Hastings' additivity counterexample by concentration of measure

Fernando G.S.L. Brandão
Universidade Federal de Minas Gerais, Brazil

Michal Horodecki
Gdansk University, Poland

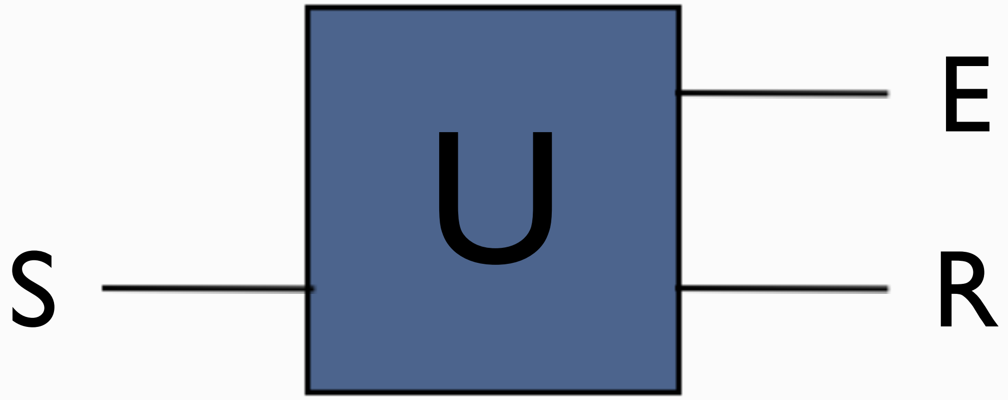
arXiv:0907.3210

Random Matrix Techniques in QIT, PI 05/07/2010

Quantum channel

A quantum channel Λ : CP trace preserving map from $S \cong C^{|S|}$ to $R \cong C^{|R|}$

Stinespring form: $\Lambda(\rho) = tr_E(U\rho U^*)$ for an isometry $U_\Lambda \equiv U : S \to RE$



The additivity conjecture[†]

$$\boxed{S_{\min}(\Lambda_1 \otimes \Lambda_2) = S_{\min}(\Lambda_1) + S_{\min}(\Lambda_2)}$$

$$S_{\min}(\Lambda) := \min_{\rho} S(\Lambda(\rho)) \qquad S(\rho) = -tr(\rho \log \rho)$$

If true, it would imply nice formulas for many quantities of interest in quantum information theory:, e.g. classical capacity, entanglement cost, distillable common randomness, distillable local purity

[†] 199? - 2008

Counterexample to additivity

(Hastings 08): The additivity conjecture is wrong. A random choice of the channel gives a violation w.h.p. (for suitable choices of input, output and environment dimensions)

This talk: present Hastings' counterexample using tools from *concentration of measure*

M.B. Hastings, arXiv:0809.3972

Aubrun, Szarek, Werner arXiv:1003.4925

Fukuda, King, Moser, arXiv:0905.3697, 0907.544

Collins, Nechita arXiv:1006.3247

Proof Strategy

- As the two channels for the counterexample, we consider a channel Λ and its conjugate $\overline{\Lambda}$, defined as

$$\overline{\Lambda}(\rho) = tr_E\left(U^* \rho U^T\right)$$

- We prove a lower bound on $S_{min}(\Lambda \otimes \overline{\Lambda})$, valid for every channel Λ

- We prove an upper bound on $S_{min}(\Lambda)$, valid w.h.p. for a random choice of the channel Λ

- Observe the lower bound is smaller than twice the upper bound...

Lower bound

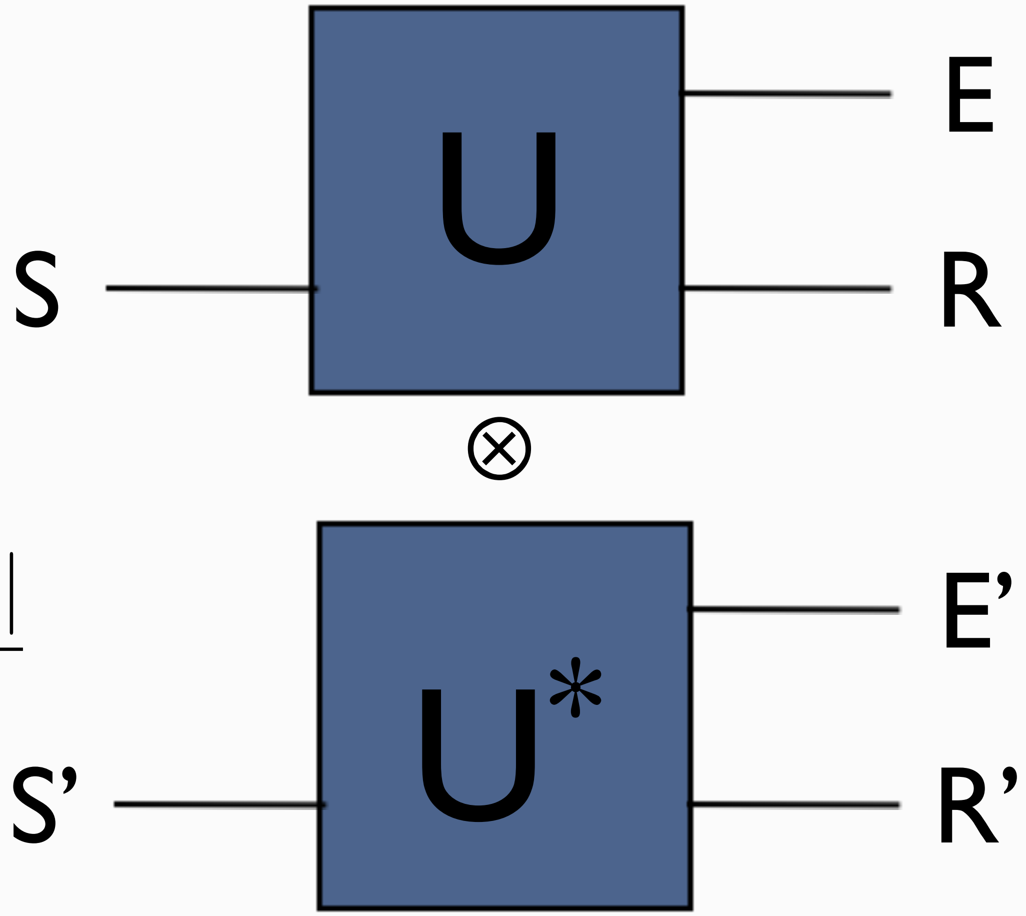
The idea of the lower bound (from Hayden-Winter, first applied to the p-Renyi entropies case (p>1)) is to use as an input the maximally entangled state of the two input states.

One can show:

$$\|\Lambda \otimes \overline{\Lambda}(\Phi_{SS'})\|_\infty \geq \frac{|S|}{|R||E|}$$

which implies:

$$S(\Lambda \otimes \overline{\Lambda}(\Phi_{SS'})) \leq 2\log(|R|) - \frac{|S|}{|E|}\frac{\log|R|}{|R|}$$



1. A. Winter, arXiv:0707.0402
2. P. Hayden, arXiv:0707.3291
3. P. Hayden and A. Winter, arXiv:0807.4753

The lower bound

Rest of the talk

Entangled Subspaces

Given the channel $\Lambda(\rho) = tr_E(U\rho U^*)$ we can associate to it a subspace of R⊗S:

$$\mathcal{S}_\Lambda := \{U|\psi\rangle,\ |\psi\rangle \in C^{d_S}\}$$

Lemma:

$$\boxed{S_{min}(\Lambda) = \min_{|\psi\rangle \in \mathcal{S}_\Lambda} S(\psi_R)}$$

Proof:

$$S_{min}(\Lambda) = \min_\rho S(\Lambda(\rho)) = \min_{|\psi\rangle\langle\psi|} S(\Lambda(|\psi\rangle\langle\psi|)) = \min_{|\psi\rangle \in \mathcal{S}_\Lambda} S(\psi_R)$$

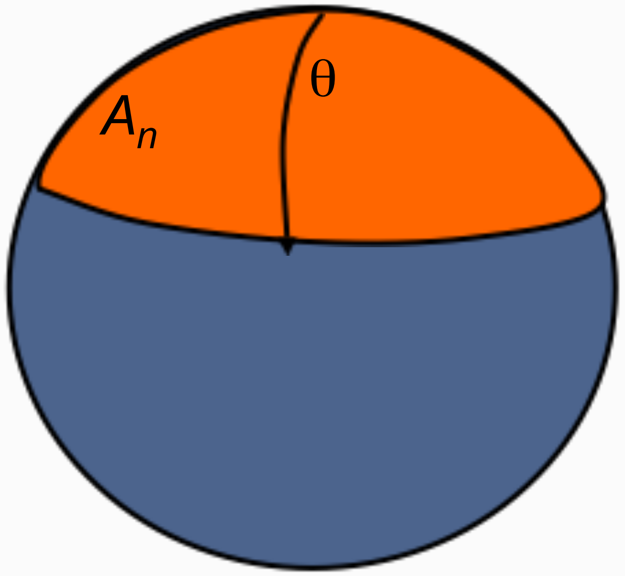
Entangled Subspaces

Therefore we would like to find a subspace S of $R \otimes E$ of dimension $|S|$ for which all states are highly entangled:

$$\boxed{\min_{|\psi\rangle \in \mathcal{S}} S(\psi_R) > \log(|R|) - \frac{1}{2}\frac{|S|}{|E|}\frac{\log|R|}{|R|}}$$

We will see that by choosing $\mathcal{S}$ from the Haar measure, i.e. the subspace associated to $P_S := U\left(\sum_{k=1}^{|S|}|i\rangle\langle i|\right)U'$ for a Haar unitary U, the Eq. above is satisfied w.h.p. for |S|=|E| >>|R|

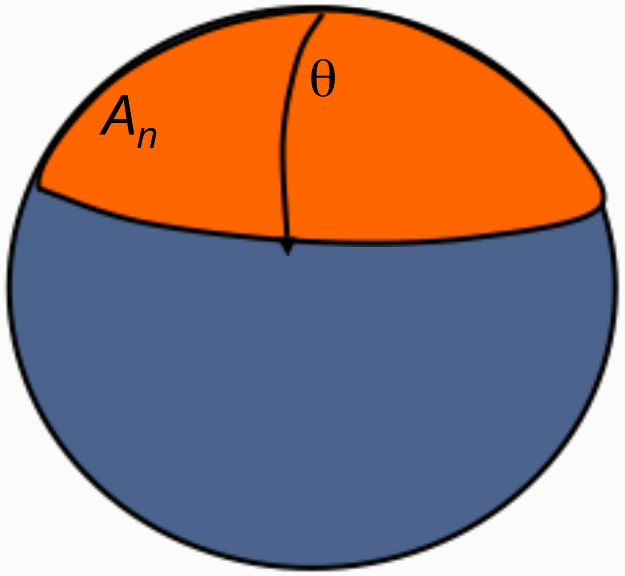
Concentration of Measure on the sphere



Take any set M in the sphere of measure greater than ½. Consider M_ϵ as the set of all points epsilon-close to M (e.g. in the euclidean distance). Then for a random choice of x in S^n

$$Pr\left(x \notin M_\epsilon\right) \leq e^{-c\epsilon^2 n}$$

Concentration of Measure on the sphere



Levy's Lemma: Given any η-Lipschitz* function f: S^n → R, with average value *M*, for a random choice of x in S^n

$$Pr\left(|f(x) - M| \geq \epsilon\right) \leq e^{-c\epsilon^2 n/\eta^2}$$

* η-Lipschitz: $|f(x) - f(y)| \leq \eta \|x - y\|$

A pure state $|\psi\rangle \in C^d$ can be identified with a point in S^{2d-1}. Therefore any well-behaved function of $|\psi\rangle$ will be extremely concentrated around its average in high dimensions!

Entangled subspaces from Levy’s lemma

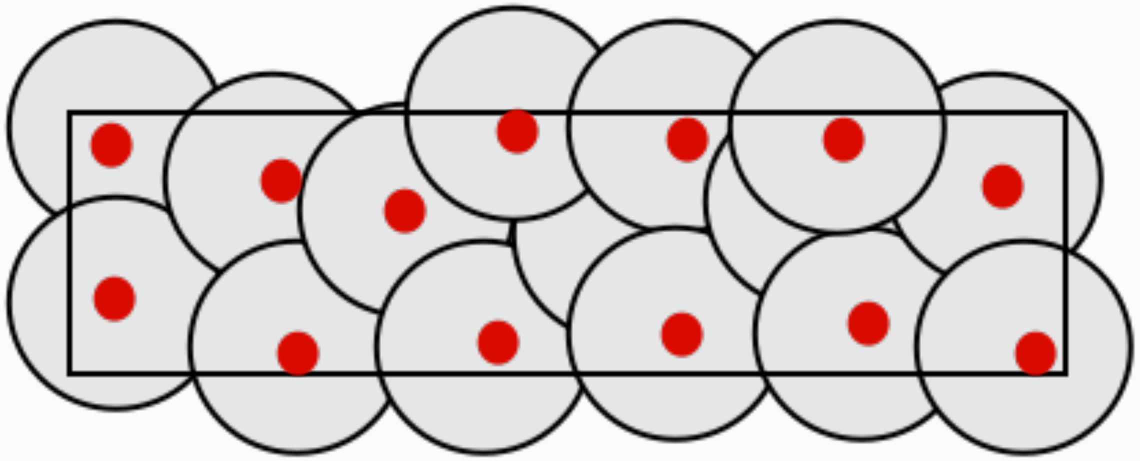
(Hayden, Leung and Winter 04) Applying Levy’s Lemma to the von Neumann entropy we find that for $|\psi\rangle \in R \otimes E$

$$\boxed{Pr_{|\psi\rangle}\left(S(\psi_R) \leq \log(|R|) - \frac{|R|}{\ln 2|E|} - \epsilon\right) \leq e^{-\frac{c|R||E|\epsilon^2}{(\log|R|)^2}}}$$

We can then combine this large deviation bound with the idea of *epsilon-nets* to get highly entangled subspaces of large dimension.

Epsilon-Net

An epsilon-net in *A* is a set of points *N* such that for every point x in A there is a x'in *N* with || x - x' || $\leq$ ε



For the set of pure states in C^{d} there is an epsilon-net *N* of cardinality |*N*| $\leq (5/\varepsilon)^{2d}$

Highly Entangled Subspaces

Combining the large deviation bound from before and the union bound:

$$Pr\left(\max_{|\psi\rangle\in\mathcal{S}_U} S(\psi_R) \leq \log|R| - \frac{|R|}{\ln 2|E|} - \epsilon/2\right) \leq |\mathcal{N}_\delta| e^{-c\frac{|R||E|}{(\log|R|)^2}\epsilon^2}$$

with $\mathcal{S}_U = U\left(\sum_{k=1}^{|S|} |i\rangle\langle i|\right)\overline{U}$ and $\delta = \epsilon/\sqrt{8}\log|R|$ Then from |N| ≤ $(5/\varepsilon)^{2|S|}$

W.h.p. a random subspace *S* of dimension $|S| = c' \frac{|R||S|\epsilon^{5/2}}{(\log|R|)^{5/2}}$ only contains states such that

$$S(\psi_R) \geq \log|R| - \frac{|R|}{\ln|E|} - \epsilon$$

Not Entangled Enough

Alas, for the counterexample we need a subspace *S* of dimension

$$|S| > \frac{|E||R|\epsilon}{\log |R|}$$

The construction only gives: $|S| > c' \frac{|E||R|\epsilon^{2.5}}{\log |R|^{2.5}}$ .....

For Renyi entropies this construction *does* work and it's the idea of Hayden-Winter counterexample.

1. A. Winter, arXiv:0707.0402
2. P. Hayden, arXiv:0707.3291
3. P. Hayden and A. Winter, arXiv:0807.4753

An useful idea

This technique (large deviation + epsilon-net) has been successfully applied to many other problems in QIT.

1. one-time pad, data hiding, locking (Hayden, Leung, Shor, Winter 03; Aubrun 08)
2. remote state preparation (Bennett, Hayden, Leung, Shor, Winter 03)
3. superdense coding (Harrow, Hayden, Leung 03; Abeysinghe, Hayden, Smith, Winter 04)
4. encryption with reference frames (Bartlett, Hayden, Spekkens 05)
5. foundations of statistical mechanics (Popescu, Short, Winter 05)
6. quantum identification (Hayden, Winter 10)
7. no measurement-based QC for generic states (Gross, Flammia, Eisert 08;
Bremner, Mora, Winter 08)
8. Counterexamples minimum output additivity of Renyi entropies (Hayden, Winter 08), etc...

Hasting’s construction of the counterexample gives two (maybe three) interesting new ideas on how to sometimes improve the technique.

Plan of attack

We can follow the general idea (Levy’s+epsilon-nets) by adding three new ingredients:

1. Bound the von Neumann entropy indirectly, using the 2-norm

2. Improve the large deviation bound, using Levy’s lemma in a more refined way

3. Improve the epsilon-net estimate (either by a different probabilistic argument or by using a better version thereof)

1. Bounding the entropy with 2-norm

Lemma: For a subspace *S* of R⊗S we have (with τ=id/|R|)

$$\min_{|\psi\rangle\in\mathcal{S}} S(\psi_R) \geq \log|R| - |R| \max_{|\psi\rangle\in\mathcal{S}} \|\psi_R - \tau\|_2^2$$

Proof:

$$S(\rho) \geq -\log(|R|tr(\rho^2)) + \log|R| \geq 1 - |R|tr(\rho^2) + \log|R|$$

$$\log x \leq x - 1,\ \ x \geq 1$$

1. Bounding the entropy with 2-norm

Lemma: For a subspace *S* of R⊗S we have (with τ=id/|R|)

$$\min_{|\psi\rangle\in\mathcal{S}} S(\psi_R) \geq \log|R| - |R| \max_{|\psi\rangle\in\mathcal{S}} \|\psi_R - \tau\|_2^2$$

Next we prove there is a *S* of R⊗S with |S| = |E| >> |R| s.t.

$$\max_{|\psi\rangle\in\mathcal{S}} \|\psi_R - \tau\|_2^2 \leq \frac{c}{|R|^2}$$

Then

$$\min_{|\psi\rangle\in\mathcal{S}} S(\psi_R) \geq \log|R| - \frac{c}{|R|}$$

(Remember, we needed:

$$\min_{|\psi\rangle\in\mathcal{S}} S(\psi_R) > \log(|R|) - \frac{1}{2}\frac{|S|}{|E|}\frac{\log|R|}{|R|}$$

)

2. Large Deviation Bound for 2-norm

A naive application of Levy’s lemma gives

$$Pr\left(\|\psi_R - \tau\|_2^2 \geq \epsilon\right) \leq 2^{-c|R||E|\epsilon^2}$$

since the function is 2-Lipschitz and its average is smaller than 1/|E| (we assume it’s zero, for simplicity)

From it and epsilon-nets we can only find a *S* s.t.: $\max_{|\psi>\in\mathcal{S}} \|\psi_R - \tau\|_2^2 \leq \sqrt{\frac{\log|R|}{|R|}}$

However, the Lipschitz constant estimate was too conservative. For the vast majority of states, it’s *much* smaller.... We’ll explore this.

Improved Lipschitz constant

For the entire state space, a constant Lipschitz constant is the best we can have (take e.g. the maximally entangled state and the |0, 0> state). But

If two states $|\psi\rangle$ and $|\phi\rangle$ are such that $\|\psi_R\|_\infty, \|\phi_R\|_\infty \leq \frac{a}{|R|}$

Then $|f(|\psi\rangle) - f(|\phi\rangle)| \leq \sqrt{\frac{4a}{|B|}} \| |\psi\rangle - |\phi\rangle \|_2$

for $f(|\psi\rangle) := \|\psi_R - \tau\|_2$

And with probability $1 - e^{-c|E|}$, $\|\psi_R\|_2 \leq \frac{a}{|R|}$

Levy's for the intersection of two events

From the concentration of measure in the sphere, in complete analogy with standard Levy's lemma, we have

$$Pr\left(\|\psi_R - \tau\|_2 \ \ and \ \ \|\psi_R\|_\infty \leq \frac{a}{|R|}\right) \leq e^{-\frac{c}{a^2}|E||R|^2\epsilon^2}$$

Moreover, we have the following large deviation bound for infinity norm (which can be derived from Levy's Lemma)

$$Pr\left(\|\psi_R\|_\infty \geq \frac{C}{|R|}\right) \leq e^{-C'|E|}$$

Improved Large Deviation Bound

Putting them together and using $Pr(A\ and\ B) \geq Pr(A) - Pr(B^c)$

$$Pr\left(\|\psi_R - \tau\|_2 \geq \epsilon\right) \leq Pr\left(\|\psi_R - \tau\|_2 \geq \epsilon\ and\ \|\psi_R\|_\infty \leq a/|R|\right)$$

$$+Pr\left(\|\psi_R\|_\infty \geq \frac{a}{|R|}\right)$$

$$= e^{-\frac{c}{a^2}|E||R|^2\epsilon^2} + e^{-C'|E|}$$

Thus:

$$\boxed{Pr\left(\|\psi_R - \tau\|_2 \geq \frac{a}{|R|}\right) \leq e^{-c' a|E|}}$$

Still not enough

So we have

$$\boxed{Pr\left(\|\psi_R-\tau\|_2^2 \geq \frac{a}{|R|^2}\right) \leq e^{-ca|E|}}$$

From epsilon-net we get

$$Pr\left(\max_{|\psi\rangle\in\mathcal{S}} \|\psi_R-\tau\|_2^2 \geq \frac{a}{|R|^2}\right) \leq e^{\tilde{c}|S|\log(|R|)}e^{-ca|E|}$$

Then we find there is a subspace *S* s.t.

$$\min_{|\psi\rangle\in\mathcal{S}} S(\psi_R) \geq \log|R| - c'\frac{|S|}{|E|}\frac{\log|R|}{|R|}$$

This is a constant away from the result we want...

3. Improve epsilon-net argument

To complete the proof, we need a way to get rid of the extra
log|R|
factor in the epsilon-net. There are two different approaches here:

1. we can replace the epsilon-net part by another probabilistic argument. This is the idea originally used by Hastings

2. we can use a chaining argument for epsilon nets (which was introduced in this context in Aubrun, Szarek, Werner 10 and attributed to Schechtman, who in turn attributed it to Kolmogorov)

Hasting’s lower bound on the probability

$$\boxed{Pr_{|\psi\rangle}\left(\|\psi_R-\tau\|_2^2 \geq \frac{a}{|R|^2}\right) \geq e^{-c'|S|}\left(Pr\left(\max_{|\psi\rangle\in\mathcal{S}}\|\psi_R-\tau\|_2^2 \geq \frac{\tilde{c}a}{|R|^2}\right)-o(1)\right)}$$

Comparing to

$$\boxed{Pr\left(\|\psi_R-\tau\|_2^2 \geq \frac{a}{|R|^2}\right) \leq e^{-ca|E|}}$$

and remembering |E| = |S|:

$$\boxed{Pr\left(\max_{|\psi\rangle\in\mathcal{S}}\|\psi_R-\tau\|_2^2 \geq \frac{\tilde{c}a}{|R|^2}\right) \leq o(1)}$$

Details on blackboard...

Open questions

- Hastings’ counterexample is probabilistic and non-constructive. Can we find explicit counterexamples?

- The best violations of additivity are of order 10^{-6}. The violations for Renyi entropies, on the other hand, are extensive. Can we find larger violations for the von Neumann entropy?

- Can we find a counterexample to the additivity of the classical capacity? An equivalent problem is to find counterexamples to the *regularization* of the minimum output entropy.