CO781 / QIC 890:

Theory of Quantum Communication

Prelude to topics 4-6

Quantum entropies and some important properties

This lecture and set of slides are highlights from the lecture notes for the F2016 offering, lecture 10 (relinked in the F2020 website).

Please read through the notes offline.

Important conventions (I)

Recall the von Neumann entropy $S(\rho)$ is the Shannon entropy of the spectrum.

Let $\rho = U D U^\dagger$, $\log \rho = U (\log D) U^\dagger$

spectral decomp

So: $S(\rho) := -\mathrm{tr}\, D \log D = -\mathrm{tr} \begin{bmatrix} \lambda_1 & & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_d \end{bmatrix} \begin{bmatrix} \log \lambda_1 & & & 0 \\ & \log \lambda_2 & & \\ & & \ddots & \\ 0 & & & \log \lambda_d \end{bmatrix}$

$= -\mathrm{tr}\, U D U^\dagger U (\log D) U^\dagger = -\mathrm{tr}\, \rho \log \rho$

cyclic property of trace

Important conventions (II)

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

Definition: Conditional entropy (on a state on AB)

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

Definition: Quantum mutual information (on a state on AB)

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

Similarities:

Quantum	Classical
N/A	$H(X\|Y) := \sum_y p(y) H(X\|Y=y)$
$S(A\|B) := S(AB) - S(B)$ chain rule: $S(AB) = S(B) + S(A\|B)$	$H(X\|Y) = H(XY) - H(Y)$ $H(XY) = H(Y) + H(X\|Y)$
$S(A:B) := S(A) + S(B) - S(AB)$ Klein's inequality (see notes) $S(A:B) \geqslant 0$ "=" iff $\rho = \rho_A \otimes \rho_B$ subadditivity: $S(AB) \leqslant S(A) + S(B)$ conditioning reduces entropy: $S(A:B) = S(B) - S(B\|A)$ so, $S(B) \geqslant S(B\|A)$ sym(A<->B)	$I(X:Y) = H(X) + H(Y) - H(XY)$ $I(X:Y) \geqslant 0$ "=" iff X,Y indep $H(XY) \leqslant H(X) + H(Y)$ conditioning reduces entropy: $H(Y) \geqslant H(Y\|X)$

Examples:

ρ	S(A)	S(B)	S(AB)	S(A|B) S(AB) - S(B)	S(A:B) S(A) + S(B) - S(AB)
$\left(\frac{I}{2}\right)_A \otimes \|0\rangle\langle 0\|_B$	1	0	1	1	0
$\|0\rangle\langle 0\|_A \otimes \left(\frac{I}{2}\right)_B$	0	1	1	0	0
$\frac{1}{2}\|00\rangle\langle 00\| + \frac{1}{2}\|11\rangle\langle 11\|$	1	1	1	0	1
$\frac{1}{\sqrt{2}}(\|00\rangle+\|11\rangle)$ $\;\;\|\Phi\rangle\langle\Phi\|$	1	1	0	-1	2

* have B, do we know everything about A?
not if we measure A in X-basis ...

* quantum conditional entropy can be negative
NOT a convex combination of entropies ...

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

Special properties for classical-quantum systems

1. Entropy of a classical-quantum system:

each state on the classical system X is projector onto a basis states

each state on the quantum system Q is labelled by one x, arbitrary otherwise

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

same format as one drawn of an ensemble of states

$\mathcal{E} = \{ p(x), \rho_x \}$

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

Shannon entropy of classical part

average over X

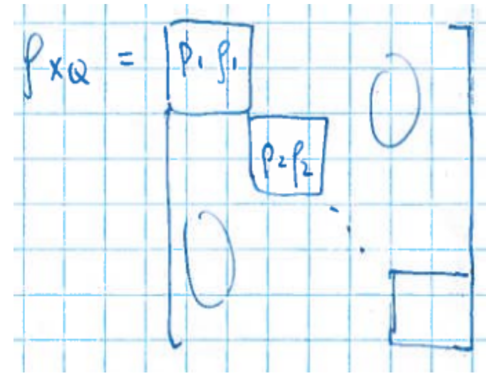
von Neumann entropy of Q given x

* 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.

on X a classical system

Proof: $\rho_{XQ} = \sum_i p_i |i\rangle\langle i|_X \otimes \rho_{iQ}$



$|i=1\rangle$

$|i=2\rangle$

...

If ρ_1 has eigenvalues $\lambda_{11}, \lambda_{12}, \ldots$

ρ_2 has eigenvalues $\lambda_{21}, \lambda_{22}, \ldots$

then ρ has eigenvalues $p_1\lambda_{11}, p_1\lambda_{12}, \ldots$
$p_2\lambda_{21}, p_2\lambda_{22}, \ldots$

$$S(\rho) = -\sum_{ij} p_i \lambda_{ij} \log(p_i \lambda_{ij})$$

$$= -\sum_{ij} p_i \lambda_{ij} (\log p_i + \log \lambda_{ij})$$

$$= -\sum_{ij} p_i \lambda_{ij} \log p_i - \sum_{ij} p_i \lambda_{ij} \log \lambda_{ij}$$

$$= -\sum_{ij} p_i \lambda_{ij} \log p_i - \sum_{ij} p_i \lambda_{ij} \log \lambda_{ij}$$

$$= \underbrace{-\sum_i p_i \log p_i}_{H(X)} + \sum_i p_i S(\rho_i)$$

Special properties for classical-quantum systems

2. Quantum mutual information of a classical-quantum system:

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

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

$$\begin{aligned}
\text{Pf:} \quad S(X:Q) &= S(X) + S(Q) - S(XQ) \\
&= \cancel{S(X)} + S(Q) - \cancel{H(X)} - \sum_x p(x) S(\rho_x) \qquad \text{by part 1} \\
&= S\Big(\sum_x p_x \rho_x\Big) - \sum_x p(x) S(\rho_x).
\end{aligned}$$

Special properties for classical-quantum systems

2. Quantum mutual information of a classical-quantum system:

$$\rho_{XQ} = \sum_x p(x)\, |x\rangle\langle x|_X \otimes \rho_{x\,Q}$$

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

Corollary for arbitrary state

Mixing increases entropy (concavity of entropy)

If $p_x \geq 0$, $\sum_x p_x = 1$, ρ_x are density matrices

then $S\Big(\sum_x p_x \rho_x\Big) \geq \sum_x p(x) S(\rho_x)$

Proof: since S(X:Q) above non-negative.

The most important entropic inequality in q info theory:

Strong subadditivity (SSA) and 4 more equivalent statements

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

NB. System C is special.

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

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

Proofs (several listed in the notes, possible term project)

The most important entropic inequality in q info theory:

Strong subadditivity (SSA) and 4 more equivalent statements

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

Equivalent statements:

(E1) Conditioning reduces conditional entropy

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

(E2) Conditional mutual information is nonnegative

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

E1, E2 are basic rewritings of SSA.

The most important entropic inequality in q info theory:

Strong subadditivity (SSA) and 4 more equivalent statements

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

Further equivalent statements:

E3 Monotonicity of QMI with respect to discarding

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

Proof (E3 <=> SSA):

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)

The most important entropic inequality in q info theory:

Strong subadditivity (SSA) and 4 more equivalent statements

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

Further equivalent statements:

(E3) Monotonicity of QMI with respect to discarding

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

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

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

I: on A; $\mathcal{E}$: TCP map from B to C; ρ: state on AB

E4 says that local processing does not increase QMI, so, E4 is quantum analogue of data processing inequality.

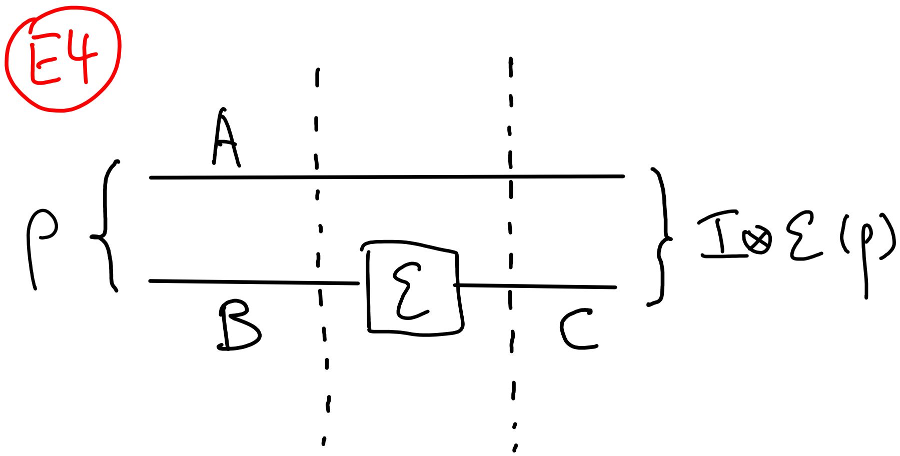
Proof (E3<=>E4): Assume E4 is true.
Applying E4 with B=CD, {\cal E}=partial trace of D gives E3.

Proof (E3<=>E4): Assume E3 is true.

Stinespring dilation
unitary representation

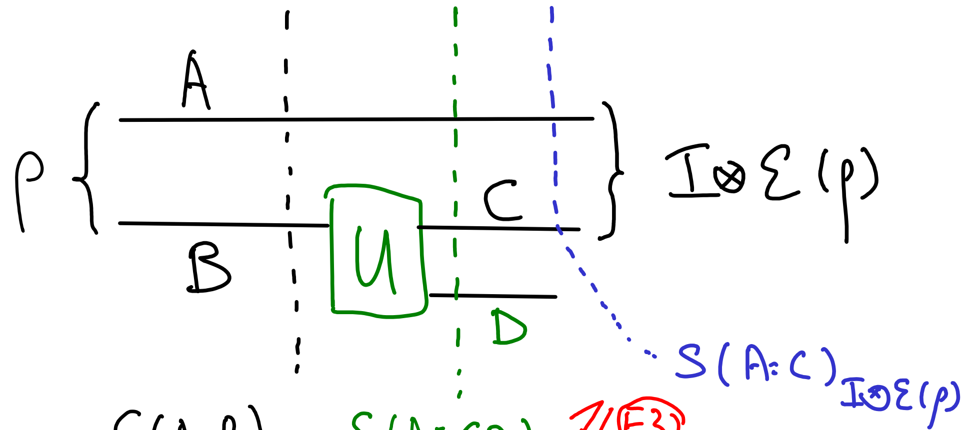
First examine what E4 says:

Now express $\mathcal{E}$ as isometric extension



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

E4 says $\mathcal{E}$ cannot ↑ QMI



$$S(A:B)_\rho = S(A:CD)_{I\otimes U\rho I\otimes U^\dagger} \quad // \text{E3}$$

QMI inv under local unitaries.

So, if E3 holds, E4 also holds.

How much do the entropy and QMI change
if a system B is added or removed?

The Araki-Lieb inequality

(a) $| S(AB) - S(A) | \leqslant S(B)$

(b) $| S(A{:}BC) - S(A{:}C) | \leqslant 2\, S(B)$

Proof (see notes)

How much does the entropy change if the underlying state changes a little?

Fannes inequality (Continuity of S)

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

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

dim dependence

binary entropy function

What about S(A:B) = S(A) + S(B) - S(AB)?

Can use Fannes inequality on each term ... suboptimal if dB large

Fannes-Alicki inequality (Continuity of conditional entropy)

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

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

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

indep of dB

Then, S(A:B) = S(A) - S(A|B) continuous (so is quantum capacity)!