Free compression norms and applications to QIT

Ion Nechita

TU Munich and CNRS, LPT Toulouse

Bristol, March 17th 2017

Outline of the talk

1. Free compression norms
2. The minimum output entropy of quantum channels
3. Random positive maps and free additive convolution powers of probability measures

Free compression norms

Free Probability Theory

Invented by Voiculescu in the 80s to solve problems in operator algebras.

- A non-commutative probability space $(\mathcal{A}, \tau)$ is an algebra $\mathcal{A}$ with a unital state $\tau : \mathcal{A} \to \mathbb{C}$. Elements $a \in \mathcal{A}$ are called random variables.
- Examples:
  - classical probability spaces $(L^\infty(\Omega, \mathcal{F}, \mathbb{P}), \mathbb{E})$;
  - group algebras $(\mathbb{C}G, \delta_e)$;
  - matrices $(\mathcal{M}_n, n^{-1}\operatorname{Tr})$;
  - random matrices $(\mathcal{M}_n(L^\infty(\Omega, \mathcal{F}, \mathbb{P})), \mathbb{E} \circ n^{-1}\operatorname{Tr})$.
- Several notions of independence:
  - classical independence, implies commutativity of the radom variables;
  - free independence.
- If a, b are freely independent random variables, the law of (a, b) can be computed in terms of the laws of a and b. Freeness provides an algorithm for computing joint moments in terms of marginals.
- Example: if $\{a_1, a_2\}$ and $\{b_1, b_2\}$ are free, then

$$\tau(a_1 b_1 a_2 b_2) = \tau(a_1 a_2)\tau(b_1)\tau(b_2) + \tau(a_1)\tau(a_2)\tau(b_1 b_2) - \tau(a_1)\tau(b_1)\tau(a_2)\tau(b_2).$$

Asymptotic freeness of random matrices

Theorem (Voiculescu '98)

Let (A_n) and (B_n) be sequences of $n \times n$ matrices such that A_n and B_n converge in distribution (with respect to $n^{-1}\,\mathrm{Tr}$) for $n \to \infty$. Furthermore, let (U_n) be a sequence of Haar unitary $n \times n$ random matrices. Then, A_n and $U_n B_n U_n^*$ are asymptotically free for $n \to \infty$.

If A_n, B_n are matrices of size n, whose spectra converge towards μ_a, μ_b, the spectrum of $A_n + U_n B_n U_n^*$ converges to $\mu_a \boxplus \mu_b$; here, $\mu_a \boxplus \mu_b$ is the distribution of $a + b$, where $a, b \in (\mathcal{A}, \tau)$ are free random variables having distributions resp. μ_a, μ_b.

If A_n, B_n are matrices of size n such that $A_n \geq 0$, whose spectra converge towards μ_a, μ_b, the spectrum of $A_n^{1/2} U_n B_n U_n^* A_n^{1/2}$ converges to $\mu_a \boxtimes \mu_b$.

Example: truncation of random matrices

Let $P_n \in \mathcal{M}_n$ a projection of rank $n/2$; its eigenvalues are 0 and 1, with multiplicity $n/2$. Hence, the distribution of P_n converges, when $n \to \infty$, to the Bernoulli probability measure $\frac{1}{2}\delta_0 + \frac{1}{2}\delta_1$.

Let $C_n \in \mathcal{M}_{n/2}$ be the top $n/2 \times n/2$ corner of $U_n P_n U_n^*$, with U_n a Haar random unitary matrix. What is the distribution of C_n ?

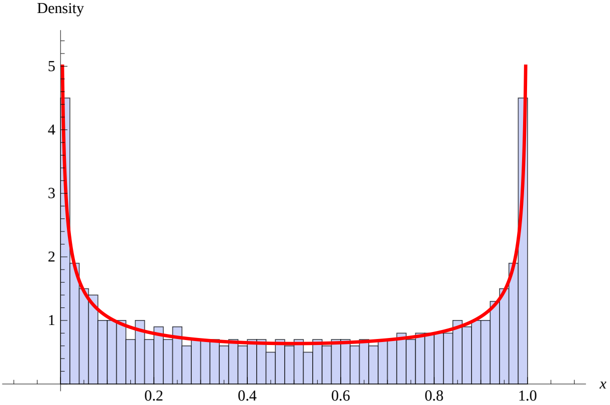
Up to zero blocks, $C_n = Q_n(U_n P_n U_n^*)Q_n$, where Q_n is the diagonal orthogonal projection on the first $n/2$ coordinates of $\mathbb{C}^n$. The distribution of Q_n converges to $\frac{1}{2}\delta_0 + \frac{1}{2}\delta_1$.

Free probability theory tells us that the distribution of C_n will converge to

$$(\frac{1}{2}\delta_0 + \frac{1}{2}\delta_1) \boxtimes (\frac{1}{2}\delta_0 + \frac{1}{2}\delta_1) = \frac{1}{\pi\sqrt{x(1-x)}}\mathbf{1}_{[0,1]}(x)dx,$$

which is the arcsine distribution.

Histogram of eigenvalues of a truncated randomly rotated projector of relative rank $1/2$ and size $n = 4000$; in red, the density of the arcsine distribution.



The t-norm

Definition

For a positive integer k, embed $\mathbb{R}^k$ as a self-adjoint real subalgebra $\mathcal{R}$ of a C^*-ncps $(\mathcal{A}, \tau)$, so that $\tau(x) = (x_1 + \cdots + x_k)/k$. 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 introduce the following norm, called the (t)-norm:

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

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

- One can show that $\|\cdot\|_{(t)}$ is indeed a norm, which is permutation invariant.
- When $t > 1 - 1/k$, $\|\cdot\|_{(t)} = \|\cdot\|_\infty$ on $\mathbb{R}^k$.
- $\lim_{t\to 0^+} \|x\|_{(t)} = k^{-1}|\sum_i x_i|$.

Computing the t-norm

Proposition

For a compactly supported probability measure μ,

$$\mu \boxtimes b_t = D_t \mu^{\boxplus 1/t},$$

where b_t is the Bernoulli distribution $b_t = (1-t)\delta_0 + t\delta_1$ and D_t is the dilation operator.

Let $G_\mu(z) = \int \frac{d\mu(a)}{z-a}$ be the Cauchy-Stieltjes transform of the measure μ and by $F_\mu = 1/G_\mu$.

Proposition

For any $x \in \mathbb{R}^k$,

$$\|x\|_{(t)} = w_x - (1-t)F_{\mu_x}(w_x),$$

where w_x is the largest in absolute value solution to the equation

$$F_{\mu_x}(w)\left(F'_{\mu_x}(w) - \frac{1}{1-t}\right) = 0.$$

Corners of randomly rotated projections

Theorem (Collins '05)

In $\mathbb{C}^n$, choose at random according to the Haar measure two independent subspaces V_n and V'_n of respective dimensions $q_n \sim sn$ and $q'_n \sim tn$ where $s, t \in (0, 1]$. Let P_n (resp. P'_n) be the orthogonal projection onto V_n (resp. V'_n). Then, almost surely,

$$\lim_n \|P_n P'_n P_n\|_\infty = \varphi(s,t) = \sup \mathrm{supp}((1-s)\delta_0 + s\delta_1) \boxtimes ((1-t)\delta_0 + t\delta_1),$$

with

$$\varphi(s,t) = \begin{cases} s + t - 2st + 2\sqrt{st(1-s)(1-t)} & \text{if } s + t < 1; \\ 1 & \text{if } s + t \geq 1. \end{cases}$$

Hence, we can compute

$$\| \underbrace{1, \cdots, 1}_{j \text{ times}}, \underbrace{0, \cdots, 0}_{k-j \text{ times}} \|_{(t)} = \varphi(\frac{j}{k}, t).$$

The minimum output entropy of quantum channels

Quantum states and entropies

- Quantum states (or density matrices)

$$\mathcal{M}_d^{1,+}(\mathbb{C}) = \{\rho \in \mathcal{M}_d(\mathbb{C}) \,:\, \rho \geq 0 \text{ and } \operatorname{Tr}\rho = 1\}.$$

- Extremal states (i.e. rank one projectors) are called pure states.
- von Neumann and Rényi entropies

$$H(\rho) = H^1(\rho) = -\operatorname{Tr}(\rho\log\rho) \qquad H^p(\rho) = \frac{\log \operatorname{Tr}\rho^p}{1-p}, \quad p > 0.$$

- Two quantum systems: tensor product of Hilbert spaces

$$\rho_{12} \in [\mathcal{M}_{d_1}(\mathbb{C}) \otimes \mathcal{M}_{d_2}(\mathbb{C})]^{1,+}.$$

- Entropies are additive

$$H^p(\rho_1 \otimes \rho_2) = H^p(\rho_1) + H^p(\rho_2).$$

- A bipartite quantum state $\rho_{12} \in \mathcal{M}_{d_1 d_2}^{1,+}(\mathbb{C})$ is called separable if it can be written as a convex combination of product states

$$\rho_{12} \in \mathcal{SEP} \iff \rho_{12} = \sum_i t_i \rho_1(i) \otimes \rho_2(i),$$

  where $t_i \geq 0$, $\sum_i t_i = 1$, $\rho_1(i) \in \mathcal{M}_{d_1}^{1,+}$, $\rho_2(i) \in \mathcal{M}_{d_2}^{1,+}$
- Non-separable states are called entangled

Additivity for MOE of quantum channels

- Quantum channels: CPTP maps $\Phi : \mathcal{M}_{\text{in}}(\mathbb{C}) \to \mathcal{M}_{\text{out}}(\mathbb{C})$
  - CP - complete positivity: $\Phi \otimes \mathrm{id}_r$ is a positive map, $\forall r \geq 1$
  - TP - trace preservation: $\mathrm{Tr} \circ \Phi = \mathrm{Tr}$.
- p-Minimal Output Entropy of a quantum channel

$$\begin{aligned} H^p_{\min}(\Phi) &= \min_{\rho \in \mathcal{M}^{1,+}_{\text{in}}(\mathbb{C})} H^p(\Phi(\rho)) \\ &= \min_{x \in \mathbb{C}^{\text{in}}} H^p(\Phi(P_x)). \end{aligned}$$

- Is the p-MOE additive ?

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

- NO !!!
  - $p > 1$: Hayden + Winter '08;
  - $p = 1$: Hastings '08
- Why care? Simple formula for the (classical) capacity of quantum channels: if additivity holds, then there is no need to use inputs entangled over multiple uses of Φ.

Random quantum channels

- Counterexamples to additivity conjectures are random.
- Random quantum channels from random isometries

$$\Phi(\rho) = [\mathrm{id}_{\mathrm{out}} \otimes \mathrm{Tr}_{\mathrm{anc}}](V \rho V^*),$$

where V is a Haar random partial isometry

$$V : \mathbb{C}^{\mathrm{in}} \to \mathbb{C}^{\mathrm{out}} \otimes \mathbb{C}^{\mathrm{anc}}.$$

Equivalently, via the Stinespring dilation theorem

$$\Phi(\rho) = [\mathrm{id}_{\mathrm{out}} \otimes \mathrm{Tr}_{\mathrm{anc}}](U(\rho \otimes P_y) U^*),$$

where $y \in \mathbb{C}^{\frac{\mathrm{out}\cdot\mathrm{anc}}{\mathrm{in}}}$ and $U \in \mathcal{M}_{\mathrm{out}\cdot\mathrm{anc}}(\mathbb{C})$ is a Haar random unitary matrix.
- Random quantum channels from i.i.d. random unitary matrices

$$\Phi(\rho) = \sum_{i=1}^{k} p_i U_i \rho U_i^*,$$

for (random) probabilities p_i and i.i.d. Haar distributed unitary operators U_i.

Model of interest

Here, we focus on random quantum channels coming from random isometries, with the following parameters.

- in $= tnk$,
- out $= k$,
- anc $= n$,

where $n, k \in \mathbb{N}$ and $t \in (0, 1)$. In general, we shall assume that

- $n \to \infty$
- k is fixed
- t is fixed.

In other words, we are interested in $\Phi : \mathcal{M}_{tnk}(\mathbb{C}) \to \mathcal{M}_k(\mathbb{C})$,

$$\Phi(\rho) = [\mathrm{id}_k \otimes \mathsf{Tr}_n](V \rho V^*),$$

where V is a random isometry obtained by keeping the first tnk columns of a $nk \times nk$ Haar random unitary.

How to get counterexamples ?

- Choose Φ to be random and $\Psi = \bar{\Phi}$; this way, $H^p_{\min}(\Psi) = H^p_{\min}(\Phi)$.
- Bound

$$H^p_{\min}(\Phi \otimes \bar{\Phi}) \leq B_2 < 2B_1 \leq 2H^p_{\min}(\Phi).$$

- Use $B_2 := [\Phi \otimes \bar{\Phi}](E_{tnk})$, where $E_d = \Omega_d \Omega_d^*$ is the projection on the maximally entangled state

$$\mathbb{C}^d \otimes \mathbb{C}^d \ni \Omega_d = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} e_i \otimes e_i.$$

Theorem (Collins + N. '09)

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

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

Computing $H^{\min}(\Phi)$

Strategy for B_1

- Remember: we want

$$H^p_{\min}(\Phi \otimes \bar{\Phi}) \leq B_2 < 2B_1 \leq 2H^p_{\min}(\Phi).$$

- We shall do more: we compute the exact limit (as $n \to \infty$) of $H^p_{\min}(\Phi)$.

Theorem (Belinschi, Collins, N. '13)

For all $p \geq 1$,

$$\lim_{n\to\infty} H_p^{min}(\Phi) = H_p(a, \underbrace{b, b, \dots, b}_{k-1}),$$

where a, b do not depend on p, $b = (1-a)/(k-1)$ and $a = \varphi(1/k, t)$ with

$$\varphi(s,t) = \begin{cases} s + t - 2st + 2\sqrt{st(1-s)(1-t)} & \text{if } s + t < 1; \\ 1 & \text{if } s + t \geq 1. \end{cases}$$

Entanglement of a vector

For a vector

$$x = \sum_{i=1}^{k} \sqrt{\lambda_i(x)} e_i \otimes f_i,$$

define $H(x) = H(\lambda(x)) = -\sum_i \lambda_i(x) \log \lambda_i(x)$, the entropy of entanglement of the bipartite pure state x.

Note that

1. The state x is separable, $x = e \otimes f$, iff $H(x) = 0$.
2. The state x is maximally entangled, $x = k^{-1/2} \sum_i e_i \otimes f_i$, iff $H(x) = \log k$.

Recall that we are interested in computing

$$H^{\min}(\Phi) = \min_{x \in \mathbb{C}^d,\, \|x\|=1} H(\Phi(P_x)) = \min_{y \in \mathrm{Im}\, V,\, \|y\|=1} H([\mathrm{id}_k \otimes \mathrm{Tr}_n] P_y)$$
$$= \min_{y \in \mathrm{Im}\, V,\, \|y\|=1} H(y).$$

Entanglement of a subspace

For a subspace $V \subset \mathbb{C}^k \otimes \mathbb{C}^n$, define

$$\boxed{H_p^{\min}(V) = \min_{y \in V,\, \|y\|=1} H_p(y),}$$

the minimal entanglement of vectors in V.

Here, we abuse notation: recall that we are interested in random isometries $V : \mathbb{C}^{tnk} \to \mathbb{C}^k \otimes \mathbb{C}^n$. Since the quantities $H_p^{\min}$ only depend on the range of V, also write $V = \operatorname{ran} V$.

A subspace V is called entangled if $H^{\min}(V) > 0$, i.e. if it does not contain separable vectors $x \otimes y$.

Singular values of vectors from a subspace

$\rightsquigarrow$ Entropy is just a statistic, look at the set of all singular values directly!

For a subspace $V \subset \mathbb{C}^k \otimes \mathbb{C}^n$ of dimension $\dim V = d$, define the set eigen-/singular values or Schmidt coefficients

$$\boxed{K_V = \{\lambda(x) \, : \, x \in V, \|x\| = 1\}.}$$

$\rightsquigarrow$ Our goal is to understand K_V.

- The set K_V is a compact subset of the ordered probability simplex $\Delta_k^{\downarrow}$.
- Local invariance: $K_{(U_1 \otimes U_2)V} = K_V$, for unitary matrices $U_1 \in \mathcal{U}(k)$ and $U_2 \in \mathcal{U}(n)$.
- Monotonicity: if $V_1 \subset V_2$, then $K_{V_1} \subset K_{V_2}$.
- Recovering minimum entropies:

$$H_p^{\min}(\Phi) = H_p^{\min}(V) = \min_{\lambda \in K_V} H_p(\lambda).$$

Examples

The anti-symmetric subspace: non-random counter-example for additivity, when $p > 2$ [Grudka, Horodecki, Pankowski '09].

- Let $k = n$ and put $V = \Lambda^2(\mathbb{C}^n)$
- The subspace V is almost half of the total space: $\dim V = n(n-1)/2$.
- Example of a vector in V:

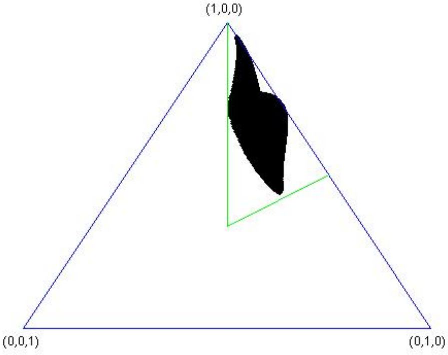
$$V \ni x = \frac{1}{\sqrt{2}}(e \otimes f - f \otimes e).$$

- Fact: singular values of vectors in V come in pairs.
- Hence, the least entropy vector in V is as above, with $e \perp f$ and $H(x) = \log 2$.
- Thus, $H^{\min}(V) = \log 2$ and one can show that

$$K_V = \{(\lambda_1, \lambda_1, \lambda_2, \lambda_2, \ldots) \in \Delta_n \,:\, \lambda_i \geq 0, \sum_i \lambda_i = 1/2\}.$$

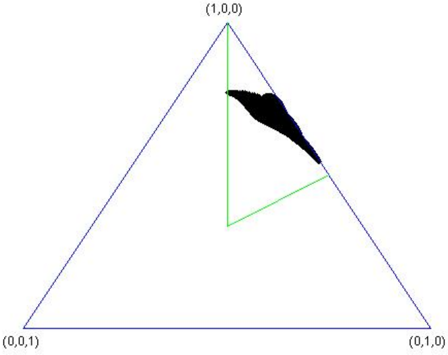
Examples - K_V

$V = \mathrm{span}\{G_1, G_2\}$, where $G_{1,2}$ are 3×3 independent Ginibre random matrices.



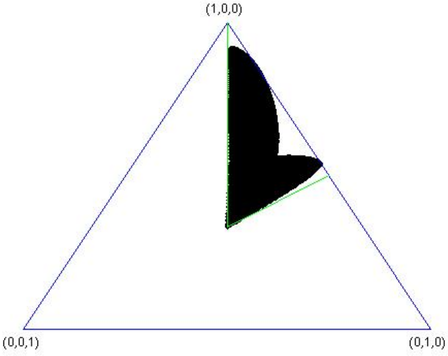
Examples - K_V

$V = \mathrm{span}\{G_1, G_2\}$, where $G_{1,2}$ are 3×3 independent Ginibre random matrices.



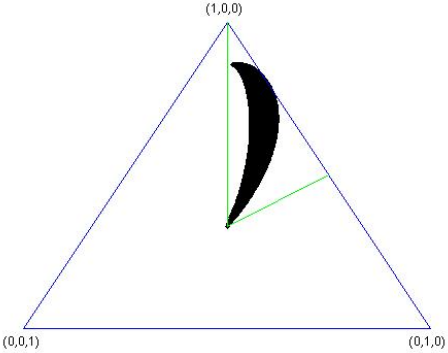
Examples - K_V

$V = \mathrm{span}\{\mathrm{I}_3, G\}$, where G is a 3×3 Ginibre random matrix.



Examples - K_V

$V = \mathrm{span}\{\mathrm{I}_3, G\}$, where G is a 3×3 Ginibre random matrix.



An open problem

Find explicit (i.e. non-random) examples of subspaces $V \subset \mathbb{C}^k \otimes \mathbb{C}^n$ with

1. large $\dim V$;
2. large $H^{\min}(V)$.

Give quantitative bounds on the trade-off between $\dim V$ and $H^{\min}(V)$ for arbitrary subspaces V.

Main result

Recall that we are interested in random isometries/subspaces in the following asymptotic regime: k fixed, $n \to \infty$, and $d \sim tkn$, for a fixed parameter $t \in (0, 1)$.

Theorem (Belinschi, Collins, N. '10)

For a sequence of uniformly distributed random subspaces V_n, the set K_{V_n} of singular values of unit vectors from V_n converges (almost surely, in the Hausdorff distance) to a deterministic, convex subset $K_{k,t}$ of the probability simplex Δ_k

$$\boxed{K_{k,t} := \{\lambda \in \Delta_k \mid \forall x \in \Delta_k, \langle \lambda, x \rangle \leq \|x\|_{(t)}\}.}$$

Corollary: exact limit of the minimum output entropy

By the previous theorem, in the specific asymptotic regime t, k fixed, $n \to \infty$, $d \sim tkn$, we have the following a.s. convergence result for random quantum channels Φ (defined via random isometries $V : \mathbb{C}^d \to \mathbb{C}^k \otimes \mathbb{C}^n$):

$$\lim_{n\to\infty} H_p^{\min}(\Phi) = \min_{\lambda \in K_{k,t}} H_p(\lambda).$$

It is not just a bound, the exact limit value is obtained.

Theorem (Belinschi, Collins, N. '16)

For all $p \geq 1$,

$$\lim_{n\to\infty} H_p^{min}(\Phi) = \min_{\lambda \in K_{k,t}} H_p(\lambda) = H_p(a, b, b, \ldots, b),$$

where a, b do not depend on p, $b = (1-a)/(k-1)$ and $a = \varphi(1/k, t)$ with

$$\varphi(s,t) = \begin{cases} s + t - 2st + 2\sqrt{st(1-s)(1-t)} & \text{if } s + t < 1; \\ 1 & \text{if } s + t \geq 1. \end{cases}$$

$K_{V_n} \to K_{k,t}$: idea of the proof

A simpler question: what is the largest maximal singular value $\max_{x \in V, \|x\|=1} \lambda_1(x)$ of vectors from the subspace V ?

$$
\begin{aligned}
\max_{x \in V, \|x\|=1} \lambda_1(x) &= \max_{x \in V, \|x\|=1} \lambda_1([\mathrm{id}_k \otimes \mathrm{Tr}_n] P_x) \\
&= \max_{x \in V, \|x\|=1} \|[\mathrm{id}_k \otimes \mathrm{Tr}_n] P_x\| \\
&= \max_{x \in V, \|x\|=1} \max_{y \in \mathbb{C}^k, \|y\|=1} \mathrm{Tr}\left[([\mathrm{id}_k \otimes \mathrm{Tr}_n] P_x) \cdot P_y\right] \\
&= \max_{x \in V, \|x\|=1} \max_{y \in \mathbb{C}^k, \|y\|=1} \mathrm{Tr}\left[P_x \cdot P_y \otimes \mathrm{I}_n\right] \\
&= \max_{y \in \mathbb{C}^k, \|y\|=1} \max_{x \in V, \|x\|=1} \mathrm{Tr}\left[P_x \cdot P_y \otimes \mathrm{I}_n\right] \\
&= \max_{y \in \mathbb{C}^k, \|y\|=1} \|P_V \cdot P_y \otimes \mathrm{I}_n \cdot P_V\|_\infty .
\end{aligned}
$$

The set $K_{k,t}$ and t-norms

- $K_{k,t} := \{\lambda \in \Delta_k \mid \forall x \in \Delta_k, \langle \lambda, x \rangle \le \|x\|_{(t)}\}$.
- Recall that

$$\max_{x \in V, \|x\|=1} \lambda_1(x) = \max_{y \in \mathbb{C}^k, \|y\|=1} \|P_V P_y \otimes \mathrm{I}_n P_V\|_\infty .$$

- For fixed y, P_V and $P_y \otimes \mathrm{I}_n$ are independent projectors of relative ranks t and $1/k$ respectively.
- Thus,

$$\begin{aligned} \|P_V \cdot P_y \otimes \mathrm{I}_n \cdot P_V\|_\infty &\to \| ((1-t)\delta_0 + t\delta_1) \boxtimes ((1-1/k)\delta_0 + 1/k\delta_1) \| \\ &= \varphi(t, 1/k) = \|(1, 0, \ldots, 0)\|_{(t)} . \end{aligned}$$

- We can take the max over y at no cost, by considering a finite net of y's, since k is fixed; remember that we are using almost sure convergence.
- To get the full result $\limsup_{n\to\infty} K_{V_n} \subset K_{k,t}$, use $\langle \lambda, x \rangle$ (for all directions x) instead of λ_1.
- The inclusion $\liminf_{n\to\infty} K_{V_n} \supset K_{k,t}$, is much easier, and follows from the convergence in distribution.

Recall

$$H^p_{\min}(\Phi \otimes \bar{\Phi}) \leq B_2 < 2B_1 \leq 2H^p_{\min}(\Phi).$$

Theorem (Collins + N. '09)

For all k, t, almost surely as $n \to \infty$, if $Z_n = (\Phi \otimes \bar{\Phi})(E_{tnk})$

$$\mathrm{spec}(Z_n) \to \left(t + \frac{1-t}{k^2}, \underbrace{\frac{1-t}{k^2}, \ldots, \frac{1-t}{k^2}}_{k^2-1 \text{ times}} \right) \in \Delta_{k^2}.$$

Theorem (Belinschi, Collins, N. '16)

For all $p \geq 1$,

$$\lim_{n\to\infty} H_p^{min}(\Phi) = H_p(a, b, b, \ldots, b),$$

where $b = (1-a)/(k-1)$ and $a = \varphi(1/k, t)$ with

$$\varphi(s,t) = \begin{cases} s + t - 2st + 2\sqrt{st(1-s)(1-t)} & \text{if } s+t < 1; \\ 1 & \text{if } s+t \geq 1. \end{cases}$$

Putting things together

Theorem (Belinschi, Collins, N. '16)

Using the limit for $H^{\min}(\Phi)$ and the upper bound for $H^{\min}(\Phi)$, the lowest dimension for which a violation of the additivity can be observed is $k = 183$. For large k, violations of size $1 - \varepsilon$ bits can be obtained.

How to improve this ?

1. Other asymptotic regimes
2. Use $\Psi \neq \bar{\Phi}$
3. For $\Phi \otimes \bar{\Phi}$, compute the actual limit of $H^{\min}(\Phi \otimes \bar{\Phi})$, and not just an upper bound.

Random positive maps and free additive convolution powers of probability measures

Separability criteria

- Recall: $\mathcal{SEP} = \{\sum_i t_i \rho_1(i) \otimes \rho_2(i) \ : \ \rho_{1,2}(i) \geq 0\}$.
- Let $\mathcal{A}$ be a C^* algebra. A map $f : \mathcal{M}_d \to \mathcal{A}$ is called
  - positive if $A \geq 0 \implies f(A) \geq 0$;
  - completely positive (CP) if $\mathrm{id}_r \otimes f$ is positive for all $r \geq 1$ ($r = d$ is enough).
- Let $f : \mathcal{M}_d \to \mathcal{A}$ be a completely positive map. Then, for every state $\rho_{12} \in \mathcal{M}_{dk}^{1,+}$, one has $[f \otimes \mathrm{id}_k](\rho_{12}) \geq 0$.
- Let $f : \mathcal{M}_d \to \mathcal{A}$ be a positive map. Then, for every separable state $\rho_{12} \in \mathcal{M}_{dk}^{1,+}$, one has $[f \otimes \mathrm{id}_k \otimes f](\rho_{12}) \geq 0$.
  - ρ_{12} separable $\implies \rho_{12} = \sum_i t_i \rho_1(i) \otimes \rho_2(i)$.
  - $[f \otimes \mathrm{id}_m](\rho_{12}) = \sum_i t_i f(\rho_1(i)) \otimes \rho_2(i)$.
  - For all i, $f(\rho_1(i)) \geq 0$, so $[f \otimes \mathrm{id}_k](\rho_{12}) \geq 0$.
- Hence, positive, but not CP maps f provide sufficient entanglement criteria: if $[f \otimes \mathrm{id}_m](\rho_{12}) \not\geq 0$, then ρ_{12} is entangled.
- The transposition map $\mathrm{t} : A \mapsto A^t$ is positive, but not CP. Define the convex set

$$\mathcal{PPT} = \{\rho_{12} \in \mathcal{M}_{dk}^{1,+} \,|\, [\mathrm{t}_d \otimes \mathrm{id}_k](\rho_{12}) \geq 0\} \supseteq \mathcal{SEP}.$$

- For $(m, n) \in \{(2,2), (2,3)\}$ we have $\mathcal{SEP} = \mathcal{PPT}$. In other dimensions, the inclusion $\mathcal{SEP} \subset \mathcal{PPT}$ is strict.

The Choi matrix of a map

- For any d, recall that the maximally entangled state is the orthogonal projection onto

$$\mathbb{C}^d \otimes \mathbb{C}^d \ni \Omega_d = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} e_i \otimes e_i.$$

- To any map $f : \mathcal{M}_d \to \mathcal{A}$, associate its Choi matrix

$$C_f = [\mathrm{id}_d \otimes f](P_{\mathrm{Bell}}) \in \mathcal{M}_d \otimes \mathcal{A}.$$

- Equivalently, if E_{ij} are the matrix units in $\mathcal{M}_d$, then

$$C_f = \sum_{i,j=1}^{d} E_{ij} \otimes f(E_{ij}).$$

Theorem (Choi '72)

A map $f : \mathcal{M}_d \to \mathcal{A}$ is CP iff its Choi matrix C_f is positive.

The Choi-Jamiołkowski isomorphism

- Recall (from now on $\mathcal{A} = \mathcal{M}_k$)

$$C_f = [\mathrm{id}_d \otimes f](E_d) = \sum_{i,j=1}^{d} E_{ij} \otimes f(E_{ij}) \in \mathcal{M}_d \otimes \mathcal{M}_k.$$

- The map $f \mapsto C_f$ is called the Choi-Jamiołkowski isomorphism.
- It sends:
  1. All linear maps to all operators;
  2. Hermicity preserving maps to hermitian operators;
  3. Entanglement breaking maps to separable quantum states;
  4. Unital maps to operators with unit left partial trace ($[\mathrm{Tr} \otimes \mathrm{id}]C_f = \mathrm{I}_k$);
  5. Trace preserving maps to operators with unit left partial trace ($[\mathrm{id} \otimes \mathrm{Tr}]C_f = \mathrm{I}_d$).

Random Choi matrices

- Let μ be a compactly supported probability measure on $\mathbb{R}$. For each d we introduce a real valued diagonal matrix X_d of $\mathbb{M}_d \otimes \mathbb{M}_k$ whose eigenvalue counting distribution converges to μ and whose extremal eigenvalues converge to the respective extrema of the support of μ.
- Let U_d be a random Haar unitary matrix in the unitary group $\mathcal{U}_{dk}$, and $f_\mu^{(d)} : \mathbb{M}_d \to \mathbb{M}_k$ be the map whose Choi matrix is $U_d X_d U_d^*$.

Theorem

Under the above assumptions, if $\mathrm{supp}(\mu^{\boxplus k}) \subset (0, \infty)$ *then, almost surely as* $d \to \infty$*, the map* $f_\mu^{(d)}$ *is positive. On the other hand, if* $\mathrm{supp}(\mu^{\boxplus k}) \cap (-\infty, 0) \neq \emptyset$ *then, almost surely as* $d \to \infty$*,* $f_\mu^{(d)}$ *is not positive.*

Proof ingredients

Let $f_\mu^{(d)} : \mathbb{M}_d \to \mathbb{M}_k$ be the map whose Choi matrix is $U_d X_d U_d^*$.

Theorem

If $\mathrm{supp}(\mu^{\boxplus k}) \subset (0, \infty)$ then, almost surely as $d \to \infty$, the map $f_\mu^{(d)}$ is positive. If $\mathrm{supp}(\mu^{\boxplus k}) \cap (-\infty, 0) \neq \emptyset$ then, almost surely as $d \to \infty$, $f_\mu^{(d)}$ is not positive.

Proposition

A map f is positive iff for any self-adjoint projection $P \in \mathcal{M}_k$ of rank 1, the operator $(I_d \otimes P) C_f (I_d \otimes P)$ is positive semidefinite.

Proposition (Nica and Speicher)

Let x, p be free elements in a ncps $(\mathcal{M}, \tau)$ and assume that p is a selfadjoint projection such that $\tau(p) = t$ ($t \in (0,1)$) and that x has distribution μ. Then, the distribution of $tpxp$ inside the contracted ncps $(p\mathcal{M}p, \tau(p \cdot p))$ is $\mu^{\boxplus 1/t}$

Example: semicircular measures

- Let $s_{a,\sigma}$ be the semi-circle distribution of mean a and variance σ^2, having support $[a-2\sigma, a+2\sigma]$.
- In free probability theory, $s_{0,1}$ plays the role of the standard Gaussian in classical probability, cf Free Central Limit Theorem.
- We have $\mathrm{supp}(s_{a,\sigma}^{\boxplus k}) = \mathrm{supp}(s_{ak,\sigma\sqrt{k}}) = [ak - 2\sigma\sqrt{k}, ak + 2\sigma\sqrt{k}]$.

Lemma

Let k be an integer and a, σ positive parameters. The map $f_{a,\sigma}^{(d)} : \mathbb{M}_d \to \mathcal{M}_k$ associated to a semi-circular distribution $s_{a,\sigma}$ is asymptotically positive as soon as $a^2 < 4k\sigma^2$.

Theorem

Let $X_d \in \mathcal{M}_{dk}^{sa}(\mathbb{C})$ a sequence of (normalized) GUE matrices, and set $Y_d := aI_{dk} + \sigma X_d$, for some constants a and $\sigma \geq 0$. If

$$\frac{1}{2} < \frac{\sigma}{a} < \frac{2}{\sqrt{k}},$$

then Y_d is asymptotically positive semidefinite, PPT, and entangled.

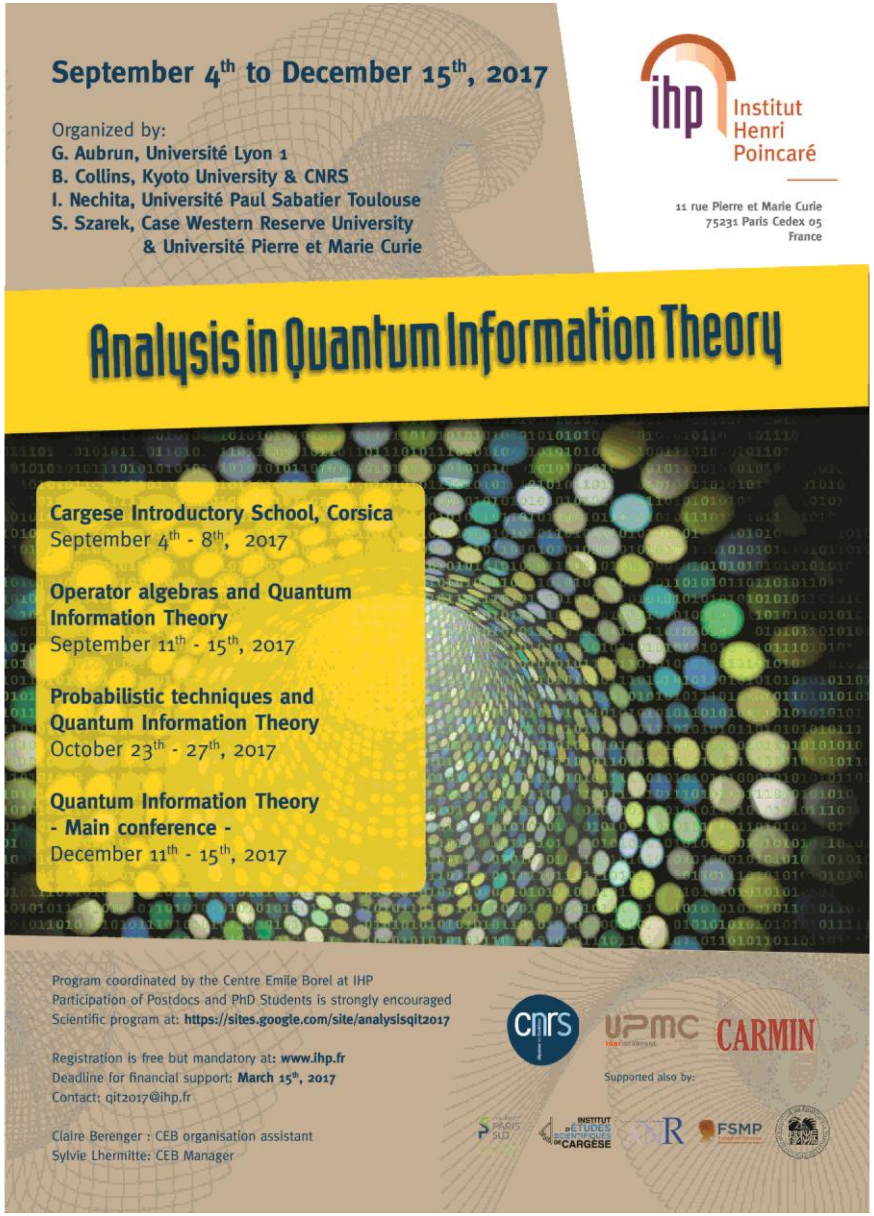
Semester "Analysis in Quantum Information Theory"
Institut Henri Poincaré, Paris, September – December 2017

- Summer school: Sep 4-8, Cargèse (Corsica)
- Workshop 1: Sep 11-15
  "Operator Algebras and QIT"
- Workshop 2: Oct 23-25
  "Probabilistic techniques and QIT"
- Workshop 3: Dec 11-15
  "Quantum Information Theory"
- Doctoral courses
- Weekly seminars
- Etc...

Financial support available for attending the summer school and the workshops. Deadline: 15/03/2017

More information at
https://sites.google.com/site/analysisqit2017/

Please register at
http://www.ihp.fr/en/CEB/T3-2017



The End

thank you for your attention

- S. Belinschi, B. Collins, I.N. - *Eigenvectors and eigenvalues in a random subspace of a tensor product* - Inv. Math. 2012, `arXiv:1008.3099`
- S. Belinschi, B. Collins, I.N. - *Almost one bit violation for the additivity of the minimum output entropy* - CMP 2016, `arXiv:1305.1567`
- B. Collins, P. Hayden, I.N. - *Random and free positive maps with applications to entanglement detection* - IMRN 2016, `arXiv:1505.08042`
- B. Collins, I.N. - *Random matrix techniques in quantum information theory* - JMP 2016, `arXiv:1509.04689`