplus \beta_2, \end{aligned}$$

where $\alpha_1, \beta_1 \in \mathcal{S}(\{1^{T,B}, 2^{T,B}, \dots, p^{T,B}\})$, $\alpha_2, \beta_2 \in \mathcal{S}(\{(p+1)^{T,B}, (p+2)^{T,B}, \dots, 2p^{T,B}\})$ are such that $\gamma_1 \rightarrow \alpha_1 \rightarrow \beta_1 \rightarrow \delta_1$ and $\gamma_2 \rightarrow \alpha_2 \rightarrow \beta_2 \rightarrow \delta_2$ are geodesics (the permutations $\gamma_{1,2}$ and $\delta_{1,2}$ are defined in an obvious way). One has also that $|\alpha| = |\alpha_1| + |\alpha_2|$, $|\beta| = |\beta_1| + |\beta_2|$ and that $\text{Mob}(\alpha\beta^{-1}) = \text{Mob}(\alpha_1\beta_1^{-1}) \text{Mob}(\alpha_2\beta_2^{-1})$. Putting all this together, one gets the final expression which ends the proof

$$\mathbb{E}[\text{Tr}(Z^p)^2] = \sum_{\substack{\gamma \rightarrow \alpha_1 \rightarrow \beta_1 \rightarrow \delta \\ \gamma \rightarrow \alpha_2 \rightarrow \beta_2 \rightarrow \delta}} k^{-(|\alpha_1| + |\alpha_1\beta_1^{-1}| + |\alpha_2| + |\alpha_2\beta_2^{-1}|)} \text{Mob}(\alpha_1\beta_1^{-1}) \text{Mob}(\alpha_2\beta_2^{-1}) + O\left(\frac{1}{n^2}\right).$$

□

6.2. Generalization of Theorem 6.3 and discussion. We finish this paper by studying a generalization of the model investigated in the previous section. We consider the case where k is a fixed integer, and $t \in (0, 1)$ is a fixed number (possibly a function of k). For each n , we consider a random unitary matrix $U \in \mathcal{M}_{nk}(\mathbb{C})$, and a projection q_n of $\mathcal{M}_{nk}(\mathbb{C})$ of rank p_n such that $p_n/(nk) \sim t$ as $n \rightarrow \infty$. Our model of a random quantum channel is

$$\Phi : \mathcal{M}_{p_n}(\mathbb{C}) \rightarrow \mathcal{M}_n(\mathbb{C})$$

given by

$$\Phi(X) = \text{Tr}_k(UXU^*)$$

where the density matrix X satisfies $X \leq q_n$ (in other words we consider the isomorphism $q_n \mathcal{M}_{nk}(\mathbb{C}) q_n \simeq \mathcal{M}_{p_n}(\mathbb{C})$). Graphically, our model amounts to Figure 15.

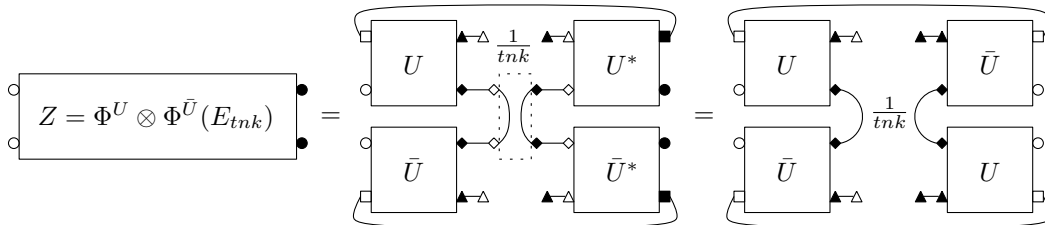


FIGURE 15. $Z = \Phi^U \otimes \Phi^{\bar{U}}(E_{tnk})$

As usual, we are interested in the process given by the eigenvalues of Z as $n \rightarrow \infty$ (in our setup, k is fixed). Here, with almost the same techniques as in Theorem 6.3, we obtain the following result.

Theorem 6.5. *Almost surely, as $n \rightarrow \infty$, the random matrix $\Phi \otimes \bar{\Phi}(E_{tnk}) \in \mathcal{M}_{n^2}(\mathbb{C})$ has non-zero eigenvalues converging towards*

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

Proof. Theorem 6.3 is a particular case of this theorem with $t = (1 - 1/k)$ and it has been worked out in great detail. Therefore we leave the reader to work out the appropriate modifications to this case. \square

The striking fact here is that the largest eigenvalue behaves almost surely like $t + (1 - t)/k^2$. The existence of a large eigenvalue was already anticipated by Hayden in [7], Lemma II.2. The lemma below is a slight generalization of Hayden’s lemma, following his idea.

Lemma 6.6. *In the above model, the largest eigenvalue is at least t .*

For the sake of being self contained, we give a proof of this fact. Moreover, the proof is graphical, using our diagrammatic calculus developed in Section 3.

Proof. Following [7], it is enough to prove that

$$\text{Tr}(Z_n E_n) = \left\langle \frac{1}{\sqrt{n}} \text{Bell}_n, \left[\Phi^U \otimes \Phi^{\bar{U}}(E_{tnk}) \right] \frac{1}{\sqrt{n}} \text{Bell}_n \right\rangle \geq t.$$

In order to accomplish this, we use the diagram invariance to stretch outside the inner parts of the diagram and then we notice that the resulting diagram is of the form $\langle X, X \rangle$ for some $X \in \mathbb{C}^{k^2}$, see Figure 16. Introducing the orthogonal projector $A = I_{k^2} - E_k \in$

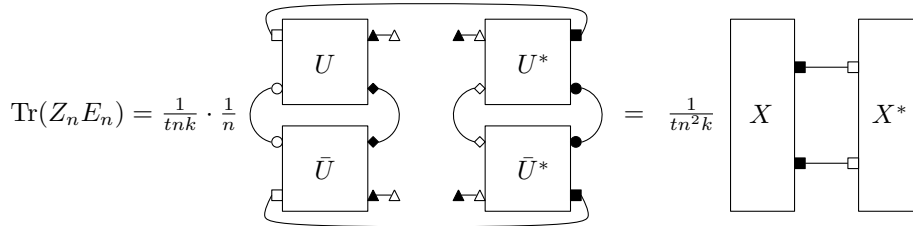


FIGURE 16. Re-writing $\text{Tr}(Z_n E_n)$

$\mathcal{M}_{k^2}(\mathbb{C})$, it is obvious that $\langle X, AX \rangle \geq 0$ and thus the inequality in Figure 17 holds. Note that we have replaced the identity operator I_{k^2} connecting X and X^* by the maximally entangled state on $\mathbb{C}^k \otimes \mathbb{C}^k$.

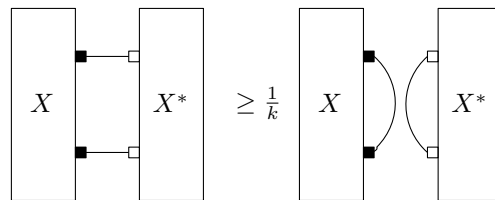


FIGURE 17. Replacing I_{k^2} by E_k

Now we use the unitary axioms on each of the two connected diagrams above and we obtain the result in Figure 18.

Putting all the factors together, we get

$$\text{Tr}(Z_n E_n) \geq \frac{1}{tn^2k^2} (tnk)^2 = t,$$

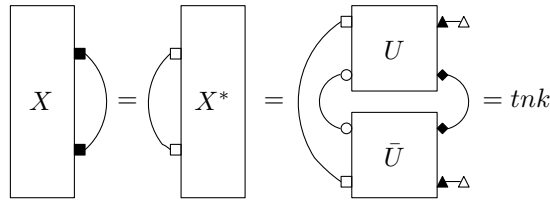


FIGURE 18. Application of the unitary axioms

and then, since E_n is an orthogonal projector, we conclude that the largest eigenvalue of Z_n is at least t . \square

To conclude, let us compare Theorem 6.5 and Lemma 6.6. Independently on the choice of t and k , the value that we obtain almost surely for the largest eigenvalue in Theorem 6.5 improves strictly the lower bound for the largest eigenvalue obtained in Lemma 6.6, as $t + (1 - t)/k^2 > t$.

For fixed t , the relative improvement $(t + (1 - t)/k^2)/t$ becomes small as k becomes big. On the other hand, if $t \leq k^{-2}$, the Lemma 6.6 does not bring new information, as the largest eigenvalue is always at least k^{-2} , whereas Theorem 6.5 brings new information.

So, the relative improvement is optimal for $t \sim k^{-2}$. This heuristic study leads us to think that it is possible to improve known counterexamples about the various entropy additivity conjectures, and this is the object of study of our second paper [3].

ACKNOWLEDGMENTS

One author (B.C.) would like to thank P. Hayden for an enlightening talk and conversations in Guadalajara during the summer 2007. This is where he discovered random quantum channels and additivity problems. He is also grateful to the audiences of two preliminary lectures about these results in Sendai and Yokohama. He also thanks T. Hayashi, R. Burstein and P. Śniady for discussions at various stages about related topics.

This research was conducted partly in Lyon 1 and Ottawa. The authors are grateful to these institutions for hosting their research. One author (I. N.) benefited from funding by the conference “Random matrices, related topics and applications” at C.R.M. and the mini-workshop “Introduction to infinite-dimensional topological groups”, in Ottawa organized by M. Neufang. He thanks the organizers of these two events for making a first visit to eastern Canada possible. B.C.’s research 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] Coecke, B. *Kindergarten quantum mechanics — lecture notes* Quantum theory: reconsideration of foundations—3, 81–98, AIP Conf. Proc., 810, Amer. Inst. Phys., Melville, NY, 2006.
- [2] Collins, B. *Moments and Cumulants of Polynomial random variables on unitary groups, the Itzykson-Zuber integral and free probability* Int. Math. Res. Not., (17):953-982, 2003.
- [3] Collins, B. and Nechita, I. *Random quantum channels II: Entanglement of random subspaces, Renyi entropy estimates and additivity problems*. arXiv:0906.1877
- [4] Collins, B. and Nechita, I. *Random Quantum Channels III*
- [5] 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.
- [6] Hastings, M.B. *Superadditivity of communication capacity using entangled inputs*. Nature Physics 5, 255 - 257 (2009).
- [7] Hayden, P. *The maximal p-norm multiplicativity conjecture is false*. arXiv/0707.3291v1.
- [8] Hayden, P., Leung, D. and Winter, A. *Aspects of generic entanglement*. Comm. Math. Phys. 265 (2006), 95–117.

- [9] 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.
- [10] Jones, V.F.R. *Planar Algebras* arXiv:math/9909027v1
- [11] Nechita, I. *Asymptotics of random density matrices*. *Ann. Henri Poincaré* 8 (2007), no. 8, 1521–1538.
- [12] 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.

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`

UNIVERSITÉ DE LYON, INSTITUT CAMILLE JORDAN, 43 BLVD DU 11 NOVEMBRE 1918, F-69622 VILLEURBANNE CEDEX, FRANCE

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