AIP | Journal of Mathematical Physics

Random matrix techniques in quantum information theory

Benoît Collins and Ion Nechita

Citation: Journal of Mathematical Physics **57**, 015215 (2016); doi: 10.1063/1.4936880
View online: http://dx.doi.org/10.1063/1.4936880
View Table of Contents: http://scitation.aip.org/content/aip/journal/jmp/57/1?ver=pdfcov
Published by the AIP Publishing

JOURNAL OF MATHEMATICAL PHYSICS **57**, 015215 (2016)

Random matrix techniques in quantum information theory

Benoît Collins[1,a)] and Ion Nechita[2,b)]
[1]*Department of Mathematics, Kyoto University, Kyoto 606-8502, Japan; Département de Mathématique et Statistique, Université d'Ottawa, 585 King Edward, Ottawa, Ontario K1N6N5, Canada; and CNRS, Lyon, France*
[2]*Zentrum Mathematik, M5, Technische Universität München, Boltzmannstrasse 3, 85748 Garching, Germany and Laboratoire de Physique Théorique, CNRS, IRSAMC, Université de Toulouse, UPS, F-31062 Toulouse, France*

(Received 15 September 2015; accepted 16 November 2015; published online 10 December 2015)

The purpose of this review is to present some of the latest developments using random techniques, and in particular, random matrix techniques in quantum information theory. Our review is a blend of a rather exhaustive review and of more detailed examples—coming mainly from research projects in which the authors were involved. We focus on two main topics, random quantum states and random quantum channels. We present results related to entropic quantities, entanglement of typical states, entanglement thresholds, the output set of quantum channels, and violations of the minimum output entropy of random channels. © *2015 AIP Publishing LLC.* [http://dx.doi.org/10.1063/1.4936880]

I. INTRODUCTION

Quantum computing was initiated in 1981 by Feynman at a conference on physics and computation at the MIT, where he asked whether one can simulate physics on a computer. As for quantum information theory (QIT), it is somehow the backbone of quantum computing, although it emerged independently in the 1960s and 1970s (with, among others, Bell inequalities). In the past 20-30 years, it has witnessed a very fast development, and it is now a major scientific field of its own.

In classical information theory, probabilistic methods have been at the heart of the theory from its inception.[101] In contrast, probabilistic methods have arguably played a less important role in the infancy of quantum information theory—although probability theory itself was cast at the heart of the postulates of quantum mechanics. However, the situation has dramatically changed in the past 10-15 years, and probabilistic techniques have nowadays proven to be very useful in quantum information theory. Quite often, these probabilistic techniques are very closely related to problems in random matrix theory.

Let us explain heuristically why random matrix theory (RMT) is a natural tool for quantum information theory, by comparing with the use of elementary probability in the concept of classical information. In classical information, the first—and arguably one of the greatest—success of the theory was to compute the relative volume of a typical set with Shannon's entropy function. Here, the main probabilistic tool was the central limit theorem (more precisely, an exponential version thereof). The central limit theorem is a tool that is very well adapted to the study of product measures on the product of (finite) sets. In quantum information, sets and probability measures on these sets, as well as measurements, are all replaced by matrices, and their non-commutative structure is central to quantum information theory. In addition, the use of "probabilistic techniques" in classical information theory is not a goal *per se*. It is a convenient mathematical tool to prove existence theorems, for which non-random proofs are much more difficult to achieve. Incidentally, it is rather natural to wonder what a "typical" set looks like.

a)Electronic address: collins@math.kyoto-u.ac.jp
b)Electronic address: nechita@irsamc.ups-tlse.fr

The situation is quite similar in quantum information theory: although there was no *a priori* need for random techniques, some problems—in particular the minimum output entropy additivity problem, which we discuss at length in this review—did not have an obvious non-random answer; therefore, it became not only natural, but also important, to consider how "typical" quantum objects behave. This was arguably initiated by the paper in Ref. 57. The results obtained in the first papers were of striking importance in quantum information theory, and they pointed at the fact that well established mathematical tools could be expected to be very useful tools to solve problems in quantum information theory. All these problems were naturally linked with probability measures on matrix spaces. The first tool that was recognized to play an important role was concentration of measure. But more generally, all techniques were connected to the theory of random matrices. Random matrix theory relies on a wide range of technical tools, and concentration of measure is one of them among others.

The first results using random techniques in quantum information theory attracted a few mathematicians—including the authors of this review, see also the bibliography—who undertook to apply systematically the state of the art in random matrix theory in order to study questions in quantum information theory.

Random matrix theory itself has a long history. Although it is considered as a field of mathematics (or mathematical physics), it was not born in mathematics, but rather in statistics and physics. Wishart introduced the distribution that bears his name in the 1920s,[112] in order to explain the discrepancy between the eigenvalues of a measured covariance matrix, and an expected covariance matrix. Later, Wigner had motivations from quantum physics when he introduced[111] the semi-circle distribution. Since then, random matrix theory has played a role in many fields of mathematics and science, which includes the following:

- theoretical physics,[113,72,78]
- combinatorics and algebraic geometry,[53,88]
- integrable systems and partial differential equations,[105]
- complex analysis and Riemann-Hilbert problems,[73]
- operator algebras,[108]
- telecommunication,[106]
- finance,[18] and
- number theory.[71]

The above list does certainly not exhaust the list of fields of application of random matrix theory, but quantum information theory is definitely one of the most recent of them (and a very natural one, too!).

Our goal in this paper is to provide an overview of a few important uses that random matrix theory had in quantum information theory. Instead of being exhaustive, we chose to pick a few topics that look important to us, and hopefully emblematic of the roles that random matrices could play in the future in QIT. Obviously, our choices are biased by our own experience.

We would like to point out that random techniques have also played very important roles in other aspects of quantum information theory, namely, Bell inequalities, and we refer to the excellent review in Ref. 92 for that.

This paper is organized as follows: Section II provides some mathematical notation for quantum information. It is followed by Section III that supplies background for random matrix and free probability theory. The remaining sections are a selection of applications of random matrix theory to quantum information, namely, Sec. IV: entanglement of random quantum states, Sec. V: properties of output of deterministic states (of interest) under quantum channels, Sec. VI: study of *all* outputs under specific random quantum channels, Sec. VII: the solution to the minimal output entropy (MOE) additivity problems, and finally Sec. VIII: other applications of RMT in quantum physics, and Sec. IX: a selection of open questions.

II. BACKGROUND ON QUANTUM INFORMATION: QUANTUM STATES AND CHANNELS

In this section we record the basic facts from quantum information theory needed in the sequel. The books in Refs. 87, 56, and 60 or the lecture notes in Ref. 96 are excellent references on the subject.

A. Quantum states

The adjoint A^* of a matrix A is the conjugate of its transpose. A matrix is said to be selfadjoint iff it is equal to its adjoint. We call $\mathcal{M}_d^{sa}$ the collection of selfadjoint $d \times d$ matrices. We denote the set of d-dimensional mixed quantum states (or density matrices) by $\mathcal{D}_d$,

$$\mathcal{D}_d := \{\rho \in \mathcal{M}_d^{sa}(\mathbb{C}) \,:\, \rho \geq 0 \text{ and } \mathrm{Tr}(\rho) = 1\}. \tag{2.1}$$

The collection of density matrices $\mathcal{D}_d$ is naturally associated to the Hilbert space $\mathbb{C}^d$. One of the fundamental postulates of quantum mechanics is that two disjoint systems can be studied together by taking their Hilbert tensor product. For example, a system with state space $\mathbb{C}^{d_1}$ and another one with state space $\mathbb{C}^{d_2}$ are studied together with the state space $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$. In particular, the density matrices have the structure of $\mathcal{D}_{d_1 d_2}$. Of particular interest is the subset

$$\mathcal{SEP}_{d_1,d_2} := \mathrm{conv}(\mathcal{D}_{d_1} \otimes \mathcal{D}_{d_2}) \subseteq \mathcal{D}_{d_1 d_2}.$$

This convex compact subset is interpreted as the collection of all "classical" density matrices on the bipartite state. Unless $d_1 = 1$ or $d_2 = 1$, it is a strict subset of $\mathcal{D}_{d_1 d_2}$. It is called the collection of *separable states*. States which are not separable are called *entangled*. The study of entangled states is one of the cornerstones of quantum information theory. As a first (and paramount) example of entangled state, consider the qubit Hilbert space $\mathbb{C}^2$ endowed with an orthonormal basis $\{e_1, e_2\}$, and the state

$$\mathcal{D}_4 \ni \Omega_2 = \omega_2 \omega_2^*,$$

where

$$\omega_2 = \frac{1}{\sqrt{2}}(e_1 \otimes e_1 + e_2 \otimes e_2),$$

called the maximally entangled qubit state. Similarly, qudits generalize qubits when $\mathbb{C}^2$ is replaced by $\mathbb{C}^d$. In this more general context, the maximally entangled state of two qudits is

$$\mathcal{D}_{d^2} \ni \Omega_d = \omega_d \omega_d^*,$$

where

$$\omega_d = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} e_i \otimes e_i. \tag{2.2}$$

B. Entropies

As in classical information theory,[101] entropic quantities play a very important role in quantum information theory. We define next the quantities of interest for the current work. Let $\Delta_k = \{x \in \mathbb{R}_+^k \,|\, \sum_{i=1}^k x_i = 1\}$ be the $(k-1)$-dimensional probability simplex. For a positive real number $p \in (0,1) \cup (1,\infty)$, define the *Rényi entropy of order p* of a probability vector $x \in \Delta_k$ to be

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

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

$$H(x) = H_1(x) = -\sum_{i=1}^{k} x_i \log x_i.$$

We also define the values for the parameters $p = 0, \infty$,

$$H_0(x) = \log \#\{i \,:\, x_i \neq 0\},$$
$$H_\infty(x) = -\log \|x\|_\infty.$$

We extend these definitions to density matrices by functional calculus,

$$\begin{aligned} H_0(\rho) &= \log \mathrm{rk}(\rho), \\ H_p(\rho) &= \frac{1}{1-p} \log \mathrm{Tr}\, \rho^p, \qquad p \in (0,1) \cup (1,\infty), \\ H(\rho) &= H_1(\rho) = -\mathrm{Tr}\, \rho \log \rho, \\ H_\infty(\rho) &= -\log \|\rho\|_\infty. \end{aligned}$$

C. 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

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

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

Proposition 2.1. A linear map $\Phi : \mathcal{M}_n(\mathbb{C}) \to \mathcal{M}_n(\mathbb{C})$ is a quantum channel if and only if one of the following three 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 operator $U \in \mathcal{U}_{nd}$ such that*

$$\Phi(X) = \mathrm{Tr}_{\mathcal{K}} \left[U(X \otimes Y)U^* \right], \quad \forall X \in \mathcal{M}_n(\mathbb{C}). \tag{2.3}$$

(2) Kraus decomposition. *There exists an integer k and matrices $L_1, \ldots, L_k \in \mathcal{M}_n(\mathbb{C})$ such that*

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

and

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

(3) Choi matrix. *The following matrix, called the* Choi matrix *of* Φ,

$$\mathcal{M}_{n^2}(\mathbb{C}) \ni C_\Phi = [\mathrm{id} \otimes \Phi](\Omega_d) = \sum_{i,j=1}^{n} E_{ij} \otimes \Phi(E_{ij}), \tag{2.4}$$

is positive-semidefinite and satisfies $[\mathrm{id} \otimes \mathrm{Tr}](C_\Phi) = \mathrm{I}$.

It can be shown that the dimension of the ancilla space $\mathcal{K}$ in the Stinespring dilation theorem can be chosen as $d = \dim \mathcal{K} = n^2$ 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.

Going back to the entropic quantities, of special interest for the computation of capacities of quantum channels to transmit classical information are the following quantities, called the *minimum*

output entropies of the channel. As the Rényi entropies, they are indexed by some positive real parameter p,

$$H_p^{\min}(\Phi) = \min_{\rho \in \mathcal{D}_n} H_p(\Phi(\rho)). \tag{2.5}$$

D. Graphical notation for tensors

Quantum states, tensors, and operations between these objects (composition, tensor product, applying a state through a quantum channel, etc.) can be efficiently represented graphically. The leading idea is that a string in a diagram means a tensor contraction. Many graphical theories for tensors and linear algebra computations have been developed in the literature.[93,24] Although they are all more or less equivalent, we will stick to the one introduced in Ref. 30, as it allows to compute the expectation of random diagrams in a diagrammatic way subsequently. For more details on this method, we refer the reader to the paper in Ref. 30 and to other work which make use of this technique.[31,29,34,35,47,27,75]

In the graphical calculus, matrices (or, more generally, tensors) are represented by boxes. Each box has differently shaped symbols, where the number of different types of them equals that of different spaces (exceptions are mentioned below). Those symbols are empty (white) or filled (black), corresponding to primal or dual spaces. Wires connect these symbols, corresponding to tensor contractions. A diagram is a collection of such boxes and wires and corresponds to an element of an abstract tensor product space. Rather than going through the whole theory, we focus next on a few key examples.

Suppose that each diagram in Figure 1 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 $V_1^* \otimes V_1 \to \mathbb{C}$ to M. The result of the diagram $\mathcal{D}_a$ is thus $T_{\mathcal{D}_a} = \mathrm{Tr}(M) \in \mathbb{C}$. 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 map $N \in \mathrm{End}(V_1 \otimes V_2, V_1 \otimes V_2)$. 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: $T_{\mathcal{D}_c} = \mathrm{Tr}_{V_1}(N) \in \mathrm{End}(V_2, V_2)$.

III. BACKGROUND ON RANDOM MATRIX THEORY AND FREE PROBABILITY

A. Gaussian random variables

The probability density of the *normal distribution* is

$$f(x \mid \mu, \sigma) = \frac{1}{\sigma\sqrt{2\pi}}\, e^{-\frac{(x-\mu)^2}{2\sigma^2}}.$$

Here, μ is the *mean*. The parameter σ is its *standard deviation* with its variance, then, σ^2. A random variable with a Gaussian distribution is said to be normally distributed.

Suppose X and Y are random vectors in $\mathbb{R}^k$ such that (X, Y) is a $2k$-dimensional normal random vector. Then, we say that the complex random vector $Z = X + iY$ has the *complex normal distribution*. The normal distribution (respectively, random vector) are also called *Gaussian distribution* (respectively, random vectors).

Historically, the first ensemble of random matrices having been studied is the Wishart ensemble,[112] see Ref. 13 [Chap. 3] or Ref. 2 [Section 2.1] for a modern presentation.

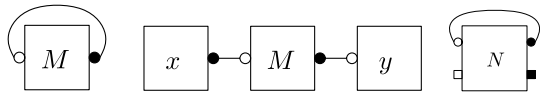

FIG. 1. Some simple diagrams.

Definition 3.1. Let $X \in \mathcal{M}_{d\times s}(\mathbb{C})$ be a random matrix with complex, standard, independent and identically distributed (i.i.d.) Gaussian entries. The distribution of the positive-semidefinite matrix $W = XX^* \in \mathcal{M}_d(\mathbb{C})$ is called a Wishart distribution *of parameters (d, s) and is denoted by $\mathcal{W}_{d,s}$.*

The study of the asymptotic behavior of Wishart random matrices is due to Marčenko and Pastur,[77] while the strong convergence in the theorem below has been proved by analytic tools such as determinantal point processes. Let us also recover it as a direct consequence of the much more general results.[76]

Theorem 3.2. *Consider a sequence s_d of positive integers which behaves as $s_d \sim cd$ as $d \to \infty$, for some constant $c \in (0, \infty)$. Let W_d be a sequence of positive-semidefinite random matrices such that W_d is distributed according to $\mathcal{W}_{d,s_d}$. Then, the sequence W_d converges strongly to the* Marčenko-Pastur distribution π_c *given by*

$$\pi_c = \max(1-c, 0)\delta_0 + \frac{\sqrt{(b-x)(x-a)}}{2\pi x}\,\mathbf{1}_{(a,b)}(x)\,dx, \tag{3.1}$$

where $a = (1-\sqrt{c})^2$ and $b = (1+\sqrt{c})^2$.

The Marčenko-Pastur distribution π_c is sometimes called the *free Poisson distribution*. We plotted in Figure 2 its density in the cases $c = 1$ and $c = 4$. The following theorem is the link between combinatorics and probability theory for Gaussian vectors: it allows to compute moments of any Gaussian vector, thanks to its covariance matrix. A *Gaussian space V* is a real vector space of random variables having moments of all orders, with the property that each of these random variables has centered Gaussian distributions. In order to specify the covariance information, such a Gaussian space comes with a positive symmetric bilinear form $(x, y) \to \mathbb{E}[xy]$. Gaussian spaces are in one-to-one correspondence with Euclidean spaces. In particular, the Euclidean norm of a random variable determines it fully (via its variance) and if two random variables are given, their joint distribution is determined by their angle. The following is usually called the Wick lemma.

Theorem 3.3. *Let V be a Gaussian space and $x_1, \ldots, x_k$ be elements in V. If $k = 2l+1$, then $\mathbb{E}[x_1 \cdots x_k] = 0$ and if $k = 2l$, then*

$$\mathbb{E}[x_1 \cdots x_k] = \sum_{\substack{p = \{\{i_1, j_1\}, \ldots, \{i_l, j_l\}\} \\ \text{pairing of } \{1, \ldots, k\}}} \prod_{m=1}^{l} \mathbb{E}[x_{i_m} x_{j_m}]. \tag{3.2}$$

In particular, it follows that if $x_1, \ldots, x_p$ are independent standard Gaussian random variables, then

$$\mathbb{E}[x_1^{k_1} \ldots x_p^{k_p}] = \prod_{i=1}^{p} (2k_i)!!.$$

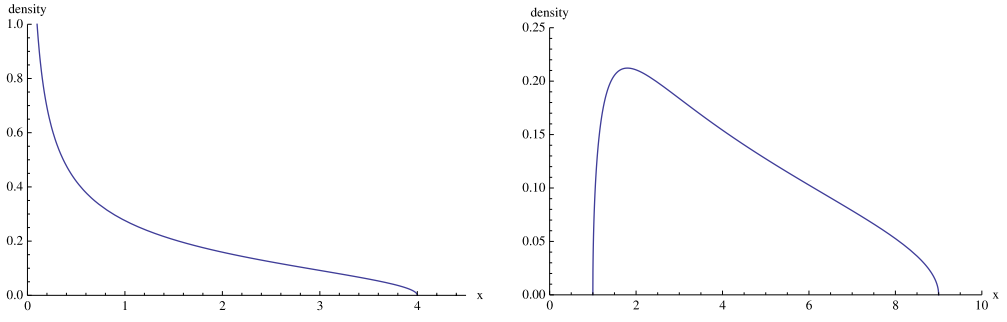

FIG. 2. The density of the Marčenko-Pastur distributions π_1 (left) and π_4 (right).

B. Unitary integration: Weingarten calculus

In this section, we gather some basic material on unitary integration and Weingarten calculus. For a more complete exposition, we refer to Refs. 25 and 36. Note that there exist similar theories for other classical groups (orthogonal, symplectic, etc.) but here, we stick to the unitary case.

Definition 3.4. Let n be a dimension parameter and σ a permutation of $\mathcal{S}_p$. The unitary Weingarten function $\mathrm{Wg}(n,\sigma)$ *is the coefficient of 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).*

To justify the introduction of the word "pseudo," we note that the function $\sigma \mapsto n^{\#\sigma}$ is invertible when n is large, as it behaves like $n^p\delta_e$ as $n \to \infty$. If $n < p$, the function is not invertible any more. The definition still makes sense if one takes the pseudo-inverse instead of the inverse.

The function Wg is related to integrals with respect to the Haar measure on the unitary group.

Theorem 3.5. *Let n be a positive integer and $(i_1,\ldots,i_p)$, $(i'_1,\ldots,i'_p)$, $(j_1,\ldots,j_p)$, $(j'_1,\ldots,j'_p)$ be p-tuples of positive integers from $\{1,2,\ldots,n\}$. Then,*

$$\int_{\mathcal{U}_n} U_{i_1j_1}\cdots U_{i_pj_p}\overline{U_{i'_1j'_1}}\cdots\overline{U_{i'_pj'_p}}\,dU = \sum_{\sigma,\tau\in\S_p} \delta_{i_1i'_{\sigma(1)}}\ldots\delta_{i_pi'_{\sigma(p)}}\delta_{j_1j'_{\tau(1)}}\ldots\delta_{j_pj'_{\tau(p)}}\mathrm{Wg}(n,\tau\sigma^{-1}). \tag{3.3}$$

If $p \neq p'$, then

$$\int_{\mathcal{U}_n} U_{i_1j_1}\cdots U_{i_pj_p}\overline{U_{i'_1j'_1}}\cdots\overline{U_{i'_{p'}j'_{p'}}}\,dU = 0. \tag{3.4}$$

Since we perform integration over large unitary groups, we are interested in the values of the Weingarten function in the limit $n \to \infty$. The following theorem describes the asymptotic behavior of the Wg function; see Ref. 25 for a proof.

Theorem 3.6. *For a permutation $\sigma \in \mathcal{S}_p$, let Cycles(σ) denote the set of cycles of σ. Then,*

$$\mathrm{Wg}(n,\sigma) = (-1)^{n-\#\sigma}\prod_{c\in Cycles(\sigma)}\mathrm{Wg}(n,c)(1+O(n^{-2})) \tag{3.5}$$

and

$$\mathrm{Wg}(n,(1,\ldots,d)) = (-1)^{d-1}c_{d-1}\prod_{-d+1\leq j\leq d-1}(n-j)^{-1}, \tag{3.6}$$

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

As a shorthand for the quantities in Theorem 3.6, we introduce the function Mob on the symmetric group. Mob is invariant under conjugation and multiplicative over the cycles. It is characterized by the following property: for any permutation $\sigma \in \mathcal{S}_p$,

$$\mathrm{Wg}(n,\sigma) = n^{-(p+|\sigma|)}(\mathrm{Mob}(\sigma)+O(n^{-2})), \tag{3.7}$$

where $|\sigma| = p - \#\sigma$ is the *length* of σ, i.e., the minimal number of transpositions that multiply to σ. The terminology for Mob comes from Moebius functions. Under identifying geodesic with non-crossing partitions, Mob can be seen as a Moebius function on the incidence algebra of the poset of non-crossing partitions. The lemma below is well-known, and it contains important combinatorial properties of the distance function on the symmetric group; this result is contained in Ref. 86.

Lemma 3.7. 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 $d(\sigma_1, \sigma_2)$; and*
- *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.*

C. Graphical interpretation of Wick and Weingarten calculi

The main motivation for the graphical calculus introduced previously is to interpret nicely the above integration Theorems 3.3 and 3.5. We consider first the case of the Weingarten calculus. The key to an interpretation relies on the concept of *removal* of boxes U and $\overline{U}$ from a diagram.

A removal r is a way to pair decorations of the U and $\overline{U}$ boxes appearing in a diagram. It consists in a pairing α of the white decorations of U boxes with the white decorations of $\overline{U}$ boxes, together with a pairing β between the black decorations of U boxes and the black decorations of $\overline{U}$ boxes. Assuming that $\mathcal{D}$ contains p boxes of type U and that the boxes U (respectively, $\overline{U}$) are labeled from 1 to p, then $r = (\alpha, \beta)$, where α, β are permutations of $\mathcal{S}_p$. The set of all removals of U and $\overline{U}$ boxes is denoted by $\mathrm{Rem}_U(\mathcal{D})$.

A removal $r \in \mathrm{Rem}_U(\mathcal{D})$ yields a new diagram $\mathcal{D}_r$ associated to r, which has the important property that it no longer contains boxes of type U or $\overline{U}$. One starts by erasing the boxes U and $\overline{U}$ but keeps the decorations attached to them. Assuming that one has labeled the erased boxes U and $\overline{U}$ with integers from $\{1, \ldots, p\}$, one connects *all* the (inner parts of the) *white* decorations of the ith erased U box with the corresponding (inner parts of the) *white* decorations of the $\alpha(i)$th erased $\overline{U}$ box. In a similar manner, one uses the permutation β to connect black decorations. In Ref. 30, we proved the following result.

Theorem 3.8. *The following holds true:*

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

In the case where diagrams also involve a box G corresponding to a *Gaussian random matrix*, we are also able to compute the expected value conditional to the σ-algebra of G by graphical methods, yielding a new interpretation of Wick formula.

Namely, the expectation value of a random diagram $\mathcal{D}$ can be computed by a *removal* procedure as in the unitary case. Without loss of generality, we assume that we do not have in our diagram adjoints of Gaussian matrices, but instead their complex conjugate box. This assumption allows for a more straightforward use of Wick Lemma 3.3. As in the unitary case, we can assume that $\mathcal{D}$ contains only one type of random Gaussian box G; the other independent random Gaussian matrices are assumed constant at this stage as they shall be removed in the same manner afterwards.

A removal of the diagram $\mathcal{D}$ is a pairing between *Gaussian boxes* G and their conjugates $\overline{G}$. The set of removals is denoted by $\mathrm{Rem}_G(\mathcal{D})$ and it may be empty: if the number of G boxes is different from the number of $\overline{G}$ boxes, then $\mathrm{Rem}_G(\mathcal{D}) = \emptyset$ (this is consistent with the first case of Wick formula (3.2)). Otherwise, a removal r can identified with a permutation $\alpha \in \mathcal{S}_p$, where p is the number of G and $\overline{G}$ boxes. The main difference between the notion of a removal in the Gaussian and the Haar unitary cases is as follows: in the Haar unitary (Weingarten) case, a removal was associated with a *pair of permutations*: one has to pair white decorations of U and $\overline{U}$ boxes and, independently, black decorations of conjugate boxes. On the other hand, in the Gaussian/Wick case, one pairs conjugate boxes: white and black decorations are paired in an identical manner; hence, only one permutation is needed to encode the removal.

To each removal r associated to a permutation, $\alpha \in \mathcal{S}_p$ corresponds to a removed diagram $\mathcal{D}_r$ constructed as follows. One starts by erasing the boxes G and $\overline{G}$ but keeps the decorations attached to these boxes. Then, the decorations (white *and* black) of the ith G box are paired with the decorations of the $\alpha(i)$th $\overline{G}$ box in a coherent manner, see Figure 3.

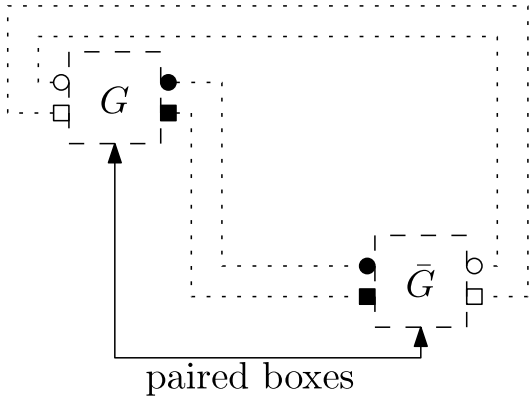

FIG. 3. Pairing of boxes in the Gaussian case.

The graphical reformulation of Wick Lemma 3.3 becomes the following theorem from Ref. 31.

Theorem 3.9. *The following holds true:*

$$\mathbb{E}_G[\mathcal{D}] = \sum_{r \in \mathrm{Rem}_G(\mathcal{D})} \mathcal{D}_r.$$

D. Some elements of free probability theory

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

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

$$\phi(a_1 \cdots a_k) = 0$$

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

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

$$\mu_{(a_1,\ldots,a_k)} : \mathbb{C}\langle X_1,\ldots,X_k\rangle \to \mathbb{C}$$
$$P \mapsto \phi(P(a_1,\ldots,a_k)).$$

In the case of a single, self-adjoint random variable x, if the moments of x coincide with those of a compactly supported probability measure μ, i.e.,

$$\forall p \geq 1, \qquad \phi(x^p) = \int t^p d\mu(t),$$

we say that x has distribution μ. The most important distribution in free probability theory is the semicircular distribution

$$\mu_{SC(0,1)} = \frac{\sqrt{4-x^2}}{2\pi}\mathbf{1}_{[-2,2]}(x)dx,$$

which is, for reasons we will not get into, the free world equivalent of the Gaussian distribution in classical probability (see Ref. 86 [Lecture 8] for the details, and Fig. 4 for a plot). A random variable

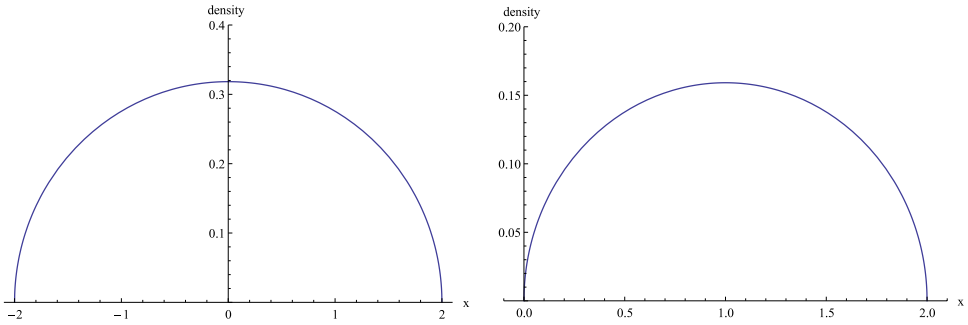

FIG. 4. The density of the semicircular distributions $\mu_{SC(0,1)}$ (left) and $\mu_{SC(1,1/4)}$ (right).

x having distribution $\mu_{SC(0,1)}$ has the Catalan number for moments,

$$\phi(x^p) = \begin{cases} \mathrm{Cat}_p := \dfrac{1}{p+1}\begin{pmatrix} 2p \\ p \end{pmatrix}, & \text{if } p \text{ is even} \\ 0, & \text{if } p \text{ is odd} \end{cases}.$$

More generally, if x has distribution $\mu_{SC(0,1)}$, we say that $y = \sigma x + m$ has distribution

$$\mu_{SC(m,\sigma^2)} = \frac{\sqrt{4\sigma^2 - (x-m)^2}}{2\pi\sigma^2}\mathbf{1}_{[m-2\sigma, m+2\sigma]}(x)dx. \tag{3.8}$$

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

The following result is contained in Ref. 107 (see also Ref. 36).

Theorem 3.10. *Let $\{U_k^{(n)}\}_{k\in\mathbb{N}}$ be a collection of independent Haar distributed random matrices of $\mathcal{M}_n(\mathbb{C})$ and $\{W_k^{(n)}\}_{k\in\mathbb{N}}$ be a set of constant matrices of $\mathcal{M}_n(\mathbb{C})$ admitting a joint limit distribution as $n \to \infty$ with respect to the state $n^{-1}\,\mathrm{Tr}$. Then, almost surely, the family $\{U_k^{(n)}, W_k^{(n)}\}_{k\in\mathbb{N}}$ admits a limit $*$-distribution $\{u_k, w_k\}_{k\in\mathbb{N}}$ with respect to $n^{-1}\,\mathrm{Tr}$, such that $u_1, u_2, \ldots, \{w_1, w_2, \ldots\}$ are free.*

Given two free random variables $a, b \in \mathcal{A}$, the distribution μ_{a+b} is uniquely determined by μ_a and μ_b. The free additive convolution of μ_a and μ_b is defined by $\mu_a \boxplus \mu_b = \mu_{a+b}$. When $x = x^* \in \mathcal{A}$, we identify μ_x with the spectral measure of x with respect to τ. The operation $\boxplus$ induces a binary operation on the set of probability measures on $\mathbb{R}$. Similarly, we write $\mu_a \boxminus \mu_b = \mu_{a-b}$.

IV. ENTANGLEMENT OF RANDOM QUANTUM STATES

A. Probability distributions on the set of quantum states

In this section, we review a few natural models of random quantum states, and we describe their typical entanglement properties.

1. Random pure quantum states

The first model for random quantum states we look at is the *uniform measure on pure quantum states*, i.e., extreme points of $\mathcal{D}_d$ (the rank one selfadjoint projections). Indeed, the set of pure quantum states of a finite dimensional Hilbert space $\mathcal{H} = \mathbb{C}^d$ can be identified, up to a phase, with the set of points on the unit sphere of $\mathcal{H}$, $\{x \in \mathbb{C}^d : \|x\| = 1\}$. On this set, there is a canonical probability measure, the uniform (or Lebesgue) measure.

Definition 4.1. A random pure quantum state $x \in \mathbb{C}^d$ is said to follow the uniform distribution *if x is uniformly distributed on the unit sphere of $\mathbb{C}^d$. We denote the uniform distribution of pure states in $\mathbb{C}^d$ by χ_d.*

The uniform distribution has the following important properties [Ref. 83, Section 2.1].

Proposition 4.2. Let $x \in \mathbb{C}^d$ be a uniformly distributed pure quantum state, $x \sim \chi_d$. Then, we have the following.

(1) *For any unitary operator $U \in \mathcal{U}_d$ (U can either be fixed or random, but independent from x), the random pure state Ux also has the uniform distribution, $Ux \sim \chi_d$.*
(2) *If $G \in \mathbb{C}^d$ is random complex Gaussian vector, $X \sim \mathcal{N}_{\mathbb{C}}(0, I_n)$, then $X/\|X\|$ is a uniform quantum pure state, $X/\|X\| \sim \chi_d$.*
(3) *Let U be a random unitary matrix distributed along the Haar measure on $\mathcal{U}_n$ and let y be the first column of U. Then, $y \in \mathbb{C}^d$ is a uniform quantum pure state, $y \sim \chi_d$.*

In applications, whenever one needs to consider generic pure quantum states and that there is no underlying structure in the Hilbert space where the states live, the uniform measure is used indiscriminately. Later, in Section IV A 4, we shall encounter another probability distribution on a Hilbert space $\mathcal{H}$, which is to be used in the case where the space has a tensor product structure $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \mathcal{H}_k$.

A different possibility was considered in Ref. 85, starting from the first point in 4.2, and replacing the Haar unitary U with the value of the unitary Brownian motion at some fixed time t (recall that the Haar measure is recovered at the limit $t \to \infty$). The resulting measure depends on the time $t > 0$ and on the initial vector x on which the unitary acts. We refer the interested reader to Ref. 85 for the details.

2. The induced ensemble

We introduce in this section a family of probability distributions on the set of (mixed) quantum states $\mathcal{D}_d$ which has a nice physical interpretation and, at the same time, a simple mathematical presentation.

The following family was introduced by Braunstein in Ref. 20 and studied by Hall,[52] and later, in great detail, by Życzkowski and Sommers.[116,104]

Definition 4.3. Given two positive integers d, s, consider a random pure quantum state $x \in \mathbb{C}^d \otimes \mathbb{C}^s$. The distribution of the random variable

$$\rho = [\mathrm{id}_d \otimes \mathrm{Tr}_s](xx^*) \in \mathcal{D}_d$$

is called the induced measure *of parameters (d, s) and it is denoted by $\nu_{d,s}$.*

We gather in the following proposition some basic facts about the measures (for the proofs, see Ref. 116).

Proposition 4.4. Let $\mathcal{D}_d \ni \rho \sim \nu_{d,s}$ be a density matrix having an induced distribution of parameters (d, s).

(1) *With probability one, ρ has rank $\min(d, s)$.*
(2) *For any unitary operator $U \in \mathcal{U}_d$ (fixed or independent from ρ), the density matrix $U\rho U^*$ has the same distribution as ρ.*
(3) *There exist a unitary matrix $U \in \mathcal{U}_d$ and a diagonal matrix $\Delta = \mathrm{diag}(\lambda_1, \ldots, \lambda_d)$ such that U is Haar distributed, U and Δ are independent, and $\rho = U\Delta U^*$; we say that the radial and the angular parts of ρ are independent.*
(4) *The eigenvalues $(\lambda_1, \ldots, \lambda_d)$ have the following joint distribution:*

$$C_{d,s} \mathbf{1}_{\lambda_1 + \cdots + \lambda_d = 1} \prod_{i=1}^{d} \mathbf{1}_{\lambda_i \geq 0} \prod_{1 \leq i < j \leq d} (\lambda_i - \lambda_j)^2 \prod_{i=1}^{d} \lambda_i^{s-d},$$

where $C_{d,s}$ is the constant

$$C_{d,s} = \frac{\Gamma(ds)}{\prod_{i=0}^{d-1}\Gamma(s-i)\Gamma(d+1-i)}.$$

Remark 4.5. Importantly, in the case $s = d$, the distribution $\nu_{d,d}$ is precisely the Lebesgue measure *on the compact set $\mathcal{D}_d$, seen as a subset of the affine subspace $\{A \in \mathcal{M}_d^{sa}(\mathbb{C}) : \mathrm{Tr}(A) = 1\}$, see Ref. 116* [Section 2.4]. *The measure $\nu_{d,d}$ is sometimes called the* Hilbert-Schmidt measure*, since it is induced by the Euclidian, or Hilbert-Schmidt, distance. Note that the volume of $\mathcal{D}_d$ is given by Ref. 117* [Equation (4.5)]*,*

$$\mathrm{vol}(\mathcal{D}_d) = \sqrt{d}(2\pi)^{d(d-1)/2}\frac{(d-1)!}{(d^2-1)!}.$$

In Ref. 83, the induced measures $\nu_{d,s}$ are shown to be closely related to the Wishart ensemble $\mathcal{W}_{d,s}$ from Definition 3.1.

Proposition 4.6. Let $W \in \mathcal{M}_d(\mathbb{C})$ be a Wishart matrix of parameters (d,s) and put $\rho := W/\mathrm{Tr}(W) \in \mathcal{D}_d$. Then, we have the following.

(1) *The random variables ρ and $\mathrm{Tr}(W)$ are independent.*
(2) *The distribution of $\mathrm{Tr}(W)$ is chi-squared, with ds degrees of freedom.*
(3) *The random density matrix ρ follows the induced measure of parameters (d,s), i.e., $\rho \sim \nu_{d,s}$.*
(4) *The random variable W, conditioned on the (zero probability) event $\mathrm{Tr}(W) = 1$, has distribution $\nu_{d,s}$.*

Let us now discuss the asymptotic behavior of the probability measures $\nu_{d,s}$. We first consider the "trivial" regime, where d is fixed and $s \to \infty$. The result here is as follows, see Ref. 83.

Proposition 4.7. For a fixed dimension d, consider a sequence of random density matrices $(\rho_s)_s$ having distribution $\rho_s \sim \nu_{d,s}$. Then, almost surely as $s \to \infty$, $\rho_s \to d^{-1}I_d$.

The interesting scaling is the fixed ratio one, where both d and $s = s_d$ grow to infinity, in such a way that $s_d/d \to c$, for a fixed constant $c \in (0,\infty)$. The next result is an easy consequence of Theorem 3.2 and Proposition 4.6.

Proposition 4.8. For a fixed positive constant c, consider a sequence of random density matrices $(\rho_d)_d$ having distribution $\rho_d \sim \nu_{d,s_d}$; here, we assume that $s_d \sim cd$ as $d \to \infty$. Then, almost surely as $d \to \infty$, the empirical eigenvalue distribution of the random matrix $s_d\rho_d$ converges weakly to the Marčenko-Pastur distribution π_c from (3.1),

$$\lim_{d\to\infty}\frac{1}{d}\sum_{i=1}^{d}\delta_{s_d\lambda_i(\rho_d)} = \pi_c.$$

Informally, the result above can be stated as follows: consider a tensor product Hilbert space $\mathcal{H} = \mathbb{C}^d \otimes \mathbb{C}^{\lfloor cd \rfloor}$ and random, uniform pure state $\psi \in \mathcal{H}$. Then, the eigenvalues of the partial trace $\rho = [\mathrm{id} \otimes \mathrm{Tr}](\psi\psi^*)$ are, up to a scaling of cd, distributed along the Marčenko-Pastur distribution π_c (3.1).

Finally, as suggested by Proposition 4.6, in order to simulate on a computer quantum states having distribution $\nu_{d,s}$, one sets

$$\rho = \frac{GG^*}{\mathrm{Tr}(GG^*)},$$

where $G \in \mathcal{M}_{d\times s}(\mathbb{C})$ is an element from the *Ginibre ensemble*, i.e., G has i.i.d. standard complex Gaussian entries; see Ref. 115 [Section III.D].

3. The Bures measure

The Bures metric on the set of density matrices (see Ref. 17) is defined as

$$d_B(\rho,\sigma) = \sqrt{2 - 2\mathrm{Tr}[(\sqrt{\rho}\sigma\sqrt{\rho})^{1/2}]}.$$

From this metric, one can define a probability distribution ν_B on $\mathcal{D}_d$, by asking that Bures balls of equal radius have the same volume.

The properties of the measure ν_B have been extensively studied in Refs. 52, 103, and 89, and we recall in the next proposition the main facts.

Proposition 4.9. Let $\rho \in \mathcal{D}_d$ be a random density matrix having distribution ν_B. Then, we have the following.

(1) *The eigenvalues $\lambda_1, \ldots, \lambda_d$ of ρ have distribution,*

$$C_B \mathbf{1}_{\lambda_1+\cdots+\lambda_d=1} \prod_{i=1}^{d} \mathbf{1}_{\lambda_i>0} \lambda_i^{-1/2} \prod_{1\leq i<j\leq d} \frac{(\lambda_i-\lambda_j)^2}{\lambda_i+\lambda_j},$$

where the constant C_B reads

$$C_B = 2^{d^2-d} \frac{\Gamma(d^2/2)}{\pi^{d/2} \prod_{i=1}^{d} \Gamma(i+1)}.$$

(2) *If $A \in \mathcal{M}_d(\mathbb{C})$ is a random Ginibre matrix and $U \in \mathcal{U}_d$ is a Haar random unitary independent from A, then the random matrix*

$$\sigma = \frac{(I+U)AA^*(I+U)^*}{\mathrm{Tr}[(I+U)AA^*(I+U)^*]}$$

has distribution ν_B.

4. Random states associated to graphs

The probability distributions on $\mathcal{D}_d$ we have considered so far do not make any assumptions on the internal structure of the underlying Hilbert space $\mathbb{C}^d$. When there is a relevant structure, it is natural to introduce other probability measures that are adapted to the concept. This line of research was carried out, among others, in Refs. 34 and 35, and we recall briefly below the notion of *random graph states* defined there.

Let a graph $G = (V, E)$ having k vertices $V_1, \ldots, V_k$ and m edges $E_1, \ldots, E_m$. Let N be a fixed positive integer. We consider the (total) Hilbert space

$$\mathcal{H} = \bigotimes_{i=1}^{k} \mathcal{H}_i,$$

where $\mathcal{H}_i = (\mathbb{C}^N)^{\otimes d_i}$ is the *local Hilbert space* at vertex i and d_i is the degree of V_i in G. Each copy of $\mathbb{C}^N$ inside $\mathcal{H}_i$ is associated to some edge E_j incident to V_i. In turn, the total Hilbert space admits two decompositions, relative to vertices and edges,

$$\mathcal{H} = \bigotimes_{i=1}^{k} \mathcal{H}_i = \bigotimes_{j=1}^{m} \mathcal{K}_j \simeq (\mathbb{C}^N)^{\otimes 2m},$$

where $\mathcal{K}_j = \mathbb{C}^N \otimes \mathbb{C}^N$. Define now the following random pure state:

$$\varphi_G = \left[\bigotimes_{i=1}^{k} U_i\right] \left[\bigotimes_{j=1}^{m} \omega_j\right],$$

where $\{U_i\}_{i=1}^{k}$ are i.i.d. Haar distributed random unitary matrices acting on the local Hilbert spaces at the vertices, and ω_j are maximally entangled states (2.2). Note that in the above expression,

the unitary operators "mix" the product of maximally entangled states at the vertices, yielding, in general, a global entangled state.

The object of study in this section is a random mixed quantum state defined as follows: for a subset $S \subseteq \{1,2,\ldots,2m\}$ of copies of $\mathbb{C}^N$, define

$$\rho_{G,S} = [\mathrm{id}_S \otimes \mathrm{Tr}_{S^c}](\varphi_G \varphi_G^*) \in \mathcal{D}_{N^{|S|}}.$$

The statistical properties of the distribution of $\rho_{G,S}$ are studied in Ref. 34 [Section 5]. Namely, one proves that for some special types of marginals (called *adapted*), the area law holds *exactly*, and a variant of it holds in a more general context.

Let us recall the definition of an adapted marginal and of the area law. To any graph state, we associate two partitions of the set of $n = 2m$ subspaces: a vertex partition $\mathcal{P}_{\mathrm{vertex}}$ which encodes the vertices of the graph, and a pair partition $\mathcal{P}_{\mathrm{edge}}$ which encodes the edges (corresponding to maximally entangled states). In particular, two subsystems $\mathcal{H}_i$ and $\mathcal{H}_j$ belong to the same block of $\mathcal{P}_{\mathrm{vertex}}$ if they are attached to the same vertex of the initial graph. Each edge (i,j) of the graph contributes a block of size two $\{i,j\}$ to the edge partition $\mathcal{P}_{\mathrm{edge}}$. Given a subset S of a set I of quantum systems (i.e., Hilbert spaces), the marginal of a state ρ on the subsystem induced by indices of S is the partial trace over the remaining subsystems $T = I \setminus S$: $\rho_S = [\mathrm{id}_S \otimes \mathrm{Tr}_T](\rho)$. Similarly, the marginal of a random graph state $\varphi_G \varphi_G^*$ is specified by a 2-set partition $\mathcal{P}_{\mathrm{trace}} = \{S,T\}$.

Definition 4.10. A marginal ρ_S is called adapted *if*

$$\mathcal{P}_{trace} \geq \mathcal{P}_{vertex} \tag{4.1}$$

for the usual refinement order on partitions. In other words, a marginal is adapted if and only if the number of traced out systems in each vertex is either zero or maximal. If this is the case, then the partition boundary, which splits the graph into parts $\{S,T\}$, does not "cross" any vertices of the graph.

Because of the above property, for adapted marginals, we can speak about *traced out vertices*, because if one subsystem of a vertex is traced out, then all the other systems of that vertex are also traced out. We now define precisely what we mean by *area laws* in the context of quantum states associated to graphs. The partition $\{S,T\}$ defines a boundary between the set of vertices that are traced out and vertices that survive entirely.

Definition 4.11. The boundary *of the adapted partition $\{S,T\}$ is defined as the set of all (unoriented) edges $e = \{i_S, j_T\}$ in the graph state with the property that $i_S \in S$ and $j_T \in T$. Equivalently, it is the set of edges of the type* ×⟵●. *The boundary of a partition shall be denoted by ∂S.*

The area *of this boundary is its cardinality $|\partial S|$, i.e., the number of edges between S and T.*

It was shown in Ref. 35 that the *area law* holds *exactly* for adapted marginals of graph states, where arbitrary dimensions of subsystem are allowed. Note that, for a given (boundary) edge $\{i,j\}$, we have $d_i = d_j$, the common dimension of the maximally entangled state corresponding to the edge $\{i,j\}$. The following result follows from linear algebra considerations, and one does not need random Haar unitary operators in this case.

Proposition 4.12. Let ρ_S be an adapted *marginal of a graph state φ_G. Then, the entropy of ρ_S has the following* exact, deterministic *value:*

$$H(\rho_S) = |\partial S| \log N. \tag{4.2}$$

For the system corresponding to the graph shown in Figure 5 with all subsystems of size N, the von Neumann entropy reads

$$H(\rho_S) = 5 \log N. \tag{4.3}$$

This follows from the fact that ρ_S is in this case a unitary conjugation of a maximally mixed state of size N^5 with an arbitrary pure state of size N^6. We refer the reader to Section VIII D for a more general result in this direction (for non-adapted marginals).

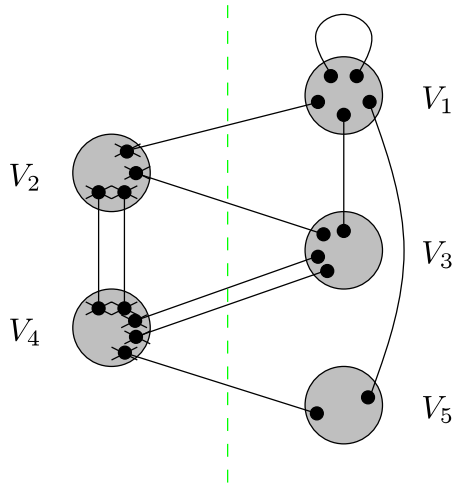

FIG. 5. An adapted marginal for a graph state. The dashed (green) line represents the *boundary* between the traced–out subsystems T and the surviving subsystems S.

B. Moments: Average entropy

In this section, we present results concerning certain quantities of interest in quantum information theory, and in particular, their average values over the different ensembles introduced previously.

Let us start with the case of the uniform measure on the set of pure quantum states. The statistics of the coordinates of a uniform random pure state can be obtained by the so-called *spherical integrals* [Ref. 40, Section 2.7]. The following result could also be deduced from the Wick formula in Section III A or from the Weingarten formula in Section III B.

Lemma 4.13. For any non-negative integers $\alpha_1, \ldots, \alpha_d \geq 0$, we have

$$\mathbb{E}_{x\sim\chi_d}\left[|x_1|^{2\alpha_1}|x_2|^{2\alpha_2}\cdots|x_d|^{2\alpha_d}\right] = (d-1)!\frac{\alpha_1!\alpha_2!\cdots\alpha_d!}{(d-1+\alpha_1+\alpha_2+\cdots+\alpha_d)!}.$$

We move now to the case of random density matrices having the induced distributions $\nu_{d,s}$ discussed in Section IV A 2. Using the relation between this distribution and the Wishart ensemble, the following result has been shown in Refs. 104 and 83.

Proposition 4.14. The moments of a random density matrix $\rho \in \mathcal{D}_d$ having distribution $\nu_{d,s}$ are given by

$$\mathbb{E}\mathrm{Tr}(\rho^q) = \frac{\Gamma(ds)}{\Gamma(ds+q)}\sum_{j=1}^{q}(-1)^{j-1}\frac{[s+q-j]_q[d+q-j]_q}{(q-j)!(j-1)!},$$

where $[a]_q = a(a-1)\cdots(a-q+1)$. In particular, the first few moments read

$$\mathbb{E}\mathrm{Tr}(\rho^2) = \frac{d+s}{ds+1},$$
$$\mathbb{E}\mathrm{Tr}(\rho^3) = \frac{d^2+3ds+s^2+1}{(ds+1)(ds+2)},$$
$$\mathbb{E}\mathrm{Tr}(\rho^4) = \frac{d^3+6d^2s+6ds^2+s^3+5d+5s}{(ds+1)(ds+2)(ds+3)}.$$

A more detailed statistical study of these quantities (and thus, of the Rényi entropies) has been performed in Refs. 39 and 82, where the existence of phase transitions has been showed. The average von Neumann entropy of a random density matrix was conjectured by page in Ref. 91 and later proved in Refs. 41, 98, and 100.

Proposition 4.15. The average von Neumann entropy of a random density matrix having distribution $\nu_{d,s}$ is

$$\mathbb{E}H(\rho) = \sum_{i=s+1}^{ds} \frac{1}{i} - \frac{d-1}{2s}.$$

C. Entanglement

The notion of quantum entanglement has been recognized to be at the center of quantum mechanics from the early days of the theory. The reader interested in entanglement theory is referred to the excellent review paper in Ref. 66. In this review, we shall only be concerned with *bipartite entanglement*. For entanglement properties of random quantum states in the multipartite setting, see Ref. 1 and Section VIII C.

Recall that a quantum state $\rho \in \mathcal{D}_{nk}$ is *separable* iff it can be written as a convex combination of tensor product states,

$$\rho = \sum_{i=1}^{r} p_i \sigma_i \otimes \tau_i,$$

where $\sigma_i \in \mathcal{D}_n$, $\tau_i \in \mathcal{D}_k$, and (p_i) is a probability vector: $p_i \geq 0$ and $\sum_i p_i = 1$. The set of separable states is denoted by $\mathcal{SEP}_{n,k} \subseteq \mathcal{D}_{nk}$ and the states in its complement are called entangled.

In this section, we are going to review some results about the (Euclidean) volume of the set of separable states. Equivalently, volumes can be expressed, up to a factor, from the probability that a quantum state is separable, under the induced measure $\nu_{nk,nk}$, see Remark 4.5.

The first result in this direction is quite remarkable.[51] It has many interesting corollaries, one of them being that the set $\mathcal{SEP}$ of separable states has non-empty interior.

Proposition 4.16. The largest Euclidean ball centered at the maximally mixed state $I/(nk)$ and contained in $\mathcal{D}_{nk}$ is separable and has radius $[nk(nk-1)]^{-1/2}$.

In the case of the Euclidean measure $\nu_{nk,nk}$, it has been shown in Ref. 8 [Theorem 1] that the ratio between the volume of $\mathcal{SEP}_{n,n}$ and $\mathcal{D}_{n^2}$ vanishes when $n \to \infty$. In the case where the parameter s of the induced measure $\nu_{nk,s}$ grows to infinity, while n and k are kept fixed, the measure $\nu_{nk,s}$ concentrates around the maximally mixed state I_{nk} (see Proposition 4.6), so

$$\lim_{s\to\infty} \mathbb{P}_{\nu_{nk,s}}[\rho \in \mathcal{SEP}_{nk}] = 1.$$

More precise estimates have been obtained in Ref. 12 in the case of the induced measures. In order to present these results, we need first to introduce the concept of *thresholds*.

Consider a family of sets of density matrices $X_d \subseteq \mathcal{D}_d$. The idea of a threshold captures the behavior of the probability that a quantum state $\rho \in \mathcal{D}_d$ is an element of X_d, when the probability is measured with the induced measure $\nu_{d,s}$; we would like to know, when $d \to \infty$, for which values of the parameter s, the probability vanishes or becomes close to 1. More precisely, we say that a *threshold phenomenon* with value c_0 on the scale f occurs when the following holds: let $s_d \sim cf(d)$ for a constant $c > 0$. Then, we have the following.

(1) If $c < c_0$, $\lim_{d\to\infty} \mathbb{P}_{\nu_{d,s_d}}[\rho \in X_d] = 0$.
(2) If $c > c_0$, $\lim_{d\to\infty} \mathbb{P}_{\nu_{d,s_d}}[\rho \in X_d] = 1$.

This definition was first considered in the quantum information theory literature by Aubrun in Ref. 6 to study the positive partial transpose (PPT) criterion (see Sec. IV D).

We state now the main result in Ref. 12, regarding the threshold for the sets $\mathcal{SEP}_{n,n}$. The following statement corresponds to Ref. 12, [Theorem 2.3], which deals with the so-called *balanced regime* $k = n$. For the *unbalanced regime* $k \neq n$, see Ref. 12 [Section 7.2].

Theorem 4.17. *There exist constants c, C and a function $f(n)$ satisfying*

$$cn^3 < f(n) < Cn^3 \log^2(n)$$

such that

(1) *if* $s_n < f(n)$, $\lim_{n\to\infty} \mathbb{P}_{\nu_{n^2,s_n}}[\rho \in \mathcal{SEP}_{n,n}] = 0$,
(2) *if* $s_n > f(n)$, $\lim_{n\to\infty} \mathbb{P}_{\nu_{n^2,s_n}}[\rho \in \mathcal{SEP}_{n,n}] = 1$.

Note that the above result does not enter precisely in the threshold framework, as it was defined just above; one would need to eliminate the logarithm factors and to compute exactly the constants in the statement above to achieve this, see Question 9.1. The result is nevertheless an important achievement, given the fact that questions dealing directly with the set of separable states are usually very difficult.

D. Entanglement criteria

The question whether a given mixed quantum state is separable or entangled has been proven to be a NP-hard one.[50] To circumvent this worse-case intractability, *entanglement criteria* are used. These are efficiently computable conditions which are necessary for separability; in other words, an entanglement criterion is a (usually convex) super-set $\mathcal{X}_d$ of the set of separable states, for which the membership problem is efficiently solvable (see Ref. 9 for the number of such criteria needed to obtain a good approximation of the set of separable states). As in Sec. IV C, from a probabilistic point of view, estimating the probability that a random quantum state (sampled from the induced ensemble) is an element of $\mathcal{X}_d$ is central. In what follows, we shall tackle this problem for different entanglement criteria in the framework of thresholds.

Let us start with the most used example, the PPT criterion. The PPT criterion has been introduced by Peres in Ref. 94: if a quantum state $\rho \in \mathcal{D}_{nk}$ is separable, then

$$\rho^\Gamma := [\mathrm{id} \otimes \mathrm{transp}](\rho) \geq 0.$$

Note that the positivity of ρ^Γ is equivalent to the positivity of $\rho^\Gamma = [\mathrm{transp} \otimes \mathrm{id}](\rho)$, so it does not matter on which tensor factor the transpose application acts. We denote by $\mathcal{PPT}_{n,k}$ the set of PPT states

$$\mathcal{PPT}_{n,k} := \{\rho \in \mathcal{D}_{nk} \,:\, \rho^\Gamma \geq 0\} \supseteq \mathcal{SEP}_{n,k}.$$

This necessary condition for separability has been shown to be also sufficient for qubit-qubit and qubit-qutrit systems ($nk \leq 6$) in Ref. 64. The PPT criterion for random quantum states has first been studied numerically in Ref. 114. The analytic results in the following proposition are from Ref. 6 (in the balanced case) and from Ref. 14 (in the unbalanced case); see also Ref. 47 for some improvements in the balanced case and the relation to meanders.

Proposition 4.18. Consider a sequence $\rho_n \in \mathcal{D}_{nk_n}$ of random quantum states from the induced ensemble ν_{nk_n,cnk_n}, where k_n is a function of n and c is a positive constant.

In the balanced regime $k_n = n$, the (properly rescaled) empirical eigenvalue distribution of the states ρ_n^Γ converges to a semicircular measure $\mu_{SC(1,1/c)}$ of mean 1 and variance $1/c$, see Eq. (3.8). In particular, the threshold for the sets $\mathcal{PPT}_{n,n}$ $(n \to \infty)$ is $c_0 = 4$.

In the unbalanced regime $k_n = k$ fixed, the (properly rescaled) empirical eigenvalue distribution of the states ρ_n^Γ converges to a free difference of free Poisson distributions (see Section III D for the definitions),

$$\pi_{ck(k+1)/2} \boxminus \pi_{ck(k-1)/2}.$$

In particular, the threshold for the sets $\mathcal{PPT}_{n,k}$ (k fixed, $n \to \infty$) is

$$c_0 = 2 + 2\sqrt{1 - \frac{1}{k^2}}.$$

We consider next the *reduction* criterion (RED). Introduced in Refs. 63 and 21, the reduction criterion states that if a bipartite quantum state $\rho \in \mathcal{D}_{nk}$ is separable, then

$$\rho^{red} := [\mathrm{id} \otimes R](\rho) \geq 0,$$

where $R : \mathcal{M}_k(\mathbb{C}) \to \mathcal{M}_k(\mathbb{C})$ is the *reduction map*,

$$R(X) = I_k \cdot \mathrm{Tr}(X) - X.$$

We denote by $\mathcal{RED}_{n,k}$ the set of quantum states having positive-semidefinite reductions (on the second subsystem),

$$\mathcal{RED}_{n,k} := \{\rho \in \mathcal{D}_{nk} \ : \ \rho^{red} \geq 0\} \supseteq \mathcal{SEP}_{n,k}.$$

Several remarks are in order at this point. First, it is worth mentioning that in the literature, the reduction criterion is sometimes defined to ask that *both* reductions, on the first and on the second subsystems, are positive-semidefinite; since going from one reduction to the other one can be done by simply swapping the roles of $\mathbb{C}^n$ and $\mathbb{C}^k$, we focus in this work on the reduction on the second subsystem. We gather in the next lemma some basic properties of the set $\mathcal{RED}_{n,k}$, see, e.g., Ref. 21 for the proof.

Lemma 4.19. The reduction criterion is, in general, weaker than the PPT criterion,

$$\mathcal{SEP}_{n,k} \subseteq \mathcal{PPT}_{n,k} \subseteq \mathcal{RED}_{n,k} \subseteq \mathcal{D}_{nk}.$$

However, at $k = 2$ (i.e., when the system on which the reduction map acts is a qubit), the two criteria are equivalent,

$$\mathcal{RED}_{n,k} = \mathcal{PPT}_{n,k}.$$

Although the reduction criterion is weaker than the PPT criterion for the purpose of detecting entanglement, its interest stems from the connection with the distillability of quantum states, see Ref. 65.

We gather in the next proposition the values of the thresholds for the sets $\mathcal{RED}_{n,k}$. Since, in the case of the reduction criterion, the tensor factor on which the reduction map R acts does matter, we need to consider two unbalanced regimes: one where n is fixed and $k \to \infty$, and a second one where $n \to \infty$ and k is kept fixed. The results below have been obtained in Ref. 67 (for the second unbalanced regime) and in Ref. 68 (for the balanced regime and the first unbalanced regime).

Proposition 4.20. The thresholds for the sets $\mathcal{RED}_{n,k}$ are as follows:

(1) *In the balanced regime, where both $n, k \to \infty$, the threshold value for the parameter s of the induced measure $\nu_{nk,s}$ is on the scale $s \sim cn$ at the value $c_0 = 1$.*
(2) *In the first unbalanced regime, where n is fixed and $k \to \infty$, the threshold value for the parameter s of the induced measure $\nu_{nk,s}$ is on the scale $s \sim c$ at the value $c_0 = n$.*
(3) *In the second unbalanced regime, where k is fixed and $n \to \infty$, the threshold value for the parameter s of the induced measure $\nu_{nk,s}$ is on the scale $s \sim cnk$ at the value*

$$c_0 = \frac{(1 + \sqrt{k+1})^2}{k(k-1)}.$$

Let us mention now that both thresholds for the PPT and the RED criterion, in the unbalanced case, have been treated, in a unified manner, in the recent preprint in Ref. 3. A general framework is developed in Ref. 3 in which many examples of entanglement criteria fit.

Criteria of the type $[\mathrm{id} \otimes f](\rho) \geq 0$ have been studied from a random matrix theory perspective in Ref. 28 in the case of random linear maps f. In Ref. 28, the authors introduce a family of entanglement criteria index by probability measures. The main idea is to consider maps f between matrix algebras obtained from random Choi matrices. More precisely, consider a compactly supported probability measure μ, and let $X_d \in \mathcal{M}_{nd}(\mathbb{C})$ a sequence of unitarily invariant random matrices converging in distribution, as $d \to \infty$, to μ (n being kept fixed). Let $f_d : \mathcal{M}_n(\mathbb{C}) \to \mathcal{M}_d(\mathbb{C})$ be a (random) linear map such that Choi matrix Eq. (2.4) of f_d is X_d. Then, the positivity of the map f_d, asymptotically as $d \to \infty$, depends only on μ and its free additive convolution powers [Ref. 28, Theorem 4.2] (see Section III D for the definition of convolutions in free probability). One can even make statements about the k-positivity of f_d—for this purpose, we recall that a map is k-positive iff it is positive when tensored by the identity map $\mathcal{M}_k(\mathbb{C}) \to \mathcal{M}_k(\mathbb{C})$.

Theorem 4.21. *The sequence of random linear maps $(f_d)_d$ has the following properties:*

(1) *if* $\mathrm{supp}(\mu^{\boxplus n/k}) \subset (0,\infty)$, *then, almost surely as* $d \to \infty$, f_d *is* k*-positive,*
(2) *if* $\mathrm{supp}(\mu^{\boxplus n/k}) \cap (-\infty, 0) \neq \emptyset$, *then, almost surely as* $d \to \infty$, f_d *is not* k*-positive.*

From the above result, if follows that probability measures μ with the property that the maps they yield are positive, but not completely positive, give interesting entanglement criteria. It was shown in Ref. 28 [Theorem 5.4] that such maps can be obtained from shifted semicircular measures (3.8), and that they can detect PPT entanglement. The global usefulness of such entanglement criteria is left open (see Question 9.3).

We discuss next that the *realignment* criterion (RLN), introduced in Refs. 97 and 22, is of different nature than the two other criteria we already discussed. For any matrix $X \in \mathcal{M}_n(\mathbb{C}) \otimes \mathcal{M}_k(\mathbb{C})$, define

$$X^{rln} = L(X) \in \mathcal{M}_{n^2 \times k^2}(\mathbb{C}),$$

where L is the realignment map, defined on elementary tensors by

$$L(e_i e_j^* \otimes f_a f_b^*) = e_i f_a^* \otimes e_j f_b^*.$$

The realignment criterion states that a separable quantum state $\rho \in \mathcal{D}_{nk}$ satisfies

$$\|\rho^{rln}\|_1 \leq 1,$$

where $\|\cdot\|_1$ is the Schatten 1-norm (or the nuclear norm). As usual, we denote by $\mathcal{RLN}_{n,k}$ the set of quantum states satisfying the realignment criterion

$$\mathcal{RLN}_{n,k} := \{\rho \in \mathcal{D}_{nk} \,:\, \|\rho^{rln}\|_1 \leq 1\} \supseteq \mathcal{SEP}_{n,k}.$$

The realignment criterion is not comparable to the PPT criterion; hence, there are PPT entangled states detected by the RLN criterion and vice-versa. Since the inclusion partial relation cannot be used to compare the two sets/criteria, the notion of threshold is particularly interesting in this situation. The result below is from Ref. 7.

Proposition 4.22. The thresholds for the sets $\mathcal{RLN}_{n,k}$ are as follows:

(1) *In the balanced regime, where $n = k \to \infty$, the threshold value for the parameter s of the induced measure $\nu_{n^2,s}$ is on the scale $s \sim cn^2$ at the value $c_0 = (8/3\pi)^2 \simeq 0.72$.*
(2) *In the unbalanced regime, where $n \to \infty$ and k is fixed, the threshold value for the parameter s of the induced measure $\nu_{nk,s}$ is on the scale $s \sim c$ at the value $c_0 = k^2$.*

In particular, comparing the values above with the ones in Proposition 4.18, one can conclude that, from a volume perspective, the realignment criterion is weaker than the PPT criterion (i.e., the thresholds for RLN are smaller than the thresholds for PPT).

We gather in Table I the values of the thresholds for the different entanglement criteria discussed in this section, as well as for the set of separable states itself. The striking feature of these values is the fact that the (bounds for the) thresholds for the set $\mathcal{SEP}$, obtained in the important work in Ref. 12, are one order of magnitude above the thresholds for the various entanglement criteria. This means that, from a volume perspective, the set $\mathcal{SEP}$ is much smaller than the set of states satisfying the different entanglement criteria.

Finally, in Ref. 75, Lancien studies the performance of r-extendibility criteria for random quantum states. Recall that a bipartite quantum state $\rho_{AB} \in \mathcal{D}_{nk}$ is said to be *r-extendible* if there exists a $(r+1)$-partite state $\sigma_{AB^r} \in \mathcal{D}_{nk^r}$ which is invariant under all permutations of the B-systems and has ρ_{AB} as a marginal,

$$[\mathrm{id}_{nk} \otimes \mathrm{Tr}_{k^{r-1}}](\sigma_{AB^r}) = \rho_{AB}.$$

Obviously, any separable state ρ_{AB} is r-extendible, for all $r \geq 1$. Doherty, Parrilo, and Spedalieri have shown in Ref. 38 that these conditions are also sufficient, see also Ref. 23.

Theorem 4.23. *A bipartite quantum state $\rho_{AB} \in \mathcal{D}_{nk}$ is separable if and only if it is r-extendible with respect to the system B for all $r \in \mathbb{N}$.*

TABLE I. Thresholds for the sets of separable states $\mathcal{SEP}$, PPT states $\mathcal{PPT}$, states satisfying the reduction criterion $\mathcal{RED}$, and states satisfying the realignment criterion $\mathcal{RLN}$.

	Balanced regime $n, k \to \infty$	Unbalanced regime $n \to \infty$, k fixed
$\mathcal{SEP}$	$n^3 \lesssim s \lesssim n^3 \log^2 n$ $[n = k]$	$nk^2 \lesssim s \lesssim nk^2 \log^2(nk)$
$\mathcal{PPT}$	$s \sim cnk$ $c_0 = 4$ $[n = k]$	$s \sim cnk$ $c_0 = 2 + 2\sqrt{1 - \frac{1}{k^2}}$
$\mathcal{RED}$	$s \sim cn$ $c_0 = 1$	$s \sim cnk$ $c_0 = \frac{(1+\sqrt{k+1})^2}{k(k-1)}$
$\mathcal{RLN}$	$s \sim cnk$ $c_0 = (8/3\pi)^2$ $[n = k]$	s fixed $c_0 = k^2$

In Ref. 75, besides computing estimates on the average width of the set of r-extendible states, Lancien computes a lower bound for the threshold value of these sets, for fixed r.

Proposition 4.24 (Ref. 75, Theorem 6.4). Fix $r \geq 1$ and consider balanced random quantum states $\rho_n \in \mathcal{D}_{n^2}$ having distribution ν_{n^2, s_n}. For any $\varepsilon > 0$, if the function s_n is asymptotically smaller than $(1 - \varepsilon)(r-1)^2/(4r)n^2$ as $n \to \infty$, then,

$$\lim_{n \to \infty} \mathbb{P}[\rho_n \text{ is } r\text{-extendible}] = 0.$$

In other words, the threshold c_0 for the set of r-extendible states in the scaling $s \sim cn^2$ is larger than $(r-1)^2/(4r)$.

Notice that the analysis in Ref. 75 does not give any upper-bounds on the threshold c_0, see Question 9.2.

E. Absolute separability

Whether a quantum state ρ is separable or entangled does not only depend on the spectrum of ρ: there are, for example, rank one (pure) states which are separable ($\rho = ee^* \otimes ff^*$) and other states which are entangled ($\rho = \Omega$, see (2.2)). In other words, the separability/entanglement of a quantum state depends also on its eigenvectors. In order to eliminate this dependence, in Ref. 74, the authors introduced the set of *absolutely separable states,*

$$\mathcal{ASEP}_{n,k} = \bigcap_{U \in \mathcal{U}_{nk}} U \cdot \mathcal{SEP}_{n,k} \cdot U^* = \{\rho \, : \, U\rho U^* \text{ is separable } \forall U \in \mathcal{U}_{nk}\} \subset \mathcal{D}_{nk}.$$

Obviously, the truth value of $\rho \in \mathcal{ASEP}_{n,k}$ depends only on the spectrum λ of the density operator ρ, so one could simply use

$$\Delta_{nk} \ni \widetilde{\mathcal{ASEP}}_{n,k} = \{\lambda \, : \, \mathrm{diag}(\lambda) \in \mathcal{ASEP}_{n,k}\}.$$

Similarly, one can define absolute versions (and the corresponding spectral variants) for the sets $\mathcal{PPT}$, $\mathcal{RED}$, and $\mathcal{RLN}$. The question whether not all, but a large fraction of quantum states having a fixed spectrum are separable has been studied in Ref. 90.

An explicit description of the set $\mathcal{APPT}$ has been obtained in Ref. 61, as a finite set of positive-semidefinite conditions. The analogue question for $\mathcal{ARED}$ has been settled in Ref. 69, whereas the problem of finding an explicit description of the set $\mathcal{ARLN}$ remains open. Interestingly, it has been shown in Ref. 70 that for qubit-qudit systems ($\min(n, k) = 2$), absolute separability is equivalent to the absolute PPT property. Later, in Ref. 4, evidence towards the general conjecture $\mathcal{ASEP}_{n,k} = \mathcal{APPT}_{n,k}$ (for all n, k) has been collected; in particular, the authors show that for all n, k, $\mathcal{APPT}_{n,k} \subseteq \mathcal{ARLN}_{n,k}$.

At the level of thresholds, the values (and even the scales) for $\mathcal{ASEP}$ and $\mathcal{ARLN}$ are completely open. The following results for $\mathcal{APPT}$ and $\mathcal{ARED}$ are from Ref. 33 and Ref. 68, respectively.

Proposition 4.25. The thresholds for the sets $\mathcal{APPT}_{n,k}$ are as follows:

(1) *In the balanced regime, where $n \geq k \to \infty$, the threshold value for the parameter s of the induced measure $\nu_{nk,s}$ is on the scale $s \sim cnk^3$ at the value $c_0 = 4$.*
(2) *In the unbalanced regime, where $n \to \infty$ and k is fixed, the threshold value for the parameter s of the induced measure $\nu_{nk,s}$ is on the scale $s \sim cnk$ at the value $c_0 = (k + \sqrt{k^2 - 1})^2$.*

The thresholds for the sets $\mathcal{ARED}_{n,k}$ are as follows:

(1) *In the balanced regime, where $n, k \to \infty$, the threshold value for the parameter s of the induced measure $\nu_{nk,s}$ is on the scale $s \sim cnk$ at the value $c_0 = 1$.*
(2) *In the first unbalanced regime, where $k \to \infty$ and n is fixed, the threshold value for the parameter s of the induced measure $\nu_{nk,s}$ is on the scale $s \sim ck$ at the value $c_0 = n - 2$.*
(3) *In the second unbalanced regime, where $n \to \infty$ and k is fixed, the threshold value for the parameter s of the induced measure $\nu_{nk,s}$ is on the scale $s \sim cnk$ at the value*

$$c_0 = \left(1 + \frac{2}{k} + \frac{2}{k}\sqrt{k+1}\right)^2.$$

V. DETERMINISTIC INPUT THROUGH RANDOM QUANTUM CHANNELS

Although a global understanding of the typical properties of a random channel is desirable (and this is the object of Section VI), obtaining results for interesting outputs of given random channels is of intrinsic interest. For example, as we explain subsequently in Section VII B, the image of highly entangled states under the tensor product of random channels is an important question, as it is one of the keys to obtain violations for the additivity of the minimum output entropy.

Our first model is a one-channel model that consists in considering matrices X_n which have a macroscopic scaling $\mathrm{Tr}(X^p) \sim n \cdot \phi(x^p)$, where x is some non-commutative random variable. In order to obtain states, we normalize

$$\tilde{X} = \frac{X}{\mathrm{Tr}X}.$$

Therefore, the moments of the output matrix $Z = \Phi(\tilde{X})$ are given by

$$\mathbb{E}[\mathrm{Tr}(Z^p)] = \mathbb{E}[\mathrm{Tr}(\Phi(\tilde{X})^p)] = \mathbb{E}\left[\mathrm{Tr}\frac{\Phi(X)^p}{(\mathrm{Tr}X)^p}\right] = \frac{\mathbb{E}[\mathrm{Tr}(\Phi(X)^p)]}{(\mathrm{Tr}X)^p}.$$

We consider different asymptotic regimes for the integer parameters n and k. It turns out that the computations in the case of the regime k fixed, $n \to \infty$ are more complicated and require the formalism of free probability, see Ref. 31. To an integer k and a probability measure μ, we associate the measure $\mu_{(k)}$ defined by

$$\mu_{(k)} = \left(1 - \frac{1}{k}\right)\delta_0 + \frac{1}{k}\mu.$$

Proposition 5.1. The almost sure behavior of the output matrix $Z = \Phi(\tilde{X})$ is given by the following:

(I) *When n is fixed and $k \to \infty$, Z converges almost surely to the maximally mixed state*

$$\rho_* = \frac{1}{n}\mathrm{I}_n.$$

(II) *When k is fixed and $n \to \infty$, the empirical spectral distribution of $\bar{\mu}knZ$ converges to the probability measure $\nu = [\mu_{(k)}]^{\boxplus k^2}$, where $\boxplus$ denotes the free additive convolution operation,*

μ is the probability distribution of x with respect to ϕ: $\phi(x^p) = \int t^p \, d\mu(t)$, and $\bar{\mu}$ is the mean of μ, $\bar{\mu} = \phi(x)$.

(III) *When $n, k \to \infty$ and $k/n \to c$, the empirical spectral distribution of the matrix nZ converges to the Dirac mass δ_1.*

VI. RANDOM QUANTUM CHANNELS AND THEIR OUTPUT SETS

This section is the continuation of the previous one. However, we are interested here in a global approach, i.e., we want to understand how the set of *all* outputs behaves. This section reviews the salient known results in the chronological order.

A. Early results on random unitary channels

1. Levy's lemma

Let us first recall briefly the statement of Levy's lemma, as this is one of the historical starting points of concentration of measure. Given μ_n the uniform probability measure on the unit sphere S^n, we call S^n_ε the subset of S^n whose first coordinate has absolute value less than ε. In some sense, S^n_ε is an ε-neighbourhood of the equator. Levy's lemma states that there exists an universal constant $c > 0$ such that $\mu_n(S^n_\varepsilon) > 1 - \exp(-cn\varepsilon)$. In other words, for any $\varepsilon > 0$ (positive, but as small as we want), an ε-neighbourhood of the equator concentrates all the mass of the sphere at exponential speed as n grows.

Some results are already available in order to quantify the entanglement of generic spaces in $\mathrm{Gr}_{pn}(\mathbb{C}^n \otimes \mathbb{C}^k)$. The best result known so far is arguably the following theorem of Hayden, Leung, and Winter in Ref. 58.

Theorem 6.1 (Ref. 58, Theorem IV.1). *Let A and B be quantum systems of dimension d_A and d_B with $d_B \geq d_A \geq 3$. Let $0 < \alpha < \log d_A$. Then, there exists a subspace $S \subset A \otimes B$ of dimension*

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

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

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

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

For large dimensions, Aubrun[5] studies quantum channels and obtains the following result.

Theorem 6.2. *Consider a random unitary channel $M_N \to M_N$ obtained with k i.i.d. Haar unitaries, as defined in Equation (6.3). For $N \gg k/\varepsilon^2$, such a channel is ε-randomizing with high probability, i.e., it maps every state within distance ε/k of the maximally mixed state.*

This slightly improves on the above result by Hayden, Leung, and Winter by optimizing their discretization argument.

B. Results with a fixed output space

In this section, we fix two parameters, $k \in \mathbb{N}, t \in [0, 1]$. We are interested in a random sequence $\Phi_n : \mathcal{M}_n(\mathbb{C}) \to \mathcal{M}_k(\mathbb{C})$ of quantum channels obtained by tracing out a random embedding V_n of $\mathbb{C}^n$ in $\mathbb{C}^k \otimes \mathbb{C}^N$, where $N = N(n) \sim tnk$. We denote $K_{n,k,t}$ the output set $\Phi_n(\mathcal{D}_n)$.

We introduce a norm on $\mathbb{R}^k$ which will have a very important role to play in the description of the set $K_{n,k,t}$ in the asymptotic limit $n \to \infty$, see Ref. 15 for the details.

Definition 6.3. Recall that a II_1 factor is a von Neumann algebra with a unique finite trace. We can assume it to be one on the identity, and we will call it ϕ. For a positive integer k, embed $\mathbb{R}^k$ as a self-adjoint real subalgebra $\mathcal{R}$ of a II_1 factor $\mathcal{A}$ endowed with trace ϕ, so that

$\phi((x_1,\ldots,x_k)) = (x_1+\cdots+x_k)/k$. *Let* p_t *be a projection of rank* $t \in (0,1]$ *in* $\mathcal{A}$, free *from* $\mathcal{R}$. *On the real vector space* $\mathbb{R}^k$, *we are interested in the following norm, called the* (t)*-norm:*

$$\|x\|_{(t)} := \|p_t x p_t\|_\infty, \tag{6.1}$$

where the vector $x \in \mathbb{R}^k$ *is identified with its image in* $\mathcal{R}$.

We now introduce the convex body $K_{k,t} \subset \Delta_k$ as follows:

$$K_{k,t} := \{\lambda \in \Delta_k \mid \forall a \in \Delta_k, \langle \lambda, a\rangle \leq \|a\|_{(t)}\}, \tag{6.2}$$

where $\langle\cdot,\cdot\rangle$ denotes the canonical scalar product in $\mathbb{R}^k$. $K_{k,t}$ is the intersection of the dual ball of the (t)-norm with the probability simplex Δ_k. Since it is defined by duality, $K_{k,t}$ is the intersection of the probability simplex with the half-spaces

$$H^+(a,t) = \{x \in \mathbb{R}^k \mid \langle x, a\rangle \leq \|a\|_{(t)}\}$$

for all directions $a \in \Delta_k$.

Let $(\Omega, \mathcal{F}, \mathbb{P})$ be a probability space in which the sequence or random vector subspaces $(V_n)_{n\geq 1}$ are defined. Since we assume that the elements of this sequence are independent, we may assume that $\Omega = \prod_{n\geq 1} \mathrm{Gr}_N(\mathbb{C}^k \otimes \mathbb{C}^n)$ and $\mathbb{P} = \otimes_{n\geq 1}\mu_n$, where μ_n is the invariant measure on the Grassmann manifold $\mathrm{Gr}_N(\mathbb{C}^k \otimes \mathbb{C}^n)$. Let $P_n \in \mathcal{M}_{nk}(\mathbb{C})$ be the random orthogonal projection whose image is V_n. For two positive sequences $(a_n)_n$ and $(b_n)_n$, we write $a_n \ll b_n$ iff $a_n/b_n \to 0$ as $n \to \infty$.

Proposition 6.4. Let ν_n *be a sequence of integers satisfying* $\nu_n \ll n$. *Almost surely, the following holds true: for any self-adjoint matrix* $A \in \mathcal{M}_k(\mathbb{C})$, *the* ν_n*th largest eigenvalues of* $P_n(A \otimes I_n)P_n$ *converge to* $\|a\|_{(t)}$, *where* a *is the eigenvalue vector of* A. *This convergence is uniform on any compact set of* $\mathcal{M}_k^{sa}(\mathbb{C})$.

For the proof of this result, we refer to Ref. 15, where it was also shown that this set converges, in a very strong sense, to the convex body $K_{k,t}$.

Theorem 6.5. *Almost surely, the following holds true:*

- *Let* O *be an open set in* Δ_k *containing* $K_{k,t}$. *Then, for* n *large enough,* $K_{n,k,t} \subset O$.
- *Let* $\mathcal{K}$ *be a compact set in the interior of* $K_{k,t}$. *Then, for* n *large enough,* $\mathcal{K} \subset K_{n,k,t}$.

C. More results about the output of random channels

More results are known about the output of random quantum channels. Instead of giving a full list, let us state the following result from Ref. 26 that supersedes many results already known.

Theorem 6.6. *Let* k *be a fixed integer, and* $\Phi_n : \mathcal{M}_n(\mathbb{C}) \to \mathcal{M}_k(\mathbb{C})$ *be a sequence of quantum channels constructed with constant matrices and unitary matrices that are independent from each other. Then, there exists a compact convex set* K *such that its random collection output sets converge almost surely to* K *in the topology induced by the Hausdorff distance between compact sets.*

This theorem includes in particular the following two important examples. First, the random unitary channels

$$\tilde{\Phi}_n(X) = k^{-1}\sum U_i X U_i^*, \tag{6.3}$$

but also, more importantly, a product $\chi_n = \Phi_n \otimes \Xi$, where Ξ is any quantum channel fixed in advance, and Φ_n is any of the sequences considered previously.

Actually, there is even more, namely, in the previous theorem, the output set K can actually be exactly realized via the collection of outputs of pure states (no need for all input states). In addition, the boundary of the collection of output sets converges to the boundary of K in the Hausdorff distance (which means that any point in the interior of K is attained within finite time with probability one), and for any finite collection of l elements in the interior of K, it is possible to find with probability one in finite time a family of pre-images by pure states which are close to orthogonal to

each other (the tolerance is arbitrary and can be fixed ahead of time). Somehow, this is the strongest convergence one can hope for, and it is actually rather counterintuitive that the image of the extreme points of a convex body (the input states) ends up filling exactly the image of the convex body.

As a corollary, however, we obtain the following.

Corollary 6.7. For the random family of quantum channels Φ_n, the Holevo capacity converges with probability one. In particular, if the image set K contains the identity, with probability one,

$$\chi(\Phi_n) + H^{\min}(\Phi_n) \to \log k.$$

Note that this result extends to many other sequences of random channels, cf. Refs. 46 and 26.

VII. THE ADDITIVITY PROBLEM FOR TENSOR PRODUCTS OF RANDOM QUANTUM CHANNELS

This section is an important application of Sec. VI: the understanding of the collection of all outputs through a typical quantum random channel enables us to obtain large violations of the MOE. We start this section by reviewing the relevant concepts and definitions.

A. The classical capacity of quantum channels and the additivity question

The following theorem summarizes some of the most important breakthroughs in quantum information theory in the last decade. It is based, in particular, on the papers of Refs. 55 and 59 and concerns the minimum output entropies of quantum channels, defined in Eq. (2.5).

Theorem 7.1. *For every $p \in [1, \infty]$, there exist quantum channels Φ and Ψ such that*

$$H_p^{\min}(\Phi \otimes \Psi) < H_p^{\min}(\Phi) + H_p^{\min}(\Psi). \tag{7.1}$$

Except for some particular cases ($p > 4.79$[109] and $p > 2$[49]), the proof of this theorem uses the random method, i.e., the channels Φ, Ψ are random channels, and the above inequality occurs with non-zero probability. At this moment, we are not aware of any explicit, non-random choices for Φ, Ψ in the case $1 \leq p \leq 2$, see Question 9.6.

The additivity property for the minimum output entropy $H_{\min}(\cdot)$ was related in Ref. 102 to the additivity of another important entropic quantity, the *Holevo quantity*

$$\chi(\Phi) = \max_{\{p_i, X_i\}} \left[H\left(\sum_i p_i \Phi(X_i) \right) - \sum_i p_i H(\Phi(X_i)) \right].$$

The regularized Holevo quantity provides[62,99] the classical capacity of a quantum channel Φ, i.e., the maximum rate at which classical information can be reliably sent through the noisy channel.

B. Conjugate quantum channels and the MOE of their tensor product

In this subsection, we gather some known results about the MOE of tensor products of conjugate channels $\Psi = \Phi \otimes \bar{\Phi}$. These results will be used in Subsection VII C on counterexamples. Let us stress from the beginning that there is much less known about the output eigenvalues of Ψ than about those of a single random channel Φ. In particular, we do not have an explicit description of the output set of Ψ, such as the one from Theorem 6.5. Actually, we have mostly upper bounds in this case, coming from the trivial inequality

$$H_p^{\min}(\Psi) \leq H_p([\Phi \otimes \bar{\Phi}](\Omega)), \tag{7.2}$$

where Ω is maximally entangled state Eq. (2.2).

The first result in this direction is a non-random one, giving a lower bound on the largest eigenvalue of the output of the maximally entangled state. To fix notation, let $\Phi : M_d(\mathbb{C}) \to M_k(\mathbb{C})$ be a quantum channel coming from an isometry $V : \mathbb{C}^d \to \mathbb{C}^k \otimes \mathbb{C}^n$; here, note that the channel

has different input and output spaces and the dimension which is traced out is n. In Ref. 59, the authors observed that in the context of two random channels given by two dilations V_1, V_2 as above, it is relevant to introduce the further symmetry $V_2 = \bar{V}_1$, as it ensures that at least one eigenvalue is always big.

Lemma 7.2. The largest eigenvalue of the output state $Z = [\Phi \otimes \bar{\Phi}](\Omega_d)$ *satisfies the following inequality:*

$$\|Z\| \geq \frac{d}{nk}.$$

This result appeared several times in the literature (and it is sometimes referred to as the "Hayden-Winter trick"), see Ref. 59 [Lemma 2.1] or Ref. 30 [Lemma 6.6] for a proof using the graphical (non-random) calculus from Section II D.

In the context of random quantum channels, one can improve on the result above, by computing the asymptotic spectrum of the output state Z_n. This has been done in Ref. 30 in different asymptotic regimes. Since in this review we focus on the regime where k is fixed and $d \sim tnk \to \infty$, we state next Theorem 6.3 from Ref. 30.

Theorem 7.3. *Consider a sequence of random quantum channels coming from random isometries* $\Phi_n : M_{d_n}(\mathbb{C}) \to M_k(\mathbb{C})$*, where* d_n *is a sequence of integers satisfying* $d_n \sim tnk$ *as* $n \to \infty$ *for fixed parameters* $k \in \mathbb{N}$ *and* $t \in (0,1)$*. The eigenvalues of the output state*

$$M_{k^2}(\mathbb{C}) \ni Z_n = [\Phi_n \otimes \bar{\Phi}_n](\Omega_{d_n})$$

converge, almost surely as $n \to \infty$*, to*

- $t + \frac{1-t}{k^2}$*, with multiplicity 1;*
- $\frac{1-t}{k^2}$*, with multiplicity* $k^2 - 1$.

In order to prove such results, one uses the method of moments: using Weingarten formula Eq. (3.3) from Section III B, it is shown in Ref. 30 [Section 6.1] that, for all $p \geq 1$,

$$\frac{1}{k^2}\mathbb{E}\mathrm{Tr}(Z_n^p) = \sum_{\alpha,\beta \in \mathcal{S}_{2p}} n^{\#(\alpha^{-1}\gamma)} k^{-2+\#\alpha} d_n^{\#(\beta^{-1}\delta)} \mathrm{Wg}_{nk}(\alpha,\beta),$$

where γ, δ are some fixed permutations in $\mathcal{S}_{2p}$; in Figure 6, the diagram for the output matrix Z_n is represented. The next step is to compute the dominating terms in the above sums, by finding the pairs (α, β) corresponding to the terms having the largest n powers; this is done by replacing $d_n = tkn + o(n)$ and using the asymptotic expression for the Weingarten factor from Theorem 3.6. It turns out that the set of dominating pairs (α, β) is small, and one can compute, up to $o(1)$ terms, the sum, proving the result. Since the matrices Z_n live in a space of fixed dimension (k^2), a simple variance computation allows to go from the convergence in moments to the almost sure convergence of the individual eigenvalues.

Note that Theorem 7.3 improves on Lemma 7.2 in two ways: the norm of the output is larger, and we obtain information on the other eigenvalues too. This turns out to be useful in obtaining better numerical constants for the counterexamples to additivity, see the discussion in Section VII C.

Finally, the last result we would like to discuss in relation to products of conjugate channels is Ref. 45 [Theorem 5.2]. The setting here is more general: the authors consider not only one copy of a channel and its conjugate, but also $2r$ channels (in what follows, r is an arbitrary fixed positive integer),

$$\Psi_n = \Phi_n^{\otimes r} \otimes \bar{\Phi}_n^{\otimes r}.$$

Informally, Ref. 45 [Theorem 5.2] states that, among a fairly large class of input states, the tensor products of Bell states ($\pi \in \mathcal{S}_r$ is an arbitrary permutation)

$$\Omega_{d_n}^{\pi} = \bigotimes_{i=1}^{r} \Omega_{d_n}^{i,\pi(i)}$$

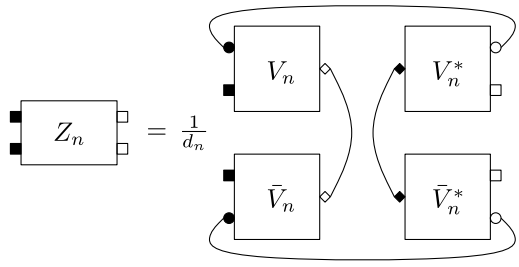

FIG. 6. Diagram for the output matrix Z_n obtained by putting a maximally entangled state through a product of two conjugate quantum channels.

are the ones producing outputs with least entropy. In the equation above, the maximally entangled state acts on the ith copy of $\mathbb{C}^{d_n}$ corresponding to non-conjugate channels Φ_n and on the $\pi(i)$th copy of $\mathbb{C}^{d_n}$ corresponding to conjugate channels $\bar{\Phi}_n$. The class of inputs among which the products of maximally entangled states are optimal are called "well-behaved," in the sense that they obey a random-matrix eigenvalue statistics; see Ref. 45 [eq. (43)] for more details.

The result above shows that inequality Eq. (7.2) is tight, when restricting the minimum on the left hand side to the class of well-behaved input states; the general question is open for random quantum channels, see Question 9.7. Moreover, an important point raised in Ref. 45 is that the optimality of maximally entangled inputs extends to tensor products of channels. This result might be useful for analyzing regularized versions of the minimum output entropies, in relation to the classical capacity problem.

C. Early results in relation to the violation of MOE, history, and the state of the art

We present next a short history of the various counterexamples to the additivity question, discussing different values of the parameter p in Eq. (7.1).

In the range $p > 1$, the first counterexample was obtained by Werner and Holevo:[109] they have shown that the channel $(1 - x) \cdot \mathrm{id} + x \cdot \mathrm{transp}$, acting on $\mathcal{M}_3(\mathbb{C})$, for $x = -1/(d - 1)$, violates the additivity of the p-Rényi entropy for all $p > 4.79$. Then, Hayden and Winter proved, in their seminal work in Ref. 59 that random quantum channels violate additivity with large probability, for all $p > 1$. The same result, using this time free probability, was obtained in Ref. 32, with smaller system dimensions. Also in the range $p > 1$, Aubrun, Szarek and Werner proved violations of random channels, using this time Dvoretzky's theorem.[10] For p close to 0, violations of additivity were proved in Ref. 37.

The most important case, $p = 1$, turned out to be much more difficult. The difficulty comes from the fact that one needs a precise control of the *entire output spectrum*, while for $p > 1$, controlling the largest eigenvalue turned out to be sufficient. The breakthrough was achieved by Hastings in Ref. 55, where he showed that random mixed unitary channels (see Eq. (6.3)) violate additivity of the von Neumann entropy. Several authors, using similar techniques as Hastings, improved, generalized, and extended his result.[44,19,43] An improved version of Dvoretzky's theorem was used in Ref. 11 to show violations at $p = 1$. Later, Fukuda provided a simpler proof of violation,[42] using this time ε-net arguments and Levy's lemma, the techniques used also in the pioneering work of Ref. 58. In Refs. 15 and 16, the authors use free probability theory to compute *exactly* the minimum output entropy of a random quantum channel [Ref. 16, Theorem 5.2]. These results lead to the largest value of the violation known to date (1 bit), and the smallest output dimension ($k = 183$), see Theorem 7.4.

Finally, let us mention that the majority of the violation results above use random constructions. The exceptions are the results in Ref. 109 ($p > 4.79$) and Ref. 49 ($p > 2$, using the antisymmetric subspace); the question of finding other explicit counterexamples is open to this day, see Question 9.6.

We state next the best result to date concerning violations of additivity for the minimum output entropy [Ref. 16, Theorem 6.3].

Theorem 7.4. *Consider a sequence* $\Phi_n : \mathcal{M}_{\lfloor tkn \rfloor}(\mathbb{C}) \to \mathcal{M}_k(\mathbb{C})$ *of random quantum channels, obtained from random isometries*

$$V_n : \mathbb{C}^{\lfloor tkn \rfloor} \to \mathbb{C}^k \otimes \mathbb{C}^n.$$

For any output dimension $k \geq 183$*, in the limit* $n \to \infty$*, there exist values of the parameter* $t \in (0,1)$ *such that almost all random quantum channels violate the additivity of the von Neumann minimum output entropy. For any* ε*, there are large enough values of* k *such that the violation can be made larger than* $1 - \varepsilon$ *bits.*

Moreover, in the same asymptotic regime, for all $k < 183$*, the von Neumann entropy of the output state* $[\Phi_n \otimes \bar{\Phi}_n](\Omega_{\lfloor tkn \rfloor})$ *is almost surely larger than* $2H_{\min}(\Phi_n)$*. Hence, in this case, one cannot exhibit violations of the additivity using Bell state (2.2) as an input for the product of conjugate random quantum channels.*

The above theorem leaves open the maximal possible value of the violation for conjugate random quantum channels, due to the fact that the maximally entangled state is not known to be optimal in this scenario, see Question 9.7.

VIII. OTHER APPLICATIONS OF RMT TO PROBLEMS IN QIT

A. Maximum entropy principle for random matrix product states

Random matrix techniques play other roles in quantum spin chain theory. In this section we follow Ref. 27.

In the theory of quantum spin chains, it is nowadays widely well justified, both numerically[110] and analytically,[54] that ground states can be represented by the set of matrix product states with *polynomial* bond dimension. In the situation of a chain with boundary effects in exponentially small regions of size b at both ends, tracing out the boundary terms leads to a bulk state given by

$$\rho = \sum_{i_{b+1},\ldots i_{N-b}, j_{b+1},\ldots j_{N-b}=1}^{d} \mathrm{Tr}(LA_{i_{b+1}} \cdots A_{i_{N-b}} R A^*_{j_{N-b}} \cdots A^*_{j_{b+1}}) e_{i_{b+1}\ldots i_{N-b}} e^*_{j_{b+1}\ldots j_{N-b}}, \tag{8.1}$$

where all A_i, $L \geq 0$, and $R \geq 0$ are $D \times D$ matrices with $D = \mathrm{poly}(N)$.

It is known[95] that this set has a natural (over)parametrization by the group $\mathcal{U}(dD)$, via the map $U \mapsto A_i = \langle e_1, Ue_i \rangle$. In $\mathcal{U}(dD)$, one can use the symmetry-based assignment of prior distributions to sample from the Haar measure.

It is natural to look for the generic reduced density matrix ρ_l of $l \ll N$ sites. It corresponds to asking about generic observations of 1D quantum systems. This idea has been already exploited for the non-translational invariant case in Ref. 48. The main result of Ref. 27 is that ρ_l has generically maximum entropy.

Theorem 8.1. *Let* ρ_l *be taken at random from the ensemble introduced with* $D \geq N^{1/5}$*. Then,* $\|\rho_l / \mathrm{Tr}\rho_l - 1/d^l\|_\infty \leq (d^l - 1)\sqrt{d^l} O(D^{-1/10})$ *except with probability exponentially small in* D*.*

To prove the theorem, one needs the graphical Weingarten calculus provided in Ref. 30 (see Sections II D and III C) and a uniform estimate of the Weingarten function, more subtle than the one stated in Theorem 3.6. Finally, in the same context of condensed matter physics, let us mention the work of Movassagh and Edelman, containing applications of random matrix theory and free probability to the study of the eigenvalue distribution of quantum many body systems having generic interactions.[81]

B. Multiplicative bounds for random quantum channels

Once the additivity questions for the minimum p-Rényi entropy of random quantum channels had been settled in Refs. 59 and 55, the attention shifted towards the *amount* of the possible violations of the minimum output entropy. In Ref. 80, Montanaro shows that random quantum channels are not very far from being additive by bounding the minimum output ∞-Rényi entropy of a tensor power of a channel by the same quantity for one copy of the channel. His idea is to bound the desired entropy by an *additive quantity*, the norm of the partial transposition of the projection on the image subspace of the random isometry defining the channel. The following theorem is a restatement of Ref. 80 [Theorem 3].

Theorem 8.2. *Let $\Phi : \mathcal{M}_d(\mathbb{C}) \to \mathcal{M}_k(\mathbb{C})$ be a random quantum channel having ancilla dimension n. Suppose $k \leq n$, $\min\{d,k\} \geq 2(\log_2 n)^{3/2}$ and $d = o(kn)$. Then, for any $p > 1$, with high probability as $n \to \infty$, the following inequality holds $\frac{1}{r} H^p_{\min}(\Phi^{\otimes r}) \geq \beta(1 - 1/p) H^p_{\min}(\Phi)$, where*

$$\beta \simeq \begin{cases} 1/2 & \text{if } d \geq n/k \\ 1 & \text{if } d \leq n/k \end{cases}.$$

Soon after, Montanaro's ideas were pursued in Ref. 46. There, different additive quantities (e.g., the operator norm of the partial transpose of the Choi matrix of the quantum channel) were used to bound the minimum output 2-Rényi entropy. The results provide slight improvements, in the case of interest $p = 1$ over the bounds from Ref. 80. The following statement follows from Ref. 46 [Theorem 8.4].

Theorem 8.3. *Consider a sequence of random quantum channels $\Phi_n : \mathcal{M}_d(\mathbb{C}) \to \mathcal{M}_k(\mathbb{C})$ with ancilla dimension n, where k is a fixed parameter and $d \sim tnk$ for a fixed $t \in (0,1)$. Then, almost surely as $n \to \infty$, for all $p \in [0,2]$, there exist constants $\alpha_p \in [0,1]$ such that, for all $r \geq 1$,*

$$\frac{1}{r} H^{\min}_p(\Phi_n^{\otimes r}) \geq \alpha_p H^{\min}_p(\Phi_n). \tag{8.2}$$

The constants α_p satisfy the following relations.

(1) *When $0 < t < 1/2$ is a constant,*

$$\alpha_p = o(1) + \frac{p-1}{2p}\left[1 + \frac{2\log 2 + \log(1-t)}{\log t}\right] \cdot \mathbf{1}_{(1,2]}(p).$$

(2) *When k is large and $t \asymp k^{-\tau}$ with $\tau > 0$,*

$$\alpha^{\Gamma}_{p,k,t} = o(1) + \begin{cases} \dfrac{p-1}{2p} & \text{if } 0 < \tau \leq 1 - 1/p \\ \tau/2 & \text{if } 1 - 1/p \leq \tau \leq 2 \\ 1 & \text{if } \tau \geq 2 \end{cases}.$$

Incidentally, since the limiting spectrum of the partial transposition of the Choi matrix is computed in Ref. 46, the authors show the existence of PPT quantum channels violating generically the additivity of the minimum p-Rényi entropy, for all $p \geq 30.95$, see Ref. 46 [Theorem 10.5].

C. Sum of random projections on tensor products

Ambainis, Harrow, and Hastings[1] consider a problem in random matrix theory that is inspired by quantum information theory: determining the largest eigenvalue of a sum of p random product states in $(\mathbb{C}^d)^{\otimes k}$, where k and p/d^k are fixed while $d \to \infty$. When $k = 1$, the Marčenko-Pastur law determines asymptotically the largest eigenvalue $(1 + \sqrt{p/d^k})^2$, the smallest eigenvalue, and the spectral density.

More precisely, their setup is as follows: for each dimension d, let $(p^{(i)}_d)_{i \in \{1,\ldots,k\}}$ be independent uniformly distributed rank one random projections on $\mathbb{C}^d$.

Theorem 8.4. *As $d \to \infty$, the operator norm of*

$$\sum_i p_d^{(1)} \otimes \cdots \otimes p_d^{(k)}$$

still behaves almost surely like $(1 + \sqrt{p/d^k})^2$ and the spectral density approaches that of Marčenko-Pastur law (3.1).

Their proof is essentially based on moment methods. Direct computation of moments of high order allows to conclude. Various methods are proposed by the authors, including methods of Schwinger-Dyson type. It would be interesting to see whether these methods that are well established in theoretical physics and random matrix theory could be of further use in quantum information theory. This result generalizes the random matrix theory result to the random tensor case, and for the records, this is arguably one of the first precise results about the convergence of norms of sums of tensor products when the dimensions of each leg are the same. The original motivation of the authors emanates in part from problems related to quantum data-hiding. We refer to Ref. 1 for the proofs and motivations.

D. Area laws for random quantum states associated to graphs

In this section, a generalization of Proposition 4.12 to the general case of non-adapted marginals is presented, a result which was obtained in Ref. 35. The theorem in this section makes use of random matrix theory techniques, more precisely it is build on the moment computation done in Ref. 34 [Theorem 5.4].

Before we state the area law, we need to properly define the *boundary* of a marginal induced by a partition $\{S,T\}$ of the total Hilbert space. In the adapted marginal case discussed in Section IV A 4, this definition was natural; the general situation described here requires a preliminary optimization procedure.

To keep things simple, assume that all local Hilbert spaces have the same dimension N. A partition $\{S,T\}$ defines, at each vertex of the graph, a pair of non-negative integers $(s(v),t(v))$ such that $s(v) + t(v) = \deg(v)$ and $\sum_v s(v) = |S|$, $\sum_v t(v) = |T|$. The randomness in the unitary operators U_v acting on the vertices of G introduces an "incertitude" on the choice of the copies of $\mathbb{C}^N$ which should be traced out at each vertex $v \in G$. The following definition of the boundary volume (see Ref. 35 for the details) removes this incertitude by performing an optimization over all possible choices for the partial trace. Note that the case of adapted marginals (see Definition 4.11) does not require this optimization step, since there is no incertitude (at each vertex, either all or none of the subsystems are traced out).

Definition 8.5. For a graph G and a marginal ρ_S of the graphs state φ_G defined by a partition $\{S,T\}$, define the boundary volume *of the partition as*

$$|\partial S| = \max_\alpha \mathrm{cr}(\alpha),$$

where α is a function $\alpha : [2m] \to \{S,T\}$ defining which copies of $\mathbb{C}^n$ are traced out, and $\mathrm{cr}(\alpha)$ is the number of crossings *in the assignment α, that is, the number of edges in G having one vertex in $\alpha^{-1}(S)$ and the other one in $\alpha^{-1}(T)$.*

The following theorem is the main result of Ref. 35, showing that the area law holds for random graph states, with the appropriate definition of the boundary volume. Moreover, one can compute the correction term to the area law, a quantity which depends on the topology of the graph G. We refer the interested reader to Ref. 35 [Sections 5 and 6] for the definition of the correction term $h_{G,S}$ and the proofs.

Theorem 8.6. *Let ρ_S be the marginal $\{S,T\}$ of a graph state φ_G. Then, as the local dimension $N \to \infty$, the* area law *holds in the following sense:*

$$\mathbb{E}H(\rho_S) = |\partial S| \log N - h_{G,S} + o(1), \tag{8.3}$$

where $|\partial S|$ is the area of the boundary of the partition $\{S,T\}$ from Definition 8.5 and $h_{G,S}$ is a positive constant, depending on the topology of the graph G and on the partition $\{S,T\}$ (and independent of N).

IX. CONCLUSIONS AND OPEN QUESTIONS

We finish this review article with a series of questions that seem to be of interest at the intersection of random matrix related techniques and quantum information / quantum mechanics.

In relation to the various threshold results from Section IV D, we list next several important open questions.

Question 9.1. Is it possible to remove the log *factors from Theorem 4.17 and to obtain a sharper threshold result for the set $\mathcal{SEP}$ of separable states?*

Regarding the hierarchy of r-extendibility criteria, the upper bound corresponding to the threshold result in 4.24 is open, see Ref. 75 [Section 9.2].

Question 9.2. Find a constant $c_1 \geq (r-1)^2/(4r)$ such that random quantum states having distribution ν_{n^2,c_1n^2} are, with high probability as $n \to \infty$, r-extendible.

Regarding the random entanglement criteria introduced in Theorem 4.21, one can define

$$K_{\mu,m} = \{\rho \in \mathcal{D}_{nm} \ : \ [f_d \otimes \mathrm{id}_m](\rho) > 0 \text{ almost surely, for } d \text{ large enough}\}.$$

The following question, addressing the global power of such random criteria, was left open in Ref. 28.

Question 9.3. Define the set of quantum states satisfying all *random criteria from Theorem 4.21,*

$$K^{free}_{n,k,m} := \bigcap_{\mu \,:\, \mathrm{supp}\left(\mu^{\boxplus n/k}\right) \subset [0,\infty)} K_{\mu,m}.$$

Can one give an analytical description of $K^{free}_{n,k,m}$? It was shown in Ref. 28 [Proposition 3.7] that the only pure states contained in $K^{free}_{n,k,m}$ are the separable (product) ones. Are there values of the parameters n,k,m for which the set $K^{free}_{n,k,m}$ is precisely the set of k-separable states from $\mathcal{D}_{nm}$?

In Section VIII A, we have discussed a random model for matrix product states, and we have shown that it obeys the maximum entropy principle of Jaynes. There are also natural questions related to quantum spin chains.

Question 9.4. In Section VIII D, we stated an area law for random quantum states. Given a random Hamiltonian H_N acting on $\mathbb{C}^N$, let $H^{(i)}$ be the operator obtained from H_N acting on $(\mathbb{C}^N)^{\otimes k}$ by the action of H_N on the i th leg, and identity elsewhere. We assume that we come up with a model with a gap, i.e., the difference between its smallest eigenvalue and its second smallest eigenvalue is uniform. It follows from the results by Hastings[54] that the ground state of the Hamiltonian $\sum H^{(i)}_N$ satisfies an area law. If H_N has some randomness in addition, can we obtain more precise results, e.g., regarding the distribution of the ground state? In the same vein, can random techniques allow us to obtain results for other topologies, e.g., in the 2D context?

Let us now consider some open questions in quantum information theory, related to random matrices.

As discussed in Section IV A, there are several ways in which one can define random quantum states. All classes of probability measures discussed in Section IV A are very well motivated, both from the mathematical and the physical standpoints. In Ref. 84, the authors introduce a new ensemble of random quantum states, by considering iterations of random quantum channels. The following question was asked in Ref. 84 [Section 4].

Question 9.5. Compute the statistics of the probability measure ν_b on the set of quantum states $\mathcal{D}_n$ defined as follows. For a probability vector $b \in \Delta_k$, consider the quantum channel

$$\Phi(X) = [\mathrm{id}_n \otimes \mathrm{Tr}_k](U(X \otimes \mathrm{diag}(b))U^*),$$

where $U \in \mathcal{U}_{nk}$ is a random Haar unitary. Then, ν_b is the probability distribution of the unique *invariant state of Φ (uniqueness is shown in Ref. 84 [Theorem 4.4]).*

Regarding the various counterexamples in the literature for the minimum output entropy and other capacity-related questions, we list next several open problems.

Question 9.6. Construct explicit, non-random counterexamples to the additivity of the p-Rényi entropy, in the range $p \in [1,2]$.

Question 9.7. Is maximally entangled state Ω the actual minimizer of the minimum output entropy for a pair of conjugate random quantum channels $\Phi \otimes \bar{\Phi}$?

Question 9.8. Does a pair $\Phi \otimes \Psi$ of independent *random quantum channels violate additivity of the quantities $H_p^{\min}(\cdot)$?*

Regarding the known violations of the additivity of the MOE entropy for pairs of conjugate channels, it is important to note that Theorem 7.4 only allows to obtain bounds on the output dimension of the random channels. Previous results (see, e.g., Ref. 44) allow to bound also the input dimension. The approach used in Refs. 15 and 16, using free probability, uses estimates of objects existing at the limit where the input dimension is infinity. It would thus be desirable, in this framework, to be able to work at finite input dimension and thus bound *all* the relevant parameters which allow for additivity violations.

Question 9.9. A random contraction is known to be determinantal[79] and the determinant involves contour integrals. So far, many random matrix techniques used for QIT rely either on concentration of measure or on moment methods. Is it possible to use complex analysis methods (steepest descent, Riemann-Hilbert problem analysis) in order to refine existing estimates. For example, can such estimates give bounds for dimensions of input spaces for violation of MOE?

Finally, we would like to end the current review with a very important open question, regarding different regularized quantities for random quantum channels.

Question 9.10. Compute the almost sure limit of the regularized $H_p^{\min}(\cdot)$ quantities, the Holevo capacity, and the classical capacity for random quantum channels.

ACKNOWLEDGMENTS

B.C.'s research was partly supported by NSERC, ERA, and Kakenhi funding. I.N.'s research has been supported by a von Humboldt fellowship and by the ANR Project Nos. OSQPI 2011 BS01 008 01 and RMTQIT No. ANR-12-IS01-0001-01. Both B.C. and I.N. were supported by the ANR Project No. STOQ ANR-14-CE25-0003. We would like to thank the anonymous referee for helping us to improve the quality of the presentation.

[1] Ambainis, A., Harrow, A. W., and Hastings, M. B., "Random tensor theory: Extending random matrix theory to mixtures of random product states," Commun. Math. Phys. **310**(1), 25–74 (2012).
[2] Anderson, G. W., Guionnet, A., and Zeitouni, O., *An Introduction to Random Matrices Number 118* (Cambridge University Press, 2010).
[3] Arizmendi, O., Nechita, I., and Vargas, C., "On the asymptotic distribution of block-modified random matrices," J. Math. Phys. (to be published); preprint arXiv:1508.05732 (2015).
[4] Arunachalam, S., Johnston, N., and Russo, V., "Is absolute separability determined by the partial transpose?," Quant. Inf. Comput. **15**(7 & 8), 0694–0720 (2015); preprint arXiv:1405.5853 (2014).
[5] Aubrun, G., "On almost randomizing channels with a short Kraus decomposition," Commun. Math. Phys. **288**(3), 1103–1116 (2009).

[6] Aubrun, G., "Partial transposition of random states and non-centered semicircular distributions," Random Matrices: Theory Appl. **1**(02), 1250001 (2012).
[7] Aubrun, G. and Nechita, I., "Realigning random states," J. Math. Phys. **53**(10), 102210 (2012).
[8] Aubrun, G. and Szarek, S. J., "Tensor products of convex sets and the volume of separable states on N qudits," Phys. Rev. A **73**(2), 022109 (2006).
[9] Aubrun, G. and Szarek, S., "Dvoretzky's theorem and the complexity of entanglement detection," preprint arXiv:1510.00578 (2015).
[10] Aubrun, G., Szarek, S., and Werner, E., "Nonadditivity of Rényi entropy and Dvoretzky's theorem," J. Math. Phys. **51**(2), 022102 (2010).
[11] Aubrun, G., Szarek, S., and Werner, E., "Hastingss additivity counterexample via Dvoretzky's theorem," Commun. Math. Phys. **305**(1), 85–97 (2011).
[12] Aubrun, G., Szarek, S. J., and Ye, D., "Entanglement thresholds for random induced states," Commun. Pure Appl. Math. **67**(1), 129–171 (2014).
[13] Bai, Z. and Silverstein, J. W., *Spectral Analysis of Large Dimensional Random Matrices* (Springer, 2010), Vol. 20.
[14] Banica, T. and Nechita, I., "Asymptotic eigenvalue distributions of block-transposed Wishart matrices," J. Theor. Probab. **26**(3), 855–869 (2013).
[15] Belinschi, S., Collins, B., and Nechita, I., "Eigenvectors and eigenvalues in a random subspace of a tensor product," Invent. Math. **190**(3), 647–697 (2012).
[16] Belinschi, S. T., Collins, B., and Nechita, I., "Almost one bit violation for the additivity of the minimum output entropy," Commun. Math. Phys. (to be published); preprint arXiv:1305.1567 (2013).
[17] Bengtsson, I. and Życzkowski, K., *Geometry of Quantum States: An Introduction to Quantum Entanglement* (Cambridge University Press, 2006).
[18] Bouchaud, J.-P. and Potters, M., *Theory of Financial Risk and Derivative Pricing: From Statistical Physics to Risk Management* (Cambridge University Press, 2003).
[19] Brandao, F. G. S. L. and Horodecki, M., "On Hastings' counterexamples to the minimum output entropy additivity conjecture," Open Syst. Inf. Dyn. **17**(01), 31–52 (2010).
[20] Braunstein, S. L., "Geometry of quantum inference," Phys. Lett. A **219**(3), 169–174 (1996).
[21] Cerf, N. J., Adami, C., and Gingrich, R. M., "Reduction criterion for separability," Phys. Rev. A **60**(2), 898 (1999).
[22] Chen, K. and Wu, L.-A., "A matrix realignment method for recognizing entanglement," Quant. Inf. Comp. **3**(3), 193–202 (2003); preprint arXiv:quant-ph/0205017 (2002).
[23] Christandl, M., König, R., Mitchison, G., and Renner, R., "One-and-a-half quantum de Finetti theorems," Commun. Math. Phys. **273**(2), 473–498 (2007).
[24] Coecke, B., "Quantum picturalism," Contemp. Phys. **51**(1), 59–83 (2010).
[25] Collins, B., "Moments and cumulants of polynomial random variables on unitarygroups, the Itzykson-Zuber integral, and free probability," Int. Math. Res. Not. **2003**(17), 953–982.
[26] Collins, B., Fukuda, M., and Nechita, I., "On the convergence of output sets of quantum channels," J. Oper. Theory **73**(2), 336–360 (2015).
[27] Collins, B., Gonzalez Guillen, C. E., and Pérez García, D., "Matrix product states, random matrix theory and the principle of maximum entropy," Commun. Math. Phys. **320**(3), 663–677 (2013).
[28] Collins, B., Hayden, P., and Nechita, I., "Random and free positive maps with applications to entanglement detection," preprint arXiv:1505.08042 (2015).
[29] Collins, B. and Nechita, I., "Eigenvalue and entropy statistics for products of conjugate random quantum channels," Entropy **12**(6), 1612–1631 (2010).
[30] Collins, B. and Nechita, I., "Random quantum channels I: Graphical calculus and the Bell state phenomenon," Commun. Math. Phys. **297**(2), 345–370 (2010).
[31] Collins, B. and Nechita, I., "Gaussianization and eigenvalue statistics for random quantum channels (III)," Ann. Appl. Probab. **21**, 1136–1179 (2011).
[32] Collins, B. and Nechita, I., "Random quantum channels II: Entanglement of random subspaces, Rényi entropy estimates and additivity problems," Adv. Math. **226**(2), 1181–1201 (2011).
[33] Collins, B., Nechita, I., and Ye, D., "The absolute positive partial transpose property for random induced states," Random Matrices: Theory Appl. **1**(03), 1250002 (2012).
[34] Collins, B., Nechita, I., and Życzkowski, K., "Random graph states, maximal flow and Fuss–Catalan distributions," J. Phys. A: Math. Theor. **43**(27), 275303 (2010).
[35] Collins, B., Nechita, I., and Życzkowski, K., "Area law for random graph states," J. Phys. A: Math. Theor. **46**(30), 305302 (2013).
[36] Collins, B. and Śniady, P., "Integration with respect to the Haar measure on unitary, orthogonal and symplectic group," Commun. Math. Phys. **264**(3), 773–795 (2006).
[37] Cubitt, T., Harrow, A. W., Leung, D., Montanaro, A., and Winter, A., "Counterexamples to additivity of minimum output p-Renyi entropy for p close to 0," Commun. Math. Phys. **284**(1), 281–290 (2008).
[38] Doherty, A. C., Parrilo, P. A., and Spedalieri, F. M., "Complete family of separability criteria," Phys. Rev. A **69**(2), 022308 (2004).
[39] Facchi, P., Marzolino, U., Parisi, G., Pascazio, S., and Scardicchio, A., "Phase transitions of bipartite entanglement," Phys. Rev. Lett. **101**(5), 050502 (2008).
[40] Folland, G. B., *Real Analysis: Modern Techniques and Their Applications* (John Wiley & Sons, 2013).
[41] Foong, S. K. and Kanno, S., "Proof of page's conjecture on the average entropy of a subsystem," Phys. Rev. Lett. **72**(8), 1148 (1994).
[42] Fukuda, M., "Revisiting additivity violation of quantum channels," Commun. Math. Phys. **332**(2), 713–728 (2014).
[43] Fukuda, M. and King, C., "Entanglement of random subspaces via the Hastings bound," J. Math. Phys. **51**(4), 042201 (2010).

[44] Fukuda, M., King, C., and Moser, D. K., "Comments on Hastings additivity counterexamples," Commun. Math. Phys. **296**(1), 111–143 (2010).
[45] Fukuda, M. and Nechita, I., "Asymptotically well-behaved input states do not violate additivity for conjugate pairs of random quantum channels," Commun. Math. Phys. **328**(3), 995–1021 (2014).
[46] Fukuda, M. and Nechita, I., "Additivity rates and PPT property for random quantum channels," Ann. Math. Blaise Pascal **22**, 1–72 (2015).
[47] Fukuda, M. and Śniady, P., "Partial transpose of random quantum states: Exact formulas and meanders," J. Math. Phys. **54**(4), 042202 (2013).
[48] Garnerone, S., de Oliveira, T. R., and Zanardi, P., "Typicality in random matrix product states," Phys. Rev. A **81**(3), 032336 (2010).
[49] Grudka, A., Horodecki, M., and Pankowski, Ł., "Constructive counterexamples to the additivity of the minimum output Rényi entropy of quantum channels for all $p > 2$," J. Phys. A: Math. Theor. **43**(42), 425304 (2010).
[50] Gurvits, L., "Classical deterministic complexity of Edmonds' problem and quantum entanglement," in *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing* (ACM, 2003), pp. 10–19.
[51] Gurvits, L. and Barnum, H., "Largest separable balls around the maximally mixed bipartite quantum state," Phys. Rev. A **66**(6), 062311 (2002).
[52] Hall, M. J. W., "Random quantum correlations and density operator distributions," Phys. Lett. A **242**(3), 123–129 (1998).
[53] Harer, J. and Zagier, D., "The Euler characteristic of the moduli space of curves," Invent. Math. **85**(3), 457–485 (1986).
[54] Hastings, M. B., "Entropy and entanglement in quantum ground states," Phys. Rev. B **76**(3), 035114 (2007).
[55] Hastings, M. B., "Superadditivity of communication capacity using entangled inputs," Nat. Phys. **5**(4), 255–257 (2009).
[56] Hayashi, M., *Quantum Information* (Springer, 2006).
[57] Hayden, P., Leung, D., Shor, P. W., and Winter, A., "Randomizing quantum states: Constructions and applications," Commun. Math. Phys. **250**(2), 371–391 (2004).
[58] Hayden, P., Leung, D. W., and Winter, A., "Aspects of generic entanglement," Commun. Math. Phys. **265**(1), 95–117 (2006).
[59] Hayden, P. and Winter, A., "Counterexamples to the maximal p-norm multiplicativity conjecture for all $p > 1$," Commun. Math. Phys. **284**(1), 263–280 (2008).
[60] Heinosaari, T. and Ziman, M., *The Mathematical Language of Quantum Theory: From Uncertainty to Entanglement* (Cambridge University Press, 2011).
[61] Hildebrand, R., "Positive partial transpose from spectra," Phys. Rev. A **76**(5), 052325 (2007).
[62] Holevo, A. S., "The capacity of quantum channel with general signal states," IEEE Trans. Inf. Theory **44**(1), 269–273 (1998).
[63] Horodecki, M. and Horodecki, P., "Reduction criterion of separability and limits for a class of distillation protocols," Phys. Rev. A **59**(6), 4206 (1999).
[64] Horodecki, M., Horodecki, P., and Horodecki, R., "Separability of mixed states: Necessary and sufficient conditions," Phys. Lett. A **223**(1), 1–8 (1996).
[65] Horodecki, M., Horodecki, P., and Horodecki, R., "Mixed-state entanglement and distillation: Is there a bound entanglement in nature?," Phys. Rev. Lett. **80**(24), 5239 (1998).
[66] Horodecki, R., Horodecki, P., Horodecki, M., and Horodecki, K., "Quantum entanglement," Rev. Mod. Phys. **81**(2), 865 (2009).
[67] Jivulescu, M. A., Lupa, N., and Nechita, I., "On the reduction criterion for random quantum states," J. Math. Phys. **55**(11), 112203 (2014).
[68] Jivulescu, M. A., Lupa, N., and Nechita, I., "Thresholds for reduction-related entanglement criteria in quantum information theory," Quantum Inf. Comput. **15**(13-14), 1165–1184 (2015).
[69] Jivulescu, M. A., Lupa, N., Nechita, I., and Reeb, D., "Positive reduction from spectra," Linear Algebra Appl. **469**, 276–304 (2015).
[70] Johnston, N., "Separability from spectrum for qubit-qudit states," Phys. Rev. A **88**(6), 062330 (2013).
[71] Katz, N. M. and Sarnak, P., *Random Matrices, Frobenius Eigenvalues, and Monodromy* (American Mathematical Society, 1999), Vol. 45.
[72] Kontsevich, M., "Homological algebra of mirror symmetry," preprint arXiv:alg-geom/9411018 (1994).
[73] Kuijlaars, A. B. J., McLaughlin, K. T.-R., Van Assche, W., and Vanlessen, M., "The Riemann–Hilbert approach to strong asymptotics for orthogonal polynomials on $[-1, 1]$," Adv. Math. **188**(2), 337–398 (2004).
[74] Kuś, M. and Życzkowski, K., "Geometry of entangled states," Phys. Rev. A **63**(3), 032307 (2001).
[75] Lancien, C., "k-extendibility of high-dimensional bipartite quantum states," preprint arXiv:1504.06459 (2015).
[76] Male, C., "The norm of polynomials in large random and deterministic matrices," Probab. Theory Relat. Fields **154**(3-4), 477–532 (2012).
[77] Marčenko, V. A. and Pastur, L. A., "Distribution of eigenvalues for some sets of random matrices," Sb.: Math. **1**(4), 457–483 (1967).
[78] Mehta, M. L., *Random Matrices* (Academic Press, 2004), Vol. 142.
[79] Metcalfe, A. P., "Universality properties of Gelfand–Tsetlin patterns," Probab. Theory Relat. Fields **155**(1-2), 303–346 (2013).
[80] Montanaro, A., "Weak multiplicativity for random quantum channels," Commun. Math. Phys. **319**(2), 535–555 (2013).
[81] Movassagh, R. and Edelman, A., "Density of states of quantum spin systems from isotropic entanglement," Phys. Rev. Lett. **107**(9), 097205 (2011).
[82] Nadal, C., Majumdar, S. N., and Vergassola, M., "Statistical distribution of quantum entanglement for a random bipartite state," J. Stat. Phys. **142**(2), 403–438 (2011).
[83] Nechita, I., "Asymptotics of random density matrices," Ann. Henri Poincare **8**(8), 1521–1538 (2007).
[84] Nechita, I. and Pellegrini, C., "Random repeated quantum interactions and random invariant states," Probab. Theory Relat. Fields **152**(1-2), 299–320 (2012).

[85] Nechita, I. and Pellegrini, C., "Random pure quantum states via unitary Brownian motion," Electron. Commun. Probab. **18**, 1–13 (2013).
[86] Nica, A. and Speicher, R., *Lectures on the Combinatorics of Free Probability* (Cambridge University Press, 2006), Vol. 13.
[87] Nielsen, M. A. and Chuang, I. L., *Quantum Computation and Quantum Information* (Cambridge University Press, 2010).
[88] Okounkov, A., "Random surfaces enumerating algebraic curves," preprint arXiv:math-ph/0412008 (2004).
[89] Osipov, V., Sommers, H.-J., and Życzkowski, K., "Random Bures mixed states and the distribution of their purity," J. Phys. A: Math. Theor. **43**(5), 055302 (2010).
[90] Oszmaniec, M. and Kuś, M., "Fraction of isospectral states exhibiting quantum correlations," Phys. Rev. A **90**(1), 010302 (2014).
[91] Page, D. N., "Average entropy of a subsystem," Phys. Rev. Lett. **71**(9), 1291 (1993).
[92] Palazuelos, C., "Random constructions in Bell inequalities: A survey," preprint arXiv:1502.02175 (2015).
[93] Penrose, R., *The Road to Reality* (Alfred A. Knopf, New York, 2005).
[94] Peres, A., "Separability criterion for density matrices," Phys. Rev. Lett. **77**(8), 1413 (1996).
[95] Perez-Garcia, D., Verstraete, F., Wolf, M. M., and Ignacio Cirac, J., "Matrix product state representations," Quantum Inf. Comput. **7**, 401 (2007).
[96] Preskill, J., in "Lecture notes for the course information for physics 219 = computer science 219," *Quantum Computation*, Technical Report (Caltech, Pasadena, California, 1999), http://theory.caltech.edu/people/preskill/ph229/.
[97] Rudolph, O., "On the cross norm criterion for separability," J. Phys. A: Math. Gen. **36**(21), 5825 (2003).
[98] Sánchez-Ruiz, J., "Simple proof of page's conjecture on the average entropy of a subsystem," Phys. Rev. E **52**(5), 5653 (1995).
[99] Schumacher, B. and Westmoreland, M. D., "Sending classical information via noisy quantum channels," Phys. Rev. A **56**(1), 131 (1997).
[100] Sen, S., "Average entropy of a quantum subsystem," Phys. Rev. Lett. **77**(1), 1 (1996).
[101] Shannon, C. E., "A mathematical theory of communication," Bell Syst. Tech. J. **27**(3), 379–423 (1948).
[102] Shor, P. W., "Equivalence of additivity questions in quantum information theory," Commun. Math. Phys. **246**(3), 453–472 (2004).
[103] Sommers, H.-J. and Życzkowski, K., "Bures volume of the set of mixed quantum states," J. Phys. A: Math. Gen. **36**(39), 10083 (2003).
[104] Sommers, H.-J. and Życzkowski, K., "Statistical properties of random density matrices," J. Phys. A: Math. Gen. **37**(35), 8457 (2004).
[105] Tracy, C. A. and Widom, H., "Distribution functions for largest eigenvalues and their applications," preprint arXiv:math-ph/0210034 (2002).
[106] Tulino, A. M. and Verdú, S., *Random Matrix Theory and Wireless Communications* (Now Publishers, Inc., 2004), Vol. 1.
[107] Voiculescu, D., "A strengthened asymptotic freeness result for random matrices with applications to free entropy," Int. Math. Res. Not. **1998**(1), 41–63.
[108] Voiculescu, D. V., Dykema, K. J., and Nica, A., *Free Random Variables Number 1* (American Mathematical Society, 1992).
[109] Werner, R. F. and Holevo, A. S., "Counterexample to an additivity conjecture for output purity of quantum channels," J. Math. Phys. **43**(9), 4353–4357 (2002).
[110] White, S. R., "Density matrix formulation for quantum renormalization groups," Phys. Rev. Lett. **69**(19), 2863 (1992).
[111] Wigner, E. P., "Characteristic vectors of bordered matrices with infinite dimensions," Ann. Math. **62**, 548–564 (1955).
[112] Wishart, J., "The generalised product moment distribution in samples from a normal multivariate population," Biometrika **20A**, 32–52 (1928).
[113] Witten, E., "Physics and geometry," in *Proceedings of the International Congress of Mathematicians* (Berkeley, USA, 1986), pp. 267–303.
[114] Žnidarič, M., Prosen, T., Benenti, G., and Casati, G., "Detecting entanglement of random states with an entanglement witness," J. Phys. A: Math. Theor. **40**(45), 13787 (2007).
[115] Życzkowski, K., Penson, K. A., Nechita, I., and Collins, B., "Generating random density matrices," J. Math. Phys. **52**(6), 062201 (2011).
[116] Życzkowski, K. and Sommers, H.-J., "Induced measures in the space of mixed quantum states," J. Phys. A: Math. Gen. **34**(35), 7111 (2001).
[117] Życzkowski, K. and Sommers, H.-J., "Hilbert-Schmidt volume of the set of mixed quantum states," J. Phys. A: Math. Gen. **36**(39), 10115 (2003).