Lecture 4:

Recall: von Neumann entropy S is defined on a state (say ρ) in a quantum system (say Q).

Qn: How much can S change when part of Q is removed?

More precisely, let $Q=Q_1Q_2$. Removing Q_2 results in a state $tr_{Q2}\,\rho$ in Q_1. How's its von Neumann entropy compared to $S(Q)_\rho$? Note it's equivalent to ask how much S can change when a system T is added to Q with TQ in any arbitrary joint state.

Likewise, how much can the quantum mutual information (QMI) change when a system is added/removed? What about I_{acc} and χ?

Starting from the ensemble $\{p_x, \rho_x\}$ on Q, removing Q_2 induces an ensemble $\{p_x, tr_{Q2}\,\rho_x\}$ on Q_1. Similarly for adding a system.

Intuitively, the change should be commensurate with the size of the system added/removed.

That's true for S, QMI, and χ.
Application: forward communication bounds given ebits and back communication.

Intuition fails for I_{acc}, giving an effect called locking.

Theorem 1 [Araki-Lieb inequality]: $S(AB) \geq S(A) - S(B)$

NB 1. The classical analogue is true but uninteresting:
$H(AB) \geq H(A) \geq H(A) - H(B)$.

NB 2. Cf SA: $S(AB) \leq S(A) + S(B)$.

NB 3. Let size A >> size B. The Araki-Lieb ineq + SA implies $|S(AB) - S(A)| \leq S(B)$. So adding or subtracting a system B changes S at most by S(B).

NB4. The Araki-Lieb hold when A and B are interchanged. Thus, it's equivalent to $S(AB) \geq |S(A)-S(B)|$.

Theorem 1 [Araki-Lieb inequality]: $S(AB) \geq S(A) - S(B)$

Proof:

(1) Go to the Church of larger Hilbert space

There is a system C and a pure state $|\psi\rangle$ on ABC s.t. $tr_C\,|\psi\rangle\langle\psi| = \rho_{AB}$. We say that C "purifies" AB.

(2) By purity of ABC, S(AB) = S(C), S(A) = S(BC).

(3) Apply SA to BC:
$S(B) + S(C) \geq S(BC)$

Same as $S(B) + S(AB) \geq S(A)$

Same as what we want.

Theorem 2: Let τ be a state on ABC and $\rho = tr_C\,\tau$.
$|\,S(A:BC)_\tau - S(A:B)_\rho\,| \leq 2\,S(C)$

NB. If Alice and Bob are to increase their QMI mutual by sending qubits back and for, the above says that n qubits of communication (total in both directions) can at most increase the QMI by 2n. This is attained if they use every qubit of communication to share an ebit.

Theorem 2: Let τ be a state on ABC and $\rho = tr_C\,\tau$.
$|\,S(A:BC)_\tau - S(A:B)_\rho\,| \leq 2\,S(C)$

Proof:

$S(A:BC)_\tau = S(A) + S(BC) - S(ABC)$
$S(A:B)_\rho = S(A) + S(B) - S(AB)$
} evaluated on the reduced states

evaluated on the same state

tracing C from the state on BC gives the state on B

etc

Thus $|\,S(A:BC) - S(A:B)\,|$
$\leq |S(BC) - S(B)| + |S(ABC) - S(AB)|$
$\leq 2\,S(C)$ from previous slide

Corollary 3:
Let $\mathscr{E} = \{p_x, \rho_x\}$ and $\mathscr{F} = \{p_x, \tau_x\}$ be two ensembles where each τ_x lives in systems BC, and $\rho_x = \mathrm{tr}_C\, \tau_x$. Then, $|\chi(\mathscr{F}) - \chi(\mathscr{E})| \leq 2\, S(C)$.

Proof: Define $\tau = \sum_x p_x\, |x\rangle\langle x|_A \otimes \tau_{x\,BC}$
$\rho = \sum_x p_x\, |x\rangle\langle x|_A \otimes \rho_{x\,B}$

Then, applying Theorem 2,

$$| S(A:BC)_\tau - S(A:B)_\rho | \leq 2\, S(C)$$
$$\| \qquad\qquad \|$$
$$\chi(\mathscr{F}) \qquad \chi(\mathscr{E})$$

NB this says Holevo info can only increase by 2 S(C) when C is communicated, even in the presence of shared entanglement, giving an extension to Holevo's bdd.

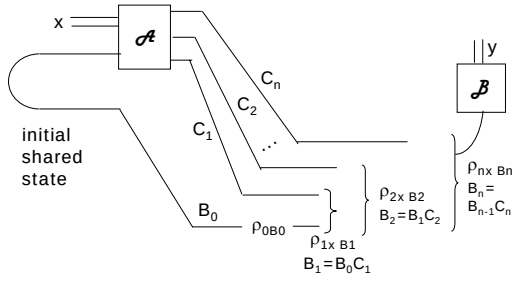
Theorem 4:

Suppose Alice and Bob share an arbitrary finite dim state of their choice, and Alice can send n qubits to Bob. She can communicate at most 2n bits to Bob.

In particular, ∞ ebits + n qbit$_\rightarrow$ $\geq \beta$ cbit$_\rightarrow$ only if $\beta \leq 2$.

The most general communication protocol :

Alice performs an encoding operation $\mathscr{A}$ which acts on the intended message x, perhaps some ancillas, and her half of the stated with Bob.



So with probability p_x (that the message is x) Bob is given the state $\rho_{nx\,Bn}$ which he measures to get y. Denote his ensemble at the jth step by $\mathscr{E}_j = \{p_x, \rho_{jx\,Bj}\}$.

His information gained on X:

$I(X:Y) \leq \chi(\mathscr{E}_n)$
$\leq \chi(\mathscr{E}_{n-1}) + 2$ by corollary 3
$\leq \chi(\mathscr{E}_{n-2}) + 4$ by corollary 3
...
$\leq \chi(\mathscr{E}_0) + 2n$ by corollary 3

But $\mathscr{E}_0$ only has 1 state ρ_{0B0} independent of x, so, $\chi(\mathscr{E}_0) = 0$

Hence at most 2n bits can be communicated.

Theorem 4:

Suppose Alice and Bob share an arbitrary finite dim state of their choice, and Alice can send n qubits to Bob. She can communicate at most 2n bits to Bob.

In particular, ∞ ebits + n qbit$_\rightarrow$ $\geq \beta$ cbit$_\rightarrow$ only if $\beta \leq 2$.

In the presence of free ebits, 2 cbits = 1 qbit, since the above is equiv to:

Theorem 5:

Suppose Alice and Bob share an arbitrary finite dim state of their choice, and Alice can send n qubits to Bob. She can communicate at most n qubits to Bob.

In particular, ∞ ebits + n qbit$_\rightarrow$ $\geq \gamma$ qbit$_\rightarrow$ only if $\gamma \leq 1$.

How much can back communication help?

Theorem 6:

Suppose Alice is allowed to send n_A qubits to Bob and Bob n_B qubits back, in any order. Then, Alice can communicate at most $n_A + n_B$ bits to Bob.

i.e., n_A qbit$_\rightarrow$ + n_B qbit$_\leftarrow$ $\geq \beta$ cbit$_\rightarrow$ only if $\beta \leq n_A + n_B$.

Proof:

Again, define Bob's state as $\rho_{jx\,Bj}$ after the jth qubit of communication, and the ave state $\rho_j = \sum_x p_x\, \rho_{jx\,Bj}$.

$I(X:Y) \leq \chi(\mathscr{E}_n) \leq S(\rho_n) \leq S(\rho_{n-1}) + 1 \leq \ldots \leq n_A + n_B$

How much can back communication help?

Theorem 6:

Suppose Alice is allowed to send n_A qubits to Bob and Bob n_B qubits back, in any order. Then, Alice can communicate at most n_A+n_B bits to Bob.

i.e., n_A qbit$_{\rightarrow}$ + n_B qbit$_{\leftarrow}$ $\geq \beta$ cbit$_{\rightarrow}$ only if $\beta \leq n_A + n_B$ and if $\beta \leq 2\, n_A$

This theorem assumes no share state between Alice and Bob but Theorem 4 clearly applies.

What about I_{acc}?

Last time, example 3:

Let $\mathscr{E} = \{p_{xt}, \rho_{xt}\}$ ⟵ use composite label XT.

where $\rho_{xt} = U^t |x\rangle\langle x| U^{\dagger t}$, $t \in \{0,1\}$, $x \in \{0,\cdots,n-1\}$,

$p_{xt} = 1/2n$, $U|x\rangle = \sum_y \omega^{xy}|y\rangle$ for $\omega = n^{th}$ root of unity

It was asserted that $\chi(\mathscr{E}) = ½ \log n$.

One extra bit t increases I_{acc} by $1+½ \log n$!

Let $\mathscr{F} = \{p_{xt}, \tau_{xt}\}$

where $\tau_{xt} = U^t |x\rangle\langle x| U^{\dagger t} \otimes |t\rangle\langle t|$

It is clear that $\chi(\mathscr{F}) = 1+\log n$.

Intuitively, the extra bit can't carry $1+½ \log n$ bits; rather it unlocks I_{acc} in the $\log n$ existing qubits.

Unlike S(A), S(A:B), and χ, I_{acc} can change much more than the size of the additional system.

Also note that this is nonclassical. In fact, classical mutual info cannot increase by more than H(C) when C is added.

The classical analogue of the ensemble is for Alice to send either $x \in \{0,\cdots,n-1\}$ or $\pi(x)$ where $\pi \in S_n$ is a permutation with a fixed point. If Bob gets y, then x = y or $\pi^{-1}(y)$ so H(XT|Y) = 1, and I(XT:Y) = log n (the missing bit concerning x is perfectly correlated with the bit t). It changes to I(XT:Y) = 1+log n if t is given.

How to prove $I_{acc}(\mathscr{E}) = ½ \log n$?

Note there's no closed form expression for I_{acc}.

Qn: how hard is it to perform the optimization in expression for I_{acc}?

Here, measuring along $\{|x\rangle\}$ or $\{U|x\rangle\}$ at random gives $I_{acc} \geq ½ \log n$. Turns out $I_{acc} \leq ½ \log n$ also (thus =).

Observation:

WLOG the optimal measurement in the expression for I_{acc} has only rank-1 measurement operators.

Reason: for any measurement $\mathscr{M}$ with a measurement operator $M_y = \sum_{k=1}^{r} \lambda_k |\alpha_k\rangle\langle\alpha_k|$, consider $\mathscr{M}'$ which has M_y replaced by r measurement operators $M_{yk} = \lambda_k |\alpha_k\rangle\langle\alpha_k|$

$\mathscr{M}$ can be implemented by first performing $\mathscr{M}'$ and then coarse-graining the outcomes {yk} to y. Since mutual info is not increased by the coarse graining (local), $\mathscr{M}'$ yields no less info than $\mathscr{M}$.

Proof ideas behind $I_{acc}(\mathscr{E}) = ½ \log n$:

Let the optimal measurement operators be $M_y = \lambda_y |\alpha_y\rangle\langle\alpha_y|$.

$I(XT:Y) = H(XT) - H(XT|Y)$

$= \sum_y p(y)\, H(XT|Y=y)$

$I(XT:Y) \leq H(XT) - \min_y H(XT|Y=y)$

Proof ideas behind $I_{acc}(\mathscr{E}) = \frac{1}{2} \log n$:

$I(XT:Y) \leq H(XT) - \min_y H(XT|Y=y)$ and $M_y = \lambda_y |\alpha_y\rangle\langle\alpha_y|$

(1) $p(y) = \mathrm{tr}\,(\lambda_y |\alpha_y\rangle\langle\alpha_y| \, I/n) = \lambda_y/n$

(2) $p(xt|y) = p(xt \text{ and } y) / p(y)$ ← average state

$= \mathrm{tr}\,(\lambda_y |\alpha_y\rangle\langle\alpha_y| \, U^t |x\rangle\langle x| \, U^{\dagger t} \, 1/2n) \,/\, (\lambda_y/n)$

$= \frac{1}{2} |\langle\alpha_y|U^t|x\rangle|^2$

$H(XT|Y=y) = -\sum_{xt} \frac{1}{2} |\langle\alpha_y|U^t|x\rangle|^2 \log \frac{1}{2} |\langle\alpha_y|U^t|x\rangle|^2$

$= -\sum_{xt} \frac{1}{2} |\langle\alpha_y|U^t|x\rangle|^2 \log \frac{1}{2}$ ← $= 1$

$+ \frac{1}{2} \sum_t (-1) \sum_x |\langle\alpha_y|U^t|x\rangle|^2 \log |\langle\alpha_y|U^t|x\rangle|^2$

$H_t(|\alpha_y\rangle)$: entropy of outcome when measuring $|\alpha_y\rangle$ along the basis $U^t|x\rangle$. Note Meas op and state swapped.

Proof ideas behind $I_{acc}(\mathscr{E}) = \frac{1}{2} \log n$:

$I(XT:Y) \leq H(XT) - \min_y H(XT|Y=y)$

$\leq \log n + \cancel{1} - \cancel{1} - \min_{|\alpha\rangle} \frac{1}{2} \sum_t H_t(|\alpha\rangle) \leq \frac{1}{2} \log n$

where $H_t(|\alpha\rangle)$: entropy of outcome when measuring $|\alpha\rangle$ along the basis $U^t|x\rangle$.

In general, for k bases (t=0,1,⋯,k-1), a lower bound to

$\min_{|\alpha\rangle} \sum_{t=0}^{k-1} H_t(|\alpha\rangle)$

is called an entropic uncertainly inequality. This quantifies how incompatible the basese are.

Maassen & Uffink (PRL **60** 1103, 1988) proved that for 2 conjugate bases in n-dims, $\forall\, |\alpha\rangle$ $H_0(|\alpha\rangle) + H_1(|\alpha\rangle) \geq \log n$.

Can we further amplify the effect?

Are there k bases s.t.

- without knowing the basis, $I_{acc} \leq (1/k) \log n$?
- knowing the basis, $I_{acc} = \log k + \log n$?

Unfortunately, the natural guess of taking k MUBs doesn't work – can find measurement giving more I_{acc}.

PS MUBs = mutually unbiased bases. Each state in a basis has overlap-squared = 1/n with all other state in all other bases.

Can we further amplify the effect?

We can show that choosing

$k=(\log n)^3$, $\log n \geq (16/c\,\varepsilon) \log (20/\varepsilon)$, $n \geq 7$, $\varepsilon < 1/5$

we can find k bases such that $\forall\, |\alpha\rangle$

$1/k \sum_{t=1}^{k} H_t(|\alpha\rangle) \geq (1-\varepsilon) \log n - 3$

Essentially, n has to be large, the above entropic ineq is more loose than the (k-1)/k log n previously seek.

Still, $I_{acc}(\mathscr{E}) \leq 3 + \varepsilon \log n$ where $\mathscr{E}$ is the uniform ensemble of states in the k bases

$I_{acc}(\mathscr{T}) = \log n + \log k = \log n + 3 \log \log n.$

So, $I_{acc}(\mathscr{E}) \,/\, I_{acc}(\mathscr{T})$ is vanishing, so is "size of the extra system (key)" / $I_{acc}(\mathscr{T})$.