Lecture 21

Thursday, December 04, 2014
10:25 AM

Entanglement-assisted Classical Capacity (Ch. 20)

Communication Resources : 1.) Memoryless Channel $(\mathcal{N}^{A\to B})^{\otimes n}$

2.) Entanglement : Arbitrary state $\phi^{A'B'}$

Encoder : $\mathcal{E}_m^{A'\to A^n}(\phi^{A'B'})$

Decoder : $\Lambda_m^{B'B^n}$

Prob. error : $p_e(m) = 1 - \mathrm{Tr}\left(\Lambda_m^{B'B^n}\mathcal{N}^{A^n\to B^n}\left(\mathcal{E}_m^{A'\to A^n}\left(\phi^{A'B'}\right)\right)\right)$

<u>Theorem</u> (Bennett-Shor-Smolin-Thapliyal):

$$\sup\{R : \text{achievable}\} = I(\mathcal{N})$$

First observation:

All entanglement is equal (iid pure states)

Let ρ^{AB} be a pure state.

$$\rho^{AB} = H(A)_\rho\ [qq]$$

Entanglement concentration gives $\rho^{AB} \geq H(A)_\rho\ [qq]$

The other direction works too.

<u>Proof:</u>

Achievability:

Main idea: Use the entanglement to construct a new channel.

Use previous theorem (lower bound) about classical communication.

Review of lower bound:

$$\chi(\vec{N}) = \sup_{\substack{\rho^{\bar{X}\bar{A}} \\ \text{CQ state}}} I(\bar{X};\bar{B}) = \sup_{\substack{\rho^{\bar{X}\bar{A}} \\ \text{CQ state}}} H(\bar{B}) - H(\bar{B}|\bar{X})$$

$$= \sup_{\{(p(x),\, \rho_x^{\bar{B}})\}} H(\bar{B})_{E_x \rho_x^{\bar{B}}} - E_x H(\bar{B})_{\rho_x^{\bar{B}}}$$

$\rho_x^{\bar{B}} = \mathcal{N}(\rho_x^{\bar{A}})$

Bottom line:

If an ensemble of channel outputs $\bar{B}$ can be constructed then

$$H(\bar{B})_{E_x \rho_x} - E_x H(\bar{B})_{\rho_x} \quad \text{is achievable.}$$

(i.e. a code can be constructed randomly from the ensemble)

A special case:

Suppose $I(\mathcal{N}) = I(X;B)_{\mathcal{N}^{A\to B}(\Phi^{XA})}$

Bell state

(Recall, $I(\mathcal{N})$ is always optimized by a pure state.
$\Rightarrow$ Pick input density ρ^A and consider its purification.
Assumption about is that $\rho^A = \pi$ is optimal.)

Let the entanglement resource be a Bell state $\Phi^{A'B'}$ with the same dimension as A.

Consider the following set of operations at the transmitter:

$$X^{A'}(x)\, Z^{A'}(z)\, |\Phi\rangle^{A'B'} \quad \text{then isomorphically map } A' \to A$$

Call the resulting state $|\Phi_{xz}\rangle^{AB'}$ (this is the Bell basis)

Choose X and Z uniformly at random to produce an ensemble, $\bar{B} = (B, B')$

1.) $E_{xz}\, \Phi_{xz}^{AB'} = \pi^A \otimes \pi^{B'}$

$$\Rightarrow E_{xz}\, \mathcal{N}^{A\to B}(\Phi_{xz}^{AB'}) = \mathcal{N}^{A\to B}(E\, \Phi_{xz}^{AB'}) = \mathcal{N}^{A\to B}(\pi^A) \otimes \pi^{B'}$$

$$\Rightarrow H(\bar{B})_{E\rho_x} = H(B,B')_{E_{xz}\mathcal{N}^{A\to B}(\Phi_{xz}^{AB'})} = H(B)_{\mathcal{N}(\pi)} + H(B')_{\pi}$$

2.) $E_x\, H(\bar{B})_{\rho_x} = E_{xz}\, H(B,B')_{\mathcal{N}^{A\to B}(\Phi_{xz}^{AB'})}$

Transpose result : Exercise 3.6.12

$$(M^A \otimes I^B)|\Phi\rangle^{AB} = (I^A \otimes (M^T)^B)|\Phi\rangle^{AB}$$

$$\Rightarrow |\Phi_{xz}\rangle^{AB'} = Z^{T\,B'}(z)\, X^T(x)^{B'}\, |\Phi\rangle^{AB'}$$

$$\Rightarrow \mathcal{N}^{A\to B}(\Phi_{xz}^{AB'}) = \mathcal{N}^{A\to B}\left(Z^{T\,B'}(z)\, X^{T\,B'}(x)\, \Phi_{xz}^{AB'}\, X^{T\,B'}(x)\, Z^{T\,B'}(z)\right)$$

$$= Z^{T\,B'}(z)\, X^{T\,B'}(x)\, \mathcal{N}^{A\to B}(\Phi^{AB'})\, X^{T\,B'}(x)\, Z^{T\,B'}(z)$$

$$\Rightarrow E_{xz}\, \underbrace{H(B,B')_{\mathcal{N}^{A\to B}(\Phi_{xz})}}_{\text{constant } \forall x,z} = H(B,B')_{\mathcal{N}^{A\to B}(\Phi)}$$

Conclusion: $H(B)_{\mathcal{N}(\pi)} + H(B')_{\pi} - H(B,B')_{\mathcal{N}^{A\to B}(\Phi)} = I(B,B')_{\mathcal{N}^{A\to B}(\Phi^{AB'})}$

is achievable.

$\Rightarrow I(\mathcal{N})$ is achievable by assumption.

Superdense coding is a special case with noise-free channel.

Generalize : (Idea 1)

Map Bell state to a type matching the capacity achieving input density.

This is like a constant composition code.

Don't know an easy way to complete the proof.

Generalization: (Idea 2)

Ensemble over super-symbols.

Entanglement resource is iid capacity achieving pure state $(\rho^{A'B'})^{\otimes n}$

Use schmidt decomposition and method of types.

$$|\rho\rangle^{A'^nB'^n} = \sum_t \sqrt{p(t)}\,|\Phi_t\rangle^{A'^nB'^n}$$

Construct ensemble from the following set of operations at the transmitter:

For each type let $V_t(x_t, z_t) = X_t(x_t)\, Z_t(z_t)$

Pauli operators within type subspace.

Let $U = \sum_t (-1)^{b_t} V_t(x_t, z_t)$

This is a unitary operator parameterized by $((b_t, x_t, z_t))_t$

Choose the parameters uniformly at random, apply U at transmitter, and map isomorphically to A^n to construct ensemble $\varphi_{(b_t,x_t,z_t)_t}^{B^nB'^n} = (N^{\otimes n}\times I)(I^{A'^n\to A^n}U^{A'^n}\rho^{A'^nB'^n}U^{\dagger}I^{\dagger})$

Verify that U is unitary:

A unitary transformation is equivalent to $\{|\psi_i\rangle \to |\varphi_i\rangle\}_i$ where $\{|\psi_i\rangle\}_i$ and $\{|\varphi_i\rangle\}_i$ are both orthonormal bases.

$\Rightarrow \sum_i |\varphi_i\rangle\langle\psi_i|$

Furthermore, $V_t(x_t, z_t) = \sum_j |\varphi_{t,j}\rangle\langle\psi_{t,j}|$ where $\{|\varphi_{t,j}\rangle\}_j$ and $\{|\psi_{t,j}\rangle\}_j$ are orth. bases for type subspace.

Since, type subspaces are orth. and span A'^n, U is unitary.

* Notice that U does not imply a measurement of the type and a conditional operation.

Claim 1: $U^{A'^n}\rho^{A'^nB'^n} = U^{T\,B'^n}\rho^{A'^nB'^n}$

Claim 1: $\mathcal{U}^{A^{n}} \rho^{A'^n B'^n} = \mathcal{U}^{T\,B} \rho^{A'^n B'^n}$

$$\Rightarrow H(B^n, B'^n)_{\varphi_{(b_t, x_t, z_t)_t}} = H(B^n, B'^n)_{\varphi^{B^n B'^n}}$$

$\rho^{A^n B'^n}$

Proof:

$$\mathcal{U}^{A^n} \rho^{A'^n B'^n} = \Big(\sum_t (-1)^{b_t} V(x_t, z_t) \Big)^{A'^n} \Big(\sum_t \sqrt{p(t)}\, |\Phi_t\rangle^{A'^n B'^n} \Big)$$

$$= \sum_T (-1)^{b_T} \sqrt{p(t)}\; V(x_T, z_T)^{A'^n} |\Phi_T\rangle^{A'^n B'^n}$$

$$= \sum_T (-1)^{b_T} \sqrt{p(t)}\; V^T(x_T, z_T)^{B'^n} |\Phi_T\rangle^{A'^n B'^n}$$

Claim 2: $$\mathbb{E}\, \varphi^{B^n B'^n}_{(b_t, x_t, z_t)_t} = \sum_t p(t)\, \mathcal{N}^{A^n \to B^n}(\Pi_t^{A^n}) \otimes \Pi_t^{B'^n}$$

Not entangled but correlated based on the type.

$$\Rightarrow H(\mathbb{E}\,\varphi^{B^n B'^n}) = H(B^n)_{\mathcal{N}(\rho^{\otimes n})} + H(B'^n | T)_{\rho^{\otimes n}}$$

$$= H(B^n)_{\mathcal{N}(\rho^{\otimes n})} + H(B'^n)_{\rho^{\otimes n}} - I(B'^n; T)_{\rho^{\otimes n}}$$

$$\geq \quad \downarrow \quad + \quad \downarrow \quad - \dim(B') \log n$$

Conclusion:

$$H(B^n)_{\mathcal{N}(\rho^{\otimes n})} + H(B'^n)_{\rho^{\otimes n}} - H(B^n, B'^n)_{\varphi^{B^n B'^n}} - \dim(B') \log n$$

$$= n \Big(H(B)_{\mathcal{N}(\rho)} + H(B')_\rho - H(B, B')_{(\mathcal{N} \otimes I)(\rho^{A'B'})} - \dim(B') \frac{\log n}{n} \Big)$$

is acheivable for supersymbols of length n.

$$\Rightarrow R < I(B; B')_{(\mathcal{N} \otimes I)(\rho^{A'B'})} \text{ is achievable.} \quad \square$$

Converse:

Use reliable communication to construct correlated states $(M, \hat{M})$ such that

$\hat{M}$ 2^{nR} $\hat{M}$

Use reliable communication to construct correlated states $(M, \hat{M})$ such that

$$w^{M\hat{M}} \approx \sum_{i=1}^{2^{nR}} |i\rangle\langle i|^{M} \otimes |i\rangle\langle i|^{\hat{M}}$$

$$\triangleq \Phi^{M\hat{M}}$$

$$\Rightarrow \quad nR = I(M;\hat{M})_{\Phi}$$

$$\leq I(M;\hat{M})_{w} + n\varepsilon' \qquad \text{Fannes}$$

$$\leq I(M;B^n B'^n) + n\varepsilon' \qquad \text{DPI}$$

$$\leq I(M B'^n; B^n) + \underbrace{I(M;B'^n)}_{0} + n\varepsilon'$$

$$= I(M B'^n; B^n) + n\varepsilon'$$

$$\leq I(\mathcal{N}^{\otimes n}) + n\varepsilon' \qquad \square$$

Stronger conclusion:

$$\mathcal{N} + H(A)_{\rho^*}[qq] \geq I(\mathcal{N})[c \to c]$$
