Lecture 4

Conditional quantum mutual information is a fundamental entropic function of a tripartite quantum state ρ_{ABC}, defined as

$$I(A;B|C)_\rho = H(AC)_\rho + H(BC)_\rho - H(C)_\rho - H(ABC)_\rho$$

An important theorem in QIT is strong subadditivity of quantum entropy:

$$I(A;B|C)_\rho \geq 0 \qquad \forall \text{ states } \rho_{ABC}$$

Many different proofs of this entropy inequality are now known.

In fact, it is possible to show that strong subadditivity is equivalent to monotonicity of quantum relative entropy. So they are both fundamental...

Consider the conditional mutual information of a classical distribution P_{XYZ} for RVs. X, Y, Z.

Working w/ the definition, one can show that

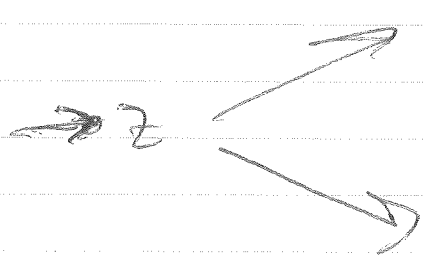
$$I(X;Y|Z) = D(P_{XYZ} \| P_{X|Z} P_{Y|Z} P_Z)$$

where P_Z is the marginal of P_{XYZ}

& $P_{X|Z}$, $P_{Y|Z}$ are conditional distributions

i.e., $P_{X|Z} = \frac{P_{XZ}}{P_Z}$ $\quad P_{Y|Z} = \frac{P_{YZ}}{P_Z}$

the distribution $P_{X|Z} P_{Y|Z} P_Z$ is a short Markov chain, meaning that we can understand it in terms of the following diagram:



that is, Z is the "common cause" of X + Y

Given a realization z of R.V. Z, $P_{X|Z=z}$ & $P_{Y|Z=z}$ are independent.

Writing CMI as

$$D(P_{XYZ} \| P_{X|Z} P_{Y|Z} P_Z)$$

we can think of it as a "relative entropy distance" from P_{XYZ} to the short Markov chain distribution $P_{X|Z} P_{Y|Z} P_Z$

Is there a quantum notion of this idea? There has been work in QIT on this topic since 2003, but we will focus on recent developments since 2014.

The recent idea has been to focus on the notion of recoverability. That is, a different way to characterize a Markov dist. is via the notion of recoverability:

$p(x|z)\, p(y|z)\, p(z)$ Suppose that we lose access to system X or R.V. X. Then the marginal is described via a partial trace (sum over x)

$$\sum_x p(x|z)\, p(y|z) p(z) = p(y|z)\, p(z)$$

How could we then get X back,

such that the resulting distribution is the same as the original?

Just send z through the channel $p(x|z)$ & the resulting overall distribution will be

$$p(x|z)\,p(y|z)\,p(z)$$

So Markov dist.s are perfectly recoverable & we can think of $I(X;Y|Z)$ as measuring how recoverable is X from Z alone. The notion is robust in the sense that if $I(X;Y|Z) \leq \varepsilon$ then P_{XYZ} is ε-close to Markov dist.

Via an inequality known as the Pinsker inequality, one can show that

$$I(X;Y|Z) \geq c \left\| P_{XYZ} - P_{X|Z} P_{Y|Z} P_Z \right\|_1^2$$

where $\|\cdot\|_1$ is the classical trace norm.

How to generalize these ideas to the quantum world? We can use the notion of recoverability...

Very recently, Fawzi & Renner proved the following lower bound for conditional mutual information in terms of a recoverability quantity:

$$I(A;B|C) \geq -\log F(\rho_{ABC}, R_{C\to AC}(\rho_{BC}))$$

where R is a recovery map.

Interpret the lower bound as system A is lost & then we use C to get a state $R_{C\to AC}(\rho_{BC})$ which is compared to ρ_{ABC}

If $I(A;B|C)$ is small, then the fidelity of recovery is large (the largest that the fidelity of recovery can be is 1, in which case ρ_{ABC} is perfectly recoverable).

Recoverability is another way to characterize classicality of a quantum state. If we can recover A well from C, then we can keep doing this over & over again to produce many copies of A. Due to the no-cloning theorem

this should not be possible for general quantum states.

Fawzi & Renner proved that

$R_{C\to AC}$ has a particular form

of 1) a unitary on C

2) the Petz channel on $C\to AC$, i.e.,

$$\rho_{AC}^{1/2}\left[\rho_C^{-1/2}(\cdot)_C\rho_C^{-1/2}\otimes I_A\right]\rho_{AC}^{1/2}$$

3) a unitary on AC

From this result, we cannot conclude anything about the form of the unitaries.

From a new result in arXiv:1505.04661, we can conclude that

1') unitary on C has the form ρ_C^{-it}

3') unitary on AC has the form ρ_{AC}^{it}

for some $t\in\mathbb{R}$

$\rho_C+\rho_{AC}$ must be positive definite.

From these results, we could also just optimize over all recovery maps to get

$$I(A;B|C) \geq -\log \sup_{R_{C\to AC}} F(\rho_{ABC}, R_{C\to AC}(\rho_{BC}))$$

call this the "fidelity of recovery"

& abbreviate as $F(A;B|C)$

can then call

$$-\log F(A;B|C) = I_F(A;B|C)$$

this quantity obeys many of the same properties as CMI.

both proofs of the lower bounds are somewhat complicated, w/ the first relying on advanced concepts from representation theory & the second relying on the theory of complex interpolation.

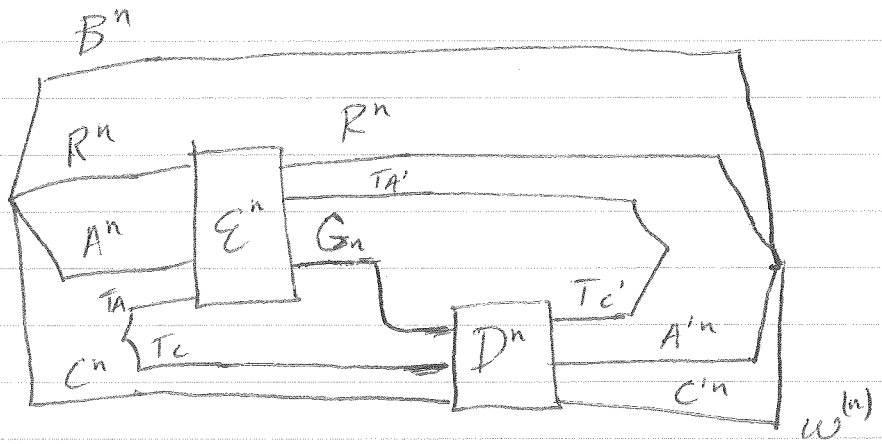
We will discuss a proof based on the quantum state redistribution protocol & a property of fidelity of recovery. (and so we learn a new QIT protocol along the way)

The objective of quantum state redistribution is to use as little noiseless q. comm. & entanglement as possible in order to send one system from a sender to receiver. Many other protocols emerge as a special case of this protocol.

In more detail, let ψ_{BRAC} be a four-party pure state & suppose that we have n copies of the state where n is a large number. An inactive, reference party possesses the B systems, the sender possesses the RA systems, & the receiver possesses the C systems.

The goal is to transmit the A systems from sender to receiver.

A protocol for state redistribution has the following form:



it consumes entanglement in $T_A T_C$,
sends G_n over a q. comm. channel,
& generates entanglement in $T_{A'} T_{C'}$.

Also, an (n, R, ε) protocol has

rate $R = \frac{\log_2 |G_n|}{n}$ qubits per copy of state

&

$$F\left(\Psi_{BRAC}^{\otimes n}, W^{(n)}_{B^n R^n A'^n C'^n}\right) \geq 1 - \varepsilon$$

can prove a converse that

achievable rates are necessarily larger than $\frac{1}{2} I(A;B|C)$

How to achieve this? use the idea of random coding again (quantum style)

Suppose we act w/ a random unitary U on the A^n systems & the U has 3 output systems, called $\hat{A}_1, \hat{A}_2, \& \hat{A}_3$.

Thinking of the typical projected A^n systems, the size of the A^n systems is $\approx 2^{nH(A)}$

Now one can show that for a randomly selected U, on average the state after the U satisfies

$$\mathrm{Tr}_{\hat{A}_2\hat{A}_3 C^n}\left\{ U_{A^n\to\hat{A}_1\hat{A}_2\hat{A}_3}\left(\psi_{BRAC}^{\otimes n}\right) U^{\dagger}_{A^n\to\hat{A}_1\hat{A}_2\hat{A}_3}\right\}$$

$$\approx \pi_{\hat{A}_1}\otimes \psi_{BR}^{\otimes n} \qquad (*)$$

if $|\hat{A}_1| \approx 2^{n\frac{1}{2}I(A;C)}$

$\pi_{\hat{A}_1}$ is maximally mixed state

"decoupling theorem"

Similarly, one can show that on average

$$\mathrm{Tr}_{\hat{A}_1\hat{A}_2R^n}\left\{ U_{A^n\to\hat{A}_1\hat{A}_2\hat{A}_3}\left(\psi_{BRAC}^{\otimes n}\right) U^{\dagger}_{A^n\to\hat{A}_1\hat{A}_2\hat{A}_3} \right\}$$

$$\approx \pi_{\hat{A}_3}\otimes \psi_{BC}^{\otimes n} \qquad (**)$$

$$\text{if } |\hat{A}_3| \approx 2^{n\frac{1}{2}I(A;R)}$$

due to the properties of entropy for pure states, one can show that

$$H(A) - \tfrac{1}{2}I(A;C) - \tfrac{1}{2}I(A;R)$$

$$= \tfrac{1}{2}I(A;B|C) = \tfrac{1}{2}I(A;B|R)$$

the decoupling theorem guarantees the existence of a U that realizes both decouplings simultaneously (a bi-decoupling theorem)

so now let's suppose we have such a U

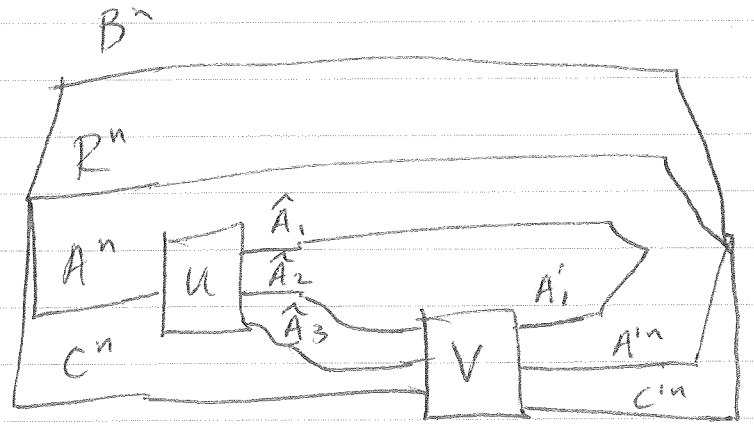
~~Applying~~ Inspecting (ψ), we see that a purification of the RHS is

$$\Phi_{\hat{A}_1 A_1'} \otimes \psi^{\otimes n}_{BRA'C'}$$

while the LHS is purified by

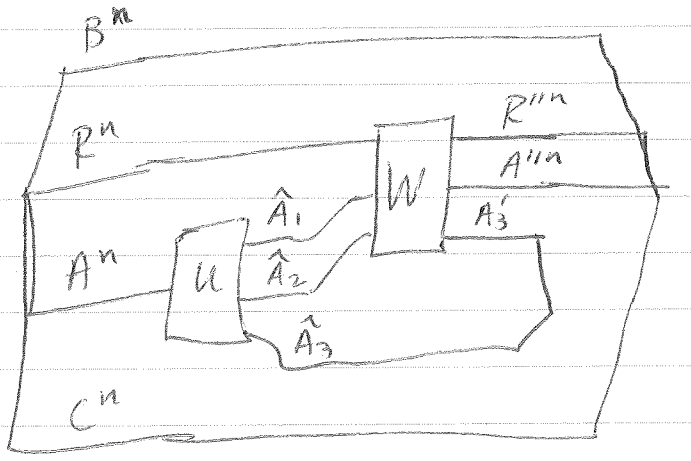
$$U_{A^n \to \hat{A}_1 \hat{A}_2 A_3} |\psi\rangle^{\otimes n}_{BRAC}$$

Uhlmann's theorem guarantees the existence of an isometry $V_{\hat{A}_2 \hat{A}_3 C^n \to A_1' A'^n C'^n}$ such that



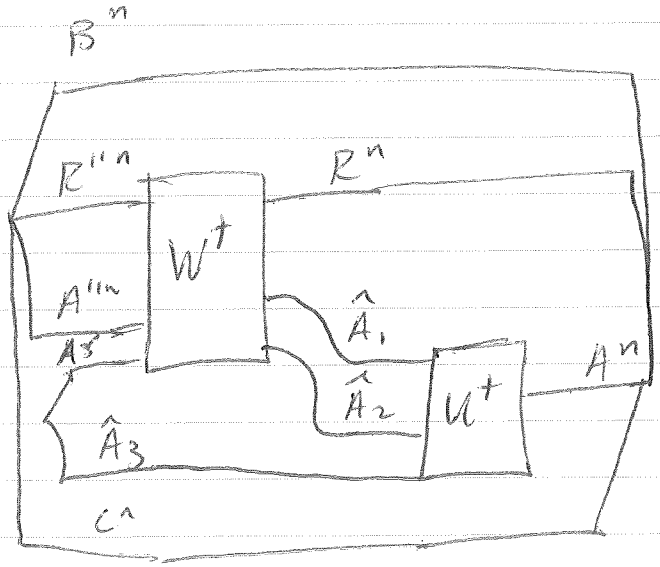
fidelity is high

Similarly, from (**) we can conclude $\exists\ W_{\hat{A}_1\hat{A}_2 R^n \to A_3' R''^n A''^n}$ such that

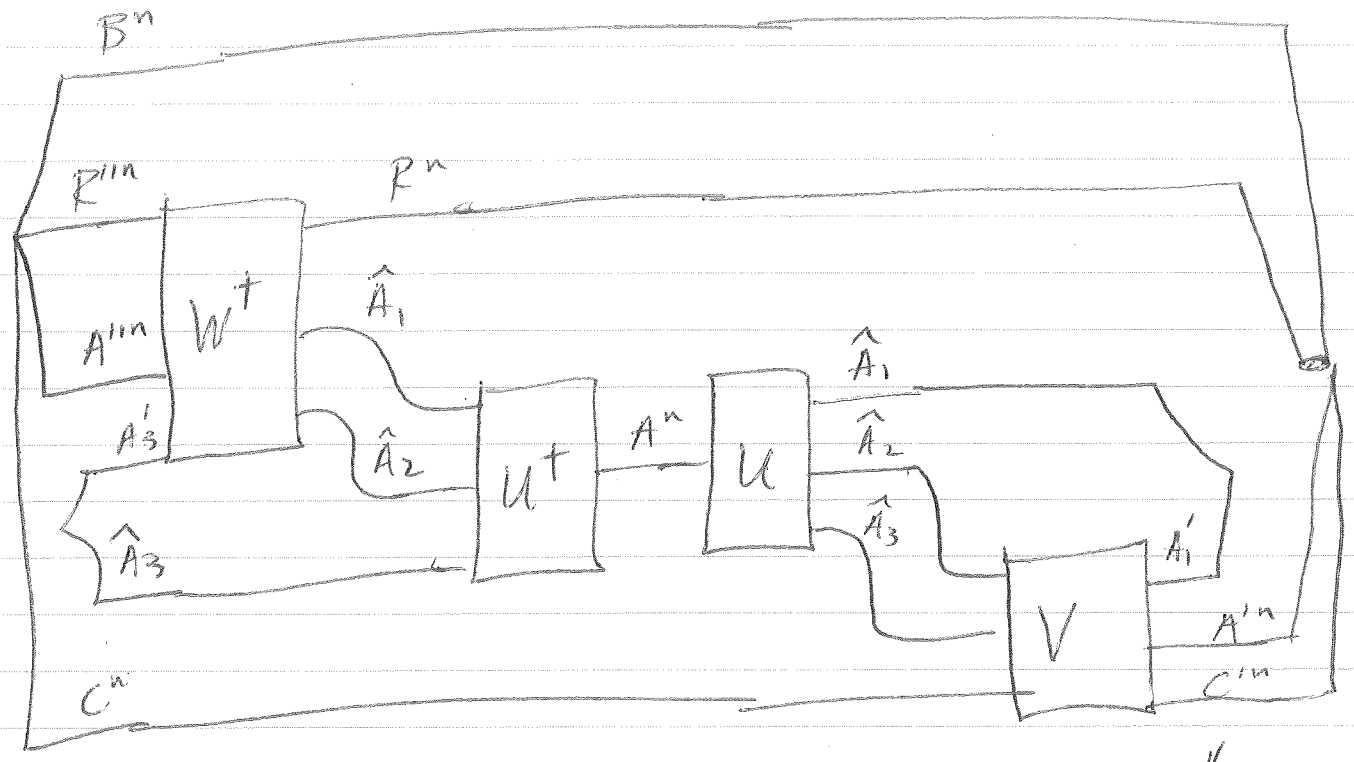


fidelity is high

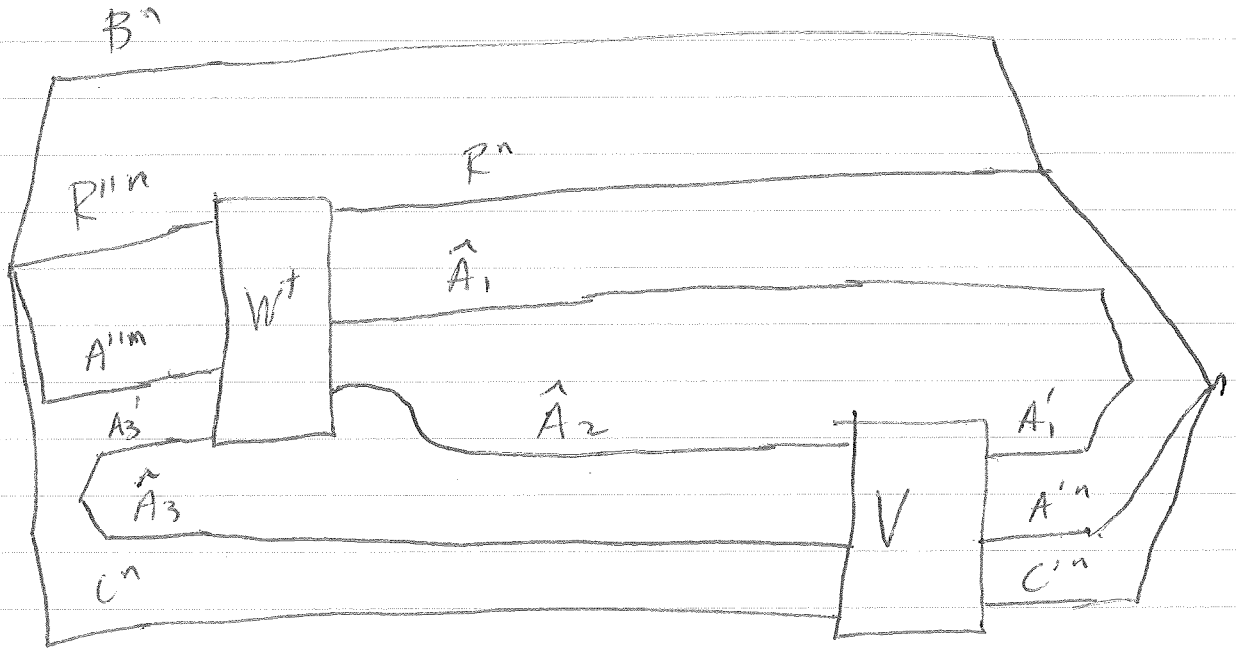
time reversing this circuit gives



But then we can serially concatenate the 1st circuit to this one to get a protocol for state redistribution



This picture simplifies to (cancelling $U^\dagger U$)



So the entanglement in ~~A'_3~~ $A'_3 + \hat{A}_3$ can be shared before comm. begins, the protocol generates entanglement in $\hat{A}_1 + A'_1$, & $\hat{A}_2$ is quantum comm.

rate of quantum comm. is

$$\frac{1}{2} I(A;B|C)$$

rate of entanglement generation is

$$\frac{1}{2} I(A;C) - \frac{1}{2} I(A;R)$$

How to get fidelity of recovery bound? on CMI

Consider state

$W_{B^n \hat{A}_2 \hat{A}_3 C^n}$ before decoder

For any state ρ_{KL} there is an operator inequality

$$\rho_{KL} \leq |K|^2 \, \pi_K \otimes \rho_L$$

Apply this to w to get

$$W_{B^n \hat{A}_2 \hat{A}_3 C^n} \leq |\hat{A}_2|^2 \, \pi_{\hat{A}_2} \otimes W_{B^n \hat{A}_3 C^n}$$

$$= |\hat{A}_2|^2 \, \pi_{\hat{A}_2} \otimes \pi_{\hat{A}_3} \otimes \psi_{BC}^{\otimes n}$$

The op. inequality is preserved under the action of CPTP maps. Now apply the state relist. decoder to get

$$\mathcal{D}_{\hat{A}_2\hat{A}_3C^n\to A'^nC'^n}\left(\omega_{B^n\hat{A}_2\hat{A}_3C^n}\right)$$

$$\leq |\hat{A}_2|^2\,\mathcal{D}_{\hat{A}_2\hat{A}_3C^n\to A'^nC'^n}\left(\pi_{\hat{A}_2}\otimes\pi_{\hat{A}_3}\otimes\psi_{BC}^{\otimes n}\right)$$

this can be understood as a recovery map

we can then use monotonicity of square root function to conclude that

$$F\left(\psi_{BAC}^{\otimes n},\ \mathcal{D}_{\hat{A}_2\hat{A}_3C^n\to A'^nC'^n}\left(\omega_{B^n\hat{A}_2\hat{A}_3C^n}\right)\right)$$

$$\leq |\hat{A}_2|^2\ F\left(\psi_{BAC}^{\otimes n},\ \mathcal{R}_{C^n\to A'^nC'^n}\left(\psi_{BC}^{\otimes n}\right)\right)$$

LHS is $\geq 1-\varepsilon$ by achievability part

take supremum over all recovery maps to upper bound RHS, leading to

$$1-\varepsilon \leq |\hat{A}_2|^2\ F(A^n;B^n|C^n)_{\psi^{\otimes n}}$$

use result that FoR is multiplicative to get

$$1-\varepsilon \leq |\hat{A}_2|^2\left(F(A;B|C)_\psi\right)^n$$

Finally take a logarithm & move around to get

$$\log(1-\varepsilon) - n \log F(A;B|C)_\psi \leq \log |\hat{A}_2|^2 = 2 \log |\hat{A}_2|$$

But we argued that

$$|\hat{A}_2| \approx 2^{n \frac{1}{2} I(A;B|C)}$$

$$\Rightarrow \log(1-\varepsilon) - n \log F(A;B|C)_\psi \leq {}_n I(A;B|C)_\psi$$

Divide by n & take limit to get

$$I(A;B|C)_\psi \geq -\log F(A;B|C)_\psi$$