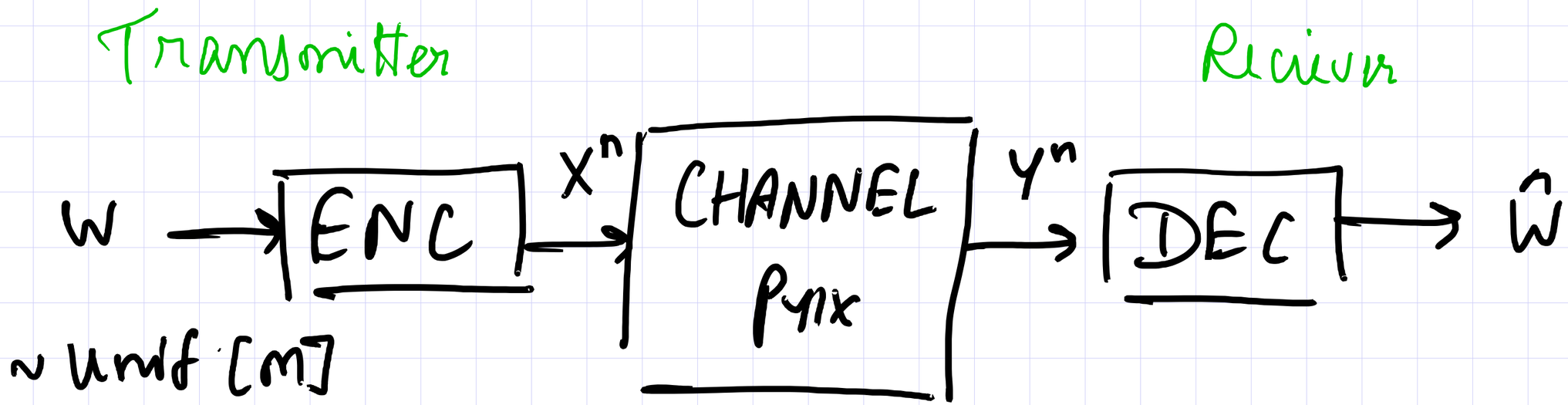
PROOF OF THE CHANNEL CODING THEOREM

EE 6317



$$R = \frac{\log_2 M}{n}$$

$$P_e = \frac{1}{M} \sum_{i=1}^{M} Pr[\hat{W} \neq W | W = i]$$

Channel coding theorem

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

$$\alpha(P_{Y|X})$$

For every $\epsilon > 0$

① $\exists$ sequence of (n, M_n) codes $\lim_{n\to\infty} P_e^{(n)} = 0$

(Achievability)

$$\lim_{n\to\infty} \frac{\log_2 M_n}{n} \geq \alpha(P_{Y|X}) - \epsilon$$

② (Converse) For any sequence of (n, M_n) codes with

$$\lim_{n\to\infty} \frac{\log_2 M_n}{n} > \alpha(P_{Y|X}) + \epsilon,$$

$$\lim_{n\to\infty} P_e^{(n)} = 1$$

Lemmas

(L1) Fano's inequality $W, \hat{W}$ $P_e = P_r[W \neq \hat{W}]$

$$H(W|\hat{W}) \leq H_2(P_e) + P_e \log_2 |\mathcal{W}|$$
$$\leq 1 + P_e \log_2 |\mathcal{W}| \leq 1 + P_e nR$$

(L2) For any X^n, if Y^n obtained by passing X^n through DMC $p_{Y|X}$, then

$$I(X^n; Y^n) \leq nC$$

Any distributions (iid, correlated)

Proof of converse

For any R,

$$
\begin{aligned}
nR &= H(W) && W \sim \mathrm{Unif}([M]) \\
&= H(W|\hat{W}) + I(W;\hat{W}) \\
&\le 1 + P_e(nR) + I(W;\hat{W}) && (L1) \\
&\le 1 + P_e(nR) + I(X^n;Y^n) \\
&\le 1 + P_e \times nR + nC && (L2)
\end{aligned}
$$

$$
\begin{aligned}
R &\le \frac{1}{n} + P_e \times R + C \\
P_e \times R &\ge R - C - \frac{1}{n} \\
P_e &\ge 1 - \frac{C}{R} - \frac{1}{nR} \\
\lim_{n\to\infty} P_e &\ge 1 - \frac{C}{R} > 0 \quad \text{if} \quad R > C.
\end{aligned}
$$

Proof of L2 : $I(X^n; Y^n) \leq nC$

$$I(X^n; Y^n) = H(Y^n) - H(Y^n/X^n)$$

$$= H(Y^n) - \sum_{i=1}^{n} H(Y_i | X^n, Y_1 \cdots Y_{i-1})$$

$$\overset{?}{=} H(Y^n) - \sum_{i=1}^{n} H(Y_i | X_i) \longrightarrow \text{DMC}$$

$$= \sum_{i=1}^{n} H(Y_i | Y_1 \cdots Y_{i-1}) - \sum_{i=1}^{n} H(Y_i | X_i)$$

$$\leq \sum_{i=1}^{n} H(Y_i) - \sum_{i=1}^{n} H(Y_i | X_i)$$

$$= \sum_{i=1}^{n} I(X_i; Y_i) \leq nC$$