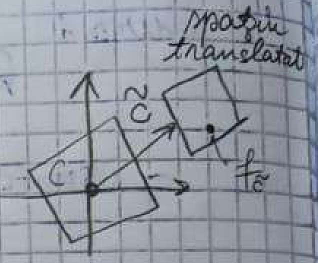
Curs 2 STLS II

Maximum Likelihood

- Syndrome decoding

~~greșeală~~ cuvânt greșit — $\tilde{c} \in K^n$ cuvânt recepționat



? $c \in C$ a.î. $f = \tilde{c} - c$ — greșeala

$wt(f) = $ minim.

$$H\tilde{c}^T = H(f+c)^T = Hf^T + \underbrace{Hc^T}_{0} = Hf^T$$

Def $Hv^T \in K^{n-k}$ sindrom al lui v

$\Rightarrow$ $\tilde{c}$ și f au același sindrom

$\Rightarrow$ f se poate recunoaște după sindrom

i.e. (se poate face un dicționar al erorilor corectabile)

Pentru o clasă de echivalență $v + C \subset K^n$ găsim un reprezentant $f_v \in v + C$ a.î.

$$wt(f_v) = \min\{wt(v+c) \mid c \in C\}$$

$$\tilde{c} \rightsquigarrow c = \tilde{c} - f_{\tilde{c}}$$

Th Fie C cod de tip $[n, k]$ peste K (corp finit) și H matricea de control. Atunci:

$d(C) = wt(C) = \min\{w \mid \exists\ w$ coloane liniar dependente în $H\} =$

$= \max\{w \mid \forall (w-1)$ coloane din H sunt liniar independente$\}$

Dem: Fie $h_1, \dots, h_n$ coloanele lui H.

„$\leq$" $C \neq 0 \Rightarrow$ familie liniar dependentă, deci $\exists\, w$ minimal a.î. $h_{i_1}, \dots, h_{i_w}$ liniar dependente.

$\Rightarrow \exists$ relație de dependență liniară:

$$\sum_{j=1}^{n} c_j h_j = 0 \qquad \underset{\text{scalari}}{c_j \in K}, \quad c_k \neq 0 \Leftrightarrow k \in \{i_1, \dots, i_w\}$$

Fie $c = (c_1, \dots, c_n)$; $Hc^T = 0 \Rightarrow c \in C$

$wt(c) = w \Rightarrow \boxed{wt(C) \leq w}$ (codul conține un cuvânt de pondere $\underset{wt}{w}$)

„$\geq$" Presupunem că $\exists\, \tilde{c} \neq 0$, $\tilde{c} \in C$, $wt(\tilde{c}) < w$.

$H\tilde{c}^T = 0 \Rightarrow \exists$ un nr. $< w$ de coloane liniar dependente în H. ↯

$$\underset{H}{\begin{pmatrix} \cdots x \cdots x \cdots x \cdots \\ x \quad x \quad x \\ \cdots \quad \cdots \\ x \quad x \quad x \end{pmatrix}} \underset{\tilde{c}^T}{\begin{pmatrix} 0 \\ x \\ 0 \\ x \\ 0 \\ \vdots \\ x \\ 0 \\ x \\ 0 \end{pmatrix}} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

$x \stackrel{not}{=}$ elem. nenule

Coduri Hamming

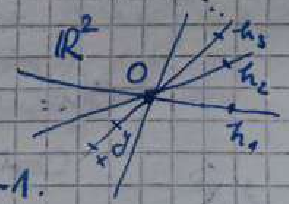
— determinat până la izomorfism

K corp finit, $|K| = q$ elemente $= p^\alpha$, p prim, $\alpha \in \mathbb{N}$

($\alpha = 1 \Rightarrow K$ inel de resturi)

$\underset{\text{corp}}{\mathbb{F}_{25}} \neq \underset{\text{inel}}{\mathbb{Z}_{25}}$ dar $\mathbb{F}_5 = \mathbb{Z}_5$

$xy = 0 \Rightarrow x = 0 \vee y = 0$ $\qquad 5 \cdot 5 = 0$



• Spațiul proiectiv de dimensiune $k-1$.

$x \sim y \Leftrightarrow 0, x, y$ coliniare $\Leftrightarrow \exists\, \lambda \neq 0$ a.î. $y = \lambda x$.

pe $\mathbb{R}^2 \setminus \{0\}$

$$\mathbb{R}^2 \setminus \{0\} /_{\sim} + \text{"}\infty\text{"} = \mathbb{P}^1(\mathbb{R})$$

"∞" ... punctul de la infinit

$\mathbb{P}^1(\mathbb{R})$: dreapta proiectivă

$/_{\sim}$: factorizare la rel. de echiv.

Spațiul proiectiv de dim $K-1$

$$\mathbb{P}^{K-1}(q) = \{ \langle u \rangle \mid 0 \neq u = (u_1, \dots, u_k)^T, u_i \in K \}$$

clasa de echiv.

$$\langle u \rangle = \langle v \rangle \iff \exists \lambda \in K^{\times}, u = \lambda v$$

$$n = |\mathbb{P}^{k-1}(q)| = \frac{q^k - 1}{q - 1}$$

nr. de drepte care formează punctele spațiului pr.

h_i: reprezentanți

$$\mathbb{P}^{k-1}(q) = \{ \langle h_1 \rangle, \langle h_2 \rangle, \dots, \langle h_n \rangle \}$$

$$H = (h_1, \dots, h_n) \in \mathcal{M}_{k \times n}(K)$$ k linii, n coloane

liniar indep: nu pot fi scrise ca combinații liniare una a celeilalte.

Def. Codul Hamming este codul care are pe H ca matrice de control.

$$C = \{ c \mid c \in K^n, Hc^T = 0 \} \leq K^n$$ subspațiu vectorial

$\text{rk}\, H = k$ rang maxim

$\boxed{\dim C = n - k}$. Orice 2 coloane din H sunt liniar independente (din construcție)

dar $\langle h_1 \rangle, \langle h_2 \rangle, \langle h_1 + h_2 \rangle$ liniar dependente

$\Rightarrow wt(c) = d(C) = 3$

Codul Hamming are parametrii $[n, n-k, 3]$ (lungime, dimensiune, distanța minimă)

unde $n = \frac{q^k - 1}{q - 1}$.

Obs: $3 \geq 2 \cdot 1 + 1 \Rightarrow$ codul este 1-corector.

Codul este perfect

reuniune disjunctă; se alege o a contează doar a nenulităților; toate bilele au același nr. de elem

$$\left| \bigcup_{c \in C} B_1(c) \right| = |C| \cdot \underbrace{|B_1(0)|}_{\text{lungimea bilei}} = q^{n-k}\left(1 + n(q-1)\right) =$$

$$= q^{n-k}\left(1 + \frac{q^k - 1}{\cancel{q-1}}\cancel{(q-1)}\right) = q^{n-k} \cdot q^k = q^n$$

$Ham_q(k)$

multime de coduri definită de q și k.

Coduri Simplex

un cod C peste corpul finit K care o are pe H ca matrice generatoare.

$$C = \{ aH \mid a \in K^k \} \underset{\text{subs.v.}}{\leq} K^n$$ H are k linii

invariantă la translații

Th $c \in C \setminus \{0\} \Rightarrow wt(c) = q^{k-1}$ (distanța Hamming între orice elem. și centru / orice 2 elem)

, oricare 2 pcte se află la aceeași distanță Hamming

Dem. z_i = liniile lui H

$$0 \neq c = (c_1, \dots, c_n) = \sum_{i=1}^{k} a_i z_i = \sum a_i (z_{i_1}, \dots, z_{i_n}) \in C$$

$$U = \{ (b_1, \dots, b_k)^T \mid b_i \in K, \sum_{i=1}^{k} a_i b_i = 0 \}$$ $\dim(U) = k-1$, q^{k-1} elem.

Un număr de $\frac{q^{k-1}-1}{q-1}$ coloane ale lui H sunt echivalente cu elemente din U.

$c_j = 0 \Leftrightarrow \exists b \in U \ \exists j \ \langle h_j \rangle = \langle b \rangle$

$$wt(c) = n - \frac{q^{k-1}-1}{q-1} = \frac{q^k-1}{q-1} - \frac{q^{k-1}-1}{q-1} = \frac{q^{k-1}(q-1)}{q-1} = q^{k-1}$$ dist. min.

$$\left[\frac{q^k-1}{q-1}, k, q^{k-1} \right]$$ $Sim_q(k)$ mulțimea codurilor simplex date de acești parametri.

Ex1 | Un cod Hamming $[7,4,3]_{/\mathbb{F}_2}$ are matricea de control

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}. \qquad \underbrace{\quad}_{3 = rk} \quad \underbrace{x_4 \; x_5 \; x_6 \; x_7}_{corang = 4} \qquad \vec{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_7 \end{pmatrix} \qquad \vec{0} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

Găsiți matricea generatoare.

Rezolvare: $H\vec{x} = \vec{0}$ ca sistem:

$$\begin{cases} x_1 + x_4 + x_5 + x_7 = 0 \\ x_2 + x_4 + x_6 + x_7 = 0 \\ x_3 + x_5 + x_6 + x_7 = 0 \end{cases}$$

$(x_4 \ x_5 \ x_6 \ x_7) = (a, b, c, d)$ pot fi declarate parametri

$$\begin{cases} x_1 = a + b + d \\ x_2 = a + c + d \\ x_3 = b + c + d \end{cases} \qquad \begin{matrix} x_1 \\ \vdots \\ x_7 \end{matrix} \begin{pmatrix} a + b + d \\ a + c + d \\ b + c + d \\ a \\ b \\ c \\ d \end{pmatrix} =$$

$$= a \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + b \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + c \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + d \begin{pmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

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

$$C = \{\vec{x} G\}_{\vec{x} \in \mathbb{F}_2^4} = (a, b, c, d) \begin{pmatrix} | & | & | & | \end{pmatrix}$$

Ex 2 $G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$ generează cod $[7,4,3]$

nr. linii, rang maximal, cod Hamming

minor = matricea unitate, rk = 4 maximal = dim (Im (G)) = 4

$H = ?$ matr. de control

Rez. H are 3 linii și 7 coloane $HG^T = 0$

O linie arbitrară a lui H este (a,b,c,d,e,f,g)

$$(a,b,c,d,e,f,g) \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = (0,0,0,0)$$

îi aleg ca parametri

$\Downarrow$

$$(a, b, c, a+b, a+c, b+c, a+b+c)$$

$$= a(1,0,0,1,1,0,1) + b(0,1,0,1,0,1,1) + c(0,0,1,0,1,1,1)$$

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

Ex 3 $H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$ Hamming $[7,4,3]$ Simdromuri?

1-error correcting

$f_i = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ — poziția i

$Hf_1 = (1,0,0)$ $Hf_4 = (1,1,0)$

$Hf_2 = (0,1,0)$ $Hf_5 = (1,0,1)$

$Hf_3 = (0,0,1)$ $Hf_6 = (0,1,1)$

$Hf_7 = (1,1,1)$

$\boxed{\text{Ex 4}}$ $\tilde{c} = (1, 1, 0, 0, 1, 1, 1)$ Nu

- este corect cuv. de cod?
- dacă nu, care este originalul?

$$\tilde{c}^T = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{pmatrix} \qquad H\tilde{c}^T = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

sindromul $\rightsquigarrow f_7$ = greșeala

$$\tilde{c} - f_7 = (1, 1, 0, 0, 1, 1, \underline{0}) = c \in C$$

Curs 2

RE

(readable machine code)

Assembly

Binaries

hexed

circu