CHANNEL CODING AND CAPACITY

EE 6317

Shashank Vatedka

Discrete memoryless channels

$$X^n \longrightarrow \boxed{P_{Y|X}} \longrightarrow Y^n$$

$\in \mathcal{X}^n$ $\qquad\qquad$ $\in \mathcal{Y}^n$

$(\mathcal{X}, \mathcal{Y}, P_{Y|X})$

$\mathcal{X} \times \mathcal{Y}$

channel transition prob

$\mathcal{X} \neq \mathcal{Y}$.

$\mathcal{X} \to$ input alphabet $\quad \{0,1\} \quad \mathbb{R} \quad \mathbb{C}$

$\mathcal{Y} \to$ output alphabet $\quad \{0,1\} \quad \mathbb{R}, \quad \mathbb{C}$

$$P_{Y^n|X^n}(y^n \mid x^n) = \prod_{i=1}^{n} P_{Y|X}(y_i \mid x_i)$$

Trivial channels

Noiseless channel

$$X = Y \qquad p_{Y|X}(y|x) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{otherwise} \end{cases}$$

"Worst" channel

$$p_{Y|X}(y|x) = p_Y(y) \quad \forall x.$$

$$p_{XY}(x,y) = p_X(x)\, p_Y(y)$$

$$\Rightarrow X \perp\!\!\!\perp Y$$

Binary symmetric channel (BSC)

$\mathcal{X} = \{0, 1\}$

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

$$P_{Y|X}(y|x) = \begin{cases} p & \text{if } y \neq x \\ 1-p & \text{if } y = x \end{cases}$$

crossover prob

$$\begin{array}{cccc} & & \multicolumn{2}{c}{\mathcal{Y}} \\ & & 0 & 1 \\ \mathcal{X} & \begin{array}{c} 0 \\ 1 \end{array} & \multicolumn{2}{c}{\begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix}} \end{array}$$

Hamming distance: $d_H(x^n, y^n)$ = # locations in which they differ

$$P_{Y^n|X^n}(y^n|x^n) = p^{d_H(x^n, y^n)} (1-p)^{n - d_H(x^n, y^n)}$$

Binary erasure channel BEC(p)

$\mathcal{X} = \{0, 1\}$

$\mathcal{Y} = \{0, 1, e\}$

erasure sym

$$P_{Y|X}(y|x) = \begin{cases} p & \forall\ y = e \\ 1-p & \forall\ y = x \\ 0 & \forall\ y = x \oplus 1 \end{cases}$$

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

$$P_{Y^n|X^n}(y^n|x^n) = \begin{cases} p^{\alpha(y^n)}(1-p)^{n-\alpha(y^n)} & y_i = x_i \text{ if } y_i \neq e \\ 0 & y_i \neq x_i \in \{0,1\} \end{cases}$$

$\alpha(y^n) = \#\ e\text{'s in } y^n$

The channel coding problem

$$W \to \boxed{ENC} \xrightarrow{X^n} \boxed{P_{Y|X}} \xrightarrow{Y^n} \boxed{DEC} \to \hat{W} = g(Y^n)$$

$[M]$ $\quad W \sim \mathrm{Unif}[M]$

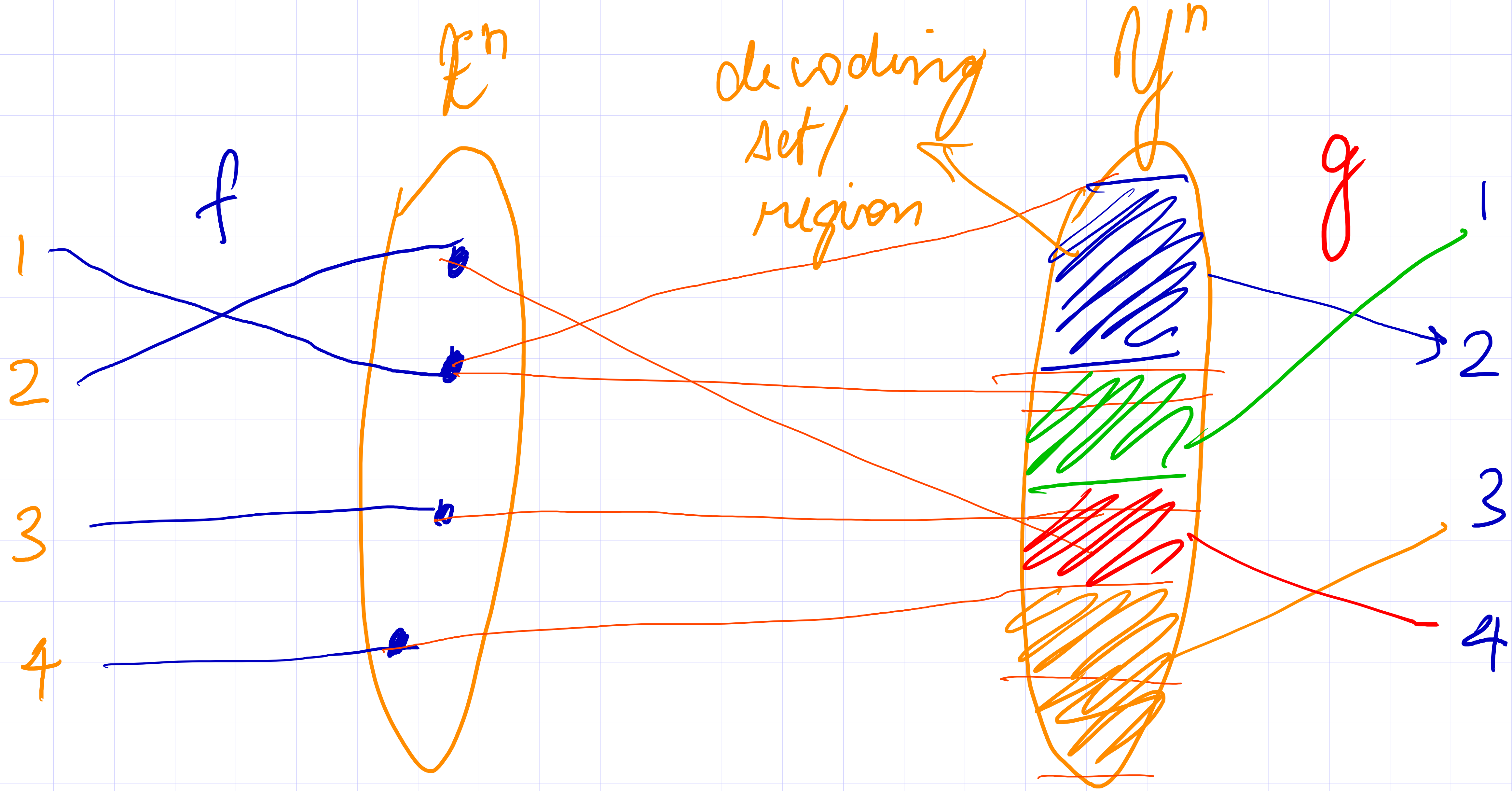
$X^n = f(W)$

$f(W) \to$ codeword

(M, n) code $\mathcal{C}$ for $(\mathcal{X}, \mathcal{Y}, P_{Y|X})$

1. Index set / message set $\{1, 2, \dots M\} = [M]$
2. Encoder $f : [M] \to \mathcal{X}^n$

   Codebook : $\{x^n(1), x^n(2), \dots x^n(M)\}$
3. Decoder $g : \mathcal{Y}^n \to [M]$



ENC
DEC
} Deterministic

Probability of error

Conditional probability of error

$$\lambda_w = \Pr[g(Y^n) \neq w \mid M = w]$$

Maximum probability of error

$$\lambda^{(n)} = \max_{1 \le w \le M} \lambda_w \rightarrow \text{worst case}$$

Average probability of error

$$P_e^{(n)} = \frac{1}{M} \sum_{w=1}^{M} \lambda_w \rightarrow \text{avg case}$$

random (uniform) W

$$P_e^{(n)} \le \lambda^{(n)}$$

Rate

$$R = \frac{\log_2 M}{n} \longrightarrow \# \text{ bits of info}$$

bits per channel use

bpcu

A rate R is achievable over $(\mathcal{X}, \mathcal{Y}, P_{Y|X})$

if $\exists$ (n, M_n) code st

$\lambda^{(n)}$

R is ach $P_e^{(n)}$

$\Downarrow$

ach $\lambda^{(n)}$

① $\lim_{n\to\infty} P_e^{(n)} = 0$

② $\lim_{n\to\infty} \frac{\log_2 M_n}{n} = R$.

Capacity

$$C = \sup\{R : R \text{ is achievable for } (\mathcal{X}, \mathcal{Y}, P_{Y|X})\}$$

Shannon's channel coding theorem

For any DMC $(\mathcal{X}, \mathcal{Y}, p_{Y|X})$,

$$\boxed{C = \max_{p_X} I(X;Y)}$$

CHANNEL CAPACITY

$$C = \max_{p_X} I(X;Y) \qquad p_{Y|X}$$

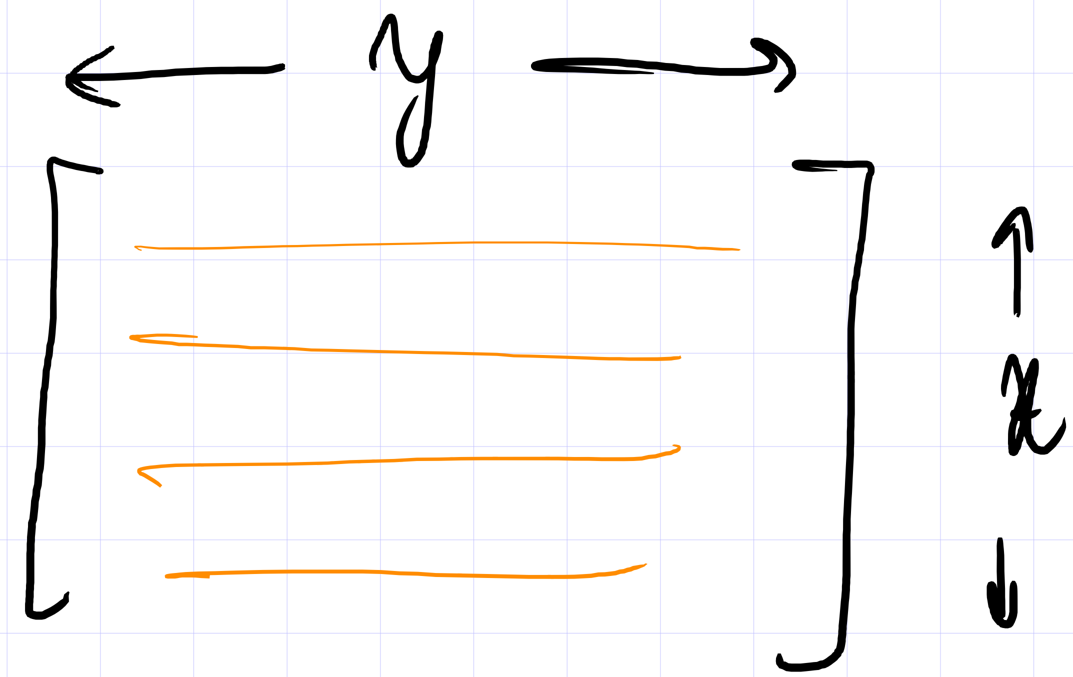
$I(X;Y)$ is concave in p_X

Any convex optimization algorithm

- Gradient descent
- Lagrange mult KKT

Blahut-Arimoto algorithm $\rightarrow$ iterative

Symmetric channel

$P_{Y|X} =$ 

Symmetric
1. every row is a permutation of 1st row
2. every col. is a — " — col.

Weakly symmetric
1. every row is a perm of 1st row
2. col. sums are the same.

FOR such channels,

$$C = \log_2 |\mathcal{Y}| - H(\text{row } 1)$$

$$P_X^* = \text{unif}(\mathcal{X})$$

$$\max_{p_X} I(X;Y) = \max_{p_X} \left(H(Y) - H(Y|X) \right) = \log|\mathcal{Y}| - H(\text{row})$$

For a weakly symmetric,

① $H(Y|X)$ = entropy of any row

$$H(Y|X) = \sum_{x} p_X(x) \underbrace{H(Y|X=x)}_{\text{entropy of row } x}$$

$$= H(\text{row } 1) \sum_{x} p_X(x),$$

② $\max_{p_X} H(Y) = \log_2 |\mathcal{Y}|$

$$p_Y = \sum_x p_X(x)\, p_{Y|X}(y|x)$$

BSC

$$P_{Y|X} = \begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix}$$

Weakly symmetric — Y

Symmetric — Y

BEC

$$P_{Y|X} = \begin{bmatrix} 1-p & p & 0 \\ 0 & p & 1-p \end{bmatrix}$$

NOT symmetric

$1-p = 2p$

$p = 1/3$

NOT weakly symm if $p \neq 1/3$

Capacity of a symmetric channel

Q1 : If $p_X \sim \text{Unif}(\mathcal{X})$, then what is p_Y?

$p_Y \sim \text{Unif}(\mathcal{Y})$

Q_2 : For any p_X, what is $H(Y|X)$?

$$C = \underline{\log_2 |\mathcal{Y}| - H(\text{row})}$$

Capacity of the BSC

$$\begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix}$$

$$C = \log_2 2 - H(p, 1-p)$$

$$= 1 - H_2(p)$$

$$\parallel$$

$$-p\log_2 p - (1-p)\log_2(1-p)$$

Repetition code

nR bit message

$W_1 \quad W_2 \quad \cdot \quad W_{nR}$

$\underbrace{w_1 \cdots w_1}_{k} \; w_2 \cdots w_2$

ENC: Repeat each bit k times

DEC: Majority rule

$$R = \frac{1}{k} \to 0 \quad \text{as } n \to \infty \text{ if } P_e \to 0$$

Prob(W_i is in error)

$$\alpha = \sum_{l=k/2}^{k} p^{l}(1-p)^{k-l} \binom{k}{l} \to {}^{k}C_{l}$$

$$P_e = \Pr[\, W^{nR} \neq \hat{W}^{nR} \,]$$

$$= 1 - (1-\alpha)^{nR}$$

$$P(\text{correct}) = (1-\alpha)^{nR}$$

$\alpha \to 0$
as $n \to \infty$

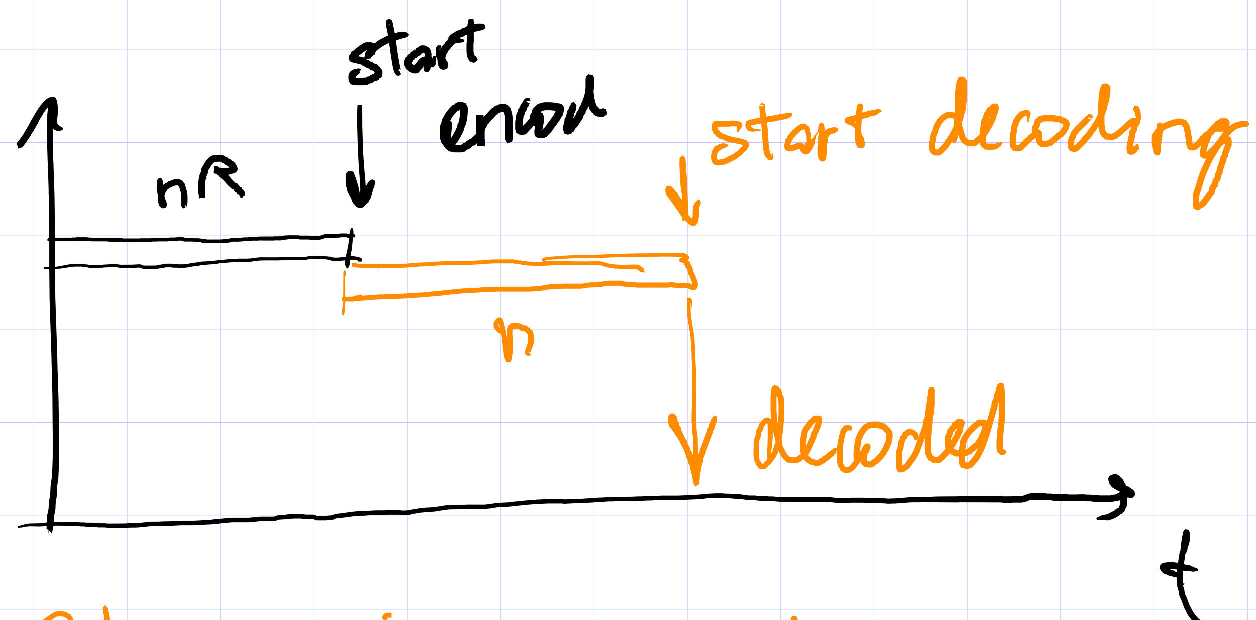
Delay in channel coding

$W \in [M] \qquad M = 2^{nR}$

$W = \underbrace{[0\,1\,0\,\cdots\,1]}_{nR} \xrightarrow{ENC} (X_1 \,\cdots\, X_n)$

Wait nR

$\longrightarrow \boxed{ENC} \xrightarrow{X^n} \boxed{CH} \xrightarrow{Y^n} \boxed{DEC} \longrightarrow \hat{W}$



delay $\geq \underline{n}$

Streaming codes ↳

Capacity of the BEC $= 1-p$

$$\begin{bmatrix} 1-p & p & 0 \\ 0 & p & 1-p \end{bmatrix}$$

$$H(Y|X) = H_2(p)$$

$$\max_{P_X} I(X;Y) = \max_{P_X} H(Y) - H_2(p)$$

$$= H_2(p) + 1-p - H_2(p)$$

$$= 1-p$$

$E = \mathbb{1}\{Y=e\}$

$$H(Y) = H(Y,E) - \cancel{H(E|Y)}_{0}$$

$$= H(E) + H(Y|E)$$

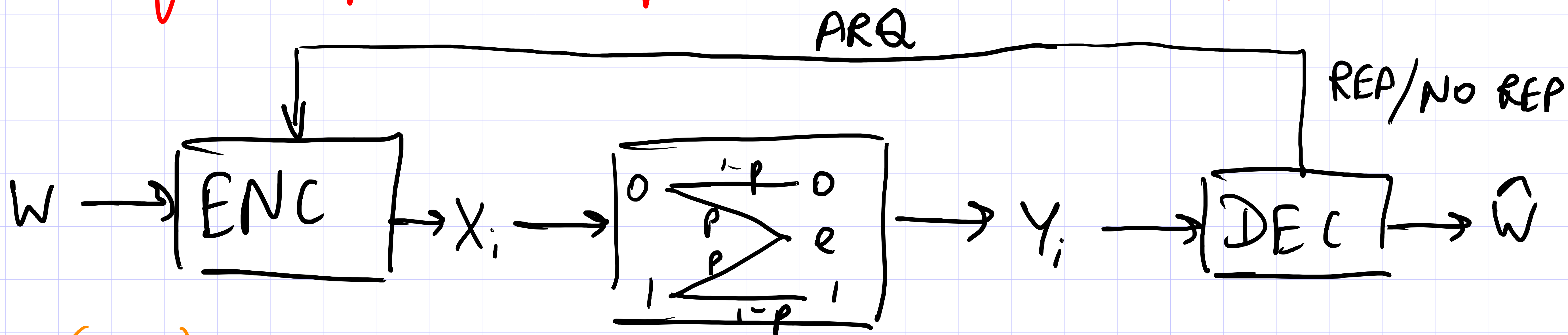
$$= H_2(p) + (1-p)\,H_2(\alpha)$$

$P_X(0) = \alpha$

$P_X(1) = 1-\alpha$

$$\max_{\alpha} H(Y) = H_2(p) + (1-p)$$

Achieving capacity of the BEC with feedback



(nR)

Error if total # transmissions $> n$

$$\mathbb{E}\left[\#\text{ transmissions required}\right] = (1-p) + 2p(1-p) + 3p^2(1-p) + 4p^3(1-p) + \cdots$$

for 1 msg bit

$$= \frac{1-p}{p} \sum_{i=1}^{\infty} i\, p^i$$

$$= \frac{1-p}{p} \frac{p}{(1-p)^2} = \frac{1}{1-p}$$

0 1 0 1 1 0

Tx 0 Rx 0

NO REP

Tx 1 Rx e

REP

Tx 1 Rx e

REP

Tx 1 Rx 1

NO REP

⋮

t

α_i = # transmissions for W_i

$$\mathbb{E}\,\alpha_i = 1/1-p$$

$$\Pr\left[\sum_{i=1}^{nR} \alpha_i > n\right]$$

$$\leq \Pr\left[\sum_{i=1}^{nR} \alpha_i > \frac{nR}{1-p}\left(\frac{1-p}{R}\right)\right]$$

$$= \Pr\left[\sum_i \alpha_i > \frac{nR}{1-p}\left(1 + \frac{1-p-R}{R}\right)\right]$$

$$\leq e^{-\left(\frac{1-p-R}{R}\right)^2 \frac{nR}{1-p}/3}$$

$$\boxed{R < 1-p,}$$

$P_e \longrightarrow 0$

$$\Pr[X \geq (1+\delta)\mu] \leq e^{-\delta^2\mu/3}$$