Random matrix models in quantum information theory

Ion Nechita

University of Ottawa
joint work with Benoît Collins

CMS Winter Meeting
Windsor, December 6, 2009

Quantum Information Theory
&
random quantum channels

Classical vs. Quantum information theory

- Unit of information: bit $b \in \{0,1\} \rightsquigarrow$ qubit $x \in \mathbb{C}^2 = \mathbb{C}e_0 \oplus \mathbb{C}e_1$, $\|x\| = 1$.
- Finite sets $A \rightsquigarrow$ finite-dimensional complex Hilbert spaces $\mathcal{H}_A = \mathbb{C}^{|A|}$.
- Probability densities $\mu = \frac{1}{3}\delta_0 + \frac{2}{3}\delta_1 \rightsquigarrow$ density matrices $\rho = \frac{1}{3}P_{e_0} + \frac{2}{3}P_{e_1}$.
- Density matrices: $\rho \in \mathcal{M}_n(\mathbb{C}), \rho \geqslant 0, \operatorname{Tr}\rho = 1$. Rank one density matrices $\rho = P_x$ are called pure states.
- Product alphabet $A \times B \rightsquigarrow$ tensor product space $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$.
- States of subsystems are given by partial traces:

$$\rho_A = \operatorname{Tr}_{\mathcal{H}_B} \rho_{AB} \qquad \text{where} \qquad \operatorname{Tr}_{\mathcal{H}_B}(X \otimes Y) = \operatorname{Tr}(Y)X.$$

- A pure state $x \in \mathcal{H}_A \otimes \mathcal{H}_B$ is called entangled if it can not be decomposed as $x = a \otimes b$ with $a \in \mathcal{H}_A$, $b \in \mathcal{H}_B$.
- Maximally entangled state (aka Bell state):

$$\mathrm{Bell}_n = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} e_i \otimes f_i \quad \in \mathbb{C}^n \otimes \mathbb{C}^n.$$

(Random) quantum channels

- Classical channels (i.e. stochastic matrices) $\rightsquigarrow$ quantum channels.
- Quantum channels: completely positive, trace preserving maps $\Phi : \mathcal{M}_{\text{in}}(\mathbb{C}) \to \mathcal{M}_{\text{out}}(\mathbb{C})$.
- von Neumann entropy of ρ: $H(\rho) = -\operatorname{Tr}(\rho \log \rho) = -\sum_i \lambda_i \log \lambda_i$.
- Minimal Output Entropy of a quantum channel

$$H_{\min}(\Phi) = \min_{\rho \in \mathcal{M}_{\text{in}}(\mathbb{C})} H(\Phi(\rho)).$$

- Is the MOE additive ?

$$H_{\min}(\Phi \otimes \Psi) = H_{\min}(\Phi) + H_{\min}(\Psi) \quad \forall \Phi, \Psi.$$

- NO !!! Hayden '07, Hayden + Winter '08, Hastings '09.
- Counterexamples to additivity conjectures are random.
- Model of random quantum channels

$$\Phi(\rho) = \operatorname{Tr}_{\text{aux}}(U(\rho \otimes P_y)U^*),$$

where $y \in \mathbb{C}^{\frac{\text{out} \times \text{aux}}{\text{in}}}$ and $U \in \mathcal{M}_{\text{out} \times \text{aux}}(\mathbb{C})$ is a Haar unitary matrix.

Choice of parameters

$$\mathcal{M}_{\text{out}}(\mathbb{C}) \ni \Phi(\rho) = \operatorname{Tr}_{\text{aux}}(U(\rho \otimes P_y)U^*) \qquad \rho \in \mathcal{M}_{\text{in}}(\mathbb{C}), P_y \in \mathcal{M}_{\frac{\text{out} \times \text{aux}}{\text{in}}}(\mathbb{C})$$

Finite rank output

- $\text{in} = tnk$,
- $\text{out} = k$,
- $\text{aux} = n$,

where $n, k \in \mathbb{N}$ and $t \in (0, 1)$. In general, we shall assume that $n \to \infty$, k is fixed, but "large" and t is fixed, but may depend on k.

Unbounded rank output

- $\text{in} = n$,
- $\text{out} = n$,
- $\text{aux} = k$,

where $n, k \in \mathbb{N}$ such that $n, k \to \infty$ at a constant ration $k/n \to c$, where $c > 0$ is a constant parameter.

How to get counterexamples ?

- Choose Φ to be random and $\Psi = \overline{\Phi}$ (conjugate channel, replace U by $\overline{U}$).
- Find lower bounds for $H_{\min}(\Phi) = H_{\min}(\overline{\Phi})$
  1. Hayden + Leung + Winter
  2. Hastings + Fukuda + King
- Find upper bounds for $H_{\min}(\Phi \otimes \Psi)$.

Strategy

- Use trivial bound

$$H_{\min}(\Phi \otimes \overline{\Phi}) \leqslant H\left([\Phi \otimes \overline{\Phi}](X_{12})\right),$$

for a particular choice of $X_{12} \in \mathcal{M}_{tnk}(\mathbb{C}) \otimes \mathcal{M}_{tnk}(\mathbb{C})$.

- $X_{12} = X_1 \otimes X_2$ do not yield counterexamples $\Rightarrow$ choose a maximally entangled state $X_{12} = E_{\text{in}} = P_{\mathrm{Bell}}$.
- Bound entropies of the (random) density matrix

$$Z = [\Phi \otimes \overline{\Phi}](E_{\text{in}}) \in \mathcal{M}_{\text{in}}(\mathbb{C}) \otimes \mathcal{M}_{\text{in}}(\mathbb{C}).$$

Main result - finite rank output

Theorem (Collins + N. '09)

For all k, t, almost surely as $n \to \infty$, the eigenvalues of $Z = [\Phi \otimes \overline{\Phi}](E_{tnk})$ converge to

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

- Previously known bound (deterministic, comes from linear algebra): for all t, n, k, the largest eigenvalue of Z is at least t.
- Two improvements:
  1. "better" largest eigenvalue,
  2. knowledge of the whole spectrum.
- Precise knowledge of eigenvalues $\rightsquigarrow$ optimal estimates for entropies.
- However, smaller eigenvalues are the "worst possible".

Main result - unbounded rank

Theorem (Collins + N. '09)

For all $c > 0$, the eigenvalues $\lambda_1 \geqslant \cdots \geqslant \lambda_{n^2}$ of $Z = [\Phi \otimes \overline{\Phi}](E_n)$ satisfy:

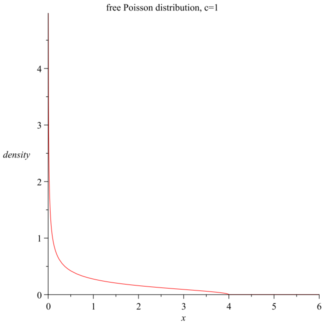
- *In probability, $cn\lambda_1 \to 1$.*
- *Almost surely, $\frac{1}{n^2-1} \sum_{i=2}^{n^2} \delta_{c^2 n^2 \lambda_i}$ converges to a free Poisson distribution of parameter c^2.*

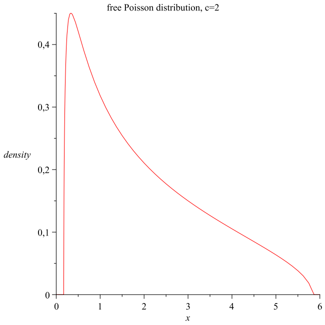
- Large eigenvalue $1/cn$ due to $\Phi - \overline{\Phi}$ symmetry.
- New phenomenon in Random Matrix Theory: eigenvalues of two different magnitude orders (n^{-1} and n^{-2}).
- Smaller eigenvalues have non-trivial distribution.
- Precise knowledge of eigenvalues $\rightsquigarrow$ optimal estimates for entropies.

Free Poisson distribution

- Free Poisson (aka Marchenko-Pastur) distribution of parameter $c > 0$:

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





- Free Poisson Central Limit Theorem:

$$\left[\left(1 - \frac{c}{n}\right)\delta_0 + \frac{c}{n}\delta_1\right]^{\boxplus n} \to \pi_c.$$

Independent channels - unbounded rank

Theorem (Collins + N. '09)

For $c > 0$, consider two independent random quantum channels Φ and Ψ. The eigenvalues $\lambda_1 \geqslant \cdots \geqslant \lambda_{n^2}$ of $Z = [\Phi \otimes \Psi](E_n)$ are such that almost surely,

$$\frac{1}{n^2} \sum_{i=1}^{n^2} \delta_{c^2 n^2 \lambda_i} \implies \pi_{c^2},$$

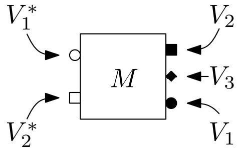
where π_{c^2} is a free Poisson distribution of parameter c^2 and the "$\implies$" denotes the convergence in distribution.

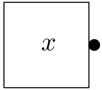
- Eigenvalue distribution identical to the Conjugate Channel Model ($\Phi \otimes \overline{\Phi}$) minus the large eigenvalue.
- All the eigenvalues are of order n^{-2}.
- Precise knowledge of eigenvalues $\rightsquigarrow$ optimal estimates for entropies.

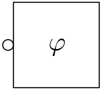
Graphical calculus for random quantum channels

Boxes & wires

- Graphical formalism inspired by works of Penrose, Coecke, Jones, etc.
- Tensors $\rightsquigarrow$ decorated boxes.

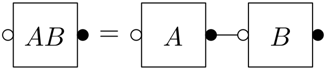


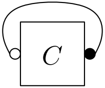


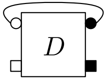


$M \in V_1 \otimes V_2 \otimes V_3 \otimes V_1^* \otimes V_2^*$ $\qquad$ $x \in V_1$ $\qquad$ $\varphi \in V_1^*$

- Tensor contractions (or traces) $V \otimes V^* \to \mathbb{C} \rightsquigarrow$ wires.

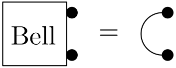






$\mathrm{Tr}(\mathrm{C})$ $\qquad$ $\mathrm{Tr}_{\mathrm{V}_1}(\mathrm{D})$

- Maximally entangled state: $\mathrm{Bell} = \sum_{i=1}^{\dim V_1} e_i \otimes e_i \in V_1 \otimes V_1$

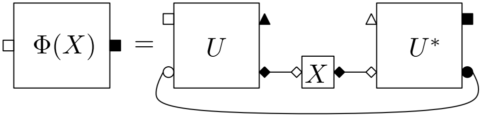


Graphical representation of quantum channels

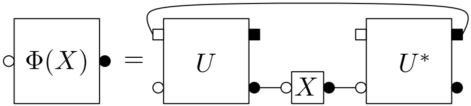
- Decorations/labels

$$\bullet/\circ = \mathbf{C}^n \qquad \blacksquare/\square = \mathbf{C}^k \qquad \blacklozenge/\lozenge = \mathbf{C}^{tnk} \qquad \blacktriangle/\triangle = \mathbf{C}^{t^{-1}}$$

- Single channel (finite rank output)



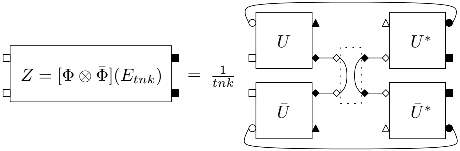
- Single channel (unbounded rank output, $n, k \to \infty$)



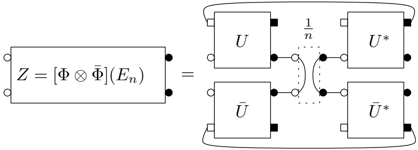
Graphical representation of quantum channels

$$\bullet\ \circ = \mathbf{C}^n \qquad \blacksquare\ \square = \mathbf{C}^k \qquad \blacklozenge\ \lozenge = \mathbf{C}^{tnk} \qquad \blacktriangle\ \triangle = \mathbf{C}^{t^{-1}}$$

- Product of conjugate channels, finite rank output



- Product of conjugate channels, unbounded rank output



Proof strategy for a.s. spectrum of random channels

- Use the method of moments
  1. Convergence in moments (finite rank case):

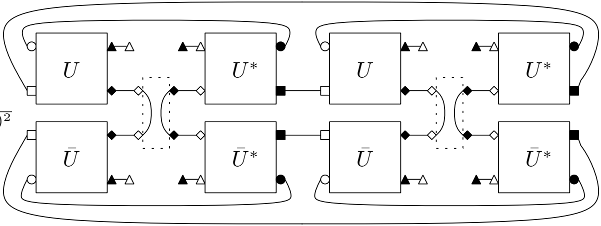
$$\mathbb{E}\,\mathrm{Tr}(Z^p) \to \left(t + \frac{1-t}{k^2}\right)^p + (k^2-1)\left(\frac{1-t}{k^2}\right)^p;$$

  2. Borel-Cantelli for a.s. convergence:

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

- We need to compute moments $\mathbb{E}\left[\mathrm{Tr}(Z^{p_1})^{q_1} \cdots \mathrm{Tr}(Z^{p_s})^{q_s}\right]$.
- Example (finite rank)

$$\mathbf{E}\mathrm{Tr}(\mathrm{Z}^2) = \mathbf{E}\frac{1}{(tnk)^2}$$



Unitary integration - Weingarten formula

- Using matrix coordinates, we can reduce our problem to computing integrals over the unitary group.

Theorem (Weingarten formula)

Let d 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 $\{1, 2, \ldots, d\}$. Then

$$\int_{\mathcal{U}(d)} U_{i_1 j_1} \cdots U_{i_p j_p} \overline{U_{i'_1 j'_1}} \cdots \overline{U_{i'_p j'_p}} \, dU = \sum_{\alpha, \beta \in \mathcal{S}_p} \delta_{i_1 i'_{\alpha(1)}} \ldots \delta_{i_p i'_{\alpha(p)}} \delta_{j_1 j'_{\beta(1)}} \ldots \delta_{j_p j'_{\beta(p)}} \mathrm{Wg}(d, \alpha\beta^{-1}).$$

If $p \neq p'$ then

$$\int_{\mathcal{U}(d)} U_{i_1 j_1} \cdots U_{i_p j_p} \overline{U_{i'_1 j'_1}} \cdots \overline{U_{i'_{p'} j'_{p'}}} \, dU = 0.$$

- There is a graphical way of reading this formula on the diagrams !

Graphical Weingarten formula: graph expansion

Consider a diagram $\mathcal{D}$ containing random unitary matrices/boxes U and U^*.
Apply the following removal procedure:

1. Start by replacing U^* boxed by $\overline{U}$ boxes (by reversing decoration shading).
2. By the (algebraic) Weingarten formula, if the number p of U boxes is different from the number of $\overline{U}$ boxes, then $\mathbb{E}\mathcal{D} = 0$.
3. Otherwise, choose a pair of permutations $(\alpha, \beta) \in \mathcal{S}_p^2$. These permutations will be used to pair decorations of $U/\overline{U}$ boxes.
4. For all $i = 1, \ldots, p$, add a wire between each white decoration of the i-th U box and the corresponding white decoration of the $\alpha(i)$-th $\overline{U}$ box. In a similar manner, use β to pair black decorations.
5. Erase all U and $\overline{U}$ boxes. The resulting diagram is denoted by $\mathcal{D}_{(\alpha,\beta)}$.

Theorem

$$\mathbb{E}\mathcal{D} = \sum_{\alpha,\beta} \mathcal{D}_{(\alpha,\beta)} \, \mathrm{Wg}(d, \alpha\beta^{-1}).$$

Example: $\mathbb{E}\,\mathrm{Tr}(Z^2)$ - finite rank case

- We have to compute a sum over all pairings of 4 "U" boxes with 4 "$\overline{U}$" boxes.
- Diagrams associated to pairings are indexed by 2 permutations $(\alpha, \beta) \in \mathcal{S}_4^2$. Consider the permutation $\delta = (1\ 4)\ (2\ 3) \in \mathcal{S}_4$.

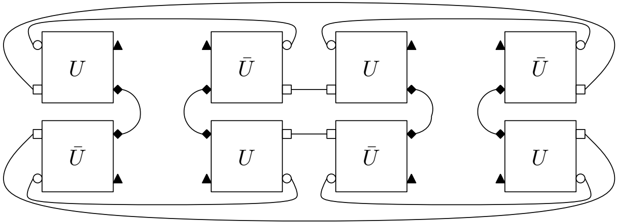
Example: $\mathbb{E}\,\mathrm{Tr}(Z^2)$ - finite rank case

- We have to compute a sum over all pairings of 4 "U" boxes with 4 "$\overline{U}$" boxes.
- Diagrams associated to pairings are indexed by 2 permutations $(\alpha, \beta) \in \mathcal{S}_4^2$. Consider the permutation $\delta = (1\;4)\;(2\;3) \in \mathcal{S}_4$.

Example: $\mathbb{E}\,\mathrm{Tr}(Z^2)$ - finite rank case

- We have to compute a sum over all pairings of 4 "U" boxes with 4 "$\overline{U}$" boxes.
- Diagrams associated to pairings are indexed by 2 permutations $({\color{red}\alpha}, {\color{blue}\beta}) \in \mathcal{S}_4^2$. Consider the permutation $\delta = (1\ 4)\ (2\ 3) \in \mathcal{S}_4$.

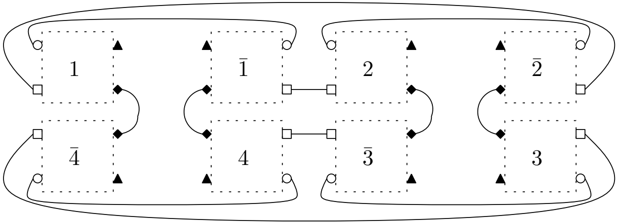
The original diagram



Example: $\mathbb{E}\,\mathrm{Tr}(Z^2)$ - finite rank case

- We have to compute a sum over all pairings of 4 "U" boxes with 4 "$\overline{U}$" boxes.
- Diagrams associated to pairings are indexed by 2 permutations $(\alpha, \beta) \in \mathcal{S}_4^2$. Consider the permutation $\delta = (1\ 4)\ (2\ 3) \in \mathcal{S}_4$.

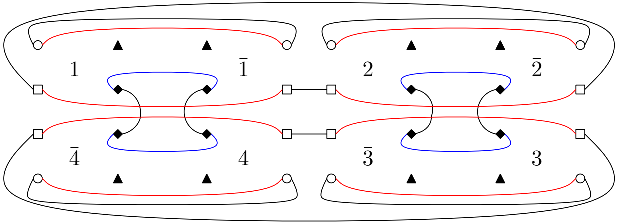
The diagram with the boxes removed



Example: $\mathbb{E}\,\mathrm{Tr}(Z^2)$ - finite rank case

- We have to compute a sum over all pairings of 4 "U" boxes with 4 "$\overline{U}$" boxes.
- Diagrams associated to pairings are indexed by 2 permutations $(\alpha, \beta) \in \mathcal{S}_4^2$. Consider the permutation $\delta = (1\ 4)\ (2\ 3) \in \mathcal{S}_4$.

The wiring for $\alpha = \beta = \mathrm{id}$.

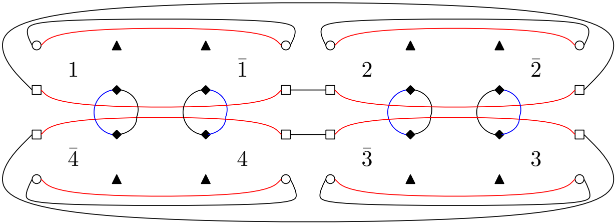


Contribution: $n^4 \cdot k^2 \cdot (tnk)^2 \cdot \mathrm{Wg}(\mathrm{id})$.

Example: $\mathbb{E}\,\mathrm{Tr}(Z^2)$ - finite rank case

- We have to compute a sum over all pairings of 4 "U" boxes with 4 "$\overline{U}$" boxes.
- Diagrams associated to pairings are indexed by 2 permutations $(\alpha, \beta) \in \mathcal{S}_4^2$. Consider the permutation $\delta = (1\ 4)\ (2\ 3) \in \mathcal{S}_4$.

The wiring for $\alpha = \mathrm{id}$, $\beta = \delta$.

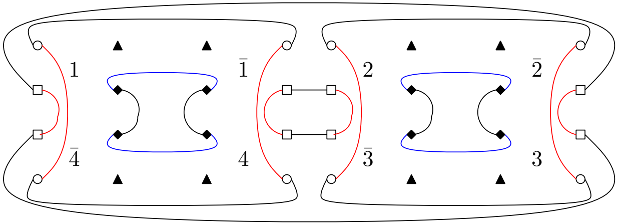


Contribution: $n^4 \cdot k^2 \cdot (tnk)^4 \cdot \mathrm{Wg}(\delta)$.

Example: $\mathbb{E}\,\mathrm{Tr}(Z^2)$ - finite rank case

- We have to compute a sum over all pairings of 4 "U" boxes with 4 "$\overline{U}$" boxes.
- Diagrams associated to pairings are indexed by 2 permutations $({\color{red}\alpha}, {\color{blue}\beta}) \in \mathcal{S}_4^2$. Consider the permutation $\delta = (1\ 4)\ (2\ 3) \in \mathcal{S}_4$.

The wiring for ${\color{red}\alpha} = \delta$, ${\color{blue}\beta} = \mathrm{id}$.

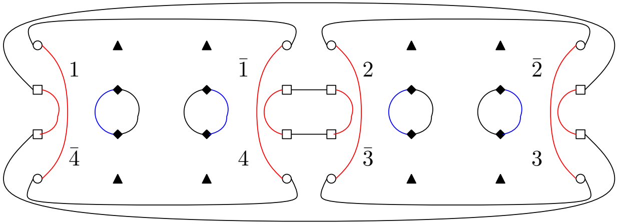


Contribution: $n^2 \cdot k^2 \cdot (tnk)^2 \cdot \mathrm{Wg}(\delta)$.

Example: $\mathbb{E}\,\mathrm{Tr}(Z^2)$ - finite rank case

- We have to compute a sum over all pairings of 4 "U" boxes with 4 "$\overline{U}$" boxes.
- Diagrams associated to pairings are indexed by 2 permutations $(\alpha, \beta) \in \mathcal{S}_4^2$. Consider the permutation $\delta = (1\ 4)\ (2\ 3) \in \mathcal{S}_4$.

The wiring for $\alpha = \beta = \delta$.

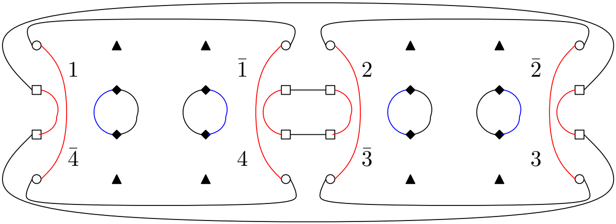


Contribution: $n^2 \cdot k^2 \cdot (tnk)^4 \cdot \mathrm{Wg}(\mathrm{id})$.

Example: $\mathbb{E}\,\mathrm{Tr}(Z^2)$ - finite rank case

- We have to compute a sum over all pairings of 4 "U" boxes with 4 "$\overline{U}$" boxes.
- Diagrams associated to pairings are indexed by 2 permutations $(\alpha, \beta) \in \mathcal{S}_4^2$. Consider the permutation $\delta = (1\ 4)\ (2\ 3) \in \mathcal{S}_4$.

The wiring for $\alpha = \beta = \delta$.



Contribution: $n^2 \cdot k^2 \cdot (tnk)^4 \cdot \mathrm{Wg}(\mathrm{id})$.

- Contributions of diagrams $\rightsquigarrow$ counting the loops $\rightsquigarrow$ statistics over permutations.

Sketch of the proof

- We want to compute, for all $p \geqslant 1$, $\mathbb{E}\,\mathrm{Tr}(Z^p)$.
- One needs to compute the contribution of each diagram $\mathcal{D}_{(\alpha,\beta)}$, where $\alpha, \beta \in \mathcal{S}_{2p}$.
- $\mathcal{D}_{(\alpha,\beta)}$ is a collection of loops associated to vector spaces of dimensions n, k and tnk.
- Asymptotic for Weingarten weights ($\sigma \in \mathcal{S}_p$):

$$\mathrm{Wg}(d,\sigma) = d^{-(p+|\sigma|)}(\mathrm{Mob}(\sigma) + O(d^{-2})).$$

- The case of independent channels is simpler, since "U" boxes cannot be paired to "V" boxes; pairings are indexed by quadruples $(\alpha_U, \beta_U, \alpha_V, \beta_V) \in \mathcal{S}_p^4$.
- The unbounded rank case for conjugate channels is more delicate, since the $n^2 - 1$ smaller eigenvalues are one order of magnitude below the largest eigenvalue. One needs to consider the eigenspace compression QZQ, where $Q = \mathrm{I} - E_n$.

Sketch of the proof

- Depending on the asymptotic regime, one has to identify asymptotically dominating terms. Computations for fixed n are intractable due to the complexity of the Weingarten function.
- After doing the loop combinatorics, one is left with maximizing over S_{2p}^2 quantities such as

$$\#(\gamma^{-1}\alpha) + \#(\alpha^{-1}\beta) + \#(\beta^{-1}\delta) \quad \text{or}$$
$$\#\alpha + \#(\gamma^{-1}\alpha) + \#(\beta^{-1}\delta) + 2\#(\alpha\beta^{-1}),$$

  where γ and δ are permutations coding the initial wiring of $U/\overline{U}$ boxes and $\#(\cdot)$ is the number of cycles function.
- Geodesic problems in symmetric groups $\Rightarrow$ non-crossing partitions $\Rightarrow$ free probability.
- The free Poisson distribution is characterized by its moments:

$$\int x^p \, d\pi_c(x) = \sum_{\substack{\alpha \in \mathcal{S}_p \\ \#\alpha + \#(\gamma^{-1}\alpha) = p+1}} c^{\#\alpha}.$$

Concluding remarks

- Graphical calculus for random matrices: unitary and Gaussian variables
- Powerful and intuitive reinterpretation of the Weingarten formula
- Adapted to tensor products and partial traces
- Gaussian case: moments of independent Wishart matrices
- Almost sure asymptotic eigenvalues for products of conjugate or independent quantum channels
- Importance of lower eigenvalues
- Improved bounds for Minimum Output Entropy of quantum channels: applications to additivity
- Other applications to QIT (work in progress with B. Collins and K. Życzkowski)

Thank you !

http://arxiv.org/abs/0905.2313
http://arxiv.org/abs/0906.1877