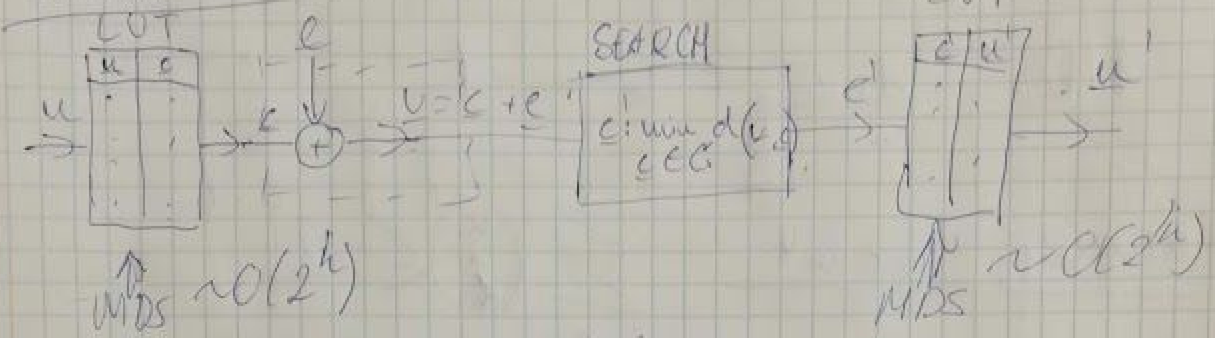
III. Előadás 2018.09.19

Emlékeztető



Kódok teljesítőképessége:

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

Hiba jelzés: $d_{min} - 1$

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

singleton határ

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

Komplexitás: $\binom{2^n}{2^k} \binom{2^k}{2}$ OFFLINE

$\sim 3 \cdot O(2^k)$ ONLINE

exponenciális $\nexists$ real time megoldhatóság

Bináris lineáris kódok

$C(n,k)$ $\qquad \mathcal{G} = \{ \underline{g}_1, \underline{g}_2 \dots \underline{g}_k \}$ dim $\mathcal{G} = k$

↓
üzenetvektorok hossza

$C \subset \mathcal{G}$

A kódkészlet a kifeszített bázis burkán van!

$$\boxed{\underline{c} = \sum_{i=1}^{k} u_i \underline{g}_i}$$

lineáris a kód, ha így állítjuk elő

$$c = \underline{u} \cdot \underline{\underline{G}} = (u_1, u_2, \dots u_k) \begin{pmatrix} g_1 \\ g_2 \\ \vdots \\ g_k \end{pmatrix}$$

generátormátrix

$$\xrightarrow{\underline{u}} \boxed{\underline{G}_{k \times n}} \xrightarrow{c}$$

$k \cdot n$ dim

$< 2^k (n+k)$ → komplexitás

Pl.: $\mathcal{G} = \{(10110); (01111)\}$ $C(5,2)$

$$\underline{\underline{G}} = \begin{pmatrix} 1 0 & 1 1 0 \\ 0 1 & 1 1 1 \end{pmatrix}$$ I. kódszó

$$\underline{c}^{(0)} = \underline{u}^{(0)} \underline{\underline{G}} = (0\,0) \cdot \underline{\underline{G}} = (0\,0|0\,0\,0)$$
$$\underline{c}^{(1)} = \underline{u}^{(1)} \cdot \underline{\underline{G}} = (0\,1) \cdot \underline{\underline{G}} = (0\,1|1\,1\,1)$$
$$\underline{c}^{(2)} = \underline{u}^{(2)} \cdot \underline{\underline{G}} = (1\,0) \cdot \underline{\underline{G}} = (1\,0|1\,1\,0)$$
$$\underline{c}^{(3)} = \underline{u}^{(3)} \cdot \underline{\underline{G}} = (1\,1) \cdot \underline{\underline{G}} = (1\,1|0\,0\,1)$$

$d_{min} = 3$ legkisebb Hamming táv

$t = \left\lfloor \frac{3-1}{2} \right\rfloor = 1$ nem MDS kód

Szisztematikus kód:

$$\underline{c} = (\underbrace{u_1\, u_2 \ldots u_k}_{\text{üzenet}}\, \underbrace{p_{n-k} \ldots p_n}_{\text{paritás ellenőrzés}})$$

$$\underline{c} = \underline{u} \cdot \underline{\underline{G}} \rightarrow \boxed{\underline{\underline{G}} = \left(\underline{\underline{I}}_{k\times k} \,|\, \underline{\underline{B}}_{k\times(n-k)}\right)}$$

!

paritás ellenőrző mátrix $\underline{\underline{H}}$

$$\underline{\underline{H}} \cdot c^T = \underline{0}$$

$$\Big(\quad \Big)_{(n-k)\times n} \Big(\quad \Big)_{n} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}_{n-k}$$

$$\underline{H} \cdot (u \cdot \underline{\underline{G}})^T = \underline{0}$$

$$\underline{\underline{H}} \cdot \underline{\underline{G}}^T \cdot u^T = \underline{0}$$

$$\underline{\underline{H}} \cdot \underline{\underline{G}}^T = \underline{0}$$

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

$$\left(\underline{A}_{(n-k)\times k} \; \underline{I}_{(n-k)\times(n-k)} \right) \begin{pmatrix} \underline{I}_{k\times k} \\ \underline{B}_{k\times(n-k)} \end{pmatrix} = 0$$

$$\boxed{\underline{A}_{(n-k)\times k} = -\underline{B}^T_{(n-k)\times k}}$$

$\downarrow$

$mod_2 \rightarrow - = +$

$\downarrow$

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

pl.:

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

$$\underline{\underline{H}} \cdot \underline{c}^{(1,1)T} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

Hibajavítás – „kulcs" egyenlet

$$\underline{c} \xrightarrow{\oplus\ \underline{e}} \underline{v} = \underline{c} + \underline{e} \longrightarrow \boxed{\underline{\underline{H}}} \longrightarrow \underline{s}$$

szindróma

$$\underline{\underline{H}}_{(n-k)\times(n)} \cdot \underline{v}^T = \underline{s}$$

$$\underline{\underline{H}}_{(n-k)\times n} \cdot (\underline{c} + \underline{e})^T = \underline{s}$$

$$\underbrace{\underline{\underline{H}} \cdot \underline{c}^T}_{=0} + \underline{\underline{H}} \cdot \underline{e}^T = \underline{s}$$

$$\boxed{\underline{\underline{H}} \cdot \underline{e}^T = \underline{s}}$$ kulcs egyenlet

adott, ?, kiszámolható

$\underline{e} \in \{0,1\}^n$

n ismeretlen

n-k egyenlet

→ megoldás halmaz

$$\underline{c} = \underline{v} - \underline{e} = \underline{v} + \underline{e}$$

$$E_s = \{ e \;;\; H \cdot e^T = s \} \quad 2^k \text{ elem}$$

$$\Downarrow$$

e_s : $\min\limits_{e \in E_s} w(e)$

$$\frac{\hat{e} \text{ csoportvezető}}{}$$

$$P_b \sim O(\exp(-w(\hat{e})))$$

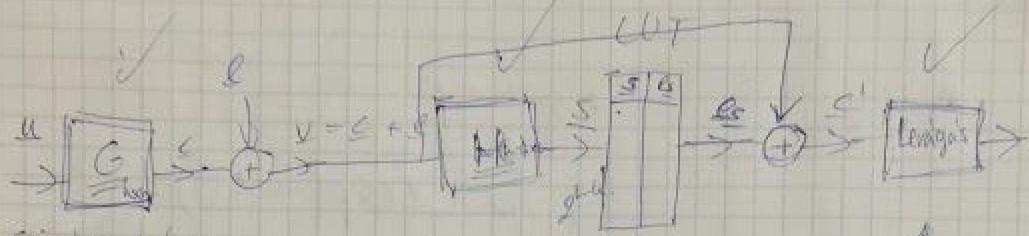
$$E_{(001)} : \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \\ \\ \\ \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

$$E_{(001)} : \left\{ \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} \right\}$$

$$\boxed{P_b (1-P_b)^4} \quad P_b^2 (1-P_b)^4 \quad P_b^4 (1-P_b) \quad P_b^3 (1-P_b)^2$$

csoportvezető

Összefoglalás:



szisztematikus kódok

$$\underline{\underline{G}} = \left(\underline{\underline{I}}_{k\times k} \quad \underline{\underline{B}}_{k\times(n-k)} \right) \qquad \underline{\underline{H}} = \left(\underline{\underline{A}}_{(n-k)\times k} \quad \underline{\underline{I}}_{(n-k)\times(n-k)} \right)$$

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

Komplexitás:

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

Pl.:

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

$C(5,2)$

$e = (00001)$

$$\underline{c} = \underline{u} \cdot \underline{\underline{G}} = (11)\begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix} = (11001)$$

$$\underline{v} = \underline{c} + e = (11000)$$

$$\underline{s} = \underline{\underline{H}} \cdot \underline{v}^T = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

$$f(001)\left\{ \boxed{\begin{array}{c} e_{001} \\ \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \end{array}} \right.$$

$$c' = v + e_{001} = (11000) + (00001) = (11001) \rightarrow u' = (11)$$