Lecture 22

Tuesday, December 09, 2014
9:35 AM

Quantum Communication: Ch. 23

Task: Reproduce quantum state. ← arbitrary

Preserve entanglement. ← arbitrary

For Schumacher compression, the marginal state was known. Here it is not.
If known, compress first.

Let φ^{RA_1} be arbitrary.

Memoryless channel $(\mathcal{N}^{A\to B})^{\otimes n}$

Encoder: $\mathcal{E}^{A_1\to A^n}(\varphi^{RA_1})$

Decoder: $\mathcal{D}^{B^n\to B_1}$

Result: $\omega^{RB_1} = \mathcal{D}^{B^n\to B_1}\left(\mathcal{N}^{A^n\to B^n}\left(\mathcal{E}^{A_1\to A^n}(\varphi^{RA_1})\right)\right)$

Error: $\|\omega^{RB_1} - \varphi^{RA_1}\|_1 < \varepsilon$

Rate: dimension $A_1 = 2^{nR}$

R is achievable if $\forall \varepsilon > 0\ \exists n, \mathcal{E}, \mathcal{D}$ at rate R s.t. this holds for arbitrary φ^{RA_1}.

Theorem: $\sup(R: \text{achievable}) = \lim_{n\to\infty} \frac{1}{n} Q(\mathcal{N}^{\otimes n})$

In other words, coherent information is a "good" lower bound.

Achievability:

One quick way to arrive there:

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

In general, $N + H(A)_\rho [qq] \geq I(X;B)_\rho \, [c \to c]$

purification of ρ.

This takes some attention.

Upgrade to coherent protocol:

$$N + H(A)_\rho [qq] \geq I(X;B)_\rho \, [q \to qq]$$

coherent comm. equality

$$= I(X;B) \left(\tfrac{1}{2}[q \to q] + \tfrac{1}{2}[qq] \right)$$

$$= \cancel{H(X)} + H(B) - H(X,B)$$

$H(A)$

$$N + \tfrac{1}{2}H(A)\,[qq] \geq \tfrac{1}{2}H(A)\,[q \to q] + \tfrac{1}{2}I(X\rangle B)\,[q \to q] + \tfrac{1}{2}I(X\rangle B)\,[qq]$$

$H(X) = H(A) > I(X\rangle B)$

$$\Rightarrow \quad N \geq I(X\rangle B)\,[q \to q] + \tfrac{1}{2}\big(H(A) - I(X\rangle B)\big)[q \to q] - \tfrac{1}{2}\big(H(A) - I(X\rangle B)\big)[qq]$$

$$\geq I(X\rangle B)\,[q \to q]$$

Entanglement distribution $([q \to q] \geq [qq])$ to cancel consumption of entanglement.

Direct approach to achievability:

First understand privacy coding:

Wyner's Wiretap Channel (Classical, '75):

Two channels with one input ("broadcast channel")

$$\begin{tikzcd} & Y \\ X \arrow[ur, "p(y|x)"] \arrow[dr, "p(z|x)"'] & \\ & Z \end{tikzcd}$$

Assume memoryless over time.

Communicate at rate R reliably to receive who sees Y^n, leak no information through Z^n.

Privacy: Encoder induces $w_m(z^n) = p(z^n \mid M = m)$

$$\| w_m(z^n) - w_{m'}(z^n) \|_1 < \varepsilon \quad \forall m, m'$$

(Equivalently, all w_m close to a constant distribution).

Easy case: Suppose input has two parts.

<u>Example</u>: Beamforming.

More interesting: Two BSC's.

<u>Result</u>: $$C_s = \max_{p(u,x)} I(U;Y) - I(U;Z)$$

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

<u>Main idea</u>: First assume $U = X$.

Achieve $I(X;Y) - I(X;Z)$.

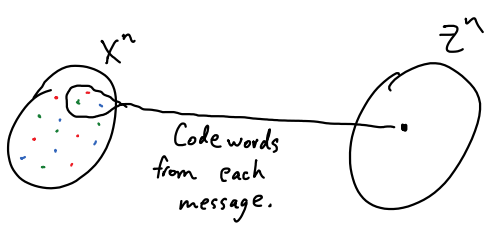
Create a codebook at rate $I(X;Y)$ ← classical capacity.

Message rate is only $R < I(X;Y) - I(X;Z)$

Remaining rate used for "dummy" random message $(R_d > I(X;Z))$

Decoder decodes both and ignores dummy.

Dummy message creates secresy:



<u>More intuition</u>: Tramitted message $M' = (M, M_d)$

If M where known (constant)

Adversary can decode dummy because $R_d < I(X;Z)$.

$$\Rightarrow I(M;Z^n) = I(M, M_d; Z^n) - I(M_d; Z^n | M)$$

$$\Rightarrow I(M;Z^n) = I(M, M_d; Z^n) - I(M_d; Z^n | M)$$
$$\leq n\, I(X;Z) - n R_d + n\varepsilon$$
$$\leq n\varepsilon'$$

Quantum Privacy Coding:

Adversary's channel is complementary channel (to environment).

Worst-case channel allowed by QM.

$$P(\mathcal{N}) = \max_{\rho^{XA}} I(X;B) - I(X;E)$$

no entanglement.
Classical – Quantum.

Holevo information optimized by pure states ρ_x^A.

Quantum Communication:

Use privacy code.
- restrict ensemble (pure, orthogonal states)

Create Coherent comm.

Use classical comm.

Argue that classical comm not necessary (messurements are independent of state.)

Restrict ensemble:

Suppose ρ_x^A is pure $\forall x$.

$$I(X;B)_\rho - I(X;E)_\rho = H(B)_\rho - \cancel{H(B|X)_\rho} - H(E)_\rho + \cancel{H(E|X)_\rho}$$

$$= H(B)_\rho - H(E)_\rho$$

$$= H(B)_{|\psi\rangle} - H(X,B)_{|\psi\rangle}$$

Let $|\psi\rangle$ be the purification of ρ^A

$$= H(X\rangle B)_{|\psi\rangle}$$

Coherent comm.:

$$|i\rangle^A \longrightarrow |i\rangle^A |i\rangle^B |i\rangle^E$$

If quantum comm. works.

Input Bell state. $|\Phi\rangle^{RA_1}$

$$\omega^{RB_1} \approx |\Phi\rangle^{RB_1}$$

$$nR = I(R\rangle B_1)_{|\Phi\rangle}$$

$$\simeq I(R\rangle B_1)_\omega$$

$$\leq I(R\rangle B^n)_\omega \qquad \text{DPI.}$$

$$\leq Q(\mathcal{N}^{\otimes n})$$