$ file ↵ magic number .elf

sectiunea .text

compiler options -O3

Curs 4 STCS II

MDS = maximum

C cod, $|F| = q$; $d = d(C)$

$d \leq n - \log_q |C| + 1$ n = lungimea lui C

(Singleton Bound) $k = \log_q |C|$

Def C este MDS $\Leftrightarrow d = n - \log_q |C| + 1$

Dualitate K corp, $n \in \mathbb{N}$

$\langle , \rangle : K^n \times K^n \to K^n$

$\langle u, v \rangle = \sum_{i=1}^{n} u_i v_i$

produs scalar, formă biliniară nedegenerată simetrică

$C \subseteq K^n$ numai' multime

$C^\perp = \{ u \in K^n \mid \forall c \in C, \langle u, c \rangle = 0 \}$

cod dual ortogonal al lui C

C autodual $\Leftrightarrow C = C^\perp$ produsul scalar al oricăror 2 elem = 0 norma = 0

C autoortogonal $\Leftrightarrow C \subseteq C^\perp$

Th C cod $[n,k]$ peste K, atunci

① H matrice de control pt. $C \iff H$ matrice generatoare pt. $C^\perp$

② $(\underbrace{E_k}_{\text{matricea unitate}} \mid A)$ generatoare pt. $C \iff (-A^T \mid E_{n-k})$ matrice generatoare pt. $C^\perp$

Consecință: $\underbrace{Ham}_{\text{cod Hamming ortogonal}}^{\perp} = \underbrace{Sim}_{\text{cod simplex}}$

Dem. ① Dacă G generatoare pt. C, atunci o matrice H : $(n-k)\times n$ este matricea de control $\iff HG^T = 0$ și $\operatorname{rang} H = n-k$.

② $(-A^T \mid E_{n-k})\left(E_k \mid A\right)^T = -A^T + A^T = 0$. □

$GRS_d(a,v)$ generalized Reed-Solomon Code

- K corp, $2 \le d \le n \le q$ $(q = |K|)$

$\Rightarrow \exists v'$ a.î. $\left(GRS_d(a,v)\right)^{\perp} = GRS_{n-d+2}(a,v')$

- v' determinat până la înmulțire cu un scalar de $\langle v' \rangle = GRS_n(a,v)$ (care dim = 1)

- $\operatorname{char} K = 2$ și $d \ge \frac{n+2}{2} \Rightarrow \exists v$ a.î. $GRS_d(a,v) \subseteq \left(GRS_d(a,v)\right)^{\perp}$ i.e. auto-ortogonal

- n par și $d = \frac{n+2}{2} \Rightarrow$ cod autodual

Th C cod, $\dim C \ge 1$. Atunci

C este MDS $\iff C^\perp$ este MDS.

Dem. $(C^\perp)^\perp = C$ $\Rightarrow$ e suficientă dem. într-o singură direcție

„⇒" n = lungime cod.

Fie $c \neq c^\perp \in C^\perp$ cu $wt(c^\perp) \leq k$

$c^\perp$ poate fi ales linie în matricea generatoare (i.e. poate fi completat la o bază) $G^\perp$ a lui $C^\perp$

NU Există $n-k$ coloane din $G^\perp$ liniar independente.

$\not\Rightarrow$ $\left\{ \begin{array}{l} d(C) = n-k+1, \text{ orice } n-k \text{ coloane sunt liniar indep.} \\ \Rightarrow d(C^\perp) \geq k+1 \end{array} \right.$ din Singleton Bound:

$k+1 \leq d(C^\perp) \leq n-(n-k)+1 = k+1$

$\Rightarrow$ Singleton Bound devine egalitate.

Def $r \in \mathbb{N}$, $r > 1$. Codul C r-n.

r-divizibil $\Leftrightarrow \forall c \in C$, $r \mid wt(c)$

Lemă C auto-ortogonal / $\mathbb{F}_2$ sau $\mathbb{F}_3$ $\Leftrightarrow C$ este 2-div respectiv 3-div
$C \subseteq C^\perp$ $\mathbb{F}_p$

Pe dinafară, $C/\mathbb{F}_2 \Rightarrow (1,\dots,1) \in C^\perp$.

Fie $c = (c_1, \dots, c_n) \in C$

dacă $p=2$ $c_i \in \{0,1\}$ respectiv $c_i \in \{0,1,-1\}$ dacă $p=3$

$c_i \neq 0 \Rightarrow c_i^2 = 1$

$0 = \langle c, c \rangle = wt(c) \bmod p$ ($\dim C \leq C^\perp$)

$\Leftrightarrow p \mid wt(c)$

[$p=2$, $v \perp \langle v, (1,\dots,1) \rangle = wt(v) \bmod 2 = 0$

$\Rightarrow (1,\dots,1) \in C^\perp$]

Lemă C cod binar $[n,k]$ $\|\ \mathbb{F}_2$

(1) $C \subseteq C^\perp$ $\wedge$ C are o bază din vectori cu $wt : 4$
$\to C$ este 4-divizibil.

(2) C este 4-divizibil $\Rightarrow C \subseteq C^\perp$ auto-ortogonal

Idee dem. $\langle c, c' \rangle = |supp(c) \cap supp(c')| \bmod 2$

$wt(c+c') = wt(c) + wt(c') - 2|supp(c) \cap supp(c')|$

Def (Extensia unui cod)

$C: [n,k]$ cod. $\hat{C} = \{(c_1,\dots,c_n,c_{n+1}) \mid (c_1,\dots,c_n) \in C, \sum_{i=1}^{n+1} c_i = 0\}$
extensia lui C

$\hat{C}$ este un $[n+1,k]$-cod
$\wedge$ $d(C) \le d(\hat{C}) \le d(C)+1$

Codul ternar Golay $Gol(11)$ generat de matricea $G_{11} = (E_6 \mid G)$

$\mathbb{F}_3$ $G = \left(\begin{array}{ccccc} 0 & 1 & -1 & -1 & 1 \\ 1 & 0 & 1 & -1 & -1 \\ -1 & 1 & 0 & 1 & -1 \\ \hline 1 & 1 & 1 & 1 & 1 \end{array}\right)$ $C = Gol(11)$

Se not. cu $Gol(12) = \hat{C}$

$Gol(12)$ este generat de G la care se adaugă coloana $\begin{pmatrix} -1 \\ -1 \\ -1 \\ -1 \\ 0 \end{pmatrix}$. $Gol(11)$ autoduală $\wedge$ $[12,6,6]$

dem: $Gol(12) \subseteq Gol(12)^\perp$ $\Rightarrow$ egalitate ($\Leftrightarrow$ auto-dualitate)
$6 \qquad 12-6=6$

$Gol(11) : [11,6,5]$

$\Rightarrow Gol(11)$ este e-corector $\wedge$ $2e+1 \le 5 \Rightarrow \boxed{e=2}$.

$3^{11} \ge \left| \bigcup_{c \in Gol(11)} B_2(c) \right| = |Gol(11)| \cdot |B_2(0)| =$

$$= 3^6 \left(1 + \binom{11}{1}\cdot 2 + \binom{11}{2}\cdot 4\right) =$$

$$= 3^6 \left(1 + 22 + \underbrace{\frac{10\cdot 11}{2}\cdot 4^2}_{220}\right) = 3^6\cdot 3\cdot 3^4 = 3^{11}$$

$$\underbrace{1 + 22 + 220}_{243 = 3\cdot \underbrace{81}_{3^4}}$$

Inegalitatea lui Hamming devine egalitate
⇒ codul Gol(11) e perfect

Urme și caractere

$K \leq E$ extensie de corpuri finite

$[\mathbb{F}_{p^\alpha} \subseteq \mathbb{F}_{p^\beta} \Leftrightarrow \alpha \mid \beta]$ $\quad \mathbb{F}_8 \subseteq \mathbb{F}_{16}$, $8 = 2^3$, $16 = 2^4$ $\quad \not\Updownarrow \quad 3|4$

G = grupul Galois al extensiei

$G = \{\varphi : E \to E \mid \varphi \text{ automorfism de corp} \wedge \forall x \in K\ \varphi(x) = x\}$

Urma (Trace) $Tr_{E/K} : E \to K$

$$Tr_{E/K}(a) = \sum_{\gamma \in G} \gamma(a)$$

$\forall \varphi \in G \quad \varphi(Tr_{E/K}(a)) = Tr_{E/K}(a) \Rightarrow$

$$\Rightarrow \boxed{Tr_{E/K}(a) \in K}$$

K corp, char $K = p \to F(x) = x^p$ automorfism

Automorfismul lui Frobenius

$\mathbb{Z}_p$: $x^p = x \cdot \underbrace{x^{p-1}}_{1} = x$

$\mathbb{F}_4 = \{0, 1, \omega, \omega+1\}$, unde $\omega^2 = \omega + 1$

(în $\mathbb{F}_2[X]$, $X^2 + X + 1$ ireductibil

$\omega^2 + \omega + 1 = 0 \qquad +1 = -1 \qquad \omega^2 = \omega + 1$)

$F(0)=0$, $F(1)=1$, $F(\omega)=\omega^2=\omega+1$

$F(\omega+1)=\omega^2+1=\omega+1+1=\omega$

$(a+b)^p=a^p+b^p$ deoarece $p \mid \binom{p}{k}$ cu $0<k<p$

$(ab)^p=a^p b^p$

$Gal(\mathbb{F}_{p^\alpha} \mid \mathbb{F}_p)=\{id, F, F^2, \dots, F^{\alpha-1}\}$

$F^k(x)=\underbrace{((x^p)^p)^p \dots}_{k \text{ de ori}}=x^{p^k}$

$|E:K|=n$; G = grupul automorfismelor = $\langle F \rangle_{\text{Frobenius}}$

$|K|=q$

$Tr_{E|K}(a)=a+a^q+a^{q^2}+\dots+a^{q^{n-1}}$

$|K|=q \quad \forall x \in K, \quad x^q=x \cdot \underbrace{x^{q-1}}_{1}=x$

Ex

C cod , $|C|=4$, $/\mathbb{F}_2$, lungime 4

$\Rightarrow$ NU este 1-error correcting

Rezolvare

1-error correcting $\Rightarrow d \geq 3$ $\quad d \geq 2e+1$

lungime 4: $d=4$ imposibil (nu ai avea decât 2 cuvinte)

$d=3?$

$16=2^4 \geq |C|\,(\overbrace{1}^{1} \cdot (2-1)^0 + \overbrace{\binom{4}{1}}^{4}(2-1)^1) =$

$|B_1(c)|$ $\quad =4 \cdot 5 = 20$ ok

imposibil

Ex ISBN 10 recunoaște transpoziție de litere

$(c_1, \dots, c_{10})$ $\quad c_i \in \mathbb{Z}_{11}^{\text{corp}} = \{0,1,2,3,\dots,9,X\}$

$\sum_{k=1}^{10} k c_k = 0 \mod 11$ (Condiția care def. cuvintele de cod)

Pp. că după o transpoziție: $\sum_{k=1}^{10} k c'_k = 0 \mod 11$ **

(i,j)

Scădere * - **: $(j-i)(c_i - c_j) = 0 \mod 11$

$j-i \neq 0$

$\Rightarrow c_i = c_j \mod 11$

Ex: $\nexists$ cod binar cu param. $(7, 8, 5)$ (ℓ, $|C|$, d max)

d min $= 5 \Rightarrow e = 2$

$5 \geq 2e+1$ și e să fie maxim

$$2^7 \geq 8\left(1 + \binom{7}{1} + \binom{7}{2}\right) = 2^3\left(1 + 7 + \frac{7!}{2!\,5!}\right) = 2^3 \cdot 3 \cdot 7$$

$$= 2^3(1+7+21) = 2^3 \cdot 29$$

$$2^7 \geq 2^3 \cdot 29 \Leftrightarrow 2^4 \geq 29 \Leftrightarrow 16 \geq 29 \text{ fals}$$

Ex: $\nexists$ cod binar de forma $(90, 2^{78}, 5)$

$d = 5 \Rightarrow e = 2$

Ineg. Hamming: $2^{90} \geq 2^{78}\left(1 + \binom{90}{1} + \binom{90}{2}\right) = 2^{78}\left(1 + 90 + \frac{89 \cdot 90}{2}\right)$

$\frac{89 \cdot 90}{2} = 89 \cdot 45$

$= 2^{78} \cdot 4096$

$2^{12} \geq 4096$ (4096 $= 2^{12}$) $\rightarrow$ codul $(90, 2^{78}, 5)$ ar fi perfect dacă ar fi binar: Gol (23), $23 \neq 90$ și $d = 5 \Rightarrow$ nu e cod Hamming $d=3$

$\Rightarrow \nexists$