# Quantum Entropy

Mary Beth Ruskai

marybeth.ruskai@tufts.edu

Department of Mathematics, Tufts University

Singapore August, 2008

Supported by U.S. National Science Foundation

von Neumann (1927) defined mixed quantum state and its entropy

$$S(\rho) = -\text{Tr } \rho \log \rho$$

$$= -\sum_k \lambda_k \log \lambda_k \qquad \text{evals of } \rho$$

Density matrix $\rho > 0$ and $\text{Tr}\, \rho = 1 \quad \Rightarrow \quad S(\rho) \geq 0$

also find $\rho = |\psi\rangle\langle\psi|$ pure $\Leftrightarrow$ $\rho^2 = \rho$ $\Leftrightarrow$ $S(\rho) = 0$

But $S(P)$ well-defined for any pos semi-def op $P$ ms

$S(\rho) \geq 0$ is result of normalization and/or phys interp

Shannon (1948): classical info with entropy equiv. to diag matrix

## Fundamental Properties of Quantum Entropy

Concave: $x\,S(\rho_1) + (1-x)S(\rho_2) \le S\big(x\rho_1 + (1-x)\rho_2\big)$

Subadditive: $S(\rho_{AB}) \le S(\rho_A) + S(\rho_B)$

with $= \Leftrightarrow \;\rho_{AB} = \rho_A \otimes \rho_B$

Strongly Subadditive $S(\rho_B) + S(\rho_{ABC}) \le S(\rho_{AB}) + S(\rho_{BC})$

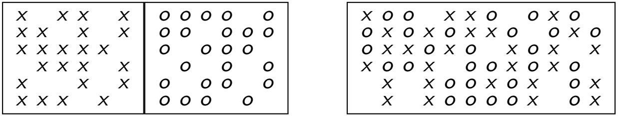
All indep of normalization as long as consistent, e.g.,

$$\mathrm{Tr}\,\rho_B = \mathrm{Tr}\,\rho_{AB} = \mathrm{Tr}\,\rho_{ABC}$$

Note: $S(\mu P) = \mu S(P) - \mu \log \mu \mathrm{Tr}\, P$

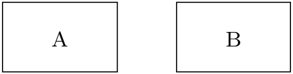
Concave: $x\,S(\rho_1) + (1-x)S(\rho_2) \leq S\big(x\rho_1 + (1-x)\rho_2\big)$

refers to mixture



Subadditive: $S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B)$

refers to regions or subsystems




SSA: $S(\rho_B) + S(\rho_{ABC}) \leq S(\rho_{AB}) + S(\rho_{BC})$

overlapping regions

Aside: Subadditive $\Rightarrow$ Concave

$$\rho_{AB} = \begin{pmatrix} x\rho_1 & 0 \\ 0 & (1-x)\rho_2 \end{pmatrix}$$

$$\rho_A = x\rho_1 + (1-x)\rho_2, \qquad \rho_B = \left(\begin{smallmatrix} x & 0 \\ 0 & 1-x \end{smallmatrix}\right)$$

$$\begin{aligned} S(\rho_{AB}) &= S(x\rho_1) + S\big((1-x)\rho_2\big) \\ &= xS(\rho_1) - x\log x + (1-x)S(\rho_2) - (1-x)\log(1-x) \end{aligned}$$

$$\begin{aligned} S(\rho_{AB}) &\leq S(\rho_A) + S(\rho_B) \\ &= S\big(x\rho_1 + (1-x)\rho_2\big) - x\log x - (1-x)\log(1-x) \end{aligned}$$

$$\Rightarrow \qquad xS(\rho_1) + (1-x)S(\rho_2) \leq S\big(x\rho_1 + (1-x)\rho_2\big)$$

Relative entropy $H(P, Q) = \text{Tr}\, P \log P - \text{Tr}\, P \log Q$

Klein's ineq: $H(P, Q) \geq \text{Tr}\,(P - Q) \qquad \geq 0$ if $\text{Tr}\, P = \text{Tr}\, Q$

assume $P, Q > 0$ strictly pos — well-def if $\ker(Q) \subset \ker(P)$

Can obtain entropy from rel ent. $H(P, \frac{1}{d} I) = -S(P) + \log d$

homogenous of degree one $H(\lambda P, \lambda Q) = \lambda H(P, Q)$

Aside: for homo fctns convex $\Leftrightarrow$ $g(A + B) \leq g(A) + g(B)$

$$g\big(xA + (1-x)B\big) \leq g(xA) + g\big((1-x)B\big) = xg(A) + (1-x)g(B)$$
$$\tfrac{1}{2}g(A + B) = g\big(\tfrac{1}{2}(A + B)\big) \leq \tfrac{1}{2}g(A) + \tfrac{1}{2}g(B) \qquad \text{cancel } \tfrac{1}{2}$$

## Fundamental Properties of Relative Entropy

Joint Convexity $H(P_1 + P_2, Q_1 + Q_2) \leq H(P_1, Q_1) + H(P_2, Q_2)$

Monotone under Partial Trace $H(P_A, Q_A) \leq H(P_{AB}, Q_{AB})$

Monotone under CPT Map $H[\Phi(P), \Phi(Q)] \leq H(P, Q)$

Ibinson-Winter: that's all folks!

Special Case of MPT $P_{AB} \to \rho_{ABC}, \; Q_{AB} \to I_A \otimes \rho_{BC}$

gives SSA $H(\rho_{AB}, \rho_B) \leq H(\rho_{ABC}, \rho_{BC})$

$$-S(\rho_{AB}) + S(\rho_B) \leq -S(\rho_{ABC}) + S(\rho_{BC})$$

MonoCPT with $\Phi = \text{Tr}_B \;\Rightarrow\;$ MPT $\;\Rightarrow\;$ SSA $\;\Rightarrow\;$ JC

Will prove JC and then show $\;\Rightarrow\;$ MPT $\;\Rightarrow\;$ MonoCPT

## Information Theory Expressions

Mutual Information: (always positive)

$$S(A:B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB}) = H(\rho_{AB}, \rho_A \otimes \rho_B) \geq 0$$

Conditional Information: (always positive for classical systems)

$$\begin{aligned} S(A|B) &= S(\rho_{AB}) - S(\rho_B) = -H(\rho_{AB}, \rho_B) \\ &= -H(\rho_{AB}, \tfrac{1}{d} I_A \otimes \rho_B) + \log d \end{aligned}$$

But for max entangled quant state $S(\rho_{AB}) - S(\rho_B) = -\log d < 0$

HOW (M. Horodecki, J. Oppenheim, A. Winter) interpretation:
*Nature* **436**, 673–676 (2005); CMP **269** , (2007). quant-ph/0512247.
Cond info measures # of bits Alice needs to transmit message
to Bob when he has partial info – same in class. and quantum info
When negative, gives # of EPR pairs A and B have left for future

write density matrix $\rho = \sum_k \lambda_k |\phi_k\rangle\langle\phi_k|$ spectral decomp

$\{g_k\}$ O.N. $|\psi\rangle = \sum_k \sqrt{\lambda_k}\, |\phi_k\rangle \otimes |g_k\rangle \quad \Rightarrow \; \mathrm{Tr}_B |\psi\rangle\langle\psi| = \rho$

For pure $\rho_{AB} = |\psi\rangle\langle\psi| \qquad \rho_A = \mathrm{Tr}_B |\psi\rangle\langle\psi|$ and $\rho_B = \mathrm{Tr}_A |\psi\rangle\langle\psi|$

have same e-vals $\quad \Rightarrow \; S(\rho_A) = S(\rho_B)$

apply to $S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B)$ purified to $|\psi_{ABC}\rangle$

$S(\rho_C) \leq S(\rho_A) + S(\rho_{AC}) \;\Rightarrow$

Triangle Ineq: $\quad |S(\rho_C) - S(\rho_A)| \leq S(\rho_{AC}) \leq S(\rho_A) + S(\rho_C)$

Purifiy SSA: $S(\rho_B) + S(\rho_{ABC}) \leq S(\rho_{AB}) + S(\rho_{BC})$ with $|\psi_{ABCD}\rangle$

$$S(\rho_B) + S(\rho_D) \leq S(\rho_{AB}) + S(\rho_{AD}) \quad \forall\; \rho_{ABD}$$

(i) Note equality for pure $\rho_{ABD}$

(ii) Can have $S(\rho_B) \geq S(\rho_{AB})$ but not for pair from tripartite $\rho_{ABD}$

# Proof of JC of rel ent and SSA

Joint convexity of $H(P,Q)$ follows from:

(I) $$H(P,Q) = \int_0^\infty \operatorname{Tr}(Q-P)\frac{1}{L_Q + tR_P}(Q-P)\frac{1}{(1+t)^2}\,dt$$

(II) $(A,P,Q) \mapsto \operatorname{Tr} A^\dagger \dfrac{1}{L_Q + tR_P} A$ is jointly convex in $A, P, Q$.

where $L_Q(A) = QA$ and $R_P(A) = AP$

Result follows by using (II) in (I) with $A = Q - P$.

$$\operatorname{Tr}(\lambda A)^\dagger \frac{1}{L_{\lambda Q} + tR_{\lambda P}}(\lambda A) = \lambda \operatorname{Tr} A^\dagger \frac{1}{L_Q + tR_P}(A) \quad H(\lambda P, \lambda Q) = \lambda H(P,Q)$$


Ruskai, quant-ph/0604206 *Reports on Math. Phys.* (2007).

"Another Short and Elementary Proof of Strong Subadditivity of Quantum Entropy"

based on Lesniewski-Ruskai *J. Math. Phys.* **40**, 5702–5724 (1999).

$d \times d$ matrices form Hilbert space with $\langle A, B \rangle = \text{Tr}\, A^\dagger B$

for lin op $\Phi : M_d \mapsto M_d$ let $\widehat{\Phi}$ denote adjoint

$$\text{Tr}\, A^\dagger \Phi(B) = \langle A, \Phi(B) \rangle = \langle \widehat{\Phi}(A), B \rangle = \text{Tr}\, [\widehat{\Phi}(A)]^\dagger B$$

Left and right mult are just linear operators on this vector space

$$L_Q(A) = QA \qquad \text{and} \qquad R_P(A) = AP$$

a) $L_P$ and $R_Q$ commute since $L_P[R_Q(A)] = PAQ = R_Q[L_P(A)]$

b) $P = P^\dagger \;\Rightarrow\; L_P$ self-adjoint in fact, $\widehat{L_P} = L_{P^\dagger}$ and $\widehat{R_P} = R_{P^\dagger}$

c) $P \geq 0 \;\Rightarrow\; L_P$ and $R_P$ are pos semi-def

$$\langle A, R_P(A) \rangle = \text{Tr}\, A^\dagger R_P(A) = \text{Tr}\, A^\dagger AP = \text{Tr}\, APA^\dagger \geq 0$$

d) $(L_P)^{-1} = L_{P^{-1}}$ and $(R_Q)^{-1} = R_{Q^{-1}}$

simple form of deep idea: Araki $\Delta_{PQ} = L_{P^{-1}} R_Q$ relative modular op

Note homo: $\mathrm{Tr}\,(\lambda A)^\dagger \dfrac{1}{L_{\lambda Q} + tR_{\lambda P}}(\lambda A) = \lambda\,\mathrm{Tr}\,A^\dagger \dfrac{1}{L_Q + tR_P}(A)$

Proof of II: Let $M = (\ )^{-1/2}(A) - (\ )^{1/2}(X)$

$$\begin{aligned} \mathrm{Tr}\,M^\dagger M &= \langle M, M\rangle \\ &= \langle \left[(\ )^{-1/2}(A) - (\ )^{1/2}(X)\right], \left[(\ )^{-1/2}(A) - (\ )^{1/2}(X)\right]\rangle \\ &= \langle A, (\ )^{-1}(A)\rangle - \langle A, X\rangle - \langle X, A\rangle + \langle X, (\ )(X)\rangle \end{aligned}$$

Choose $M = (L_P + tR_Q)^{-1/2}(A) - (L_P + tR_Q)^{1/2}(X)$

$$\mathrm{Tr}\,M^\dagger M =$$

$$\mathrm{Tr}\,A^\dagger (L_P + tR_Q)^{-1}(A) - \mathrm{Tr}\,A^\dagger X - \mathrm{Tr}\,X^\dagger A + \mathrm{Tr}\,X^\dagger (L_P + tR_Q)(X)$$

Let $M_j = (L_{P_j} + tR_{Q_j})^{-1/2}(A_j) - (L_{P_j} + tR_{Q_j})^{1/2}(X)$. Then

$$
\begin{aligned}
0 \;\leq\; \sum_j \operatorname{Tr} M_j^\dagger M_j \;=\; & \sum_j \operatorname{Tr} A_j^\dagger (L_{P_j} + tR_{Q_j})^{-1}(A_j) \\
& - \operatorname{Tr}\left(\textstyle\sum_j A_j^\dagger\right) X - \operatorname{Tr} X^\dagger \left(\textstyle\sum_j A_j\right) + \operatorname{Tr} X^\dagger \textstyle\sum_j (L_{P_j} + tR_{Q_j}) X
\end{aligned}
$$

Choose $X = \dfrac{1}{L_{\sum_j P_j} + tR_{\sum_j Q_j}}\left(\sum_j A_j\right)$. Use $\sum_j L_{P_j} = L_{\sum_j P_j}$

$$
\begin{aligned}
\operatorname{Tr} X^\dagger \textstyle\sum_j (L_{P_j} + tR_{Q_j}) X \;&=\; \operatorname{Tr}\left(\textstyle\sum_j A_j^\dagger\right) \tfrac{1}{L_{\sum_j P_j} + tR_{\sum_j Q_j}} \left(\textstyle\sum_j A_j\right) \\
&=\; \operatorname{Tr}\left(\textstyle\sum_j A_j^\dagger\right) X \;=\; \operatorname{Tr} X^\dagger \left(\textstyle\sum_j A_j\right)
\end{aligned}
$$

$$
0 \;\leq\; \sum_j \operatorname{Tr} A_j^\dagger \frac{1}{L_{P_j} + tR_{Q_j}}(A_j) \;-\; \operatorname{Tr}\left(\textstyle\sum_j A_j^\dagger\right) \tfrac{1}{L_{\sum_j P_j} + tR_{\sum_j Q_j}} \left(\textstyle\sum_j A_j\right)
$$

compare elem. C-S ineq: $\big|\sum_k \overline{v}_k w_k\big|^2 \;\le\; \sum_k |v_k|^2 \;\sum_k |w_k|^2$

For $p_k > 0$ let $v_k = p_k^{1/2},\; w_k = p_k^{-1/2} a_k$

$$\big|\sum_k a_k\big|^2 \;\le\; \sum_k p_k \;\sum_k \overline{a}_k \frac{1}{p_k} a_k$$

Rewrite $$\Big(\sum_k \overline{a}_k\Big)\frac{1}{\sum_k p_k}\Big(\sum_k a_k\Big) \;\le\; \sum_k \overline{a}_k \frac{1}{p_k} a_k$$

Lieb and Ruskai (1973) proved operator version

$$\Big(\sum_k A_k^\dagger\Big)\frac{1}{\sum_k P_k}\Big(\sum_k A_k\Big) \;\le\; \sum_k A_k^\dagger \frac{1}{P_k} A_k$$

Not suff. for SSA — need Araki rel mod op hidden in $L_Q$ and $R_P$.

Compare proof: $\big|\sum_k v_k + t w_k\big|^2 \ge 0 \;\forall\; t$ choose $t$ to minimize

$$
\begin{aligned}
H\Big(\sum_k P_k, \sum_k Q_k\Big) & \\
&= \int_0^\infty \operatorname{Tr} \textstyle\sum_k (Q_k - P_k) \frac{1}{L_{\sum_k P_k} + tR_{\sum_k Q_k}} \sum_k (Q_k - P_k) \frac{1}{(1+t)^2} dt \\
&\leq \int_0^\infty \sum_k \operatorname{Tr} (Q_k - P_k) \frac{1}{L_{P_k} + \, tR_{Q_k}} (Q_k - P_k) \frac{1}{(1+t)^2} dt \\
&= \sum_k H(P_k, Q_k)
\end{aligned}
$$

Only need to verify integral rep. Also works if $\frac{1}{(1+t)^2}$ replaced by $g(t) \geq 0$. Large class of gen. rel ent related to convex op functions

# Functions of operators

For $A = UDU^\dagger$ , define $f(A) = U\, f(D)\, U^\dagger$

$$A = U \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \dots & 0 & \lambda_m \end{pmatrix} U^\dagger \quad f(A) = U \begin{pmatrix} f(\lambda_1) & 0 & \dots & 0 \\ 0 & f(\lambda_2) & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & \dots & 0 & f(\lambda_m) \end{pmatrix} U^\dagger$$

equiv. to any reasonable def using power series, integral rep., etc.

also applies to operators, e.g., $L_Q$ acting on $M_d$ space of matrices

In particular, $\mathrm{Tr}\, L_{\log Q}(P) = \mathrm{Tr}\, (\log L_Q)(P)$

# Integral representation

$$-\log w = \int_0^\infty \left[\frac{1}{w+t} - \frac{1}{1+t}\right] dt = \int_0^\infty \frac{1}{w+t}(1-w)\frac{1}{1+t} dt$$

$$= (1-w) + \int_0^\infty \frac{(w-1)^2}{w+t}\frac{1}{(1+t)^2} dt$$

$$\operatorname{Tr} P \log Q = \operatorname{Tr} (\log Q) P = \operatorname{Tr} L_{\log Q}(P) = \operatorname{Tr} (\log L_Q)(P)$$

$$H(P,Q) = \operatorname{Tr} P(\log P - \log Q) = -\operatorname{Tr} (\log R_P^{-1})(P) - \operatorname{Tr} (\log L_Q)(P$$

$$= -\operatorname{Tr} \left[\log(L_Q R_P^{-I})\right](P)$$

$$= \operatorname{Tr} (I - L_Q R_P^{-1})(P) +$$

$$\operatorname{Tr} \int_0^\infty (L_Q R_P^{-1} - I)\frac{1}{L_Q R_P^{-1} + tI}(L_Q R_P^{-1} - I)(P)\frac{1}{(1+t)^2} dt$$

$$(L_Q R_P^{-1} - I)(P) = Q - P \quad \mathrm{Tr}\,(I - L_Q R_P^{-1})(P) = \mathrm{Tr}\,(P - Q) = 0$$

$$\begin{aligned} H(P,Q) &= \int_0^\infty \mathrm{Tr}\,(L_Q R_P^{-1} - I) \frac{1}{L_Q R_P^{-1} + tI} (Q - P) \frac{1}{(1+t)^2} dt \\ &= \int_0^\infty \mathrm{Tr}\,(L_Q - R_P) \frac{1}{L_Q + tR_P} (Q - P) \frac{1}{(1+t)^2} dt \\ &= \int_0^\infty \mathrm{Tr}\,(Q - P) \frac{1}{L_Q + tR_P} (Q - P) \frac{1}{(1+t)^2} dt \end{aligned}$$

Used

$$\begin{aligned} \mathrm{Tr}\,(L_Q - R_P)(B) &= \langle I, (L_Q - R_P)(B) \rangle = \langle (L_Q - R_P)(I), B \rangle \\ &= \langle (Q - P), B \rangle = \mathrm{Tr}\,(Q - P)B \end{aligned}$$

Completes proof of joint convexity of $H(P,Q)$

Prove MPT: Recall gen Pauli ops,

$$Z|e_n\rangle = e^{2\pi i n/d}|e_n\rangle \qquad X|e_n\rangle = |e_{n+1}\rangle$$

$$\sum_j Z^j \rho Z^{-j} = d\rho_{\mathrm{diag}} \qquad \sum_j X^j \rho_{\mathrm{diag}} X^{-j} = (\operatorname{Tr}\rho) I$$

$$\tfrac{1}{d_B}\sum_j \sum_k (I_A \otimes X_B^j Z_B^k)\,\rho_{AB}\,(I_A \otimes X_B^j Z_B^k)^\dagger = \rho_A \otimes I_B$$

$$H(\rho_A, \gamma_A) \;=\; H\big(\rho_A \otimes \tfrac{1}{d_B} I, \gamma_A \otimes \tfrac{1}{d_B} I\big) \;=$$

$$H\Big[\tfrac{1}{d^2}\sum_{jk}(I\otimes X^j Z^k)\rho_{AB}(I\otimes X^j Z^k)^\dagger\,,\,\tfrac{1}{d^2}\sum_{jk}(I\otimes X^j Z^k)\gamma_{AB}(I\otimes X^j Z^k)^\dagger\Big]$$

$$\leq\; \tfrac{1}{d^2}\sum_{jk} H\big[(I\otimes X^j Z^k)\rho_{AB}(I\otimes X^j Z^k)^\dagger\,,\,(I\otimes X^j Z^k)\gamma_{AB}(I\otimes X^j Z^k)^\dagger\big]$$

$$=\; \tfrac{1}{d^2}\sum_{jk} H(\rho_{AB}, \gamma_{AB}) \;=\; H(\rho_{AB}, \gamma_{AB})$$

used $H(V\rho V^\dagger, V\gamma V^\dagger) = H(\rho, \gamma)$

Proof of Mono for CPT $\qquad \Phi : \mathcal{B}(\mathcal{H}_B) \mapsto \mathcal{B}(\mathcal{H}_A)$

Lindblad/Stinespring for $A = B$ $\qquad \Phi(\rho) = \text{Tr}_E\, U_{AE}\, \rho \otimes |e\rangle\langle e| U_{AE}^\dagger$

OR $\quad \Phi(\rho) = \text{Tr}_E\, V_{AE}\, \rho_B V_{AE}^\dagger \qquad V^\dagger V = I \qquad V : \mathcal{H}_B \mapsto \mathcal{H}_{AE}$

Then by cyclicity of trace

$$H(\widetilde{\rho}_{AE}, \widetilde{\gamma}_{AE}) \equiv H(V_{AE}\, \rho_B V_{AE}^\dagger, V_{AE}\, \gamma_B V_{AE}^\dagger) = H(\rho_B, \gamma_B)$$

$$H[\Phi(\rho), \Phi(\gamma)] = H(\widetilde{\rho}_A, \widetilde{\gamma}_A) \leq H(\widetilde{\rho}_{AE}, \widetilde{\gamma}_{AE}) = H(\rho, \gamma)$$

Notes: $\widetilde{\rho}_{AE} = V_{AE}\, \rho V_{AE}^\dagger$ and $\rho$ have same non-zero e-vals

$H(\rho_A, \gamma_A) \leq H(\rho_{AB}, \gamma_{AB})$ proved as cor to SSA in original paper joint convexity of $H(\rho_{AB}, \rho_A \otimes \frac{1}{d} I_B) = -S(\rho_{AB}) + S(\rho_A) + \log d$

$$\Rightarrow \quad \rho_{AB} \longmapsto S(\rho_{AB}) - S(\rho_A) \text{ is concave}$$

$$\Rightarrow \quad \widetilde{\rho}_{AE} \longmapsto S(\widetilde{\rho}_{AB}) - S(\widetilde{\rho}_A) \text{ is concave}$$

But $S(\rho) = S(\widetilde{\rho}_{AE})$ and $S[\Phi(\rho)] = S(\widetilde{\rho}_A)$

$$\Rightarrow \quad \rho \longmapsto S(\rho) - S[\Phi(\rho)] \text{ is concave}$$

since $\widetilde{\rho}_{AE} = V_{AE}\, \rho V_{AE}^\dagger$ and $\rho$ have same non-zero e-vals

alt form of SSA $\qquad S(\rho_B) - S(\rho_{AB}) + S(\rho_D) - S(\rho_{AD}) \leq 0$

$=$ for pure $\rho_{ABD}$ extreme; sum of convex fctns $\Rightarrow \leq$ ext $\leq 0$

POVM $\{E_m\}$ with $E_m \geq 0$ and $\sum_M E_m = I$.

special CPT map called QC: $\Omega_{\mathcal{M}}(\rho) = \sum_m |e_m\rangle\langle e_m| \text{Tr}\, \rho E_m$.

Ensemble: $\{\pi_j, \rho_j\}$ with $\pi_j > 0$, $\sum_j \pi_j = 1$ and $\rho_j$ dens. matrix

Holevo bound on accessible info or max

mutual info between ensemble and measurement outcome

$$S[\Omega_{\mathcal{M}}(\rho_{\rm av})] - \sum_j \pi_j S[\Omega_{\mathcal{M}}(\rho_j)] \;\leq\; S(\rho_{\rm av}) - \sum_j \pi_j S(\rho_j)$$

$\rho_{\rm av} = \sum_j \pi_j \rho_j$ with $=$ if and only if all $\rho_j$ commute

Cor: Access info $\leq S(\rho_{\rm av}) \leq \log d \quad = n$ if $d = 2^n$

Holevo: direct proof in 1973 (same as SSA) without using SSA.

Will give 3 simple proofs of Holevo bound based on SSA

I. formal mutual info $\gamma_{AB} = \begin{pmatrix} \pi_1\rho_1 & 0 & \dots & \dots & 0 \\ 0 & \pi_2\rho_2 & \dots & \dots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & \dots & 0 & \pi_m\rho_m \end{pmatrix}$

Then $\gamma_A = \sum_j \pi_j\rho_j = \rho_{\rm av}$, and $\gamma_B = \sum_j |j\rangle\langle j|\,\pi_j$

$$\begin{aligned} H[\gamma_{AB}, \gamma_A \otimes \gamma_B] &= -S(\gamma_{AB}) + S(\gamma_A) + S(\gamma_B) \\ &= -\sum_j S(\pi_j\rho_j) + S(\rho_{\rm av}) + S[\pi_j] \\ &= -\sum_j \pi_j S(\rho_j) + \sum_j \pi_j \log \pi_j + S(\rho_{\rm av}) + S[\pi_j] \\ &= S(\rho_{\rm av}) - \sum_j \pi_j S(\rho_j) \end{aligned}$$

$$H[(\Omega_{\mathcal{M}} \otimes I)(\gamma_{AB}), (\Omega_{\mathcal{M}} \otimes I)(\gamma_A \otimes \gamma_B)] \le H[\gamma_{AB}, \gamma_A \otimes \gamma_B]$$

LHS is mutual info between ensemble and POVM outcome

II. Yuen-Ozawa (1993): Rewrite

$$\begin{aligned} S(\rho_{\mathrm{av}}) - \sum_j \pi_j S(\rho_j) &= \sum_j \pi_j \operatorname{Tr} \rho_j \log \rho_j - \sum_j \operatorname{Tr} \pi_j \rho_j \log \rho_{\mathrm{av}} \\ &= \sum_j \pi_j \operatorname{Tr} \rho_j \big( \log \rho_j - \log \rho_{\mathrm{av}} \big) \\ &= \sum_j \pi_j H(\rho_j, \rho_{\mathrm{av}}) \end{aligned}$$

Then by monotonicity of relative entropy

$$\begin{aligned} S[\Omega_{\mathcal{M}}(\rho_{\mathrm{av}})] - \sum_j \pi_j S[\Omega_{\mathcal{M}}(\rho_j)] &= \sum_j \pi_j H\big[\Omega_{\mathcal{M}}(\rho_j), \Omega_{\mathcal{M}}(\rho_{\mathrm{av}})\big] \\ &\leq \sum_j \pi_j H(\rho_j, \rho_{\mathrm{av}}) \\ &= S(\rho_{\mathrm{av}}) - \sum_j \pi_j S(\rho_j) \end{aligned}$$

III. Lieb-Seiringer

observed: $\rho \mapsto S(\rho) - S[\Omega_{\mathcal{M}}(\rho)]$ concave means

$$S(\rho_{\rm av}) - S[\Omega_{\mathcal{M}}(\rho_{\rm av})] \quad \geq \quad \sum_j \pi_j \big( S(\rho_j) - S[\Omega_{\mathcal{M}}(\rho_j)] \big)$$

equiv to

$$S(\rho_{\rm av}) - \sum_j \pi_j S(\rho_j) \quad \geq \quad S[\Omega_{\mathcal{M}}(\rho_{\rm av})] - S[\Omega_{\mathcal{M}}(\rho_j)]$$

All three proofs exend to partial measurement

$$\Omega_{\mathcal{M}_B} : \gamma_{AB} \mapsto \sum_j |j\rangle\langle j| \, \mathrm{Tr}_B \, \gamma_{AB} \, I_A \otimes F_j \qquad \sum_j F_j = I_B$$

“no transparent proof of SSA is known”

p. 645 of *Quantum Computation and Quantum Information*

Michael A. Nielsen and Isaac L. Chuang (Cambridge Press, 2000)

based on B. Simon's version adapted from Uhlmann (1977)

of “elementary” proof using only Schwarz inequality

of Lieb's Thm: $(A, B) \mapsto \operatorname{Tr} A^{1-t} K^* B^t K$ jointly concave

similar argument in Wehrl *Rev. Mod. Phys* (198?).

MBR, “Lieb's simple proof of concavity of $\operatorname{Tr} A^p K^* B^{1-p} K$ ...”
*Int. J. Quant Info.* **3**, 579–590 (2005); arXiv:quant-ph/0404126
Need only Schwarz inequality and maximum modulus principle

Petz – another argument in book and arXiv:quant-ph/0408130

MBR – proof presented here for SSA works for $\operatorname{Tr} A^p K^* B^{1-p} K$

## Wigner-Yanase-Dyson revisited

WYD skew entropy $\frac{1}{2}\mathrm{Tr}\,[K,\gamma^p][K,\gamma^{1-p}]$ for $0 < p < 1,\ K = K^\dagger$

WY Proved concave for $p = \frac{1}{2}$; Dyson suggested $p \in (0,1)$

led to Conjecture $\mathrm{Tr}\,K\gamma^p K\gamma^{1-p} - \mathrm{Tr}\,K\gamma K$ concave in $\gamma$

Lieb threw away linear term — seems reasonable but .....

proved $(A,B) \mapsto \mathrm{Tr}\,K^\dagger A^p K B^{1-p}$ concave for $A,B \geq 0,\ p \in (0,1)$.

Ando (1978, but ignored) proved joint convexity $p \in (1,2)$

until recent Lieb-Carlen work on $\left(\mathrm{Tr}_1(\mathrm{Tr}_2 A_{12}^p)^{q/p}\right)^{1/q}$

Jencova-Ruskai: Unified treatment – retain linear term in WYD

$$J_p(K,P,Q) = \frac{1}{p(1-p)}\big(\operatorname{Tr} K^\dagger P K - \operatorname{Tr} K^\dagger P^p K Q^{1-p}\big)$$

well-def for $p \in (0,2)$; by cont at $p = 1$, $J_1(I,P,Q) = H(P,Q)$

Thm: $(P,Q) \mapsto J_p(K,P,Q)$ is jointly convex for $p \in (0,2)$

Cor: Lieb concavity for $p \in (0,1)$ because of sign change at $p = 1$.

$$g_p(x) = \begin{cases} \frac{x - x^p}{p(1-p)} & p \neq 1 \\ x \log x & p = 1 \end{cases} \qquad J_p(K,P,Q) = \operatorname{Tr} K^* g_p\big(L_P R_Q^{-1}\big)(KQ)$$

operator convexity of $g_p(x)$ $\Rightarrow$ int rep as for $H(P,Q)$ $\Rightarrow$ Thm

apparent symmetry $p \leftrightarrow 1-p$ to $P \leftrightarrow Q$ more subtle

$$\widetilde{g}_p(x) = w\, g_{1-p}(w^{-1}) = \begin{cases} \frac{1 - x^p}{p(1-p)} & p \neq 0 \\ -\log x & p = 0 \end{cases}$$

$J_p(K,P,Q) = \widetilde{J}_{1-p}(K^\dagger, Q, P)$ with $\widetilde{J}_p$ well-def on $(-1,1)$

$$J_p(K,P,Q) = \frac{1}{p(1-p)}\big(\mathrm{Tr}\, K^\dagger P K - \mathrm{Tr}\, K^\dagger P^p K Q^{1-p}\big)$$

also has same monotonicity props as $H(P,Q)$

$$J_p(K_A,P_A,Q_A) \leq J_p(K_{AB},P_{AB},Q_{AB})$$

analogue of SSA $\qquad J_p(I,\rho_{AB},\rho_B) \leq J_p(I,\rho_{ABC},\rho_{BC})$

$$\frac{1}{p(1-p)}\mathrm{Tr}\,\rho_{AB}^p\,\rho_B^{1-p} \leq \frac{1}{p(1-p)}\mathrm{Tr}\,\rho_{ABC}^p\,\rho_{BC}^{1-p}$$

very different, but more natural than Renyi or Tsallis entropy

log enters only in weight in integral rep – doesn't affect props

No obvious connection to additivity conj – maybe why so hard

Equality conds for Carlen-Lieb or any $J_p$ are exactly same as SSA

- For SSA go back to Klein's inequality in original proof

quantum Markov cond $\log \rho_{ABC} - \log \rho_{AB} = \log \rho_{BC} - \log \rho_B$

- Petz (1986) used Connes co-cycle: $\rho_{AB}^{it} \rho_B^{-it} = \rho_{ABC}^{it} \rho_{BC}^{-it} \ \forall \ t$
- Jencova-Ruskai (2008) equal from C-S argument $\text{Tr}\, M_j^\dagger M_j \geq 0$

$M_j = (L_{P_j} + tR_{Q_j})^{-1/2}(A_j) - (L_{P_j} + tR_{Q_j})^{1/2}(X) = 0 \quad \forall\, j\, \forall\, t \ \geq 0$
Insert $X$ modified to include $K$ and let $P = \sum_j P_j$ etc.

$$\frac{1}{I + tL_{P_j}^{-1} R_{Q_j}}(K) = \frac{1}{I + tL_P^{-1} R_Q}(K) \quad \forall\, j\, \forall\, t \ \geq 0$$

can anal cont except $(-\infty, 0]$ and extend to $g(L_P^{-1} R_Q)(K)$

$\rho_{ABC} = \rho_A \otimes \rho_{BC}$ or $\rho_{AB} \otimes \rho_C$ but not necessary

$\rho_{ABC} = \rho_{AB_1} \otimes \rho_{B_2 C}$ where $\mathcal{H}_B = \mathcal{H}_{B_1} \otimes \mathcal{H}_{B_2}$

Most general nasc (HJPW) $\rho_{ABC} = \bigoplus_k \rho_{A_k B_k'} \otimes \rho_{B_k'' C_k}$

Proof of Klein's inequality: $\mathrm{Tr}\, A \log A - \mathrm{Tr}\, A \log B \geq \mathrm{Tr}\,(A - B)$

$g$ convex means diff quotients increase

$$\Rightarrow \quad \frac{g(b) - g(a)}{b - a} \leq g'(b) \quad \text{for} \quad a < b$$

$$\Rightarrow \quad g(b) - g(a) \leq (b - a) g'(b) \quad \text{for all} \quad a, b$$

$$\mathrm{Tr}\left[g'(B)(B - A) - g(B) + g(A)\right] \qquad \text{e-vec of } B$$

$$= \sum_k \left[g'(b_k)\big(b_k - \langle \beta_k, A\,\beta_k\rangle\big) - g(b_k) + \langle \beta_k, g(A)\beta_k\rangle\right]$$

Jensen $g\big(\langle \beta_k, A\,\beta_k\rangle\big) \leq \langle \beta_k, g(A)\beta_k\rangle$

$$\geq \sum_k \left[g'(b_k)\big(b_k - \langle \beta_k, A\beta_k\rangle\big) - g(b_k) + g\big(\langle \beta_k, A\beta_k\rangle\big)\right] \geq 0$$

For $g(x) = x \log x, \quad g'(x) = 1 + \log x$

$$\mathrm{Tr}\left[(B - A)(I + \log B) - B \log B + A \log A\right] \geq 0$$

## References

A. Wehrl "General Properties of Entropy"
*Rev. Mod. Phys.* **50**, 221–260 (1978).

M.B. Ruskai, "Inequalities for Quantum Entropy: A Review with Conditions for Equality" *J. Math. Phys.* **43**, 4358–4375 (2002); erratum 46, 019901 (2005). (quant-ph/0205064).

M.B. Ruskai, "Lieb's simple proof of concavity of $\mathrm{Tr}\, A^p K^\dagger B^{1-p} K$ and remarks on related inequalities"
*Int. Jour. Quant. Info.* **3**, 570–590 (2005). quant-ph/0404126

M.B. Ruskai, "Another short and elementary proof of strong subadditivity of quantum entropy"
*Reports on Math. Physics* **60**, 1–12 (2007). quant-ph/0604206