Concavity Bounds for Quantum Entropy

Mary Beth Ruskai
ruskai@member.ams.org

joint work with I. Kim arxiv:1404.5999

ILAS August, 2014

Quantum Entropy

defined by von Neumann (1927) $\quad S(\rho) = -\mathrm{Tr}\,\rho \log \rho$

$\rho \geq 0,\ \mathrm{Tr}\,\rho = 1$ a density matrix

well-known to be concave

$$S(\rho_{\mathrm{av}}) \equiv S\big(x\rho_1 + (1-x)\rho_2\big) \geq x\,S(\rho_1) + (1-x)\,S(\rho_2)$$

want bound on concavity

Aside: Chandler Davis (1961) first to observe stronger

$\rho \mapsto -\rho \log \rho \qquad$ operator concave

Aside on Relative Entropy

Klein's Inequality: for any convex function f on $(0, \infty)$

$$\mathrm{Tr}\, f(A) - f(B) \geq \mathrm{Tr}\, f'(B)(A - B) \qquad\qquad \forall\ A, B > 0$$

Pf: Expand in e-fctns of B and apply Jensen's ineq in form
$\langle \phi, f(A)\phi \rangle \geq f\big(\langle \phi, A\phi \rangle\big)$

Apply to $x \log x$ gives Klein

$$H(A, B) \equiv \mathrm{Tr}\, A \log A - \mathrm{Tr}\, A \log B \geq \mathrm{Tr}\, (A - B)$$

Relative entropy $\quad H(A, B) \geq 0 \qquad$ if $\mathrm{Tr}\, A = \mathrm{Tr}\, B$

Pinsker's Ineq $\quad H(A, B) \geq \frac{1}{2} \|A - B\|_1^2$

Kim's lower bounds

First ,for any op convex fctn, can define gen rel ent – Kim proved

$$
\begin{aligned}
S(\rho_{\rm av}) - x\,S(\rho_1) - (1-x)\,S(\rho_2) &\geq \frac{x(1-x)}{(1-2x)^2} H(\rho_{\rm rev}, \rho_{\rm av}) \\
&\geq \tfrac{1}{2}\frac{x(1-x)}{(1-2x)^2} \|\rho_{\rm rev} - \rho_{\rm av}\|_1^2 \\
&\geq \tfrac{1}{2}\, x(1-x)\, \|\rho_1 - \rho_2\|_1^2
\end{aligned}
$$

$$
\rho_{\rm av} = x\rho_1 + (1-x)\rho_2 \qquad \rho_{\rm rev} = x\rho_2 + (1-x)\rho_1
$$

Note: $\rho_{\rm av} - \rho_{\rm rev} = (1-2x)(\rho_2 - \rho_1)$

Simple Proof

Simple Proof of second inequality

$$S(\rho_{\rm av}) - x\,S(\rho_1) - (1-x)S(\rho_2)$$

$$\begin{aligned}
&= x\,\mathrm{Tr}\,\rho_1 \log \rho_1 + (1-x)\mathrm{Tr}\,\rho_2 \log \rho_2 - \mathrm{Tr}\,[x\rho_1 + (1-x)\rho_2] \log \rho_{\rm av} \\
&= x\,H(\rho_1, \rho_{\rm av}) + (1-x)H(\rho_2, \rho_{\rm av}) \\
&\geq \tfrac{1}{2}x\,\|\rho_1 - \rho_{\rm av}\|_1^2 + \tfrac{1}{2}(1-x)\,\|\rho_2 - \rho_{\rm av}\|_1^2 \\
&= \tfrac{1}{2}[x(1-x)^2 + (1-x)x^2]\,\|\rho_2 - \rho_{\rm av}\|_1^2 \;=\; \tfrac{1}{2}x(1-x)\,\|\rho_1 - \rho_2\|_1^2
\end{aligned}$$

Note, e.g., $\rho_{\rm av} - \rho_1 = (1-x)(\rho_2 - \rho_1)$

Carlen-Lieb bound on subadditivity

$$S(\rho_A) + S(\rho_B) - S(\rho_{AB}) \;=\; H(\rho_{AB}, \rho_A \otimes \rho_B)$$

$$\geq \begin{cases} \frac{1}{2}\|\rho_{AB} - \rho_A \otimes \rho_B\|_1 & \text{Pinsker} \\ -2\log\left[1 - \frac{1}{2}\mathrm{Tr}\left(\sqrt{\rho_{AB}} - \sqrt{\rho_A \otimes \rho_B}\right)^2\right] & \text{Carlen-Lieb} \\ \quad = \; -2\log \mathrm{Tr}\,\sqrt{\rho_{AB}}\sqrt{\rho_A \otimes \rho_B}) & H_{1/2}^{\mathrm{Ren}}(\rho_{AB}, \rho_A \otimes \rho_B) \end{cases}$$

Carlen-Lieb show their (Renyi) bound stronger in some situations

Renyi relative entropy $H_a^{\mathrm{Ren}}(\rho, \gamma) \equiv \frac{1}{a-1} \log \mathrm{Tr}\, \rho^a \gamma^{1-a}$

monotone $\frac{1}{2} \leq a \leq 2$ $\qquad H(\rho, \gamma) = H_1^{\mathrm{Ren}}(\rho, \gamma) \geq H_{1/2}^{\mathrm{Ren}}(\rho, \gamma)$

Concavity as subadditivity

If $P_{AB} = \begin{pmatrix} x\rho_1 & 0 \\ 0 & (1-x)\rho_2 \end{pmatrix}$ then $P_A = \rho_{\rm av}, \;\; P_B = \begin{pmatrix} x & 0 \\ 0 & 1-x \end{pmatrix}$

so that

$$\begin{aligned} H(P_{AB}, P_A \otimes P_B) &= S(P_A) + S(P_B) - S(P_{AB}) \\ &= S(\rho_{\rm av}) + h(x) \\ &\quad + \mathrm{Tr}\, x\rho_1 \log x\rho_1 + \mathrm{Tr}\,(1-x)\rho_2 \log(1-x)\rho_2 \\ &= S(\rho_{\rm av}) + h(x) - h(x) - xS(\rho_1) - (1-x)S(\rho_2) \\ &= S(\rho_{\rm av}) - xS(\rho_1) - (1-x)S(\rho_2) \end{aligned}$$

$h(x) = -x\log x - (1-x)\log(1-x)$ binary entropy

Apply Carlen-Lieb or Renyi $\frac{1}{2}$

$$S(\rho_{\rm av}) - xS(\rho_1) - (1-x)S(\rho_2) = H(P_{AB}, P_A \otimes P_B)$$

$$\begin{aligned}
&\geq -2 \log \operatorname{Tr} \sqrt{P_{AB}}\sqrt{P_A \otimes P_B}) \\
&= -2 \log \operatorname{Tr} \begin{pmatrix} \sqrt{x}\sqrt{\rho_1} & 0 \\ 0 & \sqrt{1-x}\sqrt{\rho_2} \end{pmatrix} \begin{pmatrix} \sqrt{x}\sqrt{\rho_{\rm av}} & 0 \\ 0 & \sqrt{1-x}\sqrt{\rho_{\rm av}} \end{pmatrix} \\
&= -2 \log \operatorname{Tr} \left[x\sqrt{\rho_1} + (1-x)\sqrt{\rho_2} \right] \sqrt{\rho_{\rm av}} \\
&\geq -2 \log \operatorname{Tr} \sqrt{\rho_{\rm av}}\sqrt{\rho_{\rm av}} = -2 \log \operatorname{Tr} \rho_{\rm av} = 0
\end{aligned}$$

Pinsker direct $\quad H(P_{AB}, P_A \otimes P_B) \geq 2x^2(1-x)^2 \quad$ appears weaker

Which bound is better?

Pinsker

$$S(\rho_{\rm av}) - xS(\rho_1) - (1-x)S(\rho_2) \;\geq\; \tfrac{1}{2}x(1-x)\|\rho_1 - \rho_2\|_1^2$$

Carlen-Lieb/Renyi

$$S(\rho_{\rm av}) - xS(\rho_1) - (1-x)S(\rho_2) \;\geq\; -2\log \operatorname{Tr}\left[x\sqrt{\rho_1} + (1-x)\sqrt{\rho_2}\right]\sqrt{\rho_{\rm av}}$$

Numerical examples show sometimes one, sometimes the other

Carlen-Lieb sometimes even better than stronger Kim bound.

But Carlen-Lieb (Renyi) also weaker for some ρ_1, ρ_2.

Holevo χ bounds

$$\chi(x_k,\rho_k) \equiv S(\rho_{\rm av}) - \sum_k x_k S(\rho_k)$$
$$= \sum_k x_k H(\rho_k,\rho_{\rm av}) \ \geq\ \tfrac{1}{2}\sum_k x_k \|\rho_k - \rho_{\rm av}\|_1^2$$

Don't get single term form, but Renyi approach also extends

$P_{AB} = \oplus_k x_k \rho_k$ as block diagonal matrix with blocks $x_k\rho_k$.

$$\chi(x_k,\rho_k) = H(P_{AB}, P_A \otimes P_B)$$
$$\geq -2\log \operatorname{Tr} \sqrt{P_{AB}}\sqrt{P_A \otimes P_B})$$
$$= -2\log \Big(\sum_k x_k \sqrt{\rho_k}\Big)\sqrt{\rho_{\rm av}}$$

$$\chi(x_k,\rho_k) = S(\rho_{\rm av}) - \mathrm{Av}[S(\rho_k)] \geq -2\log \sqrt{\rho_{\rm av}}\,\mathrm{Av}\big(\sqrt{\rho_k}\big)$$

Upper Bounds

Operator montonicity of log $\Rightarrow$ $\log x\rho_1 < \log \rho_{\rm av}$

$$\log(1-x)\rho_2 < \log \rho_{\rm av}$$

$$\text{Tr}\, x\rho_1 \log x\rho_1 + \text{Tr}\,(1-x)\rho_2 \log(1-x)\rho_2 \leq \text{Tr}\,[x\rho_1 + (1-x)\rho_2] \log \rho_{\rm av}$$

$$-x \log x - (1-x)\log(1-x) + xS(\rho_1) + (1-x)S(\rho_2) \geq S(\rho_{\rm av})$$

$$h(x) \geq S(\rho_{\rm av}) - xS(\rho_1) - (1-x)S(\rho_2)$$

$h(x) = -x \log x - (1-x)\log(1-x)$ binary entropy

More recent bounds

$$\begin{aligned} S(\rho_{\rm av}) - xS(\rho_1) - (1-x)S(\rho_2) &\leq h(x) 2\Big[1 - \text{Tr}\left(\sqrt{\rho}\,\gamma\,\sqrt{\rho}\right)^{1/2}\Big] \\ &\leq h(x)\|\rho_1 - \rho_2\|_1 \end{aligned}$$

first ineq due to Roga, Fannes and Zyczkowski (2010)

second ineq due to Fuchs and van de Graph (1999)

Not clearly better since can have $2 \geq \|\rho_1 - \rho_2\|_1 > 1$

$$S(\rho_{\rm av}) - xS(\rho_1) - (1-x)S(\rho_2) \leq h(x)\tfrac{1}{2}\|\rho_1 - \rho_2\|_1$$

Audenaert (arxiv: 1304.5935) definitely stronger bound

Renyi relative entropies

$$H_a^{\rm Ren}(\rho,\gamma) \equiv \frac{1}{a-1} \log \operatorname{Tr} \rho^a \gamma^{1-a} \qquad \forall\ a \in (0,2]$$

traditional, many applications $\quad \lim_{a\to 1} (\ ) = H(\rho,\gamma)$

Main interest is $a \in [\frac{1}{2}, 2]$

Aside: $\quad \frac{1}{a(a-1)} \log \operatorname{Tr} \rho^a \gamma^{1-a} \quad \forall\ a \in [-1,2] \qquad \lim_{a\to 0} (\ ) = H(\gamma,\rho)$

$$\widetilde{H}_a^{\rm Ren}(\rho,\gamma) \equiv \frac{1}{a-1} \log \operatorname{Tr} \left(\gamma^{\frac{1-a}{2a}} \rho \gamma^{\frac{1-a}{2a}} \right)^a \qquad \forall\ a > 0$$

"sandwiched" Renyi entropy – independently by two groups

arXiv:1306.1586, arXiv:1306.3142

Properties of Renyi relative entropy

$$H_a^{\mathrm{Ren}}(\rho,\gamma) \equiv \frac{1}{a-1} \log \mathrm{Tr}\, \rho^a \gamma^{1-a} \qquad \forall\, a \in (0,2]$$

$$\widetilde{H}_a^{\mathrm{Ren}}(\rho,\gamma) \equiv \mathrm{Tr}\, \frac{1}{a-1} \log \mathrm{Tr} \left(\gamma^{\frac{1-a}{2a}} \rho \gamma^{\frac{1-a}{2a}}\right)^a \qquad \forall\, a > 0$$

- $\widetilde{H}_a^{\mathrm{Ren}}(\rho,\gamma) \geq H_a^{\mathrm{Ren}}(\rho,\gamma)$
- both $\to H(\rho,\gamma)$ as $a \to 1$
- both monotone increasing in a for $a \geq \frac{1}{2}$
- both decrease under CPT maps (quantum channels)

Max relative entropy

Renner (ETH thesis, 2005) introduced max and min entropy

Def: $H_{\min}(\rho) = -\log \lambda_{\max}(\rho)$ $\quad$ $H_{\max}(\rho) = \log \mathrm{rank}(\rho)$

smoothed and conditioned versions, which $\rightarrow$ usual in suitable limit

extremely useful in cryptography and QIT

Def. or Thm: $H_{\min}(\rho, \gamma) = \lim_{a \to 0} H_a^{\mathrm{Ren}}(\rho, \gamma)$

Def: $H_{\max}(\rho, \gamma) \equiv \log \inf\{w : \rho \leq w\gamma\} = \log \lambda_{\max}(\gamma^{-1/2}\rho\gamma^{-1/2})$

Thm: $\lim_{a \to \infty} \widetilde{H}_a^{\mathrm{Ren}}(\rho, \gamma) = H_{\max}(\rho, \gamma)$

Improved bounds

Thm: For any fixed, $x \in (0,1)$ and $\rho_1 \neq \rho_2$ one can find $a_c > 1$ and $b_c \in [\frac{1}{2}, 1)$ such that

$$
\begin{aligned}
h(x)\tfrac{1}{2}\|\rho_1 - \rho_2\|_1 &\geq x\widetilde{H}_a^{\mathrm{Ren}}(\rho_1, \rho_{\mathrm{av}}) + (1-x)\widetilde{H}_a^{\mathrm{Ren}}(\rho_2, \rho_{\mathrm{av}}) \\
&\qquad\qquad \forall\ a \geq a_c \\
&\geq S(\rho_{\mathrm{av}}) - xS(\rho_1) - (1-x)S(\rho_2) \\
&= xH_1(\rho_1, \rho_{\mathrm{av}}) + (1-x)H_1(\rho_1, \rho_{\mathrm{av}}) \\
&\geq xH_b^{\mathrm{Ren}}(\rho_1, \rho_{\mathrm{av}}) + (1-x)H_b^{\mathrm{Ren}}(\rho_2, \rho_{\mathrm{av}}) \\
&\qquad\qquad \forall\ b \in [b_c, 1) \\
&\geq \tfrac{1}{2}x(1-x)\|\rho_1 - \rho_2\|_1^2
\end{aligned}
$$

Would like strict inequality – expect generic,

but not possible if e.g., ρ_1, ρ_2 orthog rank one projs.

Better bounds?

Can one find universal bounds with some of x, ρ_1, ρ_2 fixed?

Try $a = 2$ (dual of $\frac{1}{2}$)

$$\begin{aligned} \chi(x_k, \rho_k) &= S(\rho_{\rm av}) - \sum_k x_k S(\rho_k) \\ &\leq \sum_k x_k H_2^{\rm Ren}(\rho_k, \rho_{\rm av}) \\ &= -\tfrac{1}{2} x_k \sum_k \log \operatorname{Tr}\, \rho_k \frac{1}{\rho_{\rm av}} \rho_k \\ ? &\leq \; ?\ h(\{x_k\}) \end{aligned}$$

Can only show last ineq when all $x_k = \frac{1}{n}$, $\qquad h(\{x_k\}) = \log n$

Mosonyi's bound

Thm: (Mosonyi) For all $a > 1$,

$$
\begin{aligned}
h(\{x)\} &\geq \sum_k x_k \widetilde{H}_a^{\mathrm{Ren}}(\rho_k, \rho_{\mathrm{av}}) \\
&\geq S(\rho_{\mathrm{av}}) - \sum_k x_k S(\rho_k) \;=\; \chi(x_k, \rho_k)
\end{aligned}
$$

Pf: Since $\rho_k \leq \frac{1}{x_k}\rho_{\mathrm{av}}$, $\quad H_{\max}(\rho, \gamma) \equiv \log \inf\{w : \rho \leq w\gamma\}$

$$
\begin{aligned}
-\log x_k &= \log \tfrac{1}{x_k} \geq H_{\max}(\rho_k, \rho_{\mathrm{av}}) \\
&\geq \widetilde{H}_a^{\mathrm{Ren}}(\rho_k, \rho_{\mathrm{av}}) \geq H_1(\rho_k, \rho_{\mathrm{av}})
\end{aligned}
$$

The End – Almost

That's all folks. Thank You.

Open Problem: How to number slides in reverse using beamer?

Serious Open Problem

Audenaert-Ruskai conjecture arxiv.0708.1902 See Section 2.

Block matrix gen of Horn's lemma. Several formulations:

- Every CPT map can be written as evenly weighted convex comb of extreme pts. (generalized to mean Choi rank $\leq d$)
- See paper for more and why this is Horn's Lemma.

Really finished - Thank You.