

Realigning random states

Guillaume Aubrun and Ion Nechita

Citation: *Journal of Mathematical Physics* **53**, 102210 (2012); doi: 10.1063/1.4759115

View online: <http://dx.doi.org/10.1063/1.4759115>

View Table of Contents: <http://scitation.aip.org/content/aip/journal/jmp/53/10?ver=pdfcov>

Published by the [AIP Publishing](#)

Articles you may be interested in

[On the reduction criterion for random quantum states](#)

J. Math. Phys. **55**, 112203 (2014); 10.1063/1.4901548

[Gibbs states on random configurations](#)

J. Math. Phys. **55**, 083513 (2014); 10.1063/1.4891992

[Time dependent quantum thermodynamics of a coupled quantum oscillator system in a small thermal environment](#)

J. Chem. Phys. **139**, 214108 (2013); 10.1063/1.4833566

[Generating random density matrices](#)

J. Math. Phys. **52**, 062201 (2011); 10.1063/1.3595693

[Entanglement of random subspaces via the Hastings bound](#)

J. Math. Phys. **51**, 042201 (2010); 10.1063/1.3309418

Did your publisher get
18 MILLION DOWNLOADS in 2014?
AIP Publishing did.



THERE'S POWER IN NUMBERS. Reach the world with AIP Publishing.



Realigning random states

Guillaume Aubrun^{1,a)} and Ion Nechita^{2,b)}

¹*Institut Camille Jordan, Université Claude Bernard Lyon 1, 43 Boulevard du 11 Novembre 1918, 69622 Villeurbanne CEDEX, France*

²*CNRS, Laboratoire de Physique Théorique, IRSAMC, Université de Toulouse, UPS, 31062 Toulouse, France*

(Received 13 September 2012; accepted 1 October 2012; published online 22 October 2012)

We study how the realignment criterion (also called computable cross-norm criterion) succeeds asymptotically in detecting whether random states are separable or entangled. We consider random states on $\mathbf{C}^d \otimes \mathbf{C}^d$ obtained by partial tracing a Haar-distributed random pure state on $\mathbf{C}^d \otimes \mathbf{C}^d \otimes \mathbf{C}^s$ over an ancilla space \mathbf{C}^s . We show that, for large d , typically, the realignment criterion is successful in detecting entanglement if and only if $s \leq (\frac{8}{3\pi})^2 d^2$. In this sense, the realignment criterion is asymptotically weaker than the partial transposition criterion. © 2012 American Institute of Physics. [<http://dx.doi.org/10.1063/1.4759115>]

I. INTRODUCTION

A central problem in quantum information theory is to decide whether a state is separable or entangled. Although this is a computationally hard task,¹⁰ several operational criteria have been proposed to detect entanglement, such as the Peres positive partial transpose criterion (PPT)¹⁸ and the realignment criterion due to Rudolph and Chen–Wu.^{5,6,19}

In this paper, we focus on the realignment criterion, study its behaviour on large dimensional bipartite systems and compute the threshold for random induced states, in the following sense. Induced quantum states are random states on $\mathcal{H} = \mathbf{C}^d \otimes \mathbf{C}^d$ which are obtained as the partial trace over an ancilla space \mathbf{C}^s of a Haar-distributed random pure state on $\mathcal{H} \otimes \mathbf{C}^s$. We show that a *threshold* for the realignment criterion occurs at $s_0 = (\frac{8}{3\pi})^2 d^2 \approx 0.72d^2$, in the following sense: if the ancilla dimension s is smaller than s_0 , with large probability the realignment criterion detects that the random state is entangled; when s is larger than s_0 , the realignment criterion fails and we cannot conclude whether the state is entangled or separable. Since the threshold for the PPT criterion is larger (it occurs at $s = 4d^2$, see Ref. 2), this means that the realignment criterion is asymptotically weaker than the Peres criterion.

Here is a more striking illustration of the relative power of the two criteria: take a random state uniformly distributed (with respect to the Lebesgue measure) on the convex body of all mixed states on $\mathbf{C}^d \otimes \mathbf{C}^d$ (this corresponds to $s = d^2$, see Ref. 21). Then, with probability tending to 1 as d tends to infinity, the following occurs: this state is entangled, and its entanglement is detected by the Peres criterion but not by the realignment criterion.

Our proofs are based on a new model in random matrix theory: realigned Wishart matrices. Let W be a Wishart random matrix ($W = XX^*$, where X is a $d^2 \times s$ matrix with i.i.d. Gaussian entries). We consider the realignment of the difference $W - sI$. The resulting matrix is not Hermitian, and we show that the asymptotic singular value distribution is given, under proper normalization, by the quarter-circle law.

The fact that the realignment criterion is generically asymptotically weaker than the Peres criterion is illustrated in a qualitative fashion when we focus on unbalanced bipartite systems. We consider random induced states on $\mathbf{C}^{d_1} \otimes \mathbf{C}^{d_2}$ (the dimension of the environment being still s).

a) aubrun@math.univ-lyon1.fr.

b) nechita@irsamc.ups-tlse.fr.

When d_1 is fixed and d_2 tends to infinity, we show that the threshold for the realignment criterion is $s = d_1^2$. This is to be compared with the corresponding threshold for the Peres criterion, which is not bounded with respect to d_2 (it was shown in Ref. 3 that this threshold is $s = \alpha(d_1)d_2$, with $\alpha(d_1) = 2d_1 + 2\sqrt{d_1^2 - 1}$).

The paper is organized as follows: Sec. II introduces the background and states the main theorem about the threshold for the realignment criterion on $\mathbf{C}^d \otimes \mathbf{C}^d$ (Theorem 2.1). Section III introduces realigned Wishart matrices, and contains Theorem 3.1 about convergence to the quarter-circle distribution. Section IV contains a derivation of Theorem 2.1 from Theorem 3.1. Section V introduces the graphical calculus which is used in the proof of Theorem 3.1. In Sec. VI, we compute the moments of realigned Wishart matrices, and the proof of Theorem 3.1 is completed in Sec. VII. Finally, Sec. VIII deals with unbalanced tensor products.

II. BACKGROUND AND STATEMENT OF THE RESULTS

A. Notation

We denote by $M_{d_1 \times d_2}(\mathbf{C})$, the space of $d_1 \times d_2$ matrices with complex-valued entries. The Hermitian conjugate of a matrix A is denoted A^* , and we denote $|A| := (AA^*)^{1/2}$. For $1 \leq p < +\infty$, the Schatten p -norms are defined by the formula $\|A\|_p := (\text{Tr } |A|^p)^{1/p}$. Also, we denote by $C, c, c_0 \dots$ numerical constants whose value may change from occurrence to occurrence.

B. Permutation criteria

We consider a bipartite Hilbert space $\mathcal{H} = \mathbf{C}^{d_1} \otimes \mathbf{C}^{d_2}$. Let $\{e_i\}_{i=1}^{d_1}$ and $\{f_j\}_{j=1}^{d_2}$ be the canonical bases of \mathbf{C}^{d_1} and \mathbf{C}^{d_2} . Any operator A on \mathcal{H} admits a (double-indexed) matrix representation

$$A = \sum_{i,k}^{d_1} \sum_{j,l}^{d_2} A_{ij,kl} |e_i \otimes f_j\rangle \langle e_k \otimes f_l|.$$

For every permutation σ of the indices $\{i, j, k, l\}$, we can introduce the corresponding reshuffling operation, which maps the matrix $A = (A_{ij,kl})$ to the (possibly non-square) matrix $A^\sigma = (A_{\sigma(i)\sigma(j), \sigma(k)\sigma(l)})$. This operation depends on the particular choices of bases.

If ρ is a pure product state, then ρ^σ has rank one, and $\|\rho^\sigma\|_1 = 1$. Consequently, for any separable state ρ , we have $\|\rho^\sigma\|_1 \leq 1$. In this way, each permutation produces an operational separability criterion. Such reshufflings were studied in Ref. 13, where it was proved that each of these 24 reshufflings is equivalent to one of the following.

- (1) The trivial reshuffling, where $\|A^\sigma\|_1 = \|A\|_1$ for every A .
- (2) The partial transposition,¹⁸ denoted A^Γ , which corresponds to swapping the indices j and l . This operation is equivalently described as $A^\Gamma = (\mathbf{I} \otimes T)A$, where T is the usual transposition of $d \times d$ matrices. Note that for a state ρ , the condition $\|\rho^\Gamma\|_1 \leq 1$ is equivalent to $\rho^\Gamma \geq 0$, and this is known as the PPT criterion (positive partial transpose).
- (3) The realignment,^{6,19} denoted A^R , which corresponds to swapping the indices j and k . We have

$$A^R = \sum_{i,k}^{d_1} \sum_{j,l}^{d_2} A_{ij,kl} |e_i \otimes e_k\rangle \langle f_j \otimes f_l|.$$

The resulting matrix A^R has dimension $d_1^2 \times d_2^2$. The fact that a separable state ρ must satisfy $\|\rho^R\|_1 \leq 1$ is called the *realignment criterion* or the *computable cross-norm criterion*.

Except in Sec. VIII, we focus on the balanced case ($d_1 = d_2 = d$). In this case, the matrix A^R is square; however, note that the realignment of a Hermitian matrix does not produce a Hermitian matrix in general. Note also that $\mathbf{I}^R = dE$, where $E = E_d$ is the maximally entangled state $E = |\psi\rangle\langle\psi|$, with $|\psi\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d |e_i \otimes e_i\rangle$. Obviously, one has also $\mathbf{I} = (dE)^R$.

It is known¹⁹ that when $d \geq 3$, neither of the PPT or realignment criteria is stronger (one can find entangled states which violate one criterion and satisfy the other one). In this paper, we show that when d is large, the PPT criterion is generically stronger than the realignment criterion.

The Choi–Jamiołkowski isomorphism J sheds a different light on the realignment criterion. If ρ is a state on $\mathbf{C}^{d_1} \otimes \mathbf{C}^{d_2}$, then $J(\rho)$ is a quantum channel, mapping states on \mathbf{C}^{d_1} to states on \mathbf{C}^{d_2} . The matrix of $J(\rho)$ (in the canonical matrix basis) is given by $d_1 \rho^R$. Since the state ρ is separable if and only if the channel $J(\rho)$ is entanglement-breaking (EB), we obtain the following reformulation of the realignment criterion: any EB quantum channel Φ satisfies $\|\Phi\|_1 \leq d_1$, where $\|\cdot\|_1$ denotes the trace class norm from maps between matrix spaces. In this formulation, this statement appears in Ref. 16 (Appendix A).

C. Random states

We consider the standard model of random induced states. These mixed states are obtained as partial traces (over some environment) of Haar-distributed random pure states. More precisely, we denote by $\mu_{n,s}$ the distribution of the state

$$\mathrm{Tr}_{\mathbf{C}^s} |\psi\rangle\langle\psi|,$$

where ψ is uniformly distributed on the unit sphere in $\mathbf{C}^n \otimes \mathbf{C}^s$. In the following, we identify \mathbf{C}^n with $\mathbf{C}^d \otimes \mathbf{C}^d$, for $n = d^2$.

Generically, a random induced state with distribution $\mu_{n,s}$ has rank $\min(n, s)$. When $s \geq n$, the probability measure $\mu_{n,s}$ has a density with respect to the Lebesgue measure on the set of states on \mathbf{C}^n which has a simple form²¹

$$\frac{d\mu_{n,s}(\rho)}{d\mathrm{vol}}(\rho) = \frac{1}{Z_{n,s}} (\det \rho)^{s-n}, \quad (1)$$

where $Z_{n,s}$ is a normalization factor. Note that formula (1) allows to define the measure $\mu_{n,s}$ for every real $s \geq n$, while the partial trace construction makes sense only for integer values of s .

The dimension s of the environment can be thought of as a parameter. The resulting mixed state is more likely to be entangled when s is small. On the other hand, if $s \rightarrow \infty$, the resulting mixed state converges to the maximally mixed state, which is separable. Therefore, for any separability criterion, we expect a threshold phenomenon—a critical value between the range of s where the criterion is generically satisfied and the range where it is generically not satisfied. Known results in this direction include, for a random state $\rho \in \mathbf{C}^d \otimes \mathbf{C}^d$ with distribution $\mu_{d^2,s}$ (see also Refs. 9 and 12).

- (1) For separability itself, the threshold is of order $s \approx d^3$. More precisely, ρ is typically entangled when $s \lesssim d^3$, and typically separable when $s \gtrsim d^3 \log^2 d$.¹
- (2) For the PPT criterion, the threshold occurs precisely at $s = 4d^2$: ρ is typically not-PPT when $s \leq 4d^2$ and typically PPT when $s \geq 4d^2$.²

(in this context, a property is called typical if the probability that it holds goes to 1 as d tends to infinity).

We show that the threshold for the realignment criterion is precisely at $s = (\frac{8}{3\pi})^2 d^2$. This is our main theorem.

Theorem 2.1. Denote $\gamma = (\frac{8}{3\pi})^2 \approx 0.72$. For every $\varepsilon > 0$, there exist positive constants $c(\varepsilon)$, $C(\varepsilon)$ such that the following holds. If ρ is a random state on $\mathbf{C}^d \otimes \mathbf{C}^d$ with distribution $\mu_{d^2,s}$, then

- (1) If $s \leq (\gamma - \varepsilon)d^2$, then

$$\mathbf{P}(\|\rho^R\|_1 > 1) \geq 1 - C(\varepsilon) \exp(-c(\varepsilon)d^{1/4}).$$

- (2) If $s \geq (\gamma + \varepsilon)d^2$, then

$$\mathbf{P}(\|\rho^R\|_1 \leq 1) \geq 1 - C(\varepsilon) \exp(-c(\varepsilon)d^{1/4}).$$

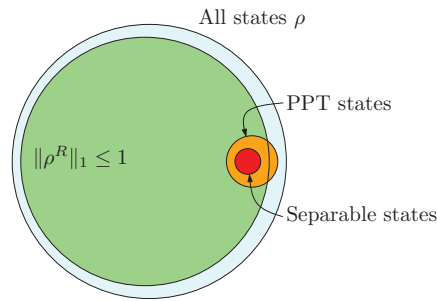


FIG. 1. Schematic representation of volumes.

A comparison between the thresholds for the PPT and realignment criteria shows that the latter is *generically asymptotically weaker*. When the environment dimension s is between $(\frac{8}{3\pi})^2 d^2$ and $4d^2$, random states are non-PPT, but the realignment criterion fails to detect entanglement. As noted in the Introduction, this range includes the special case $s = d^2$, which corresponds to the uniform measure on the set of states (the density in Eq. (1) being constant). We pictured in Fig. 1 the different convex sets involved, where the size of respective circles aims at representing faithfully the volume. With respect to the volume, a typical state ρ is non-PPT and entangled, but satisfies $\|\rho^R\| \leq 1$, hence the realignment criterion fails to detect entanglement.

The theorem will follow from the description of the limiting distribution of singular values of ρ^R , which are shown to converge towards the quarter-circle distribution. This result can be equivalently stated using Wishart matrices instead of random quantum states, which are more convenient from a random matrix theory perspective. We develop this approach in Sec. III.

We also consider the case of unbalanced states, i.e., $\mathbf{C}^{d_1} \otimes \mathbf{C}^{d_2}$ with d_1 fixed, and d_2 tending to infinity. In this asymptotic regime, we show that the threshold for the realignment criterion is exactly $s = d_1^2$. Since the threshold occurs for a finite value of s , the realignment criterion is *qualitatively weaker* in the unbalanced case than the Peres criterion (see Refs. 3 and 4).

III. SPECTRAL DISTRIBUTION OF REALIGNED WISHART MATRICES

We describe here a new result from random matrix theory, which is the main ingredient in the proof of Theorem 2.1. Let X be a $d^2 \times s$ random matrix with i.i.d. $\mathcal{N}_{\mathbf{C}}(0, 1)$ entries, and $W = XX^\dagger$ (we recall that a complex-valued random variable ξ has distribution $\mathcal{N}_{\mathbf{C}}(0, 1)$ if $\sqrt{2}\Re\xi$ and $\sqrt{2}\Im\xi$ are independent standard normal random variables). The random matrix W is known as a Wishart random matrix with parameters (d^2, s) . We consider W as an operator on $\mathbf{C}^d \otimes \mathbf{C}^d$, therefore we can consider the realignment of W , denoted $R = W^R$. We may write $W_{d^2, s}, R_{d^2, s}, \dots$ instead of W, R, \dots if we want to make dimensions explicit.

It turns out to be simpler to study the difference $W - s\mathbf{I}$ rather than W itself, or equivalently to study the operator $R - dsE$ (recall that $\mathbf{I}^R = dE$). The following theorem (proved in Sec. VII) describes the asymptotic behaviour of the singular values of $R - dsE$. We denote by $\text{Cat}_p := \frac{1}{p+1} \binom{2p}{p}$ the p th Catalan number.

Recall that the (standard) quarter-circle distribution is the probability measure

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

The even moments of this measure are given by the Catalan numbers

$$\int_0^2 x^{2p} d\mu_{qc}(x) = \text{Cat}_p,$$

whereas the odd moments are

$$\int_0^2 x^{2p+1} d\mu_{qc}(x) = \frac{2^{4p+5} p!(p+2)!}{\pi(2p+4)!}.$$

In particular, the average of μ_{qc} is $8/(3\pi)$.

Theorem 3.1. For all integers s, d , let $R_{d^2,s}$ be the realignment of a Wishart matrix $W_{d^2,s}$, and $Q = Q_{d^2,s} = \frac{1}{d\sqrt{s}}(R_{d^2,s} - dsE)$. Then, when d and s tend to infinity,

$$\lim_{d,s \rightarrow \infty} \mathbf{E} \frac{1}{d^2} \text{Tr}[(QQ^*)^p] = \text{Cat}_p,$$

$$\lim_{d,s \rightarrow \infty} \mathbf{Var} \frac{1}{d^2} \text{Tr}[(QQ^*)^p] = 0.$$

We emphasize that there is no assumption about the relative growth of s and d , besides the fact that they both tend to infinity.

Theorem 3.1 can be restated as follows: the empirical singular value distribution of Q , defined as $\frac{1}{d^2} \sum_{i=1}^{d^2} \sigma_i(Q)$, converges in moments towards the quarter-circle distribution μ_{qc} . Via standard arguments (see, e.g., Ref. 2 for a sketch), it follows that for every continuous function $f : \mathbf{R}^+ \rightarrow \mathbf{R}$ with polynomial growth, we have (convergence in probability)

$$\frac{1}{d^2} \text{Tr} f(|Q_{d^2,s}|) \xrightarrow{\mathbf{P}} \int_0^2 f d\mu_{qc}. \tag{2}$$

When applied to the function $f(x) = x$, Eq. (2) yields

$$\|Q_{d^2,s}\|_1 \stackrel{\mathbf{P}}{\sim} \frac{8d^2}{3\pi} \tag{3}$$

(by $X \stackrel{\mathbf{P}}{\sim} Y$ we mean that the ratio X/Y converges in probability towards 1).

IV. FROM WISHART MATRICES TO RANDOM STATES: PROOF OF THEOREM 2.1

In this section, we show how to derive Theorem 2.1 from the results on Wishart matrices. Random induced states are closely related to Wishart matrices. Indeed, it is well known that if $W = W_{d^2,s}$ is a Wishart matrix, then $\rho := (\text{Tr } W)^{-1} W$ is a random state with distribution $\mu_{d^2,s}$.

We are going to prove first a weak form of the theorem, where we show that the threshold is of order d^2 , without identifying the exact constant $\gamma = (\frac{8}{3\pi})^2$. Here is the relevant proposition; the proof will use only the expansion of $\text{Tr}(QQ^*)^p$ for $p = 1$ and $p = 2$, and will have the advantage to work for all values of s (including $s \ll d^2$ or $s \gg d^2$, which require special attention).

Proposition 4.1. There exist absolute constants c, C, c_0 , and C_0 such that, for a random state ρ on $\mathbf{C}^d \otimes \mathbf{C}^d$ with distribution $\mu_{d^2,s}$, the following holds:

- (1) If $s \leq c_0 d^2$, then $\mathbf{P}(\|\rho^R\|_1 > 1) \geq 1 - C \exp(-cd^{1/4})$.
- (2) If $s \geq C_0 d^2$, then $\mathbf{P}(\|\rho^R\|_1 \leq 1) \geq 1 - C \exp(-cd^{1/4})$.

Assume that ρ is defined by the equation $\rho := (\text{Tr } W)^{-1} W$, where W is a Wishart random matrix with parameters (d^2, s) . Define α by $\text{Tr } W = (1 + \alpha)d^2s$. The matrix Q from Theorem 3.1 is related to ρ by the equation $\frac{1}{d\sqrt{s}}Q = (1 + \alpha)\rho^R - E/d$. In particular,

$$\frac{1}{1 + \alpha} \left(\frac{\|Q\|_1}{d\sqrt{s}} - \frac{1}{d} \right) \leq \|\rho^R\|_1 \leq \frac{1}{1 + \alpha} \left(\frac{\|Q\|_1}{d\sqrt{s}} + \frac{1}{d} \right). \tag{4}$$

The random variable $\text{Tr } W$ follows a χ^2 distribution, and the next lemma implies that with large probability, $|\alpha| \leq 1/(d\sqrt{s})$.

Lemma 4.2 (see, e.g., Ref. 15, Lemma 1). If $W = W_{d^2,s}$ is a Wishart matrix, then for every $0 < \varepsilon < 1$,

$$\mathbf{P} \left(\left| \frac{\text{Tr } W}{d^2s} - 1 \right| > \varepsilon \right) \leq 2 \exp(-c\varepsilon^2 d^2s).$$

Proof of Proposition 4.1. It is possible to estimate $\|Q\|_1$ from the knowledge of $\|Q\|_2$ and $\|Q\|_4$, using the following inequalities:

$$\frac{\|Q\|_2^3}{\|Q\|_4^2} \leq \|Q\|_1 \leq d\|Q\|_2. \tag{5}$$

Since $\|Q\|_2^2 = \text{Tr}(QQ^*)$ and $\|Q\|_4^4 = \text{Tr}(QQ^*QQ^*)$ are polynomials in the matrix entries, they are easier to analyze. Here is a proposition which can be derived from the analysis in Sec. VII—more precisely see Eqs. (11), (12), and (14).

Proposition 4.3. *There are absolute constants c, C such that the following inequalities hold for every d and s :*

$$cd^2 \leq \mathbf{E} \|Q\|_2^2 \leq Cd^2, \quad cd^2 \leq \mathbf{E} \|Q\|_4^4 \leq Cd^2, \\ \mathbf{Var} \|Q\|_2^2 \leq Cd^2, \quad \mathbf{Var} \|Q\|_4^4 \leq Cd^2.$$

We now use a general concentration inequality for polynomials in Gaussian variables.

Proposition 4.4 (see Ref. 14, Theorem 6.7). *Let (G_i) be independent Gaussian variables, and P be a polynomial of (total) degree q . Consider the random variable $Y = P(G_1, \dots, G_n)$. Then for every $t > 0$,*

$$\mathbf{P}(|Y - \mathbf{E} Y| \geq t\sqrt{\mathbf{Var} Y}) \leq C_q \exp(-c_q t^{2/q})$$

(C_q and c_q being constants depending only on q).

Applied to the polynomials $\|Q\|_2^2$ and $\|Q\|_4^4$ (of degree, respectively, 4 and 8), we obtain, that with large probability, both $\|Q\|_2^2$ and $\|Q\|_4^4$ are of order d^2 (up to universal constant). Together with (5), this yields that, for some absolute constants c, C ,

$$\mathbf{P}(cd^2 \leq \|Q\|_1 \leq Cd^2) \geq 1 - C \exp(-cd^{1/4}). \tag{6}$$

From (6) and (4), we obtain that with probability larger than $1 - C \exp(-cd^{1/4})$,

$$\frac{1}{1+\alpha} \left(\frac{cd}{\sqrt{s}} - \frac{1}{d} \right) \leq \|\rho^R\|_1 \leq \frac{1}{1+\alpha} \left(\frac{Cd}{\sqrt{s}} + \frac{1}{d} \right)$$

and Proposition 4.1 follows from Lemma 4.2. □

We denote by \mathcal{R} the (convex) set of states which are not detected to be entangled by the realignment criterion

$$\mathcal{R} = \mathcal{R}(\mathcal{H}) = \{ \rho : \rho \text{ is a state on } \mathcal{H} \text{ with } \|\rho^R\|_1 \leq 1 \}.$$

We also introduce the gauge $\|\cdot\|_{\mathcal{R}}$ associated with the convex body \mathcal{R} . It is defined for any state ρ as

$$\|\rho\|_{\mathcal{R}} = \inf \left\{ t \geq 0 : \frac{\mathbf{I}}{d^2} + \frac{1}{t} \left(\rho - \frac{\mathbf{I}}{d^2} \right) \in \mathcal{R} \right\} \\ = \inf \left\{ t \geq 0 : \left\| \frac{E}{d} + \frac{1}{t} \left(\rho^R - \frac{E}{d} \right) \right\|_1 \leq 1 \right\}.$$

Lemma 4.5. *The following inequalities hold for any state ρ on $\mathbf{C}^d \otimes \mathbf{C}^d$,*

$$\frac{d}{d+1} \|\rho^R - E/d\|_1 \leq \|\rho\|_{\mathcal{R}} \leq \frac{d}{d-1} \|\rho^R - E/d\|_1.$$

Proof. Let $\lambda = \|\rho\|_{\mathcal{R}}$. Then $\left\| \frac{E}{d} + \frac{1}{\lambda} \left(\rho^R - \frac{E}{d} \right) \right\|_1 = 1$, and by the triangle inequality

$$1 - \frac{1}{d} \leq \frac{1}{\lambda} \left\| \rho^R - \frac{E}{d} \right\|_1 \leq 1 + \frac{1}{d}$$

and the result follows. □

We are going to use a result from Ref. 1, which gives a concentration inequality for the gauge of a random state (note that the inradius of \mathcal{R} equals the inradius of the set of separable states, which is $1/\sqrt{d^2(d^2 - 1)}$, see Ref. 11). We obtain the following.

Proposition 4.6 (Ref. 1, Proposition 4.2). *For every constant $\theta > 0$, there are constants c, C such that the following hold. Let $s \geq \theta d^2$, and ρ be a random state on $\mathbf{C}^d \otimes \mathbf{C}^d$ with distribution $\mu_{d^2, s}$, then*

$$\mathbf{P}(\|\rho\|_{\mathcal{R}} - M \geq \eta) \leq C \exp(-cs) + C \exp(-cs\eta^2),$$

where $M = M_{d^2, s}$ is the median of the random variable $\|\rho\|_{\mathcal{R}}$.

Note that Proposition 4.2 in Ref. 1 is stated with the restriction $s \geq d^2$; however, it can be checked that the proof extends to the range $s \geq \theta d^2$ for any $\theta > 0$, altering only the values of c and C . We are going to use Proposition 4.6 with $\theta = c_0$, where c_0 is the constant appearing in Proposition 4.1. We can now pass to the complete proof of Theorem 2.1.

Proof of Theorem 2.1. Let us show the first part of the statement, the second part being similar. Since the case when $s \leq c_0 d^2$ was covered by Proposition 4.1, we may assume $s \geq c_0 d^2$.

Denote by $\pi_{d^2, s}$ the probability that a random state on $\mathbf{C}^d \otimes \mathbf{C}^d$, with distribution $\mu_{d^2, s}$, belongs to the set \mathcal{R} . Fix $\varepsilon > 0$. For each d , let $s = s_d$ be the number with $c_0 d^2 \leq s \leq (1 - \varepsilon)\gamma d^2$ such that $\pi_{d^2, s}$ is maximal. We claim that

$$\liminf_{d \rightarrow \infty} M_{d^2, s_d} \geq \frac{1}{\sqrt{1 - \varepsilon}}.$$

Indeed, by Lemma 4.5, the random variables $\|\rho\|_{\mathcal{R}}$ and $\|\rho^R - E/D\|_1$ have asymptotically equivalent medians. Moreover, by (4), it suffices to show that

$$\liminf_{d \rightarrow \infty} \text{Median} \left(\frac{\|Q\|_1}{d\sqrt{s}} \right) \geq \frac{1}{\sqrt{1 - \varepsilon}},$$

and this last inequality follows immediately from (3).

Choose some η such that $0 < \eta < \frac{1}{\sqrt{1 - \varepsilon}} - 1$. Applying Proposition 4.6, we obtain, for d large enough,

$$\pi_{d^2, s} = \mathbf{P}(\rho \in \mathcal{R}) \leq \mathbf{P}(\|\rho\|_{\mathcal{R}} < M_{d^2, s_d} - \eta) \leq C(\varepsilon) \exp(-c(\varepsilon)s_d).$$

Small values of d are taken into account by adjusting the constants if necessary.

For the second part of the theorem, consider the number $s = s'_d$ with $s \geq (1 - \varepsilon)\gamma d^2$ such that $\pi_{d^2, s}$ is minimal. This number is well defined since for fixed d , the sequence $\pi_{d^2, s}$ converges to 1 as s tends to infinity (the measures $\mu_{d^2, s}$ converge towards the Dirac mass at the maximally mixed state). The rest of the proof is similar. \square

V. BACKGROUND ON COMBINATORICS OF NON-CROSSING PARTITIONS AND GRAPHICAL CALCULUS

Let us first recall a number of results from the combinatorial theory of non-crossing partitions; see Ref. 17 for a detailed presentation of the theory. We denote by S_p the group of permutations on $\{1, \dots, p\}$. For $\sigma \in S_p$, we introduce the following standard notation:

- $\#\sigma$ is the number of cycles of σ ;
- $|\sigma|$ is its length, defined as the minimal number k such that σ can be written as a product of k transpositions. The function $(\sigma, \pi) \rightarrow |\sigma^{-1}\pi|$ defines a distance on S_p . One has $\#\sigma + |\sigma| = p$.

Let $\xi \in S_p$ be the canonical full cycle $\xi = (12 \dots p)$. The set of permutations $\sigma \in S_p$ which saturate the triangular inequality $|\sigma| + |\sigma^{-1}\xi| = |\xi| = p - 1$ is in bijection with the set $NC(p)$ of non-crossing partitions of $[p] := \{1, \dots, p\}$. We call such permutations *geodesic* and we shall not distinguish between a non-crossing partition and its associated geodesic permutation. We also recall a well-known bijection between $NC(p)$ and the set $NC_2(2p)$ of non-crossing pairings of $2p$ elements.

To a non-crossing partition $\pi \in NC(p)$, we associate an element $\text{fat}(\pi) \in NC_2(2p)$ as follows: for each block $\{i_1, i_2, \dots, i_k\}$ of π , we add the pairings $\{2i_1 - 1, 2i_k\}, \{2i_1, 2i_2 - 1\}, \{2i_2, 2i_3 - 1\}, \dots, \{2i_{k-1}, 2i_k - 1\}$ to $\text{fat}(\pi)$. The inverse operation is given by collapsing the elements $2i - 1, 2i \in \{1, \dots, 2p\}$ to a single element $i \in \{1, \dots, p\}$.

In the rest of the paper, we shall perform moment computations for random matrices with Gaussian entries. The main tool we use is the Wick formula (see, e.g., Ref. 20 for a proof).

Lemma 5.1. *Let X_1, \dots, X_k be jointly Gaussian centered random variables. If $k = 2p + 1$, then $\mathbf{E}[X_1 \cdots X_k] = 0$. If $k = 2p$, then*

$$\mathbf{E}[X_1 \cdots X_k] = \sum_{\substack{\pi = \{(i_1, j_1), \dots, (i_p, j_p)\} \\ \text{pairing of } \{1, \dots, k\}}} \prod_{m=1}^p \mathbf{E}[X_{i_m} X_{j_m}]. \tag{7}$$

The above formula is very useful when applied to moments of Gaussian random matrices. Moreover, a *graphical formalism* adapted to random matrices was developed in Ref. 8 in order to facilitate its application. This graphical calculus is similar to the one introduced in Ref. 7 for unitary integrals and the corresponding Weingarten formula. We present next the basic ideas of the Gaussian graphical calculus and we refer the interested reader to Ref. 8 for the details.

In the Gaussian graphical calculus tensors (and, in particular, matrices) are represented by *boxes*. In order to specify the vector space a tensor belongs to, boxes are decorated with differently shaped symbols, where each symbol corresponds to a vector space. The symbols are empty (white) or filled (black), corresponding to primal or dual spaces. Tensor contractions are represented graphically by *wires* connecting these symbols. A wire should always connect two symbols of the same shape (corresponding thus to vector spaces of the same dimension). A wire connecting an empty symbol with a filled symbol of the same shape corresponds to the canonical map $\mathbf{C}^n \otimes (\mathbf{C}^n)^* \rightarrow \mathbf{C}$. However, we shall allow wires connecting two white or black symbols, by identifying non-isomorphically a vector space with its dual. Finally, a *diagram* is a collection of such boxes and wires and corresponds to an element in a tensor product space.

The main advantage of such a representation is that it provides an efficient way of computing expectation values of such tensors when some (or all) of the boxes are random matrices with i.i.d. Gaussian entries. Indeed, there exists an efficient way of implementing the Wick formula in Lemma 5.1. When the entries of the Gaussian matrices have standard normal distributions, the covariances in Eq. (7) are just delta functions. We state now the graphical Wick formula from Ref. 8.

Theorem 5.2. *Let \mathcal{D} be a diagram containing p boxes X and p boxes \bar{X} which correspond to random matrices with i.i.d. standard Gaussian entries. Then*

$$\mathbf{E}_X[\mathcal{D}] = \sum_{\alpha \in \mathcal{S}_p} \mathcal{D}_\alpha,$$

where the diagram \mathcal{D}_α is constructed as follows. One starts by erasing the boxes X and \bar{X} , but keeps the symbols attached to these boxes. Then, the decorations (white and black) of the i th X box are paired with the decorations of the $\alpha(i)$ -th \bar{X} box in a coherent manner, see Figure 2. In this way, we obtain a new diagram \mathcal{D}_α which does not contain any X or \bar{X} boxes. The resulting diagrams \mathcal{D}_α may

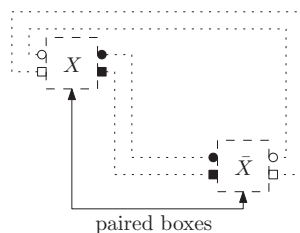


FIG. 2. Pairing of boxes in the Gaussian graphical calculus.

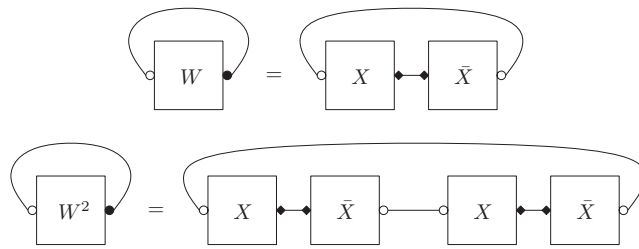


FIG. 3. Diagrams for the first two moments of a Wishart matrix. Round symbols correspond to \mathbf{C}^d and diamond symbols correspond to \mathbf{C}^s .

contain loops, which correspond to scalars; these scalars are equal to the dimension of the vector space associated with the decorations.

We now present a simple example of moment computation that makes use of the Gaussian graphical calculus. Let $W \in M_d(\mathbf{C})$ be a complex Wishart matrix of parameters (d, s) , that is $W = XX^*$ with $X \in M_{d \times s}(\mathbf{C})$ with i.i.d. standard complex Gaussian entries. The diagrams for the first and the second moment of W are presented in Figure 3. Since these diagrams contain only Gaussian boxes, the resulting expanded diagrams \mathcal{D}_α will contain only loops, so they will be scalars. For the first moment, the diagram contains only one pair of Gaussian matrices X/\bar{X} , hence the expected value of the trace is given by the following one term sum (see Figure 4),

$$\mathbf{E} \operatorname{Tr} W = \sum_{\alpha \in S_1} \mathcal{D}_\alpha = ds.$$

For the second moment, there are two pairs of Gaussian boxes, thus the formula in Theorem 5.2 contains two terms, see Figure 5,

$$\mathbf{E} \operatorname{Tr} W^2 = \sum_{\alpha \in S_2} \mathcal{D}_\alpha = \mathcal{D}_{(1)(2)} + \mathcal{D}_{(12)} = ds^2 + d^2s.$$

VI. MOMENT FORMULA FOR THE SINGULAR VALUES OF A REALIGNED WISHART MATRIX

In this section, we deduce a formula for realigned Wishart matrices, using Theorem 5.2. We are going to work in the more general setting of unbalanced tensor products. We consider Wishart matrices $W \in M_{d_1}(\mathbf{C}) \otimes M_{d_2}(\mathbf{C})$ of parameters $(d_1 d_2, s)$, i.e., $W = XX^*$ with $X \in M_{d_1 d_2 \times s}(\mathbf{C})$ having i.i.d. $\mathcal{N}_{\mathbf{C}}(0, 1)$ entries.

Let $R = W^R \in M_{d_1^2 \times d_2^2}(\mathbf{C})$ be the realigned version of W , that is

$$R_{ij,kl} = W_{ik,jl}.$$

The diagram of the matrix R is presented in Figure 6.

Proposition 6.1: The moments of the random matrix RR^* are given by

$$\mathbf{E} \operatorname{Tr}[(RR^*)^p] = \sum_{\alpha \in S_{2p}} s^{\#\alpha} d_2^{\#(\alpha\gamma^{-1})} d_1^{\#(\alpha\delta^{-1})}, \tag{8}$$

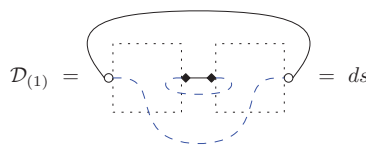


FIG. 4. Graphical expansion for the first moment of a Wishart matrix. There is only one term in the sum, corresponding to the unique permutation on one element.

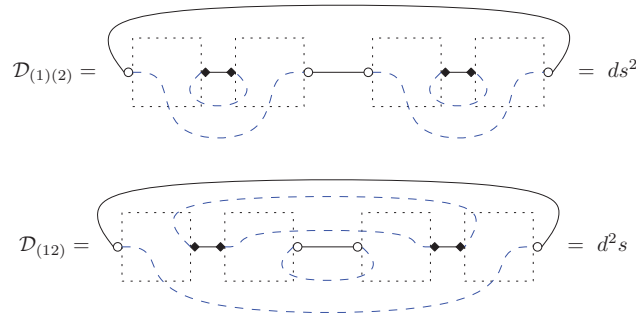


FIG. 5. Graphical expansion for the second moment of a Wishart matrix. There are two terms in the sum, corresponding to the identity permutation (1) and (2) and to the transposition (12).

where the permutations $\gamma, \delta \in S_{2p}$ are given by

$$\begin{aligned} \gamma &= (12)(34) \cdots (2p-1, 2p), \\ \delta &= (1, 2p)(23)(45) \cdots (2p-2, 2p-1). \end{aligned}$$

Proof: In Figure 7, we represent the matrix RR^* and its p th moment. The second diagram contains $2p$ W boxes, each W box being represented in Figure 6. We use Theorem 5.2 to compute the average

$$\mathbf{E} \text{Tr}[(RR^*)^p] = \sum_{\alpha \in S_{2p}} \mathcal{D}_\alpha,$$

where \mathcal{D}_α is the diagram obtained after the removal of the X and X^* boxes and connecting the i th X box with the $\alpha(i)$ -th X^* box. Since the random boxes are the only tensors appearing in the diagram, each \mathcal{D}_α will contain only loops that can be counted in the following way:

- (1) There are $\#\alpha$ loops coming from squared labels (associated with \mathbf{C}^s), because the initial wiring of these labels is given by the identity permutation.
- (2) There are $\#(\alpha\gamma^{-1})$ loops coming from the lower round labels (associated with \mathbf{C}^{d_2}). The initial wiring of these labels is given by the permutation

$$\gamma = (12)(34) \cdots (2p-1, 2p).$$

- (3) There are $\#(\alpha\delta^{-1})$ loops coming from the upper square labels (associated with \mathbf{C}^{d_1}). The initial wiring of these labels is given by the permutation

$$\delta = (1, 2p)(23)(45) \cdots (2p-2, 2p-1).$$

Taking into account all contributions, we obtain the announced moment formula for RR^* . \square

VII. PROOF OF THEOREM 3.1

Recall that in Theorem 3.1, we are considering the balanced case, $d_1 = d_2 = d$. Note that

$$QQ^* = d^{-2}s^{-1}(RR^* - dsRE_d - dsE_dR^* + d^2s^2E_d),$$

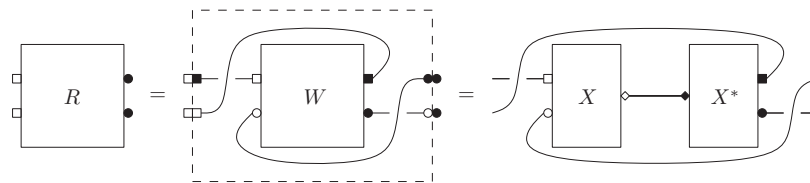


FIG. 6. The diagram of a realigned Wishart matrix. Square symbols correspond to \mathbf{C}^{d_1} , round symbols correspond to \mathbf{C}^{d_2} , and diamond-shaped labels correspond to \mathbf{C}^s .

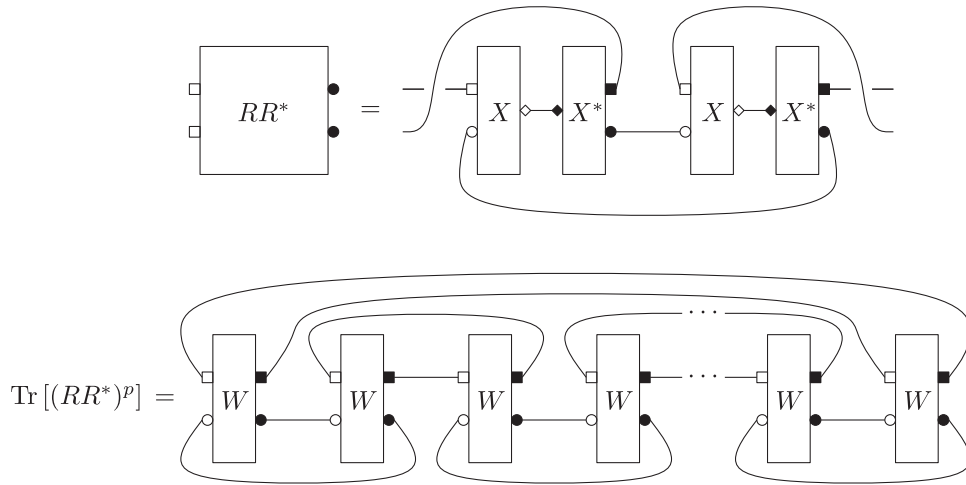


FIG. 7. The diagrams of the product RR^* and of the p th moment of RR^* .

so that one can expand the p th moment as

$$\mathbf{E} \operatorname{Tr}[(QQ^*)^p] = d^{-2p} s^{-p} \sum_{f_{1,2}: [p] \rightarrow \{0,1\}} (-1)^{\sum_i (f_1(i) + f_2(i))} \mathbf{E} \operatorname{Tr} \prod_{i=1}^p (F_1(i) F_2(i)),$$

where

$$F_1(i) = \begin{cases} R & \text{when } f_1(i) = 0, \\ dsE_d & \text{when } f_1(i) = 1, \end{cases}$$

and

$$F_2(i) = \begin{cases} R^* & \text{when } f_2(i) = 0, \\ dsE_d & \text{when } f_2(i) = 1. \end{cases}$$

We are going to use now a trick that will allow us to compute the expected value in the general term above in the same manner as we did for RR^* in Proposition 6.1. The idea, presented graphically in Figure 8, is that when one uses the graphical expansion formula for the expected value above, it is as if we had only RR^* terms, but the set of permutations we allow is restricted to

$$S_{2p}(f_1, f_2) = \{\alpha \in S_{2p} \mid \forall i \in f_1^{-1}(1), \alpha(2i - 1) = 2i - 1 \text{ and } \forall i \in f_2^{-1}(1), \alpha(2i) = 2i\}.$$

Using the result in Proposition 6.1, we obtain

$$\begin{aligned} \mathbf{E} \operatorname{Tr}[(QQ^*)^p] &= d^{-2p} s^{-p} \sum_{f_{1,2}: [p] \rightarrow \{0,1\}} (-1)^{\sum_i (f_1(i) + f_2(i))} \sum_{\alpha \in S_{2p}(f_1, f_2)} s^{\#\alpha} d^{\#(\alpha\gamma^{-1})} d^{\#(\alpha\delta^{-1})} \\ &= d^{-2p} s^{-p} \sum_{\alpha \in S_{2p}} s^{\#\alpha} d^{\#(\alpha\gamma^{-1})} d^{\#(\alpha\delta^{-1})} \sum_{(f_1, f_2) \in \mathcal{F}(\alpha)} (-1)^{\sum_i (f_1(i) + f_2(i))}. \end{aligned}$$

Note that in the last equality we inverted the summation order, so we had to restrict the set of choice functions $f_{1,2}$ to the family

$$\mathcal{F}(\alpha) = \{(f_1, f_2) \mid \alpha(2i - 1) \neq 2i - 1 \Rightarrow f_1(i) = 0 \text{ and } \alpha(2i) \neq 2i \Rightarrow f_2(i) = 0\}.$$

Let us show now that whenever a permutation $\alpha \in S_{2p}$ has a fixed point i_0 , the corresponding sum

$$\sum_{(f_1, f_2) \in \mathcal{F}(\alpha)} (-1)^{\sum_i (f_1(i) + f_2(i))} \tag{9}$$

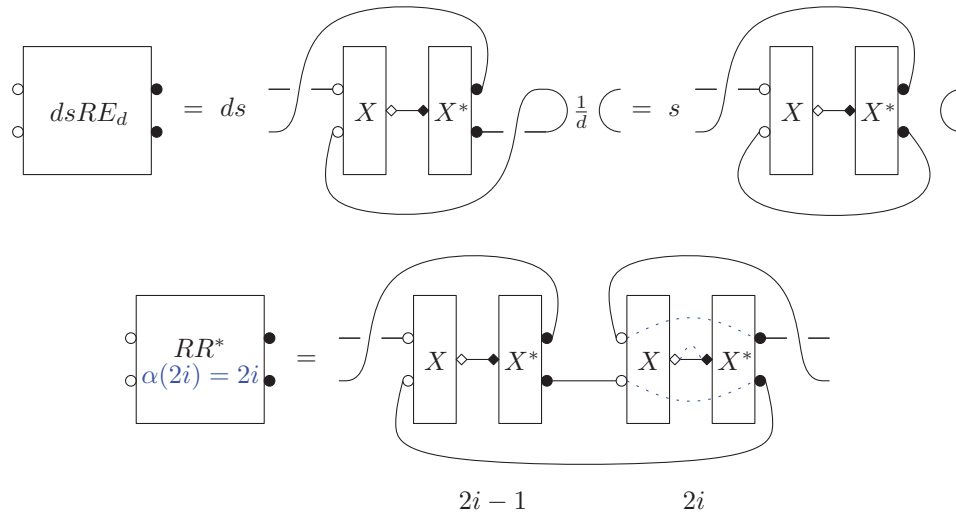


FIG. 8. The diagrams of $dsRE_d$ and of RR^* , with the constraint $\alpha(2i) = 2i$ are the same.

equals zero. For such a permutation and an element $f = (f_1, f_2) \in \mathcal{F}(\alpha)$, define another pair $\tilde{f} = (\tilde{f}_1, \tilde{f}_2)$ as follows. If i_0 is odd, $i_0 = 2j_0 - 1$, then put $\tilde{f}_2 = f_2$ and

$$\tilde{f}_1(j) = \begin{cases} 1 - f_1(j) & \text{if } j = j_0, \\ f_1(j) & \text{if } j \neq j_0. \end{cases}$$

For even $i_0 = 2j_0$, define $\tilde{f}_1 = f_1$ and

$$\tilde{f}_2(j) = \begin{cases} 1 - f_2(j) & \text{if } j = j_0, \\ f_2(j) & \text{if } j \neq j_0. \end{cases}$$

Since i_0 is a fixed point of α , we have $\tilde{f} = (\tilde{f}_1, \tilde{f}_2) \in \mathcal{F}(\alpha)$ and the map $f \rightarrow \tilde{f}$ is thus an involution without fixed points acting on $\mathcal{F}(\alpha)$. Notice also that changing a single value in a pair (f_1, f_2) changes the parity of the sum $\sum_i (f_1(i) + f_2(i))$. This concludes our argument that the sum (9) is null whenever α has a fixed point.

We have thus shown that permutations with fixed points cancel each other out, so we have

$$\mathbf{E} \text{Tr}[(QQ^*)^p] = d^{-2p} s^{-p} \sum_{\alpha \in S_{2p}^o} s^{\#\alpha} d^{\#(\alpha\gamma^{-1})} d^{\#(\alpha\delta^{-1})} \sum_{(f_1, f_2) \in \mathcal{F}(\alpha)} (-1)^{\sum_i (f_1(i) + f_2(i))},$$

where we denote by S_{2p}^o the set of permutations of $[2p]$ without fixed points. For such a permutation α , the set of admissible choices $\mathcal{F}(\alpha)$ contains only one element $f = (f_1, f_2)$ with $f_1(i) = f_2(i) = 0$ in such a way that the above formula simplifies to

$$\mathbf{E} \text{Tr}[(QQ^*)^p] = \sum_{\alpha \in S_{2p}^o} d^{-2p} s^{-p} s^{\#\alpha} d^{\#(\alpha\gamma^{-1})} d^{\#(\alpha\delta^{-1})}. \tag{10}$$

For small values of p , we obtain

$$\mathbf{E} \text{Tr}[QQ^*] = d^2, \tag{11}$$

$$\mathbf{E} \text{Tr}[(QQ^*)^2] = 2d^2 + 2s^{-1}d^2 + 1 + 4s^{-1}. \tag{12}$$

We show next that the dominating term in the sum above is of the order d^2 and that it is given by permutations α which are non-crossing pair partitions of $[2p]$. Since there are Cat_p such

permutations, we obtain

$$\mathbf{E} \operatorname{Tr}[(QQ^*)^p] = d^2 \operatorname{Cat}_p(1 + o(1)), \tag{13}$$

which is the moment formula we aimed for.

Let us consider separately the exponents of d and s in the general term of the sum (10),

$$g(\alpha) = -2p + \#(\alpha\gamma^{-1}) + \#(\alpha\delta^{-1}) = 2p - (|\alpha\gamma^{-1}| + |\alpha\delta^{-1}|),$$

$$h(\alpha) = -p + \#\alpha = p - |\alpha|.$$

Using the triangular inequality and the fact that α has no fixed points, we obtain

$$|\alpha\gamma^{-1}| + |\alpha\delta^{-1}| \geq |\gamma\delta| = |(2p - 1)(2p - 3) \cdots (531)(246 \cdots 2p)| = 2p - 2,$$

$$|\alpha| \geq p,$$

which shows that we have indeed $g(\alpha) \leq 2$ and $h(\alpha) \leq 0$. In order to conclude, it remains to be shown that the permutations which saturate both inequalities are exactly the non-crossing pair partitions of $[2p]$. The fact that α has no fixed points and that $|\alpha| = p$ implies that α is indeed a product of p disjoint transpositions, i.e., a pair partition. To show that it is non-crossing, we start from the geodesic condition $|\alpha\gamma^{-1}| + |\alpha\delta^{-1}| = |\gamma\delta| = |(2p - 1)(2p - 3) \cdots (531)(246 \cdots 2p)|$. This implies that the permutation $\gamma\alpha$ lies on the geodesic $\operatorname{id} \rightarrow \gamma\delta$. More precisely, we can write $\alpha = \gamma\Pi_o\Pi_e$ where Π_o and Π_e are permutations acting on the odd, respectively, even elements of $[2p]$. The geodesic condition implies that these permutations come from non-crossing partitions $\pi_o, \pi_e \in NC(p)$,

$$\begin{aligned} \Pi_o(2i - 1) &= 2\pi_o^{-1}(i) - 1, \\ \Pi_o(2i) &= 2i, \\ \Pi_e(2i - 1) &= 2i - 1, \\ \Pi_e(2i) &= 2\pi_e(i). \end{aligned}$$

The fact that α is an involution easily implies $\pi_e = \pi_o =: \pi \in NC(p)$ so that the action of α is given by

$$\begin{aligned} \alpha(2i - 1) &= 2\pi^{-1}(i), \\ \alpha(2i) &= 2\pi(i) - 1. \end{aligned}$$

This is equivalent to $\alpha = \operatorname{fat}(\pi)$ so that α is necessarily a non-crossing pair partition.

Let us now prove the second statement in the theorem, by giving an estimate on the second moment of the random variable $\operatorname{Tr}[(QQ^*)^p]$.

Using Theorem 5.2 for the diagram of $\mathbf{E} \operatorname{Tr}^2[(QQ^*)^p]$, which is made of two disconnected copies of the bottom diagram in Figure 7, we obtain the moment expansion

$$\begin{aligned} \mathbf{E} \operatorname{Tr}^2[(QQ^*)^p] &= d^{-4p} s^{-2p} \sum_{f_1, f_2: [2p] \rightarrow \{0,1\}} (-1)^{\sum_i (f_1(i) + f_2(i))} \\ &\quad \cdot \mathbf{E} \left[\operatorname{Tr} \left(\prod_{i=1}^p (F_1(i)F_2(i)) \right) \left(\operatorname{Tr} \prod_{i=p+1}^{2p} (F_1(i)F_2(i)) \right) \right] \\ &= d^{-4p} s^{-2p} \sum_{\alpha \in \mathcal{S}_{4p}} s^{\#\alpha} d^{\#(\alpha\gamma_{12}^{-1})} d^{\#(\alpha\delta_{12}^{-1})} \sum_{(f_1, f_2) \in \mathcal{F}(\alpha)} (-1)^{\sum_i (f_1(i) + f_2(i))}, \end{aligned}$$

where the F and f functions have the same meaning as before and the permutations γ_{12}, δ_{12} are defined by

$$\begin{aligned} \gamma_{12} &= (12)(34) \cdots (2p - 1, 2p)(2p + 1, 2p + 2) \cdots (4p - 1, 4p), \\ \delta_{12} &= (1, 2p)(23)(45) \cdots (2p - 2, 2p - 1)(2p + 1, 4p)(2p + 2, 2p + 3) \cdots (4p - 2, 4p - 1). \end{aligned}$$

We can show, by the same technique as before, that permutations α with fixed points cancel each other out in the sum above, so we have

$$\mathbf{E} \operatorname{Tr}^2[(QQ^*)^p] = d^{-4p} s^{-2p} \sum_{\alpha \in S_{4p}^o} s^{\#\alpha} d^{\#(\alpha\gamma_{12}^{-1})} d^{\#(\alpha\delta_{12}^{-1})}.$$

We investigate next the dominating term in the sum above. The exponents of d and s in the general term read

$$\begin{aligned} g_{12}(\alpha) &= -4p + \#(\alpha\gamma_{12}^{-1}) + \#(\alpha\delta_{12}^{-1}) = 4p - (|\alpha\gamma_{12}^{-1}| + |\alpha\delta_{12}^{-1}|), \\ h_{12}(\alpha) &= -2p + \#\alpha = 2p - |\alpha|. \end{aligned}$$

Using the triangular inequality and the fact that α has no fixed points, we obtain

$$\begin{aligned} |\alpha\gamma_{12}^{-1}| + |\alpha\delta_{12}^{-1}| &\geq |\gamma_{12}\delta_{12}| = 4p - 4, \\ |\alpha| &\geq 2p, \end{aligned}$$

which shows that we have $g_{12}(\alpha) \leq 4$ and $h_{12}(\alpha) \leq 0$. This proves that the sum behaves like d^4 times a constant. To evaluate this constant, we need to find the set of permutations α which saturate the above inequalities. As before, this set is made of pair partitions such that $\gamma_{12}\alpha$ lies on the geodesic $\text{id} \rightarrow \gamma_{12}\delta_{12}$. Recall that both permutations γ_{12} and δ_{12} have a product structure

$$\begin{aligned} \gamma_{12} &= \gamma_1\gamma_2, \\ \delta_{12} &= \delta_1\delta_2, \end{aligned}$$

where γ_1, δ_1 act on $[2p]$ and γ_2, δ_2 act on $2p + [2p]$. Hence, mimicking the reasoning in the first part of the proof, the permutations we want are those having also a product structure $\alpha = \alpha_1\alpha_2$, where α_1 and α_2 are non-crossing pair partitions of $[2p]$ and $2p + [2p]$, respectively. Since one can choose α_1 and α_2 independently, we conclude that

$$\mathbf{E} \operatorname{Tr}^2[(QQ^*)^p] = d^4 (\operatorname{Cat}_p^2 + o(1)),$$

which, together with (13), achieves the proof of the theorem.

Note that the function $g_{12}(\alpha)$ takes only even values, and therefore permutations α such that $g_{12}(\alpha) < 4$ must actually satisfy $g_{12}(\alpha) \leq 2$. This remark yields a bound on the variance

$$\mathbf{Var} \operatorname{Tr}[(QQ^*)^p] \leq C_p d^2, \tag{14}$$

where C_p is a constant depending only on p .

VIII. REALIGNING STATES IN AN UNBALANCED TENSOR PRODUCT

We analyze now an unbalanced tensor product $\mathbf{C}^{d_1} \otimes \mathbf{C}^{d_2}$, with $d_1 < d_2$. We consider the asymptotic regime where d_1 is fixed and $d_2 \rightarrow \infty$ and we show that the threshold occurs at a *finite* value of the parameter s , more precisely $s = d_1^2$. The more general case when both d_1 and d_2 tend to infinity at different speeds apparently leads to more involved combinatorics, hence we focus on the “fully unbalanced” case where only one local dimension tends to infinity.

Theorem 8.1. *For all integers d_1, s , there are constants $C = C(d_1, s)$ and $c = c(d_1, s)$ such that the following holds. Let ρ be a random state on $\mathbf{C}^{d_1} \otimes \mathbf{C}^{d_2}$ with distribution $\mu_{d_1 d_2, s}$, then*

(1) *If $s < d_1^2$, then*

$$\mathbf{P}(\|\rho^R\| > 1) \geq 1 - C \exp(-cd_2^{1/4}).$$

(2) *If $s > d_1^2$, then*

$$\mathbf{P}(\|\rho^R\| \leq 1) \geq 1 - C \exp(-cd_2^{1/4}).$$

Note that these statements are meaningful only for d_2 large enough: for small values of d_2 , the lower bound on the probability estimate could be negative. As in the balanced case, the result is based on a moment computation for a realigned Wishart matrix.

Theorem 8.2. *In the regime of fixed d_1, s and $d_2 \rightarrow \infty$, the empirical singular value distribution of $d_2^{-1}R$ converges in moments to a Dirac mass at \sqrt{s} . Moreover, the variances of the moments of the random matrix $d_2^{-1}R$ satisfy*

$$\mathbf{Var} \operatorname{Tr}[(d_2^{-2}RR^*)^p] = O(1/d_2^2).$$

Proof: We need to prove that for every integer p ,

$$\lim_{d_2 \rightarrow \infty} \frac{1}{d_1^2} \mathbf{E} \operatorname{Tr}[(d_2^{-2}RR^*)^p] = s^{p/2}.$$

As before, we start from the moment formula (8),

$$\mathbf{E} \operatorname{Tr}[(RR^*)^p] = \sum_{\alpha \in S_{2p}} s^{\#\alpha} d_2^{\#(\alpha\gamma^{-1})} d_1^{\#(\alpha\delta^{-1})}.$$

Since the only parameter growing to infinity in the above sum is d_2 , the dominating term is given by the permutation $\alpha = \gamma$ and thus

$$\mathbf{E} \operatorname{Tr}[(RR^*)^p] \sim d_2^{2p} s^p d_1^2, \tag{15}$$

showing the convergence in moments of the empirical singular value distribution.

The statement about the variance follows readily from the following formula:

$$\mathbf{E} \operatorname{Tr}^2[(RR^*)^p] = \sum_{\alpha \in S_{4p}} s^{\#\alpha} d_2^{\#(\alpha\gamma_{12}^{-1})} d_1^{\#(\alpha\delta_{12}^{-1})}.$$

We note that the dominating term is given by $\alpha = \gamma_{12}$ and that it cancels out with the square of the right-hand side of Eq. (15). The largest remaining terms correspond to permutations α with $\#(\alpha\gamma_{12}^{-1}) = 4p - 2$. □

We now move on to the proof of Theorem 8.1, which mimics the one of Proposition 4.1. This approach gives the exact threshold in the unbalanced case because the limiting measure is a Dirac mass, so the bounds given by the moments 2 and 4 are already tight.

Proof of Theorem 8.1 (sketch): In the present case, Eq. (5) reads

$$\frac{\|R\|_2^3}{\|R\|_4^2} \leq \|R\|_1 \leq d_1 \|R\|_2.$$

Using the previous proposition and the concentration for Gaussian polynomials (Lemma 4.5), we can find constants c, C such that for every $t > 0$,

$$\begin{aligned} \mathbf{P}(|\|R\|_2^2 - d_2^2 d_1^2 s(1 + o(1))| > Ct d_2) &\leq C \exp(-ct^{1/2}), \\ \mathbf{P}(|\|R\|_4^4 - d_2^2 d_1^2 s^2(1 + o(1))| > Ct d_2) &\leq C \exp(-ct^{1/4}). \end{aligned}$$

We choose $t = \eta d_2$ for some $\eta > 0$. The previous two facts imply that with large probability, $\|(d_1 d_2 s)^{-1} R\|_1$ is close to d_1/\sqrt{s} (the difference being smaller than any fixed $\varepsilon > 0$, for an appropriate choice of η). Finally, one can replace $R/(d_1 d_2 s)$ by ρ^R , by using the fact that the trace of the Wishart matrix W concentrates around its mean $d_1 d_2 s$ (see Lemma 4.2). □

ACKNOWLEDGMENTS

The authors would like to thank M. B. Ruskai for useful comments on an early version of the paper. This research was supported by the ANR Project No. OSvsQPI 2011 BS01 008 01. IN acknowledges financial support from the University of Toulouse, via the AO1-SdM project ECIU.

- ¹G. Aubrun, S. Szarek, and D. Ye, “Entanglement thresholds for random induced states,” *Commun. Pure Appl. Math.* (to be published); e-print [arxiv:1106.2264](https://arxiv.org/abs/1106.2264).
- ²G. Aubrun, “Partial transposition of random states and non-centered semicircular distributions,” *Random Matrices: Theory Appl.* **01**, 1250001 (2012); e-print [arxiv:1011.0275](https://arxiv.org/abs/1011.0275).
- ³T. Banica and I. Nechita, “Asymptotic eigenvalue distributions of block-transposed Wishart matrices,” *J. Theor. Probab.* (to be published).
- ⁴T. Banica and I. Nechita, “Block-modified Wishart matrices and free Poisson laws,” *Houst. J. Math.* (to be published).
- ⁵I. Bengtsson and K. Życzkowski, *Geometry of Quantum States* (Cambridge University Press, 2006).
- ⁶K. Chen and L.-A. Wu, “A matrix realignment method for recognizing entanglement,” *Quantum Inf. Comput.* **3**, 193–202 (2003); e-print [arXiv:quant-ph/0205017](https://arxiv.org/abs/quant-ph/0205017).
- ⁷B. Collins and I. Nechita, “Random quantum channels I: Graphical calculus and the Bell state phenomenon,” *Commun. Math. Phys.* **297**, 345–370 (2010).
- ⁸B. Collins and I. Nechita, “Gaussianization and eigenvalue statistics for random quantum channels (III),” *Ann. Appl. Probab.* **21**, 1136–1179 (2011).
- ⁹B. Collins, I. Nechita, and D. Ye, “The absolute positive partial transpose property for random induced states,” *Random Matrices: Theory Appl.* **01**, 1250002 (2012).
- ¹⁰L. Gurvits, in *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing* (ACM, New York, 2003), pp. 10–19.
- ¹¹L. Gurvits and H. Barnum, “Largest separable balls around the maximally mixed bipartite quantum state,” *Phys. Rev. A* **66**, 062311 (2002).
- ¹²P. Hayden, D. Leung, and A. Winter, “Aspects of generic entanglement,” *Commun. Math. Phys.* **265**, 95–117 (2006).
- ¹³M. Horodecki, P. Horodecki, and R. Horodecki, “Separability of mixed quantum states: Linear contractions and permutation criteria,” *Open Syst. Inf. Dyn.* **13**, 103–111 (2006).
- ¹⁴S. Janson, *Gaussian Hilbert Spaces*, Cambridge Tracts in Mathematics Vol. 129 (Cambridge University Press, Cambridge, 1997).
- ¹⁵B. Laurent and P. Massart, “Adaptive estimation of a quadratic functional by model selection,” *Ann. Stat.* **28**, 1302–1338 (2000).
- ¹⁶M. Nathanson and M. B. Ruskai, “Pauli diagonal channels constant on axes,” *J. Phys. A: Math. Theor.* **40**, 8171–8204 (2007).
- ¹⁷A. Nica and R. Speicher, *Lectures on the Combinatorics of Free Probability* (Cambridge University Press, 2006).
- ¹⁸A. Peres, “Separability criterion for density matrices,” *Phys. Rev. Lett.* **77**, 1413–1415 (1996).
- ¹⁹A. Rudolph, “Further results on the cross norm criterion for separability,” *Quantum Inf. Process.* **4**, 219–239 (2005); e-print [arXiv:quant-ph/0202121](https://arxiv.org/abs/quant-ph/0202121).
- ²⁰A. Zvonkin, “Matrix integrals and map enumeration: An accessible introduction,” *Math. Comput. Modell.* **26**(8–10), 281–304 (1997).
- ²¹K. Życzkowski and H.-J. Sommers, “Induced measures in the space of mixed quantum states,” *J. Phys. A* **34**, 7111–7125 (2001).