CO 781 / QIC 890 Lec 10, Oct 13 2016

All about quantum entropies:

Let ρ (or ρ_{AB}) be a quantum state on 2 sys A & B.

Shorthands: $S(AB) = S(\rho)$

$S(A) = S(\mathrm{tr}_B\, \rho)$

$S(B) = S(\mathrm{tr}_A\, \rho)$

sometimes ρ added as subscript if ambiguous

Def Conditional entropy

$$S(A|B) := S(AB) - S(B)$$

Cf Shannon conditional entropy.

Def: $H(X|Y) := \mathop{\mathbb{E}}_{y} H(X|Y=y)$ ← NOT hold in quantum

Chain rule: $H(X|Y) = H(XY) - H(Y)$ ← take Chain rule & make it a def.

* Conditioning on a quantum system B ≠ convex combination of measurement outcomes of B.

* NB $S(A|B)$ can be +ve, 0 or −ve.

eg. $\rho = |\Phi\rangle\langle\Phi|$, $S(A|B) = 0 - 1 = -1$

$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

new in Q

$\rho = \left(\frac{I}{2}\right)_A \otimes |0\rangle\langle 0|_B$, $S(A|B) = 1 - 0 = 1$

$\rho = |0\rangle\langle 0|_A \otimes \left(\frac{I}{2}\right)_B$, $S(A|B) = 1 - 1 = 0$

* NB $S(AB)$ can be $\geq$, $=$, $\leq$ $S(A)$

Def: Quantum relative entropy

$S(\rho \| \sigma) := \mathrm{tr}\, \rho (\log \rho - \log \sigma)$

if $\mathrm{supp}(\rho) \not\subseteq \mathrm{supp}(\sigma)$, $S(\rho\|\sigma) = \infty$.

(S4) * Thm: Klein's ineq

$S(\rho\|\sigma) \geq 0$ with equality iff $\rho = \sigma$

Pf: NC P511–513. Elementary dm, $D(p\|q) \geq 0$.
or Watrous book

Useful matrix analysis:

- If $\sigma = UDU^\dagger$, then $\mathrm{tr}\, \rho \log \sigma = \mathrm{Tr}\, \rho \log (UDU^\dagger) = \mathrm{tr}\, \rho (U \log D\, U^\dagger)$
- Lemma: $\log(\rho_A \otimes \rho_B) = (\log \rho_A) \otimes I_B + I_A \otimes (\log \rho_B)$.

Pf: Let $\rho_A = UDU^\dagger$, $D = \sum_i \lambda_i |i\rangle\langle i|$,

$\rho_B = VEV^\dagger$, $E = \sum_j \mu_j |j\rangle\langle j|$

Then $\log(\rho_A \otimes \rho_B) = \log (U\otimes V)(D\otimes E)(U\otimes V)^\dagger$

$= \log (U\otimes V)\left[\sum_{ij} \lambda_i \mu_j \; |i\rangle\langle i| \otimes |j\rangle\langle j|\right](U\otimes V)^\dagger$

$= U\otimes V \left[\sum_{ij} \log(\lambda_i \mu_j)\; |i\rangle\langle i| \otimes |j\rangle\langle j|\right](U\otimes V)^\dagger$

$= U\otimes V \left[\sum_{ij} (\log \lambda_i + \log \mu_j)\, |i\rangle\langle i| \otimes |j\rangle\langle j|\right](U\otimes V)^\dagger$

$= U\otimes V \begin{bmatrix} \sum_i \log\lambda_i |i\rangle\langle i| \otimes \sum_j |j\rangle\langle j| \\ + \sum_i |i\rangle\langle i| \otimes \sum_j \log \mu_j |j\rangle\langle j| \end{bmatrix} (U\otimes V)^\dagger$

$= (\log \rho_A) \otimes I_B + I_A \otimes (\log \rho_B)$

Def: $S(A:B) = S(A) + S(B) - S(AB)$

(S6) $\boxed{\text{Thm:}}$ $S(A:B) = S(\rho \| \rho_A \otimes \rho_B)$ } opposite for classical $I(X:Y)$

Pf: Recall $\mathrm{tr}_{(12)} M_{12} (N_1 \otimes I_2) = \mathrm{tr}_{(1)} \left((\mathrm{tr}_2 M_{12}) \cdot N_1 \right)$

$$\therefore \; S(\rho \| \rho_A \otimes \rho_B)$$
$$= \mathrm{tr}\, \rho \log \rho - \mathrm{tr}\, \rho \log (\rho_A \otimes \rho_B)$$
$$= -S(AB) - \mathrm{tr}\, \rho \left[(\log \rho_A) \otimes I_B + I_A \otimes (\log \rho_B) \right]$$
$$= -S(AB) - \mathrm{tr}_{(A)} \underbrace{(\mathrm{tr}_B \rho)}_{\rho_A} \cdot \log \rho_A - \mathrm{tr}_B \underbrace{(\mathrm{tr}_A \rho)}_{\rho_B} \cdot \log \rho_B$$
$$= -S(AB) + S(A) + S(B).$$

(S5) $\boxed{\text{Cor:}}$ $S(A:B) \geq 0$, with equality iff $\rho = \rho_A \otimes \rho_B$

From defs: $S(A:B) = S(B) - S(B|A) = S(A) - S(A|B)$

(S8) $\boxed{\text{Cor:}}$ $S(B) \geq S(B|A)$, $S(A) \geq S(A|B)$ w/ equality iff $\rho = \rho_A \otimes \rho_B$

eg

	ρ	$S(A)$	$S(B)$	$S(AB)$	$S(A:B)$	$S(A\|B)$
	$\|\Phi\rangle\langle\Phi\|$	1	1	0	2	-1
$\left[\begin{array}{l} \|\psi\rangle = \sum_i \sqrt{\lambda_i} \|i\rangle\|i\rangle \\ H(\lambda) = \cdots \end{array}\right]$	$\|\psi\rangle\langle\psi\|$	$H(\lambda)$	$H(\lambda)$	0	$2H(\lambda)$	$-H(\lambda)$
	$\frac{1}{2}\|00\rangle\langle 00\| + \frac{1}{2}\|11\rangle\langle 11\|$	1	1	1	1	0

includes both quantum and classical correlations

Further properties of S:

S0 : Invariance under unitaries U, U_A, U_B :

- $S(\rho) = S(U\rho U^\dagger)$
- $S(A:B)_\rho = S(A:B)_{U_A \otimes U_B \, \rho \, U_A^\dagger \otimes U_B^\dagger}$

S1 : Range : $0 \leq S(\rho) \leq \log(\dim(\mathrm{supp}(\rho)))$

"=" iff ρ pure   "=" iff $\rho = \dfrac{I_{\mathrm{supp}(\rho)}}{\dim(\mathrm{supp}(\rho))}$

S7 : Subadditivity (SA) :

$S(AB) \leq S(A) + S(B)$ (from nonneg of $S(A:B)$)

S12 : Entropy of a classical-quantum system:

Let $\rho_{XQ} = \sum_x p(x) \, |x\rangle\langle x|_X \otimes \rho^x_Q$

Then $S(XQ) = H(X) + \sum_x p(x) \, S(\rho_x)$

Pf idea : $$\rho_{XQ} = \begin{bmatrix} \boxed{p_1 \rho_1} & & & 0 \\ & \boxed{p_2 \rho_2} & & \\ & & \ddots & \\ 0 & & & \boxed{} \end{bmatrix}$$

Express eigenvalues of ρ_{XQ} in terms of p_x's & eigenvalues of ρ_x's.

* Special case in which $S(Q|X) := S(XQ) - S(X) = \sum_x p(x) \, S(\rho_x)$ where conditioning has the same interpretation as the classical case.

(S13) QMI of classical-quantum systems

ρ_{XQ} as in (S12)

$$S(X:Q) = \underbrace{S\Big(\sum_x p_x \rho_x\Big)}_{\substack{\text{Entropy of} \\ \text{the average state}}} - \underbrace{\sum_x p_x S(\rho_x)}_{\substack{\text{Average of the} \\ \text{entropies.}}} =: \underbrace{\chi\big(\{p(x), \rho_x\}\big)}_{\substack{\text{Holevo info of} \\ \text{ensemble } \{p(x), \rho_x\}}}$$

Pf: $S(X:Q) = S(X) + S(Q) - S(XQ)$

$$= \cancel{S(X)} + S(Q) - \cancel{H(X)} - \sum_x p(x) S(\rho_x) \qquad \text{from (S12)}$$

$$= S\Big(\sum_x p_x \rho_x\Big) - \sum_x p(x) S(\rho_x).$$

(S10) Concavity. (Mixing increases entropy)

$$S\Big(\sum_x p_x \rho_x\Big) \geq \sum_x p(x) S(\rho_x) \qquad \text{where } p_x \geq 0, \ \sum_x p_x = 1,$$

ρ_x are density matrices

Pf: (S13) and nonneg of QMI.

S9-11 Strong subadditivity (SSA) & equivalent statements

SSA: $\forall \rho_{ABC}$, $S(C) + S(ABC) \leq S(AC) + S(BC)$

NB: C special above.

NB: If $\dim C = 1$, SSA reduces to SA.

$$0 + S(AB) \leq S(A) + S(B)$$

Pf: Method 1: original paper by Lieb & Ruskai 1970

Method 2: NC 11.4.1 + Appendix 6 + Ex

Method 3: Watrous book 5.2.3 (P300-307) ✓

Method 4: Isaac Kim 1210.5190 v3 Sec 2

+ Effros Proc. Natl. Acad. Sci USA 106 (4) 1006-1008 (2009) (Thm 2.2)

1 page, $\frac{1}{2}$ page

Equivalent statements:

(E1) Conditioning reduces conditional entropy

$S(A|BC) \leq S(A|C)$

(E2) Conditional mutual information is nonnegative

$S(A:B|C) := S(A|C) - S(A|BC) \geq 0$

(E3) Monotonicity of QMI with respect to discarding

$S(A:C) \leq S(A:BC)$.

** (E4) Monotonicity of QMI with respect to local operations

$$\underset{I \otimes \mathcal{E}(\rho)}{S(A:C)} \leq \underset{\rho}{S(A:B)}$$

on A — TCP map from B to C — state on AB

Pf of equivalences :

SSA $\Leftrightarrow$ E1 $\Leftrightarrow$ E2 from def of conditional entropy.

E3 $\Leftrightarrow$ $S(A:BC) - S(A:C) \geq 0$

$\Leftrightarrow$ $S(A) + S(BC) - S(ABC) - [S(A) + S(C) - S(AC)] \geq 0$

$\Leftrightarrow$ $S(BC) + S(AC) \geq S(ABC) + S(C)$ (SSA)

NB: No symmetry between A, B, C in E3

but A, B exchangeable in SSA.

E4 $\Rightarrow$ E3 since discarding is a TCP map.

E3 $\Rightarrow$ E4 since any TCP map $\mathcal{E}$ can be realized by:

① Attaching ancilla E in a pure state

② Applying unitary on BE

③ Discarding E'

QMI invariant under ① ②, mono under ③ by E3.

$\therefore$ QMI mono under $I_A \otimes \mathcal{E}_B$.

(S14) Araki-Lieb inequality:

$S(AB) \geq S(A) - S(B)$

Equivalent: $S(AB) \geq S(B) - S(A)$ by exchanging A & B

$\therefore S(AB) \geq |S(A) - S(B)|$

Pf: To prove the AL ineq on any ρ_{AB}

let $|\psi\rangle_{ABC}$ purify ρ_{AB}, ie $tr_C |\psi\rangle\langle\psi| = \rho_{AB}$.

- By purity of $|\psi\rangle_{ABC}$, $S(AB) = S(C)$, $S(A) = S(BC)$

$$\therefore S(B) + S(AB) = S(B) + S(C)$$
$$\underset{SA}{\geq} S(BC) = S(A)$$

Cor: (a) $|S(AB) - S(A)| \leq S(B)$

(b) $|S(A:BC) - S(A:C)| \leq 2S(B)$

Interpretation: adding or removing sys B changes the vN entropy and QMI at most by $S(B)$ & $2S(B)$ respectively.

Pf (a) follows from AL $S(A) - S(AB) \leq S(B)$
SA $S(AB) - S(A) \leq S(B)$

(b) $|S(A:BC) - S(A:C)|$

$$= |[\cancel{S(A)} + S(BC) - S(ABC)] - [\cancel{S(A)} + S(C) - S(AC)]|$$

$$= |S(BC) - S(C) + S(AC) - S(ABC)|$$

$$\leq |S(BC) - S(C)| + |S(AC) - S(ABC)| \underset{(a)}{\leq} 2S(B)$$

§15 Continuity

Let $\rho, \sigma \in \mathcal{B}(\mathbb{C}^d)$, $\|\rho - \sigma\|_1 \leq \varepsilon$

Then $|S(\rho) - S(\sigma)| \leq \varepsilon \log d + h(\varepsilon)$ Fannes Inequality

If $\mathbb{C}^d = \underset{A}{\mathbb{C}^{d_A}} \otimes \underset{B}{\mathbb{C}^{d_B}}$,

Then $\left| S(A|B)_\rho - S(A|B)_\sigma \right| \leq 4\varepsilon \log d_A + 2h(\varepsilon)$

Fannes-Alicki Inequality