Entanglement-assisted Classical Capacity (Ch. 20)

Communication Resources:
1) Memoryless Channel \((N^{A\rightarrow B})^n\)
2) Entanglement: Arbitrary state \(\phi^{A'B'}\)

Encoder: \(E^{A \rightarrow B^n}_m (\phi^{A'B'})\)
Decoder: \(\Lambda^{B^n}_m\)

Prob. error: \(p_e(m) = 1 - \text{Tr} \left( \Lambda^{B^n}_m N^{A \rightarrow B^n}_m (E^{A \rightarrow B^n}_m (\phi^{A'B'})) \right)\)

Theorem (Bennett-Shor-Smolin-Thapliyal):

\[
\sup \{ R : \text{achievable} \} = I(N)
\]

First observation:

All entanglement is equal (iid pure states)

Let \(\rho^{AB}\) be a pure state.

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

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

The other direction works too.

Proof:

Achievability:

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

Use previous theorem (lower bound) about classical communication.
Review of lower bound:

\[ X(N) = \sup_{p_x} \mathcal{I}(X; B) = \sup_{\rho^{x_b}} H(B) - H(B|X) \]

\[ = \sup_{\{p(x), \rho_x \}} H(B)_{\mathcal{E}_{x, \rho_x}} - E_x H(B)_{\rho_x} \]

\[ = \mathcal{N}(\rho_x) \]

Bottom line:

If an ensemble of channel outputs \( B \) can be constructed then

\[ H(B)_{\mathcal{E}_{x, \rho_x}} - E_x H(B)_{\rho_x} \]

is achievable.

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

---

A special case:

Suppose \( \mathcal{I}(N) = \mathcal{I}(X; B) \uparrow_{A^0 B}^{\Lambda_{AB}} \)

(Bell state)

\[ (\text{Recall, } \mathcal{I}(N) \text{ is always optimized by a pure state}) \]

\[ (\Rightarrow \text{Pick input density } \rho^A \text{ and consider its purification}) \]

\[ (\text{Assumption about is that } \rho^A = \Xi \text{ is optimal}) \]

Let the entanglement resource be a Bell state \( \Xi^{AB'} \) with the same dimension as \( A \).

Consider the following set of operations at the transmitter:

\[ X^{A'}(x) Z^{A}(a) |\Phi^{AB'} \rangle \text{ then isomorphically map } A' \rightarrow A \]

Call the resulting state \( |\overline{\Phi}^{AB'} \rangle \) (this is the Bell basis)

Choose \( X \) and \( Z \) uniformly at random to produce an ensemble, \( \overline{B} = (B, B') \)
1) \[ E_{x^2} \Phi_{x^2}^{A \alpha B} = \Pi^A \otimes \Pi^B \]

\[ \Rightarrow E_{x^2} N^{A \rightarrow B} (\Phi_{x^2}^{A \alpha B}) = N^{A \rightarrow B} (E \Phi_{x^2}^{A \alpha B}) = N^{A \rightarrow B} (\Pi^A) \otimes \Pi^B \]

\[ \Rightarrow H(\Phi_{E x^2}^{A \alpha B}) = H(B, B') \quad N^{A \rightarrow B} (\Phi_{x^2}^{A \alpha B}) = H(B')_{\Pi^A} + H(B')_{\Pi^B} \]

2) \[ E_{x^2} H(\Phi_{E x^2}^{A \alpha B}) = E_{x^2} H(B, B') \quad N^{A \rightarrow B} (\Phi_{x^2}^{A \alpha B}) \]

**Transpose result:** Exercise 3.6.12

\[ (\Pi^A \otimes \Pi^B) |\Phi^{A \alpha B} > = (\Pi^A \otimes \Pi^B) |\Phi^{A \alpha B} > \]

\[ \Rightarrow |\Phi_{x^2}^{A \alpha B'} > = Z^{B'}(\xi(x)) X^B(x) |\Phi^{A \alpha B'} > \]

\[ \Rightarrow N^{A \rightarrow B} (\Phi_{x^2}^{A \alpha B'}) = N^{A \rightarrow B} \left( Z^{B'}(\xi(x)) X^B(x) \Phi_{x^2}^{A \alpha B'} X^B(x) Z^{B'}(\xi(x)) \Phi_{x^2}^{A \alpha B'} \right) \]

\[ \Rightarrow E_{x^2} H(B, B') \quad N^{A \rightarrow B} (\Phi_{x^2}^{A \alpha B}) = H(B, B') \quad N^{A \rightarrow B} (\Phi_{x^2}^{A \alpha}) \]

\[ \uparrow \quad constant \quad \forall x, z \]

**Conclusion:** \[ H(B')_{\Pi^A} + H(B')_{\Pi^B} - H(B, B') \quad N^{A \rightarrow B} (\Phi_{x^2}^{A \alpha B}) \]

\[ \Rightarrow I(N) \text{ is achievable by assumption.} \]

---

5-per dense 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 \( \rho^{a_1 b_1} \).

Use Schmidt decomposition and method of types.

\[
|\rho^{a_1 b_1}\rangle = \sum_i \sqrt{p(i)} |\Phi_i^{a_1 b_1}\rangle
\]

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

For each type let \( V_\lambda(x_1, z) = X_j(x_j) Z_k(z_k) \)

Let \( U = \sum_{\lambda} V_\lambda(x_1, z) \)

This is a unitary operator parameterized by \( (\lambda, x_1, z) \).

Choose the parameters uniformly at random, apply \( U \) at transmitter,

and map isomorphically to \( A^n \) to construct ensemble \( \Phi^{a_1 b_1^n} = (\mathcal{A}_n I) (I^m \otimes U \rho_{A^n}^{a_1 b_1} U^+ I^j) \)

Verify that \( U \) is unitary:

A unitary transformation is equivalent to \( \{ \Psi_1 \} \to \{ \Psi_2 \}_i \)

where \( \{ \Psi_1 \}_i \) and \( \{ \Psi_2 \}_i \) are both orthonormal bases.

\[ \sum_i |\Psi_i\rangle \langle \Psi_i| \]

Furthermore, \( V_\lambda(x_1, z) = \sum_{j} |\Phi_{ij}\rangle \langle \Phi_{ij}| \) where \( \{ |\Phi_{ij}\rangle \}_j \) and \( \{ |\Phi_{ij}\rangle \}_i \)

are ortho-bases for type subspace.

Since, type subspaces are ortho, they span \( A^n \), \( U \) is unitary.

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

**Claim 1**: \( U^{A^n B^n} \rho^{A^n B^n} = U^+ B^n A^n B^n \rho^{A^n B^n} U \)
Claim 1: \( U^{\rho A^t B^{\rho^t}} = U^{\rho B^{\rho^t}} \)
\[ \Rightarrow H(B^A, B^{\rho^t})_{(\rho^t, \rho^A)^n} = H(B^A, B^{\rho^t})_{(\rho^t, \rho^A)^n} \]

Proof: \( U^{\rho A^t B^{\rho^t}} = (\sum_t (-1)^t \sqrt{p_t} V(x_t, z_t))^{A^t} (\sum_t \sqrt{p_t} |\Phi_t^+>^{\rho^t B^{\rho^t}}) = \sum_t (-1)^t \sqrt{p_t} V(x_t, z_t) A^t \pi_t^{\rho A^t B^{\rho^t}} = \sum_t (-1)^t \sqrt{p_t} V(x_t, z_t) |\Phi_t^+> A^t \pi_t^{\rho A^t B^{\rho^t}} \)

Claim 2: \( E_{(\rho^t, \rho^A)^n} B^{\rho^t} = \sum_t p_t (\rho^t) \mathcal{N}^{\rho^t \rightarrow \rho^A} (\pi_t^{A^t}) \otimes \pi_t^{\rho^t B^{\rho^t}} \)

Not entangled but correlated based on the type.
\[ \Rightarrow H(E_{(\rho^t, \rho^A)^n} | \rho^A) = H(B^A)_{\rho^A} + H(B^{\rho^t} | T)_{\rho^A} = H(B^A)_{\rho^A} + H(B^{\rho^t})_{\rho^A} - I(B^A; T)_{\rho^A} = \dim(B^A) \log n \]

Conclusion: \( H(B^A)_{\rho^A} + H(B^{\rho^t})_{\rho^A} - H(B^A, B^{\rho^t})_{\rho^A} - \dim(B^A) \log n = n \left( H(B)_{\rho} + H(B^1)_{\rho} - H(B, B^1)_{(\rho^A)(\rho^{\rho^t})} - \dim(B) \log \frac{n}{\dim(B)} \right) \) is achievable for supersymbols of length \( n \).
\[ \Rightarrow R < I(B^1; B^1)_{(\rho^A)(\rho^{\rho^t})} \text{ is achievable. } \]

Converse:

Use reliable communication to construct correlated states \( (M, \tilde{A}) \) such that...
Use reliable communication to construct correlated states \((M, \vec{M})\) such that
\[
\sum_{i}^{n} |x_i \otimes \vec{x}_i| = \sum_{i}^{n} |x_i \otimes \vec{x}_i|
\]

\[\Rightarrow nR = I(M; \vec{M}) \leq I(M; \vec{M}) + n\varepsilon' \quad \text{Fannes}
\]
\[\leq I(M; B^n \vec{B}^n) + n\varepsilon' \quad \text{DPD}
\]
\[\leq I(MB^n \vec{B}^n) + I(M; B^n) + n\varepsilon'
\]
\[= I(MB^n \vec{B}^n) + n\varepsilon'
\]
\[\leq I(N^{\otimes n}) + n\varepsilon' \quad \Box
\]

**Stronger conclusion:**

\[N + H(A_p \otimes \vec{q} \vec{f}) \geq I(N) [c \rightarrow c]
\]