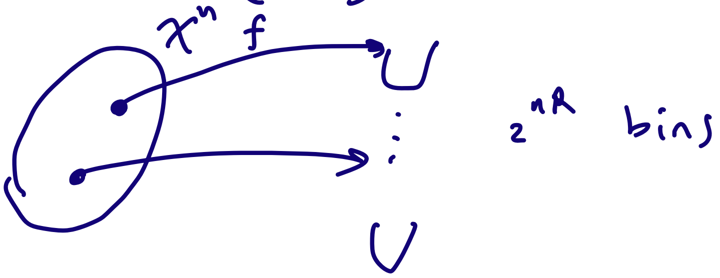
Lec 12: Duality of channel coding & Random ext.

Random binning: + Review of classical coding

$X^n, Y^n \sim P_{XY}^{\otimes n}$ $\quad \mathcal{X}^n \times \mathcal{Y}^n$

$f: \mathcal{X}^n \longrightarrow [2^{nR}]$

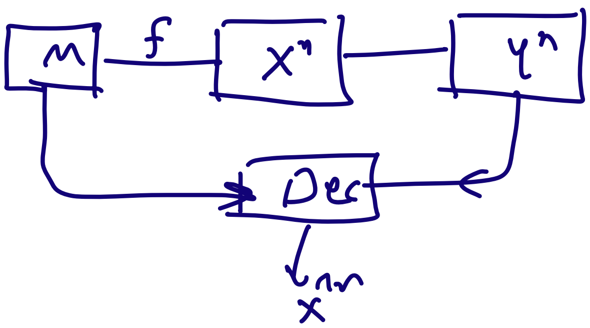


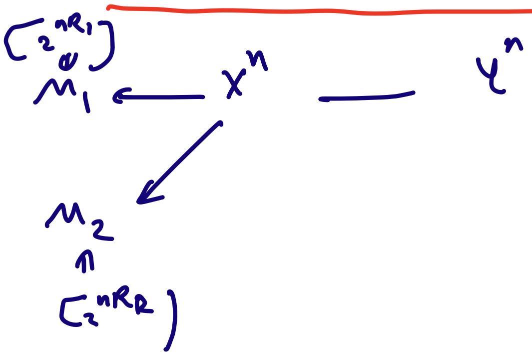
Let $M = f(X^n)$ three random variables M, X^n, Y^n

For a random choice of f

1) $R < H(X|Y)$ $\quad P_{MY^n} \approx P_{unif} \times P_{Y^n}$

2) $R > H(X|Y)$ we can decode X^n from Y^n & M





1) $R_1 + R_2 < H(X)$

2) $R_2 > H(X|Y)$

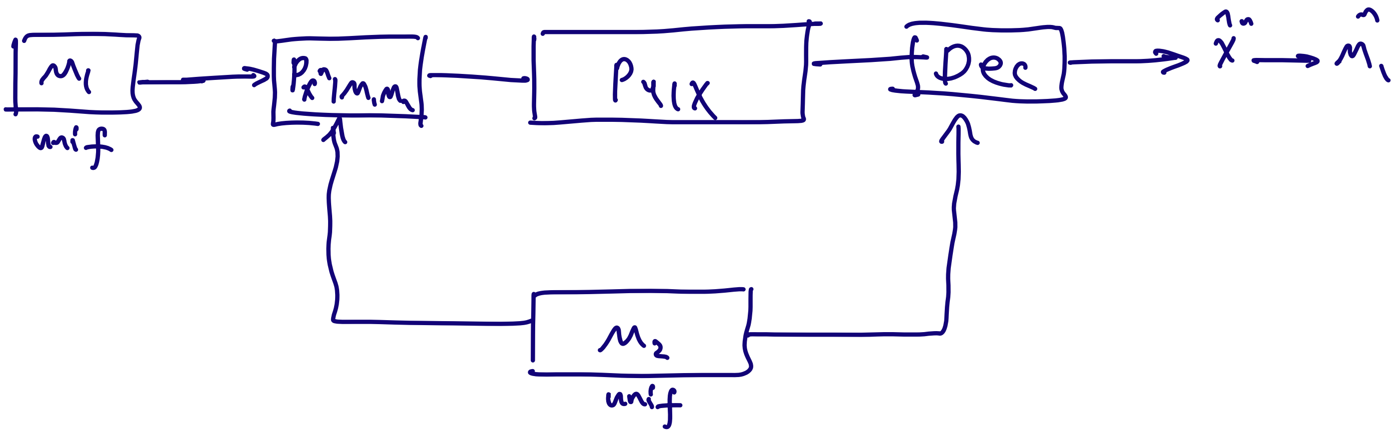
We have four random variables $M_1 M_2 X^n Y^n$

Joint dist $P_{M_1 M_2 X^n Y^n} = P_{M_1 M_2} P_{X^n | M_1 M_2} P_{Y^n | X^n}$

1) $\Longrightarrow$ $P_{M_1,M_2} \times P_{Y^n} \approx P_{unif}$

2) $\Longrightarrow$ $\exists$ $Dec : \mathcal{Y}^n \times [2^{nR_2}] \longrightarrow \mathcal{X}^n : \Pr(X^n \neq Dec(Y^n, M_2)) \approx 0$

Take Dec, $P_{X^n|M_1M_2}$



$$Q_{M_1,M_2X^nY^n} = Q_{M_1M_2} P_{X^n|M_1,M_2} P_{Y^n|X^n}$$

$$\Pr_{M_2}\left[Dec(Y^n, M_2) \neq X^n \right] \approx 0$$

$\Longrightarrow$ $\exists$ fixed m_2

$$x^n \longrightarrow \boxed{BSC} \longrightarrow y^n$$

$x^n = y^n \oplus z^n \qquad z^n$ iid $Be(p)$

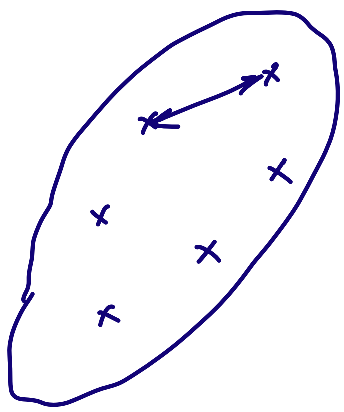
$$\underset{[2^{nR}]}{m} \longrightarrow \boxed{Enc} \xrightarrow{x^n} \boxed{BSC} \xrightarrow{y^n} \boxed{Dec} \longrightarrow \underset{[2^{nR}]}{\hat{m}}$$

$Enc: [2^{nR}] \longrightarrow \{0,1\}^n$

$Dec: \{0,1\}^n \longrightarrow [2^{nR}] \longrightarrow$

$\mathcal{C} = \{ Enc(m) : m \in [2^{nR}] \}$ codebook

$\{0,1\}^n$



A good code consists of points with large min distance

min distance $\min_{x \neq y \in \mathcal{C}} d(x,y) \longrightarrow$ Hamming distance

A code with min distance d

can detect $d-1$ errors correct $\left\lfloor \frac{d-1}{2} \right\rfloor$

Linear code: $A \subseteq \{0,1\}^n$ linear subspace i.e., $x, y \in A \implies x+y \in A$

$|A| = 2^k$, $\quad A = \{ Gx : x \in \{0,1\}^k \} \quad G \;\; n \times k$

$= \{ y \in \{0,1\}^n : Hy = 0 \} \quad H \;\; (n-k) \times n$

min distance: $\min_{x \neq 0} d(0, x)$

Repetition code: $\quad 0 \longrightarrow 0^n$

$1 \longrightarrow 1^n$

$k = 1$, $\quad G = [1 \cdots 1]$, $\quad H = \begin{pmatrix} 1 & 1 & & & \\ & 1 & 1 & & \\ & & 1 & 1 & \\ & & & & \ddots \end{pmatrix}$

min distance $= n$

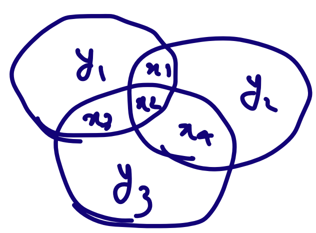
Parity check

$x_1 \cdots x_{n-1} \longrightarrow x_1 \cdots x_{n-1}, \bigoplus_{i=1}^{n-1} x_i$

$G = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \\ 1 & \cdots & 1 \end{bmatrix} \qquad H = [1 \cdots 1]$

min distance 2

Hamming code $\quad n = 7, \; k = 4$



$x_1 \cdots x_4 \longmapsto x_1 \cdots x_4 \, y_1 y_2 y_3$

min distance is 3

Singleton bound $k \leq n-d+1$

Gilbert Varshamov $\forall\ 0 \leq \delta \leq 1/2 \quad \forall\ 0 \leq \varepsilon \leq 1-h_2(\delta)$

$\exists$ linear code with n (large enough)

$k \geq n(1-h_2(\delta)-\varepsilon)$ & min distance $\geq \delta n$