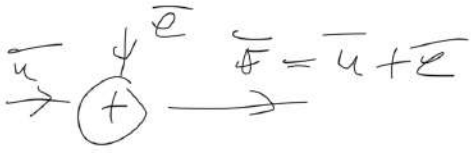
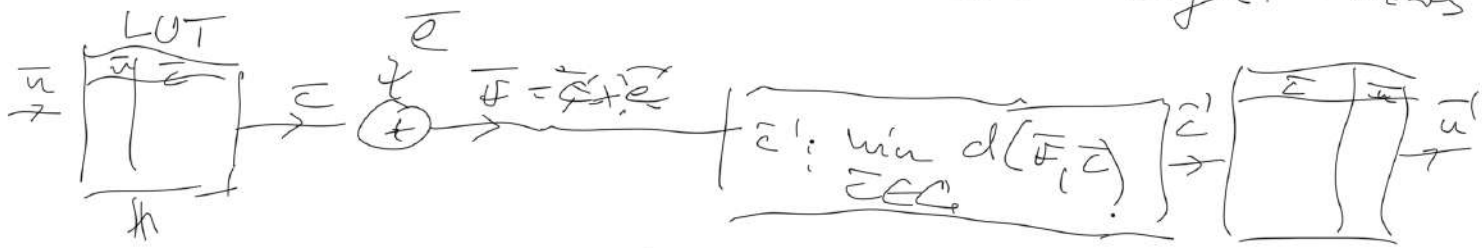



$$P(w(e)=i) = \binom{u}{i} \left(\frac{p_b}{1-p_b}\right)^i (1-p_b)^u$$

$$0 \le \frac{p_b}{1-p_b} < 1$$

$\exp(-i)$ → correcting low weight errors




Goal: max $d_{min}$ & $\frac{k}{n}$

LUT + SEARCH

$3 \cdot O(2^k)$

$C(n, k)$

# Performance of codes

$d_{min}$: $\min_{\bar{c},\bar{c}' \in C,\ \bar{c} \neq \bar{c}'} d(\bar{c},\bar{c}')$

→ Error detection capability: $d_{min} - 1$

→ Error correction capability: $t = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor$


none of them are codewords

Assume that $\bar{a}$ sent, correct detection if

$d(\bar{r},\bar{c}) < d(\bar{r},\bar{c}') \quad \forall \bar{c}' \in C,\ \bar{c}' \neq \bar{c}$


$d(\bar{r},\bar{c}) < d(\bar{c},\bar{c}') - d(\bar{r},\bar{c})$

$d(\bar{c},\bar{c}') \leq d(\bar{r},\bar{c}) + d(\bar{r},\bar{c}')$

$2\,d(\bar{r},\bar{c}) < d_{min}$

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

$d(\bar{c},\bar{c}') - d(\bar{r},\bar{c}) \leq d(\bar{r},\bar{c}')$

$n-k$ | $k$ | $t$

$d_{min}$

message | parity

$\bar{c} = (u_1 \dots u_k, p_{k+1} \dots p_n)$

$d=1$

$\bar{c}' = (u_1' \dots u_k', p_{k+1}' \dots p_n')$

Singleton bound

$n - k + 1 \geq d_{min}$

$$d_{min} = n - k + 1$$

MDS (Maximum Distance Separability)

Hamming bound: $t$ # of errors are corrected

$$\sum_{i=0}^{t} \binom{n}{i} \leq 2^{(n-k)}$$

$$2^k \sum_{i=0}^{t} \binom{n}{i} \leq 2^n$$

$$\sum_{i=0}^{t} \binom{n}{i} = 2^{n-k}$$


Perfect code

## Binary linear codes $C(n, k)$

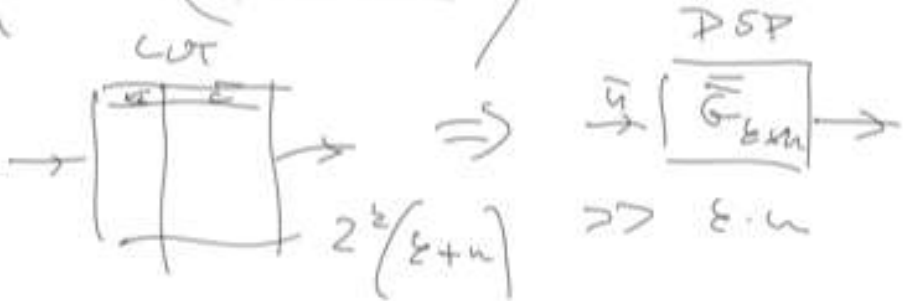
$G = \{ \bar{g}^{(1)}, \bar{g}^{(2)} \dots \bar{g}^{(k)} \}$ $\dim(\bar{g}^{(i)}) = n$, $i = 1 \dots k$

$C = \alpha c \{ G \} \rightarrow \bar{c} = \sum_{i=1}^{k} u_i \bar{g}^{(i)} \rightarrow \bar{c} = \bar{u} \bar{\bar{G}}$

Generator matrix $\bar{\bar{G}}_{k \times n} = \begin{pmatrix} \bar{g}^{(1)} \\ \bar{g}^{(2)} \\ \vdots \\ \bar{g}^{(k)} \end{pmatrix}$

$(c_1 c_2 \dots c_n) = (u_1 \dots u_k) \begin{pmatrix} & & \\ & \bar{\bar{G}}_{k \times n} & \\ & & \end{pmatrix}$

Technological importance



Systematic codes: $c = (u_1 \dots u_k, p_{k+1} \dots p_n)$

$$G_{k \times n} = \left( \underline{\underline{I}}_{k \times k} \mid \underline{\underline{B}}_{k \times (n-k)} \right)$$

E.g. $C(5,2)$ $\quad G = \{(10110), (01111)\}$

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

$$G_{2 \times 5} = \left( \begin{array}{cc|ccc} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{array} \right)$$

$I_{2 \times 2}$ $\quad B_{2 \times 3}$

$(00)\begin{pmatrix} 10110 \\ 01111 \end{pmatrix} = (00000) = \bar{c}_0$

$(01)\begin{pmatrix} 10110 \\ 01111 \end{pmatrix} = (01111) = \bar{c}_1$

$(10)\begin{pmatrix} 10110 \\ 01111 \end{pmatrix} = (10110) = \bar{c}_2$

$(11)\begin{pmatrix} 10110 \\ 01111 \end{pmatrix} = (11001) = \bar{c}_3$.

$d_{min} = 3$

Detection 2 errors

Correction $t = 1$

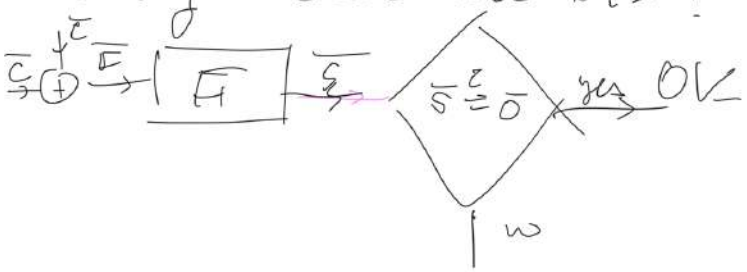
Linear $\quad \bar{c}, \bar{c}' \in C' \rightarrow \bar{c}+\bar{c}' \in C'$

$d_{min} = w_{min}$ , $d_{min} = \min_{\substack{\bar{c},\bar{c}' \\ \bar{c} \neq \bar{c}'}} d(\bar{c},\bar{c}') \sim \min_{\substack{\bar{c},\bar{c}' \\ \bar{c} \neq \bar{c}'}} w(\bar{c}+\bar{c}') \sim$

$\sim \min_{\substack{\hat{c}'' \in C' \\ \bar{c}'' \neq \bar{0}}} w(\bar{c}'') \rightarrow w_{min}$

---

Parity check matrix : $\bar{\bar{H}}_{(n-k)\times n}$ : $\bar{\bar{H}}\,\bar{c}^T = \bar{0}^T \quad \forall \bar{c} \in C'$




error correction algorithm

$$\bar{\bar{H}}\,\bar{c}^T = \bar{0}^T \rightarrow \bar{\bar{H}}\left(\bar{u}\,\bar{\bar{G}}\right)^T = \bar{0}^T \rightarrow \bar{\bar{H}}\,\bar{\bar{G}}^T\bar{u}^T = \bar{0}^T$$

$$\underbrace{\bar{\bar{H}}\,\bar{\bar{G}}^T = \bar{\bar{0}}}_{\text{h}}$$

Systematic codes

$$\bar{\bar{H}}_{(n-k)\times n} = \left(\bar{\bar{A}}_{(n-k)\times k} \mid \bar{\bar{I}}_{(n-k)\times(n-k)}\right)$$

$$\bar{G}_{k\times n} = \left(\bar{\bar{I}}_{k\times k} \mid \bar{\bar{B}}_{k\times(n-k)}\right)$$

$$\underbrace{\left(\bar{\bar{A}}_{(n-k)\times k} \mid \bar{\bar{I}}_{(n-k)\times(n-k)}\right)}_{\text{h}} \underbrace{\begin{pmatrix}\bar{\bar{I}}_{k\times k}\\ \bar{\bar{B}}^T_{(n-k)\times k}\end{pmatrix}}_{\text{h}} = \bar{\bar{A}}_{(n-k)\times k} + \bar{\bar{B}}^T_{(n-k)\times k} = \bar{\bar{0}}$$

$$\bar{\bar{A}} = \bar{\bar{B}}^T$$

$$\bar{\bar{G}}_{2\times 3} = \begin{pmatrix} 1\,0 & 1\,1\,0 \\ 0\,1 & 1\,1\,1 \end{pmatrix} \Rightarrow \bar{\bar{H}}_{3\times 5} = \begin{pmatrix} 1\,1 & 1\,0\,0 \\ 1\,1 & 0\,1\,0 \\ 0\,1 & 0\,0\,1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

# Error correction - Easy equation

$\dim(\mathcal{S}) = n-k$


$\bar{\bar{H}}\bar{r}^T = \bar{s}^T$ ← computed

$\bar{\bar{H}}(\bar{c}+\bar{e})^T = \bar{s}^T \rightarrow \bar{\bar{H}}\bar{c}^T + \bar{\bar{H}}\bar{e}^T = \bar{s}^T$

$\bar{\bar{H}}\bar{c}^T = \bar{0}^T$

known ↑ × observed

$\bar{\bar{H}}\bar{e}^T = \bar{s}^T$ ← Easy equation

known 22 computed

$\bar{\bar{H}}_{(n-k)\times n} \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = \begin{pmatrix} s_1 \\ \vdots \\ s_{n-k} \end{pmatrix}$

"n" unknowns for "n-k" equations

$E_{\bar{s}} = \{\bar{e} : \bar{\bar{H}}\bar{e}^T = \bar{s}^T\}$

$$\overline{H}_{3\times5} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} \qquad \overline{s} = (0\,0\,1)$$

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \quad \not\in$$

$$E_{\overline{s}} = \{(0\,0\,0\,0\,1), (1\,1\,0\,0\,0), (0\,1\,1\,1\,0), (1\,0\,1\,1\,1)\}$$

$$\overline{e}_{\overline{s}} : \min_{e \in E_{\overline{s}}} w(\overline{e})$$

SEARCH $\quad$ if $\overline{e} \in E_{\overline{s}} \quad \overline{e}' = \overline{e} + \overline{c} \;\rightarrow\; \overline{e}' \in E_{\overline{s}}$

$$\overline{\overline{H}}\,\overline{e}^T = \overline{s}^T \;\rightarrow\; \overline{\overline{H}}\,\overline{e}'^T = \overline{\overline{H}}\left(\overline{e}^T + \overline{c}^T\right) = \overline{\overline{H}}\,\overline{e}^T = \overline{s}^T$$

$$E_{(001)} = \{(0\,0\,0\,0\,1), (1\,1\,0\,0\,0), (0\,1\,1\,1\,0), (1\,0\,1\,1\,1)\}$$

# Syndrome decoding table

$n-k$

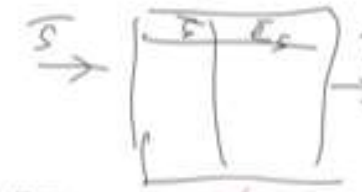
$00\ldots0$

$00\ldots1$

$\vdots$

$11\ldots1$

$\vec{s} \rightarrow E_{\vec{s}} = \{\vec{e} : H\vec{e} = \vec{s}\} \rightarrow \vec{e}_s : \min_{\vec{e} \in E_{\vec{s}}} w(\vec{e})$




$O(2^{n-k})$


$\vec{G}_{k \times n} = \left(\vec{I}_{k \times k}, \vec{B}_{k \times (n-k)}\right)$

$\vec{H}_{(n-k) \times n} = \left(\vec{A}_{(n-k) \times k}, \vec{I}_{(n-k) \times (n-k)}\right)$

$\vec{A} = \vec{B}^T$ .

$O(2^{n-k}) \ll 3 \cdot O(2^k)$