Lec 5 May 20, 2010

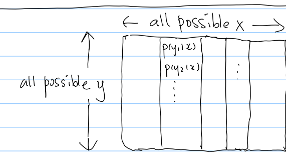
Note Title 19/05/2010

Def: A (classical) channel N is specified by:

- input alphabet X
- output " " Y
- a distribution $p(y|x)$ for each $x \in X$.

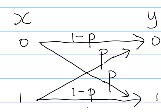
$$x \in X \rightarrow \boxed{N} \rightarrow y \in Y \quad \text{wp } p(y|x)$$

Aside: Can write N as a stochastic matrix



eg 1 Binary symmetric channel (BSC)

$X = Y = \{0,1\}$, input $\begin{cases} \text{sent wp } 1-p \\ \text{flipped wp } p \end{cases}$

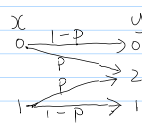


$$\begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 1-p & p \\ 1 & p & 1-p \end{array}$$

eg 2 Erasure channel (E_p)

$X = \{0,1\}$, input $\begin{cases} \text{sent wp } 1-p \\ \text{replaced by } 2 \text{ wp } p \end{cases}$

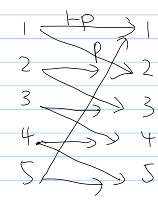
$Y = \{0,1,2\}$,



$$\begin{array}{c|cc} & 0 & 1 \\ \hline 0 & 1-p & 0 \\ 1 & 0 & 1-p \\ 2 & p & p \end{array}$$

eg 3. Pentagon channel ⬠

$X = Y = \{1,2,3,4,5\}$, input $\begin{cases} \text{sent wp } 1-p \\ \text{shifted up mod } 5 \text{ wp } p \end{cases}$



$$\begin{array}{c|ccccc} & 1 & 2 & 3 & 4 & 5 \\ \hline 1 & 1-p & 0 & \cdots & & p \\ 2 & p & 1-p & \ddots & & \\ 3 & 0 & p & \ddots & & \\ 4 & 0 & 0 & & & \\ 5 & 0 & 0 & & & 1-p \end{array}$$

General assumptions:

1. Can use channel many (n) times
2. Each use identical & independent:

For inputs $x_1 x_2 \ldots x_n$

outputs $= y_1 y_2 \ldots y_n$ wp $\prod_{i=1}^{n} p(y_i|x_i)$

"Called discrete memoryless channels DMCs"

Non DMCs:

eg 1 Time vary channel: the ith use is a BSC with prob error p_i

eg 2 Burst error: $x_1 x_2 \ldots x_n \longrightarrow x_1 x_2 \;\text{▨}\; x_n$

missing a contiguous block in the output

"Dog eats a page from your book."

eg 3 $x_1 x_2 \ldots x_i x_j \ldots x_n$

$\downarrow$

$x_1 x_2 \ldots x_j x_i \ldots x_n$

Symbols emerging in slightly wrong order

eg 4 $x_1 x_2 \ldots x_n$

$\downarrow$

$y_1 y_2 \ldots y_m \qquad m < n$

"Missing messages" - don't know which ones.

Aside: quantum analogues and coding strategies?

DMC from now on

Dealing with noise by error correcting codes:

eg 1. repeat

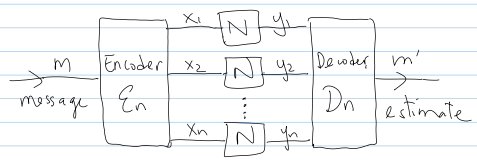
$$\left.\begin{array}{l} 0 \rightarrow \overbrace{00\cdots0}^{k \text{ times}} \\ 1 \rightarrow 11\cdots1 \end{array}\right\} \text{majority decoding}$$

↑ messages ↑ a codeword for each message

"The code" = set of code words

= subset of all possible inputs

Sending messages through n uses of a noisy channel:



An (M,n) code consists of
(1) index set $\mathcal{M} = \{1, \dots, M\}$
(2) an encoding function $\mathcal{E}_n : \mathcal{M} \to X^{\otimes n}$
(3) a decoding function $D_n : Y^{\otimes n} \to \mathcal{M}$

The codewords are $\mathcal{E}_n(1), \mathcal{E}_n(2), \dots \mathcal{E}_n(M) \leftarrow$ The code

eg 2. Hamming codes (eg encode 4 bits in 7, corrects up to 1 error)

Each codeword $x = x_1 x_2 \dots x_7$ satisfies 3 parity constraints:

$$P = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}, \quad Px = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \quad \text{ie } x_1 \oplus x_3 \oplus x_5 \oplus x_7 = 0, \; x_2 \oplus x_3 \oplus x_6 \oplus x_7 = 0 \text{ etc}$$

What's cool: if $y_i = x_i + e_i$ and only $e_i = 1$

then $Py = Pe = i$th col of P,

decoding / identifying the error is easy!

For message m, there's an error if

$$m' = D_n \circ N^{\otimes n} \circ \mathcal{E}_n(m) \neq m$$

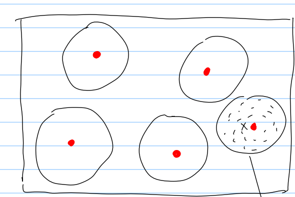
Say, happens wp $P_e(m)$

Define P_e^n = worse case prob of error = $\max_{m \in \mathcal{M}} P_e(m)$

EP_e^n = average . . . . = $\frac{1}{M} \sum_{m=1}^{M} P_e(m)$

Rate of an (M,n) code : $\frac{1}{n} \log M$

Geometrically: (say $X = Y$)



$X^{\otimes n} = Y^{\otimes n} \leftarrow$ n copies

• Code words

every output strings up to k errors from x

Can recover message if codewords are sparse enough so that these spheres don't overlap.

Def: For a channel N, a rate R is achievable if $\exists$ sequence of $(M = \lceil 2^{nR} \rceil, n)$ codes st. $P_e^n \to 0$ as $n \to \infty$

Def: Capacity of N, $C(N)$ = sup over achievable rates

NB If $C > 0$, the entire message, longer & longer ($\propto n$) comes out correctly almost surely!

Qn: For a fixed message size, to have smaller & smaller error prob, need bigger & bigger codes ..

(1) that brings more and more errors too

(2) will the rate -> 0 ?

(3) for growing message size, will prob(every part correct) -> 0?

Usually (1) not a problem if prob error small enough to start with, but (2), (3) can happen, say, with the repetition code.

Will see, we can do much much better
-- magic: iid channel use + large n

Back to $C(N) = \max\limits_{p(x)} I(X:Y)$

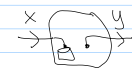
$$\boxed{\begin{array}{c}\text{Thm (Shannon's noisy coding theorem)} \\ C(N) = \max\limits_{p(x)} I(X:Y)\end{array}}$$

NB 1. $p(xy) = \underset{\uparrow \text{ max over}}{p(x)}\ \underset{\uparrow \text{ specified by } N}{p(y|x)}$

NB 2. Expression involves only 1 copy of $p(xy)$
but $C(N)$ has an asymptotic definition.

NB 3. Works in worse case, no distribution of message
"$p(x)$" in the max has meaning TBD.

NB 4. Every channel (but one) has $C>0$!



eg 1. BSC

$I(X:Y) = H(Y) - \underbrace{H(Y|X)}_{H(p) \text{ indep of } p(x)}$

$\uparrow$ max this by making y random
possible when $p(0) = p(1) = \frac{1}{2}$.

$\therefore$ Capacity of BSC $= 1 - H(p)$

eg 2 Erasure Channel

$I(X:Y) = H(X) - \underbrace{H(Y|X)}_{p\,H(X)} = (1-p)\ H(X)$

Again optimal
$p(x) = p(0) = p(1) = \frac{1}{2}$.

Capacity of erasure channel $= (1-p)$ — Same rate as if where the erasures are are known up-front!

eg 3. Pentagon channel with $p = \frac{1}{2}$

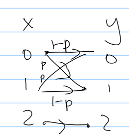
$I(X:Y) = H(Y) - \underbrace{H(Y|X)}_{\text{always} = 1}$

Again optimal $p(x)$ uniform,

$C(⬠) = \log 5 - 1 = \log(\frac{5}{2})$

eg 1-3 very symmetric
Thus optimal $p(x)$ uniform

Try eg 4



? HW

NB If we demand $p_e = 0$, but allowing many uses, we're studing the "zero-error-capacity" (lower bdd for $C(N)$)

eg. The BSC & erasure channel has 0 zero-error capacity
That of ⬠ is $\log\sqrt{5}$, That of eg 4 is 1.

Comparing ⬠ with $E^5_{10^{-10}}$ (erasure channel with $|X|=5$, $p = 10^{-10}$)

$C(E^5_{10^{-10}}) \approx \log 5 > C(⬠)$ But zero error capacity of $E^5_{10^{-10}} = 0$ $<$ that of ⬠