* Channel Coding Theorem

* The most fundamental theorem in inf. theory.
* Arguably the first application of the probabilistic method in math.

---

* We suppose the message W is drawn from an index set $\{1, \ldots, M\}$, uniformly at random (turns out to be not different from worst-case)
* Encoder $X_1^n : \{1, \ldots, M\} \to \mathcal{X}^n$.

  $\mathrm{Supp}(X_1^n) =:$ "Code book".

  each possible output is a "codeword".
* Decoder: Deterministic function

  $g : \mathcal{Y}^n \to \{1, \ldots, M\}$.
* Rate: $R = \dfrac{\log_2 M}{n}$ bits/channel use.
* Error probability:

Fix $i \in \{1, \ldots, M\}$, $\lambda_i := \Pr\left(g(Y^n) \neq i \mid W = i\right)$.

$$P_e \stackrel{\text{def}}{=} \frac{1}{M} \cdot \sum_{i=1}^{M} \lambda_i = \Pr_{(\text{uniform } W)}\left(g(Y^n) \neq W\right).$$

* Def: "Achievable rate" R is achievable if $\exists$ sequence of codes at rate $\geq R$ s.t.

$$P_e \to 0 \text{ as } n \to \infty.$$

* Def: $R^* \overset{\text{def}}{:=} \sup\{R \mid R \text{ is achievable}\}$.

* $\boxed{\text{Channel Coding Theorem: } R^* = C.}$

~~Achi~~

18

* Achievability Proof: *

[∃ a code ~]

Fix some $R < C$ and $p(x)$.

[We create a random codebook and show it performs well.]

$$\text{Codebook: } \mathcal{C} = \begin{pmatrix} x_1(1) & \sim & x_n(1) \\ \vdots & \vdots & \vdots \\ x_1(2^{Rn}) & \sim & x_n(2^{Rn}) \end{pmatrix}$$

* Each ~~word~~ entry is iid according to $P(x)$.

[sender and receiver use this code].

* Suppose a uniform random $W \in \{1, \sim, M\}$ is sent.

* Receiver uses "jointly typical decoding":

Given y_1^n, find x_1^n in the codebook such that (x_1^n, y_1^n) is jointly typical.

If x_1^n is unique, decode to the corresponding index.
else, declare an error (output 0).

(19)

<u>def:</u> $\mathcal{E}$: error event

$$\Pr(\mathcal{E}) = \sum_{\mathcal{C}} \Pr(\mathcal{C})\, P_e^{(n)}(\mathcal{C})$$

$$= \sum_{\mathcal{C}} \Pr(\mathcal{C}) \cdot \frac{1}{2^{nR}} \sum_{w=1}^{2^{nR}} \lambda_w(\mathcal{C}) \qquad (1)$$

* Suppose now that W is fixed to $W=1$.

* <u>def:</u> E_i : event that the i th codeword ~~for index~~ is jointly-typical with Y_1^n.

$$\Rightarrow \Pr(\mathcal{E} \mid W=1) \underset{[\text{union}]}{\leq} \Pr(\neg E_1 \mid W=1) + \sum_{i=2}^{2^{nR}} \Pr(E_i \mid W=1).$$

* Take n large so that $\Pr(\neg E_1 \mid W=1) \leq \varepsilon$. (by AEP)

* Also $X_1^n(1)$ and $X_1^n(i)$ for $i \neq 1$ are independent, ~~so by AEP~~, thus $X_1^n(i) \perp Y \Rightarrow$

by AEP, $\Pr(E_i \mid W=1) \leq 2^{-n(I(X;Y) - 3\varepsilon)}$

$$\Rightarrow \Pr(\mathcal{E} | W=1) \leq \varepsilon + \sum_{i=2}^{2^{nR}} 2^{-n(I(X;Y)-3\varepsilon)}$$

$$\leq \varepsilon + 2^{3n\varepsilon} \, 2^{-n(I(X;Y)-R)} \leq 2\varepsilon,$$

if $R < I(X;Y) - 3\varepsilon$ and n large.

* ~~Since this~~
* True for all fixings of $W \Rightarrow \Pr(\mathcal{E}) \leq 2\varepsilon$.
* Now take $p(x)$ to be $p^*(x)$ in capacity

  $\Rightarrow$ any $R < C$ is achievable.

* Fix the code. Can be found by exhaustive search.
* Get worst case small $\Pr(\mathcal{E})$ (i.e., for all W).

Markov: $\#\left(\Pr_W \lambda_W > 4\varepsilon\right) \leq \frac{1}{2}$

Throw away half of the codewords

$\Rightarrow$ New rate $= R - \frac{1}{n}$.

$[2^{nR-1}$ codewords$]$