Lecture 4

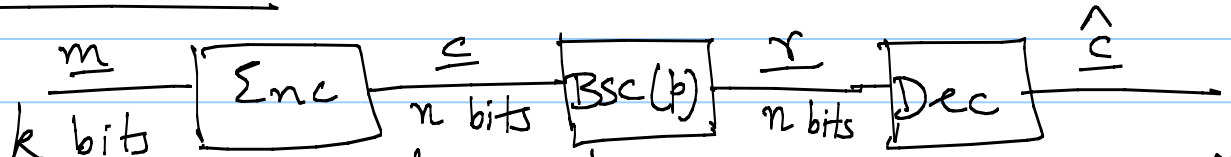
Note Title 1/9/2008

Ex:

$$H = \begin{array}{c} \begin{matrix} m_0 & m_1 & m_2 & p_0 & p_1 & p_2 \end{matrix} \\ \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \end{array} \qquad (6,3)\ \text{Code}$$

$$C = \{000000,\ 001011,\ 010110,\ 011101,\ 100101,\ 101110,\ 110011,\ 111000\}$$

Decoder:



$Pr(c \neq \hat{c})$: block-error probability

$$\Pr(\hat{\underline{c}} \neq \underline{c}) = \sum_{\underline{r}} \Pr(\hat{\underline{c}} \neq \underline{c} \mid \underline{r}) \Pr(\underline{r})$$

$$\text{Min } \Pr(\hat{\underline{c}} \neq \underline{c}) \Longleftrightarrow \text{Min } \Pr(\hat{\underline{c}} \neq \underline{c} \mid \underline{r})$$

for each $\underline{r}$

$$\text{Min } \Pr(\hat{\underline{c}} \neq \underline{c} \mid \underline{r}) \Longleftrightarrow \text{Max } \Pr(\hat{\underline{c}} = \underline{c} \mid \underline{r})$$

$$\text{Max } \Pr(\hat{\underline{c}} = \underline{c} \mid \underline{r}) = \frac{\Pr(\underline{r} \mid \underline{c} = \hat{\underline{c}}) \cdot \Pr(\underline{c} = \hat{\underline{c}})}{\Pr(\underline{r})}$$

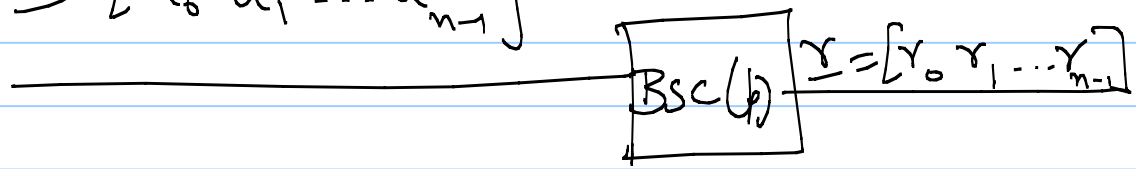
codewords equally likely

Maximum-Likelihood Decoder:

$$\max_{\hat{\underline{c}} \in C} \Pr(\underline{r} \mid \underline{c} = \hat{\underline{c}})$$

Better expression: $\hat{\underline{c}} = \arg \max_{\underline{u} \in C} \Pr(\underline{r} \mid \underline{c} = \underline{u})$

$Pr(\underline{r} \mid \underline{c} = \underline{u})$: $\underline{u} = [u_0\ u_1 \cdots u_{n-1}]$



$\underline{u} = [0\ 0\ 0]$

$\underline{r} = [1\ 1\ 0]$ (p, p, 1−p)

$$r_i = \begin{cases} u_i & \text{w. p. } 1-p \\ \overline{u}_i & \text{w. p. } p \end{cases}$$

$$Pr(\underline{r} \mid \underline{u}) = p^{(\#\text{ of places of disagreement})} (1-p)^{n-}$$

Hamming Distance $d_H(\underline{u}, \underline{v})$ = # of places of disagreement between $\underline{u}$ & $\underline{v}$

$$Pr(\underline{r} \mid \underline{u}) = p^{d_H(\underline{r},\underline{u})} \cdot (1-p)^{n-d_H(\underline{r},\underline{u})}$$

$$= (1-p)^n \cdot \left(\frac{p}{1-p}\right)^{d_H(\underline{r},\underline{u})}$$

$$\hat{\underline{c}} = \arg \max_{\underline{u} \in C} P_r(\underline{r} \mid \underline{u}) \propto \left(\frac{p}{1-p}\right)^{d_H(\underline{r},\underline{u})}$$

$$= \arg \max_{\underline{u} \in C} d_H(\underline{r},\underline{u}) \log \frac{p}{1-p}$$

$$\hat{\underline{c}} = \arg \min_{\underline{u} \in C} d_H(\underline{r},\underline{u})$$

Ex: $C = \{000, 111\}$

$\underline{r}$	$\hat{\underline{c}}$
000	000
001	000
010	000
100	000
011	111
101	111
110	111
111	111

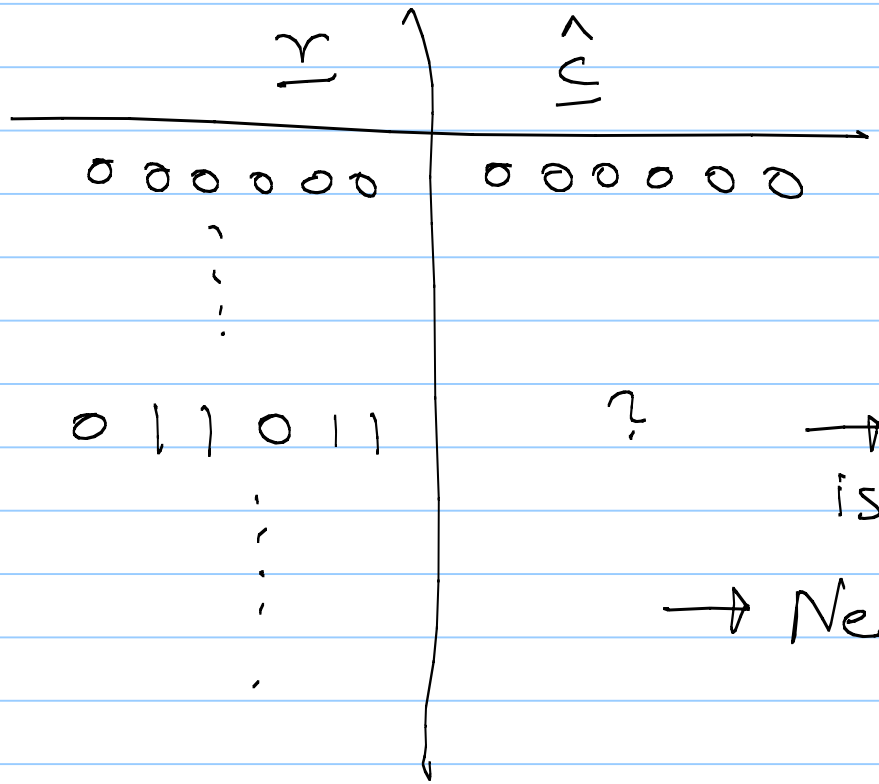
$$P_r(\text{Error}) = 3p^2(1-p) + p^3$$

$$= 3p^2 - 2p^3$$

$$R = 1/3$$

Ex: (6,3) Example

$$C = \{000000, 001011, 010110, 011101, 100101, 101110, 110011, 111000\}$$

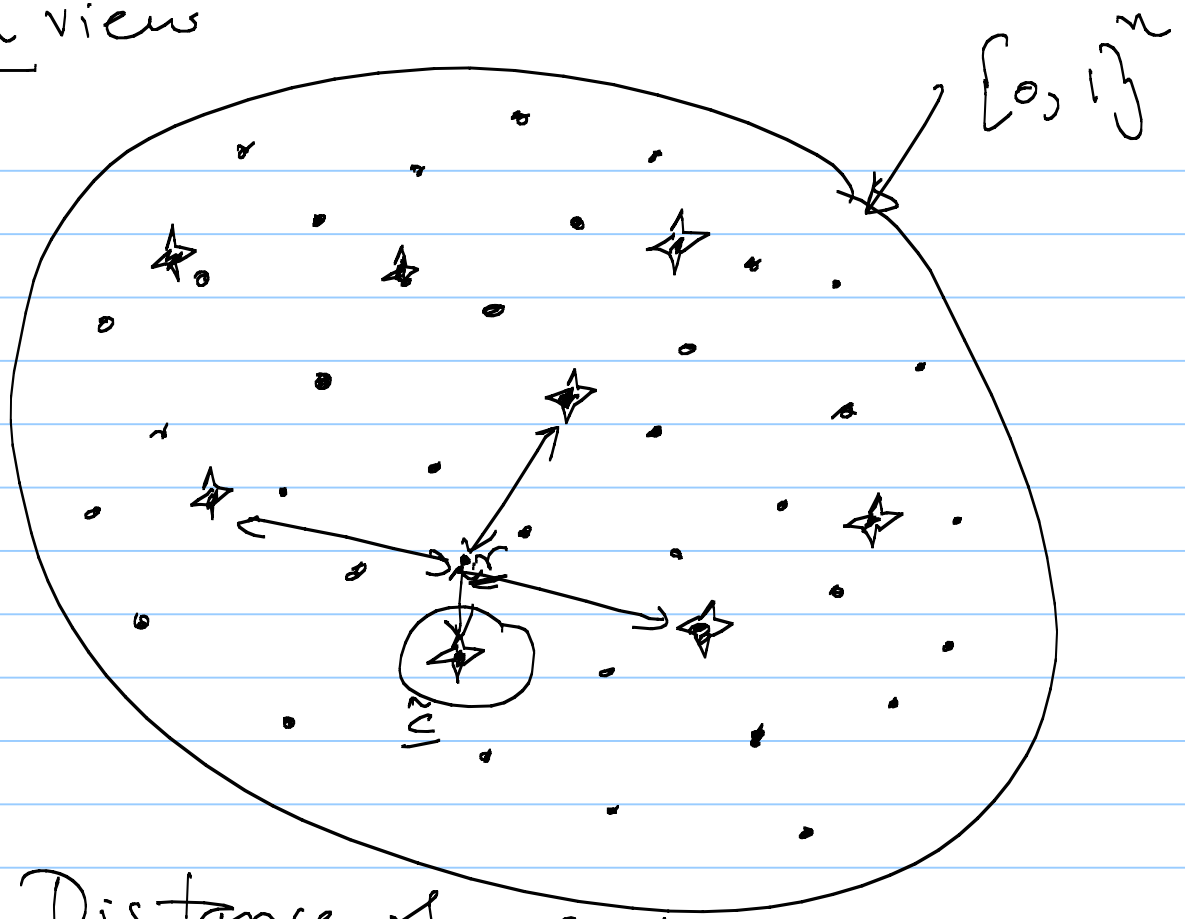


(1000,500) code ?

→ efficient implementation is non-trivial

→ Nearest neighbour decoder.

Graphical views



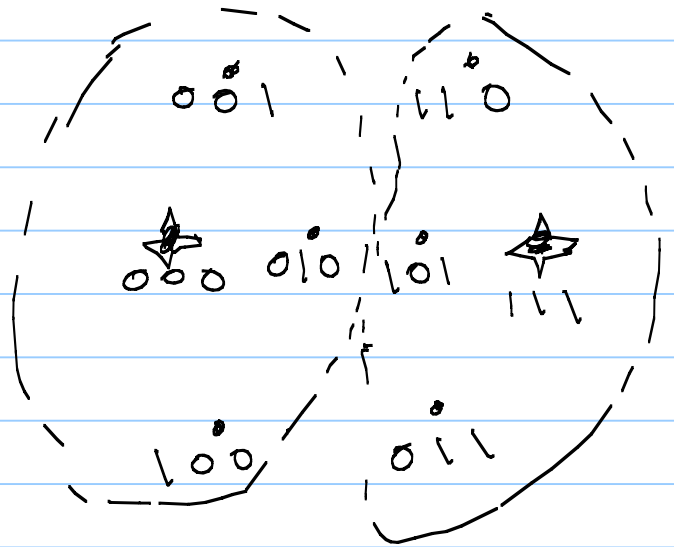
Minimum Distance of a Code

Defn: $$d = \min_{\substack{\underline{u},\underline{v} \in C \\ \underline{u} \neq \underline{v}}} d_H(\underline{u},\underline{v})$$

Error-correcting capability:

$$t = \left\lfloor \frac{d-1}{2} \right\rfloor$$ errors made by the channel are correctable for a code with minimum distance d

Ex:



(3, 1) Code

$C = \{000, 111\}$

$d = 3$

$t = 1$

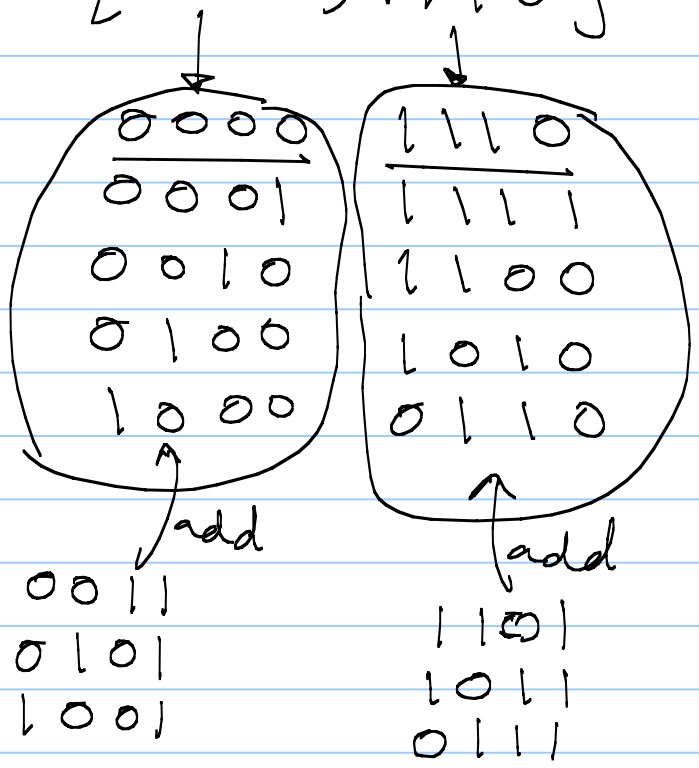
Ex: 1) $n=4,\ k=2 \quad C=\{0000, 0011, 1100, 1111\}$

$d=2,\ t=0$

2) $n=4,\ k=1,\ C=\{0000, 1110\}$

$d=3,\ t=1$

$Pr(\text{Error}) = 3p^2 - 2p^3$



Ex: (6, 3) Code

$C = \{000000, 001011, 010110, 011101, 100101, 101110, 110011, 111000\}$

$$d = \min_{\underline{u}, \underline{v} \in C, \underline{u} \neq \underline{v}} d_H(\underline{u}, \underline{v}) = wt(\underline{u} + \underline{v})$$

wt = # of 1s in a vector

$$= \min_{\underline{w} \in C, \underline{w} \neq 0} wt(\underline{w})$$

only for linear codes

$= 3$

(n, k, d) Code $\Rightarrow$ n = length, k = dimension, d = minimum distance

$C = \{000000, 001011, 010110, 011101, 100101,$
$101110, 110011, 111000\}$