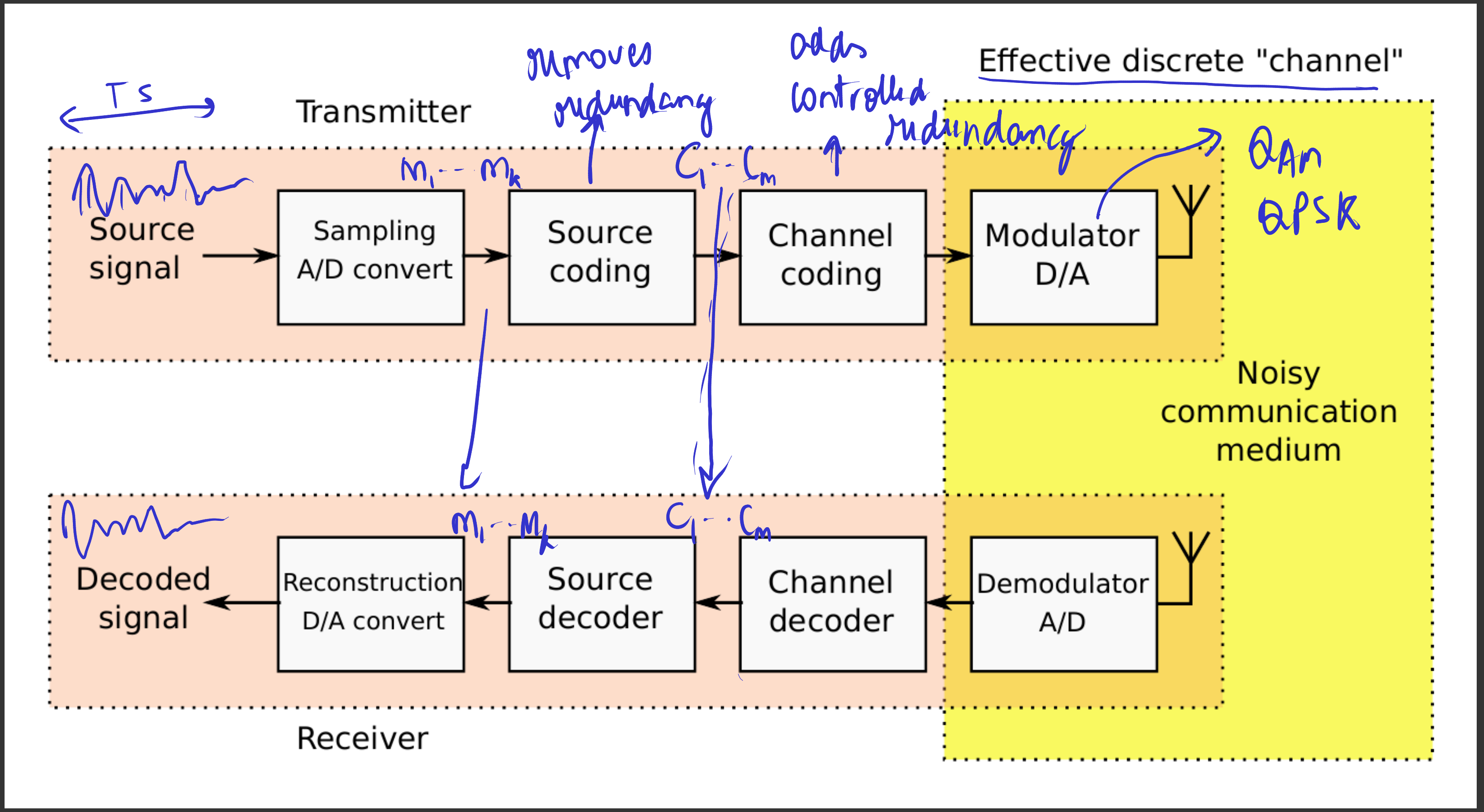
Channel Coding



Channel

"Channel law"

$P_{Y^n|X^n}$

$n \rightarrow$ # channel uses

<u>blocklength</u>

Channel is specified by $(\mathcal{X}, \mathcal{Y}, P_{Y^n|X^n})$

Input alphabet

Output alphabet

Assumptions:

1. Time slotted / discrete

2. $P_{Y^n|X^n}$ known

Discrete Memoryless Channel (DMC)

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

$$\begin{array}{ccccc} X_1 & X_2 & X_3 & \cdots & X_n \\ \downarrow & \downarrow & \downarrow & & \downarrow \\ Y_1 & Y_2 & Y_3 & & Y_n \end{array}$$

$$x^n \longrightarrow \boxed{\text{CHANNEL}} \longrightarrow y^n$$

$$P_{Y^n|X^n}(y^n|x^n) = P_{Y|X}(y_1|x_1)\, P_{Y|X}(y_2|x_2) \cdots P_{Y|X}(y_n|x_n)$$

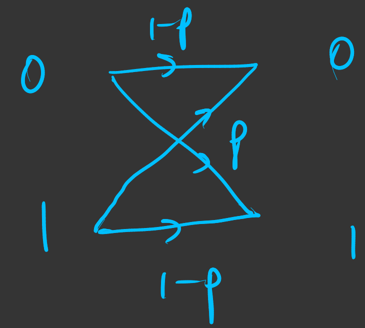
$$= \prod_{i=1}^{n} P_{Y|X}(y_i|x_i)$$

$P_{Y|X} \rightarrow$ Channel law of the DMC

Transition probabilities

① Binary Symmetric Channel with crossover probability p

$BSC(p)$



$$\begin{array}{ccccccc} X_1 & X_2 & X_3 & X_4 & X_5 & X_6 & X_7 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \end{array}$$

$X^n \quad 0 \; 1 \; 0 \; 0 \; 1 \; 1 \; 1 \; \cdots \; 1 \; 0$

$Y^n \quad 0 \; 1 \; 1 \; 1 \; 0 \; 0 \; 1 \; \cdots \; 1 \; 1$

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

$$P_{Y|X}(0|0) = 1-p = P_{Y|X}(1|1)$$

$$P_{Y|X}(1|0) = p = P_{Y|X}(0|1)$$

Hamming distance $\quad d_H(x^n, y^n) = \#$ of locations in which x^n, y^n differ

$$d_H(\underline{0}1010\underline{0}, \underline{1}1011\underline{1}) = 2$$

$$d_H(011011, 100100) = 6$$

$$\begin{array}{ccc} 0 & 1 & 1 \\ \downarrow & \downarrow & \downarrow \\ 1 & 0 & 1 \end{array}$$

$$p_{Y^n|X^n}(101 \mid 011) = p^2(1-p)$$

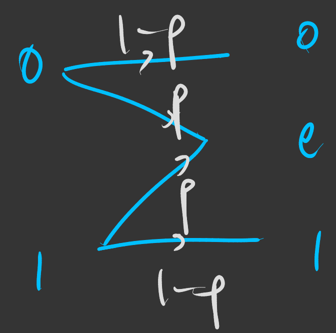
$$p_{Y^n|X^n}(010\,10 \mid 11011) = p^2(1-p)^3$$

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

① Binary Erasure Channel with erasure probability p

0 0 1 0 1 0

0 e 0 1 e 0 1 0



$\rightarrow$ erasure symbol

bi ary er su e

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

$$p_{Y|X}(0|0) = 1-p = p_{Y|X}(1|1)$$

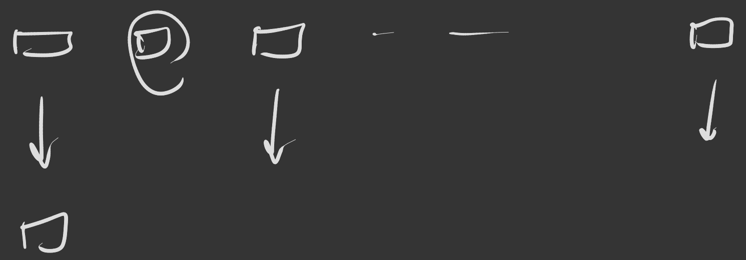
$$p_{Y|X}(e|0) = p = p_{Y|X}(e|1)$$

$$p_{Y|X}(1|0) = 0 = p_{Y|X}(0|1)$$

$$P_{Y^n|X^n}(e010 \mid 0110) = 0$$

$$\begin{array}{cccc} 0 & 1 & 1 & 0 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ e & 0 & 1 & 0 \end{array}$$

dropped.



erasure $\equiv$ packet drop

$$P_{Y^n|X^n}(0e1e \mid 0110) = p^2(1-p)^2$$

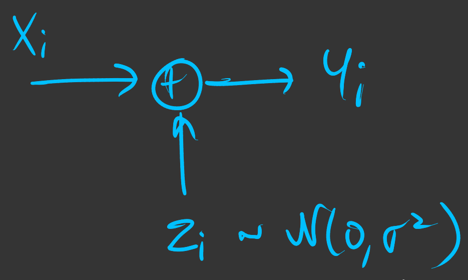
$$\begin{array}{cccc} 0 & 1 & 1 & 0 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 0 & e & 1 & e \end{array}$$

$$P_{Y^n|X^n}(y^n \mid x^n) = \begin{cases} p^{\eta}(1-p)^{n-\eta}, & (x^n, y^n) \text{ agree on all the unerased locations} \\ 0, & \text{else.} \end{cases}$$

$$\eta(y^n, x^n) = \#\text{ of erasures}$$

(3) Additive White Gaussian Noise (AWGN) channel

$$Y^n = X^n + Z^n$$



Noise variance

Constellation constrained AWGN channel

(1) Modulation scheme: BPSK

$X_i \in \{+\sqrt{P}, -\sqrt{P}\}$

$Y_i = X_i + Z_i$, $Z_i \sim \text{iid } \mathcal{N}(0, \sigma^2)$

QPSK / PAM / QAM / $X_i \in$ Constellation

$$\frac{1}{n}\sum_{i=1}^{n} X_i^2 \le P$$

$$\left\{ 1+\sqrt{2}j,\ 1-\sqrt{2}j,\ -1+\sqrt{2}j,\ -1-\sqrt{2}j \right\}$$

$Y_i = X_i + Z_i$ $\quad Z_i \sim \text{iid } \mathcal{CN}(0, \sigma^2)$

$= Z_i^{real} + j Z_i^{im}$

Z_i^r, Z_i^{im} iid $\mathcal{N}(0, \sigma^2/2)$

Power-constrained AWGN channels:

$$X^n \in \mathbb{R}^n$$

$$\boxed{\frac{1}{n}\sum_{i=1}^{n} X_i^2 \leq P} \longrightarrow \text{Power constraint}$$

$$Y_i = X_i + Z_i \qquad Z_i \text{ iid } \mathcal{N}(0,\sigma^2)$$

$$\mathcal{X} = \mathbb{R}, \quad \mathcal{Y} = \mathbb{R}, \qquad f_{Y|X}(y|x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-(y-x)^2/2\sigma^2}$$

Fading Channel

$$Y_i = h_i X_i + Z_i$$

$$Y_i = H_i X_i + Z_i$$

① Fast fading channel:

① $Y_i = h_i X_i + Z_i$

$Z_i \sim \mathcal{N}(0, \sigma^2)$

$h_i \sim$ iid f_H

} Real $\mathcal{X}, \mathcal{Y} = \mathbb{R}$

② $Y_i = h_i X_i + Z_i$ Complex $\mathcal{X}, \mathcal{Y} = \mathbb{C}$

$Z_i \sim$ iid $\mathcal{CN}(0, \sigma^2)$

$h_i \sim$ iid f_H

$Y^n \in \mathbb{C}^n$ $\quad p_{Y^n|X^n} \rightarrow$ DMC

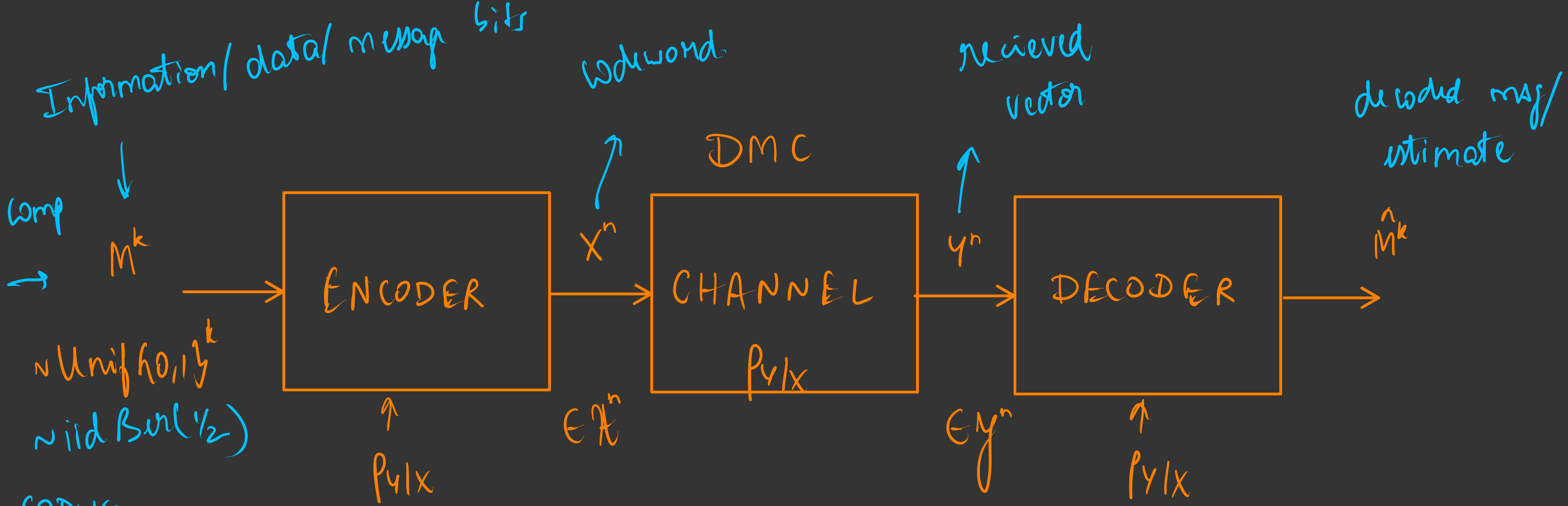
$\equiv \tilde{Y}^{2n} \in \mathbb{R}^{2n}$ $\quad p_{\tilde{Y}^{2n}|\tilde{X}^{2n}} \rightarrow$ NOT a DMC

Frequency-selective fading:

$$Y_i = h_0 X_i + h_1 X_{i-1} + h_2 X_{i-2} + Z_i$$

NOT a DMC

Has MEMORY



CODING SCHEME

ENC : $\{0,1\}^k \to \mathcal{X}^n$ —— DEC : $\mathcal{Y}^n \to \{0,1\}^k$

(1) Rate : $\frac{k}{n}$ → # of info bits sent per channel use

(2) Probability of error : $P_e = \Pr[\hat{M}^k \neq M^k]$

$$= \sum_{m^k \in \{0,1\}^k} \Pr[\hat{M}^k \neq M^k \mid M^k = m^k] \frac{1}{2^k}$$

$$P(\hat{m}^k \neq m^k \mid M^k = 00)\, p(M^k = 00)$$
$$+ \; P(\text{---''---} \mid M^k = 01)\, p(M^k = 01)$$
$$+ \; P(\text{---''---} \mid M^k = 10) \text{ --- ---}$$
$$\vdots$$

$$p(M^k = m^k) = \frac{1}{2^k}.$$

$$P_e^{max} = \max_{m^k} \Pr[\hat{m}^k \neq m^k \mid M^k = m^k]$$

Q: If we want $P_e \to 0$ as $n \to \infty$,

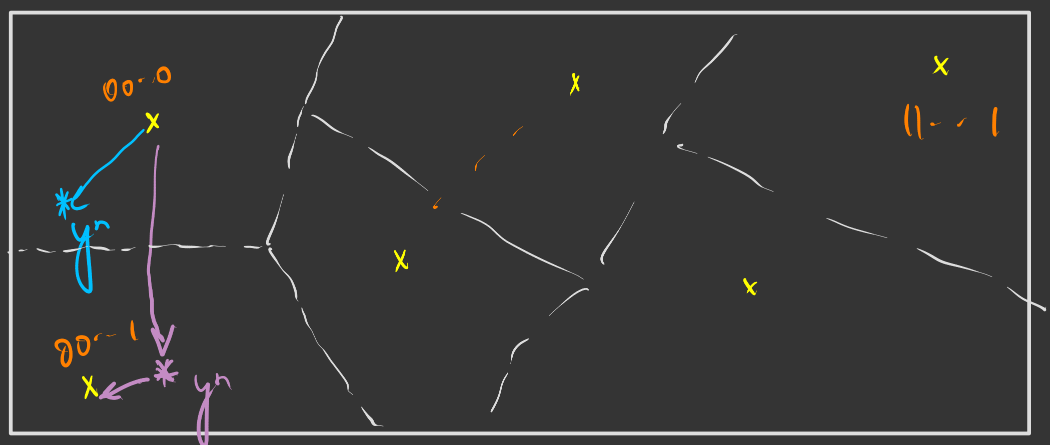
What is $\max \frac{k}{n} \to$?

$$\max_{P_e \to 0} \lim_{n \to \infty} R$$

Encoder

	messages M^k		codewords X^n	
m_0	$000 \cdots 0$	$\longmapsto$	$+\sqrt{P}, +\sqrt{P}, \cdots -\sqrt{P}, +\sqrt{P}$	$\in \mathcal{X}^n$
m_1	$00 \cdots 1$	$\longmapsto$	$+\sqrt{P}, -\sqrt{P}, \cdots +\sqrt{P}, -\sqrt{P}$	
$\vdots$	$\vdots$		$\vdots$	
m_{2^k}	$11 \cdots 1$	$\longmapsto$		

Visualization:



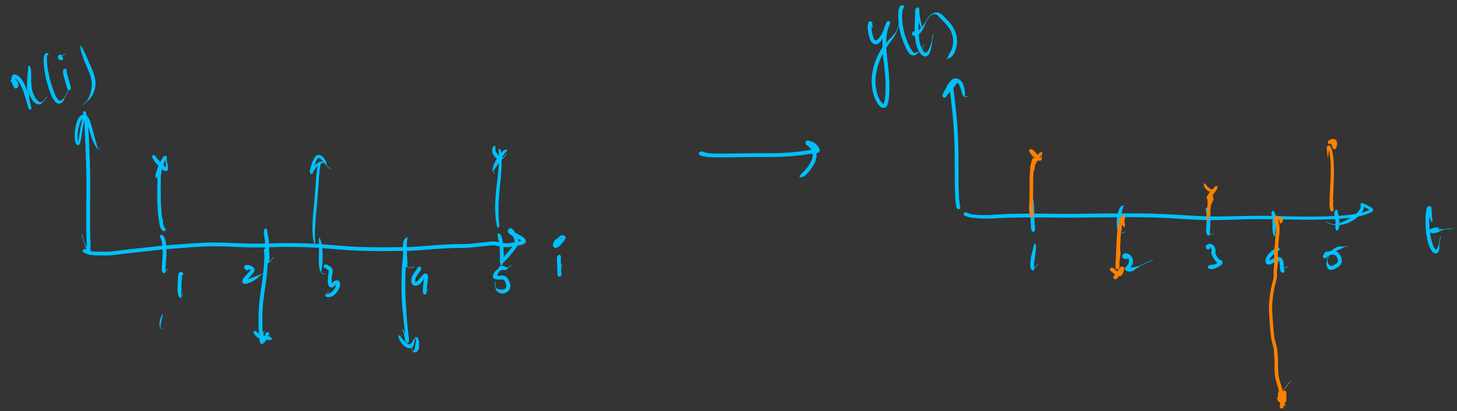
$\mathcal{X}^n = \mathcal{Y}^n$

$x \to c/w$

$$\underbrace{\overset{M^k}{0\ 0\ 0\ 0}} \longrightarrow \overset{X^n}{+\sqrt{P}\quad -\sqrt{P}\quad +\sqrt{P}\quad -\sqrt{P}\quad +\sqrt{P}}$$

$P = 4$

$$(2,\ -2,\ 2,\ -2,\ 2) \longrightarrow X^n$$



$$(1.2,\ -0.7,\ 0.2,\ -2.6,\ 1.3) \quad y^n$$

$y(t)$

Input to encoder $\rightarrow$ O/p of ENC i/p to CH $\longrightarrow$ O/p of CH i/p to DEC $\rightarrow$ O/p of DEC

DMC

m^k $\qquad X^n$ $\qquad y^n$ $\qquad \hat{m}^k$

$x(1), x(2) \sim x(n)$ $\qquad y(1) \sim y(n)$

$y(t)$ depends only on $x(t)$

$0\,0\,1\,0\,1 \mapsto +\sqrt{P}, \sqrt{P}, -\sqrt{P},$

m^k X^n are binary

$X^n = A\, m^k \longrightarrow$ linear code.

A: $n \times k$ matrix.

$X^n = A\, m^k$

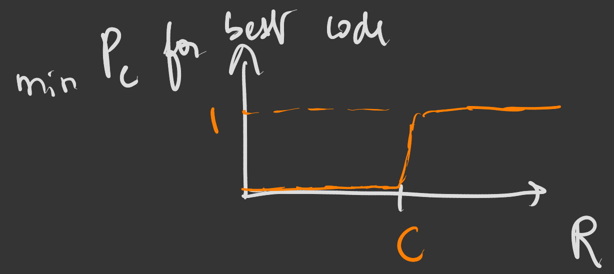
$[\;] = [\;\;][\;]$

Channel coding theorem

① for any DMC $p_{Y|X}$ on $(\mathcal{X}, \mathcal{Y})$, it is possible to construct (ENC, DEC) st

$$P_e = \Pr[\hat{m}^k \neq m^k] \to 0 \quad \text{as} \quad n \to \infty \quad \checkmark$$

as long as $R < C$



1948

90's

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

CAPACITY OF CHANNEL $p_{Y|X}$

Mutual Information : $I(X;Y) = \sum_{x,y} p_{XY}(x,y) \log_2 \frac{p_{XY}(x,y)}{p_X(x)\, p_Y(y)}$

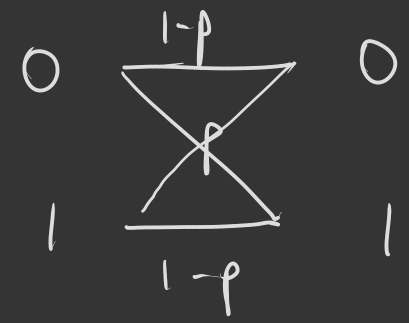
② If $R > C$, Then NO (ENC, DEC) can achive $P_e \to 0$

$X^n = G M^k$

$n \times k$

Linear code

How do we "code"? Start with a simple approach...



$$BSC(p) \qquad p \approx 0.1$$

$$X_i \sim Ber(1/2) \longrightarrow \boxed{BSC(p)} \longrightarrow Y_i$$

NO CODING: $P_e = Pr[Y_i \neq X_i] = p = 0.1$

NO CODING: $X^n \sim \text{iid } Ber(1/2) \longrightarrow \boxed{BSC(p)} \longrightarrow Y^n = \hat{X}^n$

$$0\,1\,0 \cdots 0 \qquad\qquad 1\,0\,1 \cdots 0$$

$$P_e = Pr[Y^n \neq X^n] = Pr[\text{any of the bits is flipped}]$$
$$= 1 - p(X^n = Y^n) = 1 - (1-p)^n \to 1$$

Repetition code:

$$\left.\begin{array}{l} 0 \longmapsto \overbrace{0\,0\,0 \cdots 0}^{\alpha \text{ times}} \\ 1 \longmapsto 1\,1 \cdots 1 \end{array}\right\} \text{ENC}$$

$$R = \frac{k}{n} = \frac{1}{\alpha}$$

DEC : Majority : Y^{α} if $\#$ 1's $\geq \alpha/2$, o/p 1

else o/p 0

$$M_i \longrightarrow X_i(1) \cdots X_i(\alpha) \longrightarrow Y_i(1) \cdots Y_i(\alpha)$$

$$(M_i \; M_i \cdots M_i)$$

$$0 \longrightarrow 0000 \longrightarrow 0100 \quad \text{DECLARE } 0$$

$$0111 \quad \text{DECL } 1$$

$$P_e = \Pr[\#\text{bit flips} \geq \alpha/2] = \sum_{j=\alpha/2}^{\alpha} \underbrace{\binom{n}{j} p^j (1-p)^{n-j}}_{\Pr[\#\text{ of flips} = j]}$$

$\binom{n}{j} \downarrow$ # of ways of j loc

$\longrightarrow 0$ as $\alpha \to \infty$

$$M^k \longrightarrow \boxed{\mathrm{ENC}} \xrightarrow{X^n} \boxed{\mathrm{BSC}(p)} \xrightarrow{Y^n} \boxed{\mathrm{DEC}} \longrightarrow \hat{M}^k$$

$$\mathbb{E}[\#\,\text{bit flips}] = \mathbb{E}\, d_H(x^n, y^n) =$$

$$\Pr[\, d_H(X^n, Y^n) > np(1+\varepsilon) \,] \longrightarrow 0$$

DEC: Bounded Hamming distance decoder

If there is unique c/w x^n s.t.

$d_H(x^n, y^n) \le np(1+\varepsilon)$, output x^n

Else error

Intuition:

$$2^k \approx \frac{Vol(\mathcal{X}^n)}{Vol(Ball)}$$