Note Title 1/10/2008

Lecture 5

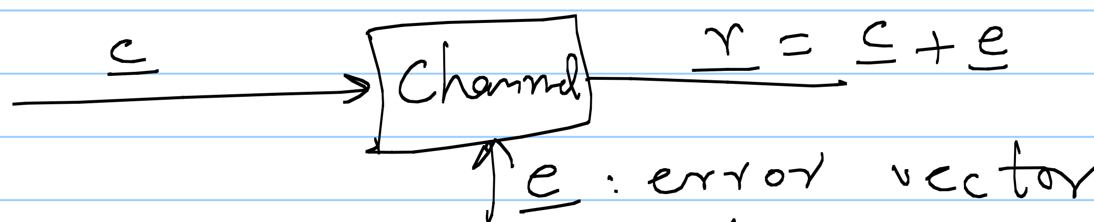
(n, k, d) Code : linear, binary

→ How do you construct?

→ How do you decode?

Syndrome Decoder: nearest neighbour for linear codes

(n, k, d) Code C : H → a parity-check matrix



$r_i = c_i + e_i$

$\Pr(e_i = 1) = p$

$\Pr(\underline{e} = \text{all-zero}) = (1-p)^n$

$\Pr(\underline{e}) = p^{wt(\underline{e})} (1-p)^{n - wt(\underline{e})}$

Decoder: $\min_{\underline{u} \in C} d_H(\underline{r}, \underline{u}) = \min_{\underline{e} : \underline{r} + \underline{e} \in C} wt(\underline{e})$

$\underline{e} : \underline{r} + \underline{e} \in C \rightarrow 2^k$ possibilities

$\underline{r} = \underline{c} + \underline{e}$

$\underline{r}$: knows this

$\underline{c}$, $\underline{e}$: find $\underline{c}$ (or) $\underline{e}$

Syndrome: $\underline{s} = H \underline{r}^T = H \underline{e}^T$

$\rightarrow$ Any $\underline{e}$ that satisfies $H\underline{e}^T = \underline{s}$ will be s.t. $\underline{r} + \underline{e} \in C$.

$$\begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_{n-k} \end{bmatrix} = \begin{array}{c} \\ n-k \end{array} \overbrace{\begin{bmatrix} & & \\ & H & \\ & & \end{bmatrix}}^{n} \begin{bmatrix} e_0 \\ e_1 \\ \vdots \\ e_{n-1} \end{bmatrix}$$

Decoder:
$$\underline{\hat{e}} = \arg\min_{\underline{e}\,:\,\underline{s} = H\underline{e}^T} wt(\underline{e})$$

$$\underline{\hat{c}} = \underline{r} + \underline{\hat{e}}$$

$\longrightarrow$ Finding minimum weight solution to the linear equation $\underline{s} = H\underline{e}^T$

Ex: (6, 3, 3) Code

$$H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

$$\underline{r} = [0\ 1\ 0\ 1\ 0\ 1]$$

$$\underline{s} = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} e_0 \\ e_1 \\ e_2 \\ e_3 \\ e_4 \\ e_5 \end{bmatrix}$$

$$\underline{\hat{e}} = [0\ 0\ 1\ 0\ 0\ 0]$$

$$\underline{\hat{c}} = [0\ 1\ 1\ 1\ 0\ 1]$$

Self-study $\rightarrow$ syndrome table

Complexity: (n, k, d) Code.

$\longrightarrow$ Try $\underline{e}$ of wt $\leq t$

$$\# = 1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{t} \simeq 2^{n f(t)} \qquad \in [0,1]$$

$\longrightarrow$ need to solve for $\underline{s} = H \underline{e}^T$ smartly ....

Ex:

$$H = n-k \begin{array}{c} \begin{array}{cccccccc} & p & n & & & & \underline{m} & \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \end{array} \qquad \begin{array}{l} n = 8 \\ k = 4 \end{array}$$

$\longrightarrow \underline{r} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \end{bmatrix} = \underline{\hat{c}} \qquad \underline{s} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$

$\longrightarrow \underline{r} = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \qquad \underline{s} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \qquad \underline{\hat{e}} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{bmatrix}$

(or) $\underline{\hat{e}} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

Minimum Distance & H

$\rightarrow \quad \underline{c} \in C \qquad H\,\underline{c}^T = \underline{0}$

$$\begin{bmatrix} | & | & & | \\ \underline{h}_0^T & \underline{h}_1^T & \cdots & \underline{h}_{n-1}^T \\ | & | & & | \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

$$c_0 \underline{h}_0^T + c_1 \underline{h}_1^T + \cdots + c_{n-1} \underline{h}_{n-1}^T = \underline{0}$$

$wt(\underline{c}) = w$ & w 1s in $\underline{c}$ are at positions $i_1, \ldots, i_w$

$\Uparrow$

$$c_{i_1} \underline{h}_{i_1}^T + c_{i_2} \underline{h}_{i_2}^T + \cdots + c_{i_w} \underline{h}_{i_w}^T = \underline{0}$$

$\Rightarrow$ Columns $i_1, i_2, \ldots, i_w$ of H are linearly dependent.

$\Rightarrow$ Min dist of C = min # of linearly dependent columns of H.