Curs 1 STLS II

examen — Teoria codurilor + Quantum Comput.
despre obiecte matematice
de la începutul materiei

$F$ - mulțime finită (alfabetul codului)

$C \subseteq F^n = \{(u_1, \dots, u_n) \mid u_i \in F\}$

$C \neq \emptyset$ cod — cuvinte pe cod, $n$ - lungimea codului

$q = |F|$

$q = 2 \to$ cod binar, $F = \mathbb{F}_2$

$q = 3 \to$ cod ternar, $F = \mathbb{F}_3$

$F \sim \mathbb{Z}_q$ inel de resturi $\quad q = p^k \to F = \mathbb{F}_q$

## Distanța Hamming (2m)

$u, v \in F^n \quad d(u, v) = |\{i \mid u_i \neq v_i\}|$

Th $d$ este o distanță

a) $d(u, v) \geq 0$ și $d(u, v) = 0 \Leftrightarrow u = v$

b) $d(u, v) = d(v, u)$

c) Inegalitatea triunghiului $\qquad$ $M$, $d: M \times M \to \mathbb{R}_+$

$$d(u, v) \leq d(u, w) + d(w, v)$$

d) $F$ grup abelian

$$d(u + w, v + w) = d(u, v)$$

deoarece $u_i \neq v_i \Leftrightarrow u_i + w_i \neq v_i + w_i$

bila (rază $r$, centru $u$)

**Def.** $B_r(u) = \{v \mid v \in F^n$ și $d(u,v) \le r\}$

**Lemă** $|F| = q$, $r \ge 0$ și $u \in F^n$, atunci

$$|B_r(u)| = \sum_{j=0}^{r} \binom{n}{j} (q-1)^j$$

combinări de n luate câte j

poziții care diferă

$$\binom{n}{j}(q-1)^j = \left|\{v \in F^n \mid d(u,v) = j\}\right|$$

litere disponibile pe pozițiile ce diferă

posibilități de a alege pozițiile care diferă din cuvânt

bila Hamming (1950) Războiul Rece - spionaj

cod $C$ t-error recognizing $\iff \forall c \in C$

$B_t(c) \cap C = \{c\}$ (bila conține doar propriul centru ca cuvânt de cod)

cod $C$ e-error correcting $\iff \forall c, c' \in C$

$B_e(c) \cap B_e(c') = \emptyset$

$C$ distanța minimală $d(C)$

$$d(C) = \min\{d(c,c') \mid c \ne c',\ c, c' \in C\}$$

Notație: $C$ este un $(n, M, d)$-cod

pt coduri generale

lungime; $M = |C|$ cardinalitate; distanța minimală

**Th** Dacă $d \geq t+1$, atunci $C$ $t$-error recognizing
distanța minimală

Dacă $d \geq 2e+1$, atunci $C$ $t$-error correcting

**Ex** • Repetition code
repetarea aceluiași caracter de un nr. de ori

$$C = \{ (c, c, \dots, c) \mid c \in F \}$$

$d(C) = n \Rightarrow \leq \frac{n-1}{2}$ error correcting

$(n, q, n)$ - cod

• Bank - account code

$F = \{0, 1, \dots, 9\}$, $Q(z)$ = suma cifrelor lui $z$
$z$ cuvânt (număr)

Obs: $z \rightsquigarrow Q(2z)$ permutare a lui $F$

$0 \to 0,\ 1 \to 2,\ 2 \to 4,\ 3 \to 6,\ 4 \to 8,\ 5 \to 1,\ 6 \to 3,$
$7 \to 5,\ 8 \to 7,\ 9 \to 9$

$(c_1, \dots, c_n)$ a.î. $c_n + Q(2c_{n-1}) +$
$+ c_{n-2} + Q(2c_{n-3}) + \dots = 0 \mod 10$

$\sim$ cod 1-error recognizing
recunoaște și o transpoziție accidentală la cifre vecine
(dacă se întâmplă o dată pe cuvântul de cod)

• ISBN-10

$F = \{0, 1, \dots, 9, X\}$ pt. 10

succesiune de coduri pt limbă, editură, titlu carte, check ...
lungime = 10

0 - 387 - 96617 - X
engleză, editura Dover, titlul cărții, cifră de control

Regulă: $10 z_1 + 9 z_2 + \dots + 2 z_9 + z_{10} = 0 \mod 11$

10 nu e prim $\Rightarrow$ $\mathbb{Z}_{10}$ nu e ~~...~~ corp

$\mathbb{Z}_{11}$ e ~~...~~ corp $\Rightarrow$ $i \rightsquigarrow iz$ permutarea corpului

- EAN - 13

$F = \{0, \dots, 9\}$, $n = 13$ (lungime)

Regulă: $c_1 + 3c_2 + c_3 + 3c_4 + \dots + 3c_{12} + c_{13} = 0 \mod 10$

$z \rightsquigarrow 3z \mod 10$ este permutare a lui $F$

aplicația $\mathbb{Z}_{10} \to \mathbb{Z}_{10}$ injectivă dacă pot simplifica cu 3

domeniu finit $\to$ fcț injectivă = bijectivă

3 ~~...~~ relativ prim cu 10 (3 inversabil în $\mathbb{Z}_{10}$)

**Def**: $C$ cod perfect $\Leftrightarrow$ $\exists e \in \mathbb{N}$ a.î.

$$F^n = \bigsqcup_{c \in C} B_e(c)$$

reuniune disjunctă

orice cuvânt primit prin eroare de transmisie apare într-o bilă și în una singură (se poate determina adevăratul c)

**Th** Hamming bound

$|F| = q$, $n$ lungime, $C$ cod, $d(C) \geq 2e+1$

(a) $q^n \geq \underbrace{|C|}_{M} \sum_{j=0}^{e} \binom{n}{j} (q-1)^j$

(b) $C$ este perfect $\Leftrightarrow$ $\geq$ este egalitate (=)

Ex: Cod Hamming perfect: Codul Hamming

$(n, |C|, d) = (7, 2^4, 3)$

$(c_1, c_2, \dots, c_7) \in \mathbb{F}_2^7$

$$\begin{cases} c_1 + c_4 + c_6 + c_7 = 0 \\ c_2 + c_4 + c_5 + c_7 = 0 \\ c_3 + c_5 + c_6 + c_7 = 0 \end{cases}$$

$\dim_{\mathbb{F}_2} \mathbb{F}_2^7 = 7$ $\qquad \dim_{\mathbb{F}_2} C = 4 \quad (7-3)$

$|C| = 2^4$ nr. elemente

$d$ (distanța Hamming) invariantă la translații

$\Rightarrow \underset{\text{distanța minimală}}{d(C)} = \min\{d(c,0) \mid c \neq 0\}$

$\underset{\text{folosim sistemul}}{d(C) \geq 3}$ adică fiecare $c \in C$ conține $\geq 3$ cifre $\neq 0$

dacă $c_1 = 1 \to$ minim unul dintre $c_4$ (să zicem), $c_6, c_7 = 1$

$\Rightarrow$ minim unul dintre $c_2, c_5, c_7 = 1$

La fel dacă pornim cu alt $c_i = 1$

$\underset{\text{se face doar prin exemplu}}{d(C) \leq 3}$ $\qquad c = (0, 0, 0, 1, 1, 1, 0) \in C$

și $d(c, 0) = 3$

$\Rightarrow d(C) = 3$

$d(C) \geq 2 \cdot 1 + 1 \to$ $e = 1$ err. corr.

$t = 2$ err. rec.

Hamming bound: $2^7 \geq |C|(1+n) =$

$= 2^4 (\underbrace{1+7}_{=2^3})$

$\Downarrow$

egalitate $2^7 = 2^7$

$\Downarrow$

$C$ este perfect.

(Toate codurile Hamming au distanța minimală 3)

(1973) Zinov'ev + Leont'ev : "The nonexistence of perfect codes over Galois fields"

↳ corpuri finite generate

extensii algebrice de grad finit peste corpuri prime

$q = p^k \Rightarrow$ singurele coduri perfecte:

— Hamming $\left(\frac{q^k - 1}{q - 1}, q^{n-k}, 3\right)$

— $(23, 2^{12}, 7)$ codul binar al lui Golay

— $(11, 3^6, 5)$ codul ternar al lui Golay

Th $C$ cod de lungime $n$ cu $|F| = q$, $d = d(C)$, atunci $d \leq n - \log_q |C| + 1$

Singleton Bound Theorem

Dem. $\alpha : F^n \to F^{n-d+1}$

$\alpha(u_1, \dots, u_n) = (u_1, \dots, u_{n-d+1})$

$d = d(C) \Rightarrow \alpha|_C$ injectivă

$$|C| = |\alpha(C)| \leq |F^{n-d+1}| = 2^{n-d+1}$$

$$\log_2 |C| \leq n-d+1 \qquad \square$$

Def

$C$ : $d = n - \log_2 |C| + 1$ maximum distance separable code (MDS-code)

(egalitatea la Singletone bound dacă asta)

coduri: $(n, M = |C|, d)$

lungime — dist. minimă

Coduri liniare $F = \mathbb{F}$ corp finit

$C \subseteq \mathbb{F}^n$ spațiu vectorial $/\mathbb{F}$.

$0 \in C$ (spațiu vectorial)

$[n, k, d]$ notație doar pt. coduri liniare.

dimensiunea peste corpul $\mathbb{F}$ a codului

$\dim_{\mathbb{F}} C \qquad 2^k = |C|$

$wt(u) = |\{i \mid u_i \neq 0\}| = d(u, 0)$

weight $\qquad wt(C) = \min\limits_{c \in C} wt(c) = d(C)$

Obs Sunt suficiente $k$ cuvinte pt. a genera toate cele $2^k$ elemente.

Def $[n, k]$-cod $C$, $G \in \mathcal{M}_{k \times n}(\mathbb{F})$ s.n. matrice generatoare a lui $C$ dacă

$G : \mathbb{F}^k \to \mathbb{F}^n \qquad G(u) = u\, G$

(vector linie)

$G$: $k$ linii
$n$ coloane

$$u \cdot \begin{pmatrix} | & | & & | \\ c_1 & c_2 & \cdots & c_n \end{pmatrix}$$

vector de lungime $k$

coloane

$$= ( \,|\; |\; |\; \ldots\; |\, )$$

$$C = G(\mathbb{F}^k) = \operatorname{Im} G$$

Deci liniile matricei formează o bază a codului

Matricea generatoare = bază a cărei vectori sunt scriși ca linii

ex: bază $C$: vectorii scriși unul sub altul

$$rk(G) = \dim(\operatorname{Im} G)$$

rank

$$rk(G) = k = \dim_{\mathbb{F}}(C)$$

Def: $C = [n, k]$-cod, $H \in \mathcal{M}_{(n-k)\times n}(\mathbb{F})$ s.n. matrice de control dacă

$$C = \{ u \mid u \in \mathbb{F}^n, Hu^T = 0 \} = \operatorname{Ker}(H)$$

$$rk(H) = n - \dim(\operatorname{Ker} H) = n - d(C) = n - k$$