3/24/2011

Lecture 22

Achievability part of entanglement-assisted classical capacity

would like to show that the quantum mutual information of the channel is an achievable rate

$$I(\mathcal{N}) \equiv \max_{\phi^{AA'}} I(A;B)_\rho$$

where $\rho^{AB} \equiv \mathcal{N}^{A'\to B}(\phi^{AA'})$

Suppose the maximizing state is $\Phi^{AA'}$

maximally entangled state

Then there is a straightforward way to achieve capacity (like super-dense coding)

Recall max. entangled qudit state

$$|\Phi\rangle^{AB} = \frac{1}{\sqrt{D}} \sum_{i=0}^{D-1} |i\rangle^A |i\rangle^B$$

Recall $X(x) \equiv \sum_{x'=0}^{D-1} |x+x'\rangle\langle x'|$ +

$$Z(z) \equiv \sum_{z'=0}^{D-1} e^{2\pi i z z'/D} |z'\rangle\langle z'|$$

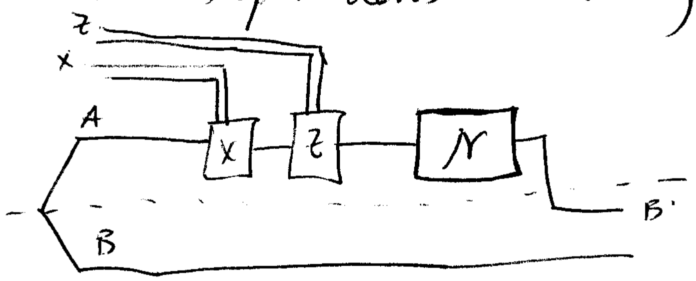
3/24/2011

Let $|\Phi_{x,z}\rangle^{AB} \equiv \{(X(x)Z(z))^{A} \otimes I^{B}\} |\Phi\rangle^{AB}$

Then $\langle \Phi_{x',z'} | \Phi_{x,z}\rangle = \delta_{x,x'}\,\delta_{z,z'}$

$$\sum_{x,z} |\Phi_{x,z}\rangle\langle\Phi_{x,z}| = I^{AB}$$

can induce the following ensemble via super-dense coding



$$\left\{\frac{1}{d^2},\ (N^{A\to B'} \otimes I^{B})(\Phi^{AB}_{x,z})\right\}$$

we know that Holevo information for this ensemble is an achievable rate for classical communication.

Let's calculate it.

3/24/2011

map ensemble to classical-quantum state

$$\rho^{XZB'B} \equiv \sum_{x,z} \frac{1}{D^2} |x\rangle\langle x|^X \otimes |z\rangle\langle z|^Z \otimes \mathcal{N}^{A\to B'}(\Phi_{x,z}^{AB})$$

calculate $I(XZ;B'B) =$

$$H(B'B) - H(B'B|XZ)$$

trace over X & Z

$$\begin{aligned}
\mathrm{Tr}_{XZ}\{\rho^{XZB'B}\} &= \sum_{x,z} \frac{1}{D^2} \mathcal{N}^{A\to B'}(\Phi_{x,z}^{AB}) \\
&= \mathcal{N}^{A\to B'}\left(\frac{1}{D^2} \sum_{x,z} \Phi_{x,z}^{AB}\right) \\
&= \mathcal{N}^{A\to B'}\left(\frac{I^{AB}}{D^2}\right) \\
&\equiv \mathcal{N}^{A\to B'}(\pi^A \otimes \pi^B) \\
&= \mathcal{N}^{A\to B'}(\pi^A) \otimes \pi^B
\end{aligned}$$

$$\therefore \quad H(B'B) = H(\mathcal{N}(\pi)) + H(\pi)$$

3/24/2011

Now let's get $H(B'B|XZ)$

$$= \sum_{x,z} \frac{1}{D^2} H\left(\mathcal{N}^{A\to B'}\left(\Phi^{AB}_{x,z}\right)\right)$$

$$= \sum_{x,z} \frac{1}{D^2} H\left(\mathcal{N}^{A\to B'}\left(V^A_{x,z} \; \Phi^{AB} (V^{\dagger}_{x,z})^A\right)\right)$$

$$= \sum_{x,z} \frac{1}{D^2} H\left(\mathcal{N}^{A\to B'}\left((V^T_{x,z})^B \; \Phi^{AB} (V^{*}_{x,z})^B\right)\right)$$

$$= \sum_{x,z} \frac{1}{D^2} H\left((V^T_{x,z})^B \; \mathcal{N}^{A\to B'}\left(\Phi^{AB}\right) (V^{*}_{x,z})^B\right)$$

$$= \sum_{x,z} \frac{1}{D^2} H\left(\mathcal{N}^{A\to B'}\left(\Phi^{AB}\right)\right)$$

$$= H\left(\mathcal{N}^{A\to B'}\left(\Phi^{AB}\right)\right)$$

So, the rate

$$H(\mathcal{N}(\pi^A)) + H(\pi^B) - H(\mathcal{N}^{A\to B'}(\Phi^{AB}))$$

is achievable by HSW

this rate is equal to

$I(A;B)_\rho$ where

$\rho^{AB} = \mathcal{N}^{A'\to B}(\Phi^{AA'})$

3/24/2011

What if $\Phi^{AB'}$ is not the state that maximizes $I(\mathcal{N})$? (this happens for amplitude damping channel)

Then we need a more general strategy...

Proof of achievability of $I(A;B)_\rho$ where $\rho^{AB} = \mathcal{N}^{A'\to B}(\varphi^{AA'})$

arbitrary

idea is still essentially super-dense coding

~~consider state~~ $\cancel{|\varphi\rangle^{AB} = \underbrace{\sum_x \sqrt{p(x)}\,|x\rangle^A|x\rangle^B}_{\text{Schmidt}}}$

From HSW, we can extract a Packing Lemma given ensemble $\{p(y), \sigma_y\}$ & projectors $\{\Pi_y\}, \Pi$ such that

$$\mathrm{Tr}\{\Pi\sigma_y\} \geq 1-\epsilon$$
$$\mathrm{Tr}\{\Pi_y\sigma_y\} \geq 1-\epsilon$$
$$\mathrm{Tr}\{\Pi_y\} \leq d$$
$$\Pi\sigma\Pi \leq \frac{1}{D}\Pi$$

then there exists code of size $\approx \frac{D}{d}$

think of d as $2^{nH(B|X)}$

& D as $\approx 2^{nH(B)}$

so $\frac{D}{d} = 2^{nI(X;B)}$

3/24/2011

So we will show ensemble & projectors for which these conditions hold in EA case

given arbitrary state $|\varphi\rangle^{AB}$, it has

Schmidt decomposition $|\varphi\rangle^{AB} = \sum_x \sqrt{p(x)}\, |x\rangle^A |x\rangle^B$

where $\{|x\rangle^A\}$ & $\{|x\rangle^B\}$ are O.N. bases.

n copies of the above state is

$$|\varphi\rangle^{A^nB^n} \equiv \sum_{x^n} \sqrt{p_{X^n}(x^n)}\, |x^n\rangle^{A^n} |x^n\rangle^{B^n}$$

$$= \sum_t \sum_{x^n \in \tau_t} \sqrt{p_{X^n}(x^n)}\, |x^n\rangle^{A^n} |x^n\rangle^{B^n}$$

$$= \sum_t \sqrt{p_{X^n}(x^n_t)} \sum_{t \in \tau_t} |x^n\rangle^{A^n} |x^n\rangle^{B^n}$$

τ_t is all sequences x^n w/ same empirical distribution (in binary case, w/ same Hamming weight)

$$= \sum_t \sqrt{p_{X^n}(x^n_t)\, d_t}\; \frac{1}{\sqrt{d_t}} \sum_{t \in \tau_t} |x^n\rangle^{A^n} |x^n\rangle^{B^n}$$

$$= \sum_t \sqrt{p(t)}\, \underbrace{|\Phi_t\rangle^{A^nB^n}}_{}$$

these are maximally entangled on "type class" subspaces

3/24/2011

can use dense-coding like strategy on these subspaces

let $V(x_t, z_t) \equiv X(x_t) Z(z_t)$ act on

$$|\Phi_t\rangle^{A^n B^n}$$

this operator does not affect any other $|\Phi_{t'}\rangle$ b/c subspaces have a direct sum structure

Alice can then make a large unitary operator

$$U(s) \equiv \bigoplus_t (-1)^{b_t} V(x_t, z_t)$$

some phases as well are needed

where $s \equiv ((x_t, z_t, b_t))_t$

can show that

$$\left(U(s)^{A^n} \otimes I^{B^n}\right) |\varphi\rangle^{A^n B^n} = \left(I^{A^n} \otimes \left(U^T(s)\right)^{B^n}\right) |\varphi\rangle^{A^n B^n}$$

b/c of special structure of $U(s)$

3/24/2011

Structure of random code

Encoding: For each message $m \in \mathcal{M}$, Alice chooses a vector $s = ((x_t, z_t, b_t))_t$ uniformly at random, can denote classical codeword as $s(m)$. This leads to an entanglement-assisted quantum codeword of the ~~form~~:

$$|\varphi_m\rangle^{A^n B^n} = \left(U(s(m))^{A^n} \otimes I^{B^n} \right) |\varphi\rangle^{A^n B^n}$$

random ensemble of potential codewords is then

$$\left\{ \frac{1}{|S|}, \left(U(s)^{A^n} \otimes I^{B^n} \right) |\varphi\rangle^{A^n B^n} \right\}$$

w/ expected density operator

$$\mathbb{E}_S \left\{ U(s)^{A^n} |\varphi\rangle\langle\varphi|^{A^n B^n} U^\dagger(s)^{B^n} \right\} =$$

$$\sum_t p(t) \, \pi_t^{A^n} \otimes \pi_t^{B^n}$$ (can prove this)

maximally mixed states on type class subspaces

codewords after going through the channel are

$$\mathcal{N}^{A^n \to B'^n} \left(U(s(m))^{A^n} |\varphi\rangle\langle\varphi|^{A^n B^n} U^\dagger(s(m))^{A^n} \right)$$

$$= U^T(s(m))^{B^n} \; \mathcal{N}^{A^n \to B'^n} \left(|\varphi\rangle\langle\varphi|^{A^n B^n} \right) U^*(s(m))^{B^n}$$

unitary commutes w/ channel!

3/24/2011

Also, observe that w/o Bob's half of entanglement, state is

$$\mathrm{Tr}_{B^n}\left\{ U^T(s(m))^{B^n}\, \mathcal{N}^{A^n\to B'^n}\left(\varphi^{A^nB^n}\right) U^*(s(m))^{B^n}\right\}$$

$$= \mathrm{Tr}_{B^n}\left\{ \mathcal{N}^{A^n\to B'^n}\left(\varphi^{A^nB^n}\right)\right\}$$

$$= \mathcal{N}^{A^n\to B'^n}\left(\varphi^{A^n}\right)$$

$\therefore$ w/o Bob's half, no information about message $\therefore$ privacy.

Also, state is a tensor-power state (use this later)

Bob's measurement POVM is $\{\Lambda_m\}$ where

$$\Lambda_m \equiv \left(\sum_{m'=1}^{|M|} \Pi_{m'}\right)^{-1/2} \Pi_m \left(\sum_{m'=1}^{|M|} \Pi_{m'}\right)^{-1/2}$$

where $\Pi_m = U^T(s(m))^{B^n}\, \underbrace{\Pi^{B^nB'^n}_{\mathcal{N}(\varphi),\delta}}_{\text{typical projector onto } \mathcal{N}^{A^n\to B'^n}(\varphi^{A^nB^n}) \text{ of size} \approx 2^{nH(BB')}}\, U^*(s(m))^{B^n}$

3/24/2011

need to prove four conditions of Packing Lemma:

1st, let large projector be

$$\Pi^{B'^n}_{\mathcal{N}(\varphi),\delta} \otimes \Pi^{B^n}_{\mathcal{N}(\varphi),\delta} \quad \text{of size} \approx 2^{n\{H(B')+H(B)\}}$$

$\boxed{1^{st}:}$

$$\mathrm{Tr}\{\Pi_m \rho_m\} \geq 1-\epsilon$$

$$\mathrm{Tr}\{U^T(s(m))^{B^n} \Pi^{B'^n B^n}_{\mathcal{N}(\varphi)} U^*(s(m))^{B^n} U^T(s(m))^{B^n} \mathcal{N}(\varphi)^{\otimes n} U^*(s(m))^{B^n}\}$$

$$= \mathrm{Tr}\{\Pi^{B'^n B^n}_{\mathcal{N}(\varphi)} \mathcal{N}(\varphi)^{\otimes n}\} \geq 1-\epsilon$$

cyclicity of trace + typicality

$\boxed{2^{nd}:}$ $$\mathrm{Tr}\{\Pi_m\} = \mathrm{Tr}\{U^T(s(m))^{B^n} \Pi^{B'^n B^n}_{\mathcal{N}(\varphi)} U^*(s(m))^{B^n}\}$$

$$= \mathrm{Tr}\{\Pi^{B'^n B^n}_{\mathcal{N}(\varphi)}\} \leq 2^{n\{H(B'B)+\delta\}}$$

3/24/2011

$\boxed{3^{rd}:}$ $\quad Tr\{\Pi_{fm}\} \geq 1-\epsilon$

$$Tr\{\Pi_{fm}\} = Tr\{\{\Pi^{B'^n}_{N(\psi)} \otimes \Pi^{B^n}_{N(\psi)}\} U^T(s(m))^{B^n} N(\psi)^{\otimes n} U^*(s(m))^{B^n}\}$$

Consider $\hat{\Pi} = I - \Pi$

then

$$\Pi^{B'^n}_{N(\psi)} \otimes \Pi^{B^n}_{N(\psi)} = (I^{B'^n} - \hat{\Pi}^{B'^n}_{N(\psi)}) \otimes (I^{B^n} - \hat{\Pi}^{B^n}_{N(\psi)})$$

$$= I^{B'^n} \otimes I^{B^n} - I^{B'^n} \otimes \hat{\Pi}^{B^n}_{N(\psi)} - \hat{\Pi}^{B'^n}_{N(\psi)} \otimes I^{B^n} + \Pi^{B'^n}_{N(\psi)} \otimes \Pi^{B^n}_{N(\psi)}$$

$$\geq I^{B'^n} \otimes I^{B^n} - I^{B'^n} \otimes \hat{\Pi}^{B^n}_{N(\psi)} - \hat{\Pi}^{B'^n}_{N(\psi)} \otimes I^{B^n}$$

3/24/2011

So $\mathrm{Tr}\left\{\left[\Pi^{B'^n}_{\mathcal{N}(\varphi)} \otimes \Pi^{B^n}_{\mathcal{N}(\varphi)}\right] U^T(s(m))^{B^n} \mathcal{N}(\varphi)^{\otimes n} U^*(s(m))^{B^n}\right\}$

$\geq \mathrm{Tr}\left\{\left(I^{B'^n} \otimes I^{B^n}\right) U^T(s(m))^{B^n} \mathcal{N}(\varphi)^{\otimes n} U^*(s(m))^{B^n}\right\}$

$- \mathrm{Tr}\left\{\left(I^{B'^n} \otimes \hat{\Pi}^{B^n}_{\mathcal{N}(\varphi)}\right)\left(\quad '' \quad \right)\right\}$

$- \mathrm{Tr}\left\{\left(\hat{\Pi}^{B'^n}_{\mathcal{N}(\varphi)} \otimes I^{B^n}\right)\left(\quad '' \quad \right)\right\}$

$= 1 - \mathrm{Tr}\left\{\hat{\Pi}^{B^n}_{\mathcal{N}(\varphi)} \varphi^{B^n}\right\}$

$\quad - \mathrm{Tr}\left\{\hat{\Pi}^{B'^n}_{\mathcal{N}(\varphi)} \mathcal{N}(\varphi^{A^n})\right\}$

$\geq 1 - \epsilon - \epsilon = 1 - 2\epsilon$

$\boxed{\text{4th:}}$ $\quad \Pi \rho \Pi \leq \frac{1}{D} \Pi$

For our case,

$$\left(\Pi^{B'^n}_{\mathcal{N}(\varphi)} \otimes \Pi^{B^n}_{\mathcal{N}(\varphi)}\right)\left(\sum_t p(t) \mathcal{N}(\pi_t) \otimes \pi_t\right)\left(\Pi^{B'^n}_{\mathcal{N}(\varphi)} \otimes \Pi^{B^n}_{\mathcal{N}(\varphi)}\right)$$

$$\leq 2^{-n\{H(B')+H(B)-\delta\}} \Pi^{B'^n}_{\mathcal{N}(\varphi)} \otimes \Pi^{B^n}_{\mathcal{N}(\varphi)}$$

(proved in notes)