Quantum Communication: Ch. 23

Task: Reproduce quantum state. Preserve entanglement.

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

Let $\varphi^{RA}$ be arbitrary.

Encoder: $E^{A_n} : A_n \rightarrow A^n(\varphi^{RA})$

Decoder: $D^{B_n} : B_n \rightarrow B$

Result: $w^{RB_i} = D^{B_n} \circ (N^{A_n} \circ E^{A_n} (\varphi^{RA}))$

Error: $\|w^{RB_i} - \varphi^{RA}\|_1 \leq \varepsilon$

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

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

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

Achievability:

One quick way to arrive there:

Recall: $N + H(A)_p [c] \geq I(N) [c \rightarrow c]$
In general, \( N + H(A)_p \[99\] \geq I(X;B)_p [c \rightarrow c] \uparrow \) (p.\#)

**Upgrade to coherent protocol:**

\[
N + H(A)_p \[99\] \geq I(X;B)_p \left[ \frac{1}{2} I_g \rightarrow 99 \right] = I(X;B) \left( \frac{1}{2} I_g \rightarrow 99 \right) + \frac{1}{2} I_g \rightarrow 99 \\
= H(A) + H(B) - H(X,B)
\]

\[
N + I\left[ H(A) \[99\] \right] \geq \frac{1}{2} I(X \rightarrow B) \left[ g \rightarrow 99 \right] + \frac{1}{2} I(X \rightarrow B) \left[ g \rightarrow 99 \right]
\]

\( H(A) = I(X \rightarrow B) \)

\[
\Rightarrow N \geq I(X \rightarrow B) \left[ g \rightarrow 99 \right] + \frac{1}{2} \left( H(A) - I(X \rightarrow B) \right) \left[ g \rightarrow 99 \right]
\]

\( \Rightarrow \geq I(X \rightarrow B) \left[ g \rightarrow 99 \right] \)

Entanglement distribution \((g \rightarrow 99) = \[99\]) 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"): Two channels with one input ("broadcast channel")

\[
X \xrightarrow{p(x)} Y \xleftarrow{p(y|x)} Z
\]

Assume memoryless over time.

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

Privacy: Encoder induces \( \omega_n(z) = p(z^n|M=x^n) \)
$$\|w_m(x^*) - w_{m'}(x^*)\|_1 < \varepsilon \quad \forall m,m'$$

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

Easy case: Suppose input has two parts.

Example: Beamforming.

More interesting: Two BSC's.

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

$$P(u,x)P(y|x)p(\tilde{z}|x)$$

Main idea: First assume $U = X$.

Achieve $I(X;Y) = I(X;\tilde{Z})$.

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

Message rate is only $R < I(X;Y) - I(X;\tilde{Z})$

Remaining rate used for "dummy" random message ($R_d < I(X;\tilde{Z})$)

Decoder decodes both and ignores dummy.

Dummy message creates secrecy:

More intuition: Truncated message $M' = (M, M_d)$

If $M$ where known (constant)

Adversary can decode dummy because $R_d < I(X;\tilde{Z})$.

$\Rightarrow I(M';\tilde{Z}^n) = I(M, M_d;\tilde{Z}^n) - I(M_d;\tilde{Z}^n|M)$
\[ I(Y;Z) = I(M, M_4; Z) - I(M_4; Z | M) \]
\[ \leq n I(X; Z) - n R_d + n \epsilon \]
\[ \leq n \epsilon' \]

---

**Quantum Privacy Coding:**

- Adversary's channel is complementary channel (to environment).
- Worst-case channel allowed by QM.

\[ P(N) = \max_{P^{B \rightarrow Z}} I(X; B) - I(X; E) \]

- no entanglement:
  - Classical - Quantum.
  - Holevo information optimized by pure states \( P^A \).

---

**Quantum Communication:**

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

Create Coherent comm.

Use classical comm.

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

---

**Restrict ensemble:**

Suppose \( P^A \) is pure \( A \).

\[ I(X; B) - I(X; E) = H(B) - H(B|X) - H(E) + H(E|X) \]
Let $|+\rangle$ be the purification of $\rho^A$

$$= H(B)_{\rho} - H(E)_{\rho}$$
$$= H(B)_{|+\rangle} - H(X \otimes B)_{|+\rangle}$$
$$= H(X \otimes B)_{|+\rangle}$$

Coherent comm.:

$$\vert i^A \rangle \rightarrow \vert i^A \otimes B \rangle \vert i^E \rangle$$

If quantum comm. works.

Input Bell state, $\vert i^A \rangle \otimes R_{A_i}$.

$$w^{RB_i} \approx \vert i^A \rangle \otimes \vert B_i \rangle$$

$$w^R = \mathcal{I}(R \otimes B)_{|+\rangle}$$
$$= \mathcal{I}(R \otimes B)_w$$
$$= \mathcal{I}(R \otimes B^n)_w \ 	ext{DP+I.}$$
$$\leq A(N^{\otimes n})$$