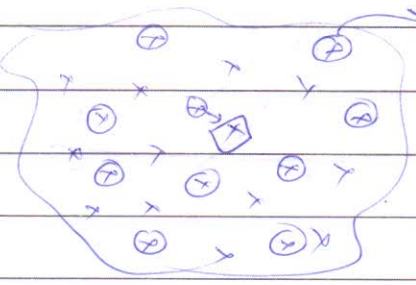
lec 19: Overview of Error correcting codes

Principle of error correction



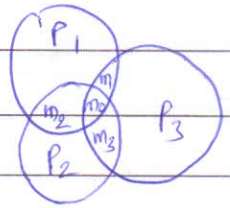
Source → Encoder → Channel → Decoder →

Code classes

- Generic
- Hamming
- Linear
  - Cyclic codes
  - RM, RS
- bounded distance issue
- LDPC Codes
- Polar Codes
- Capacity achieving codes

Hamming Code (1950)

$[n=7, M=16, d_{min}=3]$



$m_0 + m_1 + m_2 + p_1 = 0 \pmod 2$ even parity

Linear codes

$$\underline{c}^t = \underline{u}^t G$$

$$[m_0\ m_1\ m_2\ m_3] \begin{bmatrix} 1&0&0&0&1&1&1 \\ 0&1&0&0&1&0&1 \\ 0&0&1&0&1&1&0 \\ 0&0&0&1&0&1&1 \end{bmatrix} = [m_0\ m_1\ m_2\ m_3\ p_1\ p_2\ p_3]$$

Cyclic codes

$$[m_0\ m_1\ m_2\ m_3] \begin{bmatrix} 6&5&4&3&2&1&0 \\ 0&0&1&0&1&1&1 \\ 0&1&0&1&1&1&0 \\ 1&0&1&1&1&0&0 \\ 0&1&1&1&0&0&1 \end{bmatrix} = [c_0\ c_1\ \dots\ c_6]$$ (same code)

Every cyclic shift is a codeword

$$\frac{x^7+1}{x^3+x+1} = (x+1)(x^3+x^2+1) = x^4+x^3+x+x^3+x^2+1$$
$$= x^4+x^2+x+1$$

Cyclic codes - BCH codes (1959)

(Bose, Chaudhary, Hocquenghem)

For cyclic codes, there is a way to define transform

$c_0, \dots c_6 \Rightarrow \hat{c}_0, \hat{c}_1, \dots \hat{c}_6$ $\quad \hat{c}_0 \hat{c}_1 0\,0 \hat{c}_4 \hat{c}_5 \hat{c}_6$

$c_i \to (+) \to y_i$, with e_i entering the adder

channel ↓

$y_0, \dots y_6 \xrightarrow{\text{Transform}} \hat{y}_0, \hat{y}_1, \hat{y}_2, \hat{y}_3, \hat{y}_4, \hat{y}_5, \hat{y}_6$

Can recover the error pattern

Parameters of a linear code

$[n, k, d_{min}]$ ← minimum distance

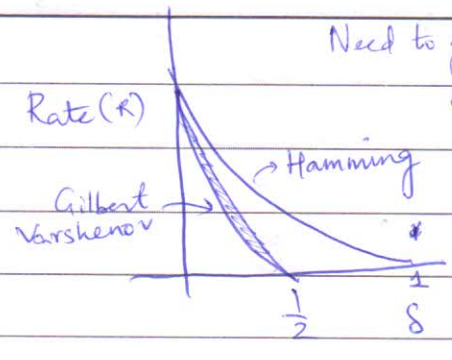
block length ⇓ dimension

linear code: A subspace of $\mathbb{F}_2^n$ with dimension k.

$\therefore M = 2^k$

no of codewords

$\therefore$ Rate$(R) = \frac{\log_2 M}{n} = \frac{k}{n}$



Need to go for decoding other than bounded distance decoding in order to achieve capacity.

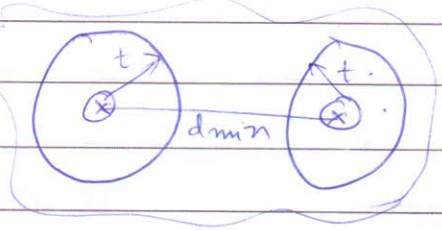
BSC

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

$= 1 - H(\epsilon, 1-\epsilon)$

$\delta = \frac{d_{min}}{n}$

$R = \frac{\log |C|}{n} = \frac{k}{n}$ (linear)



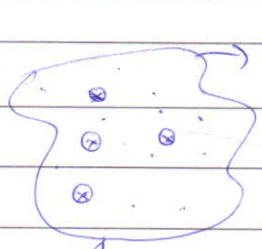
$t = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor$ $\quad d_{min} \geq 2t+1$.

Long Codes

$\{c_k\}$ → BSC → $\{y_k\}$ as $n \to \infty$, the # of errors $\to n\epsilon$ with high probability.

$P_e\left(|N_\epsilon - n\epsilon| > \rho\right)$ can be made arbitrarily small given any ρ.

Reed Muller Codes



set of all boolean functions $\{f(x_1, x_2, x_3)\}$

x_1 \ x_2x_3	00	01	10	11
0	0	0	1	1
1	1	1	0	0

$f(x) = x_1 + x_2$ (say) → XOR

Codes $\Rightarrow u_0 + u_1 x_1 + u_2 x_2 + u_3 x_3$.

$(n = 8, k = 4, d_{min} = 4)$

000	001	010	011	100	101	110	111
0	0	1	1	1	1	0	0

Codeword = [0 0 1 1 1 1 0 0]

Codeword

LDPC

$c_1 + c_2 + c_4 = 0$

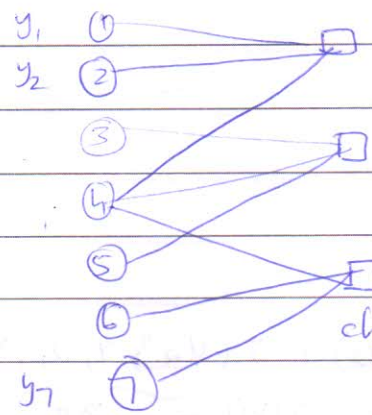
$c_3 + c_4 + c_5 = 0$

$c_4 + c_6 + c_7 = 0$.

linear codes.

Gallager (1960)

Low density parity check codes.



Gallagar A, B algorithms to choose y_i's based on belief from check nodes.

Hamming code

$$\begin{bmatrix} 1&1&1&0&1&0&0 \\ 1&0&1&1&0&1&0 \\ 1&1&0&1&0&0&1 \end{bmatrix} \begin{bmatrix} m_0 \\ m_1 \\ m_2 \\ m_3 \\ P_1 \\ P_2 \\ P_3 \end{bmatrix} = 0$$

parity check matrix H

$$\begin{bmatrix} 1&1&0&1&0&0&0 \\ 0&0&1&1&1&0&0 \\ 0&0&0&1&0&1&1 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \end{bmatrix} = \underline{0}$$

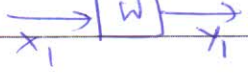
LPC.

Spatial coupling ~~of these~~ codes were shown to achieve capacity over binary-input memoryless channels. This includes BEC, BSC, Binary input AWGN

$x_i \in \{\pm 1\} \rightarrow (+) \rightarrow y_i = x_i + n_i$

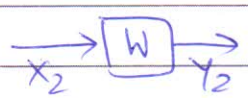
$n_i \uparrow \in \eta(0, \sigma^2)$.

Polar Codes. Achieve capacity and can be made explicit



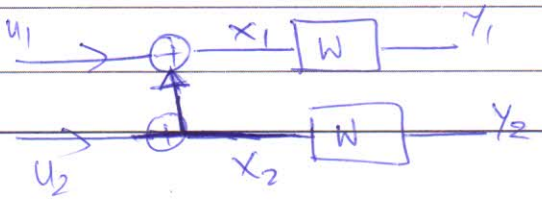
$I(x_1; y_1)$ $\quad W \equiv$ channel

$x_i \in \{0,1\}$



$I(x_2; y_2)$ $\quad$ binary input DMC $\in [0, 1]$

$I(W) = I(x_1; y_1)$



$I(x_1 x_2; y_1 y_2) = 2I(W)$

$= I(U_1 U_2; Y_1 Y_2)$

$= I(U_1; Y_1 Y_2)$

$+ I(U_2; Y_1 Y_2 | U_1)$

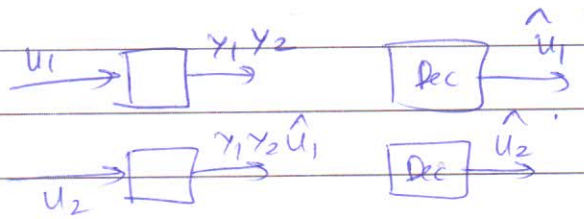
$X_2 = U_2$

$X_1 = U_1 + U_2$.

$I(U_1; Y_1 Y_2) + I(U_2; Y_1 Y_2 U_1) = I(W^-) + I(W^+)$

$\tilde{U}_1 = \hat{U}_1$

$\tilde{U}_2 = \hat{U}_2$ with $\hat{U}_1 = U_1$



It can be seen that

$$I(U_2; Y_1 Y_2 U_1) = I(U_2; Y_2) + I(U_2; Y_1, U_1 | Y_2)$$

$$\geq I(U_2; Y_2) = I(W) \qquad \geq 0.$$

$$\Rightarrow I(U_2; Y_1 Y_2 U_1) = I(W^+) \geq I(W).$$

and $I(U_1; Y_1 Y_2) \leq I(W)$

$I''(W^-)$.