

## → Curs 1 - 23.02.2023

↪ modalitate de notare: examen

→ 2 parti: Teoria codurilor + Quantum computing

### → Teoria codurilor

↪ Fie  $F$  mulțime finită (alfabetul codului) și  $C \subseteq F^n$   $\{u_1, \dots, u_m\} | u_i \in F^n$

$C \neq \emptyset$ , codul, iar  $u_1, \dots, u_m$  cuvinte ale cod și  $n$  = lungimea codului

Fie  $q = |\text{mulțimea de lățuri din alfabet}| = |F|$

dacă  $q = 2 \Rightarrow$  cod binar  $\Rightarrow F = \mathbb{F}_2$

dacă  $q = 3 \Rightarrow$  cod ternar  $\Rightarrow F = \mathbb{F}_3$

/\*  $F \cong \mathbb{Z}_q$  i.e.  $F = \{0, 1, \dots, q-1\}$ ;  $q = p^k$  cu  $k \geq 1$  și  $p$  prim  $\Rightarrow F = \mathbb{F}_q \cong \mathbb{Z}_q$   
înțeles resturi

//  $k=1 \Rightarrow \mathbb{Z}_q$  este corp

//  $k \geq 2 \Rightarrow \mathbb{Z}_q$  nu mai este corp

//  $\mathbb{Z}_p \Rightarrow$  polinom irred. de grad  $k \Rightarrow$  ec. de structură

//  $\Rightarrow$  elementele corpului  $\mathbb{F}_p$  \*

### → distanță Hamming

$u, v \in F^n$

$$d(u, v) = |\{i \mid u_i \neq v_i\}|$$

⑦ Fie  $d$  o distanță (nr. de diferențe dintre 2 cuvinte).

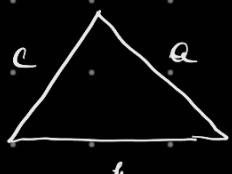
//  $\exists M$ ,  $d: M \times M \rightarrow \mathbb{R}_+$ , deoarece respectă prop.  $\Rightarrow d$  distanță în  $M \times M$  = spațiu metric

Vorbim că  $d$  este proprietabil:

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

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

c) Inegalitatea triunghiului



(f)  $\Delta \Leftrightarrow$  suma a 2 laturi  $\geq$  a treia

$$a+b > c \quad (\text{ex})$$

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

$q$  prim  $\Rightarrow \mathbb{Z}_q$  comp finit  
denumit comp Galois  $GF(2)$

(1)  $\forall e \in \mathbb{Z}_q$  are un unic  
invers multiplicativ de  
 $e \neq 0$  (nu el. nul)

(2)  $GF(2)$  are o rotație  $\rho$ ,  
primitivă  $\neq 0 \Rightarrow$  în el. e tot  
poate fi cauza că  $e = p^a$

d)  $\mathbb{F}$  e grup abelian  $\Rightarrow$  distanță și invariabilitate la translată  
 $\mathbb{F}^m$  e grup abelian

$$\hookrightarrow \text{translație: } d(u+w, v+w) = d(u, v)$$

dem.: a, b triviale, c dem. pe cosinuș general (transformare)

d) diferență  $u_i \neq v_i \Leftrightarrow u_i + w_i \neq v_i + w_i$  (A)

$\rightarrow$  Def. bila Hamming (1950)

$$Br_r(u) = \{v \mid v \in \mathbb{F}^m, d(u, v) \leq r\}$$

$\downarrow$  bilă de rază  $r$ , centru  $u$



$\rightarrow$  Lema

$$\text{Dc. } |Br_r(u)| = \sum_{j=0}^r \binom{m}{j} (q-1)^j = \sum_{j=0}^r \binom{\frac{m}{2}}{j} (q-1)^j$$

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

m. de locuri  $\underbrace{\sim}_{m}$  m. de bituri care pot fi înlocuite

m. de erori = cod. bilă Hamming.

$\rightarrow$  Criteriile codurilor

Fie  $C$  t-error recognizing // recunoaște poziția de eroare  $\Leftrightarrow \forall c \in C ; Br_t(c) \cap C = \{c\}$

e-error correcting  $\Leftrightarrow \forall c, c' \in C, c \neq c' \rightarrow Br_e(c) \cap Br_e(c') = \emptyset$   
poate urca cel mult e eroare

$C$  are distanță minimă  $d(C)$

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

Not:  $C$  este  $(n, M, d)$ -cod  
 lungime  $\downarrow$  distanță minimă  
 cod dimensiune ad

① Dc. dist. minimă  $d \geq t+1 \Rightarrow C$  t-error recognizing.

$d \geq 2t+1 \Rightarrow C$  e-error correcting.

→ Exemplu

↳ Repetition code

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

ex. de cifrareat: 000111110111100000 → 0110

$\underbrace{d(c)}_{\text{dist. min.}} = n \leq \frac{n-1}{2}$  error-correcting.

$(n, 2, n)$ -cod  
cond. minității  $\rightarrow$  dist. min.

→ Bank-account code

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

Uz:

$z \rightsquigarrow Q(2z)$  este o permutare a lui  $F$ :  $0 \rightarrow 0$      $3 \rightarrow 6$      $6 \rightarrow 3$   
 $1 \rightarrow 2$      $4 \rightarrow 8$      $7 \rightarrow 5$   
 $2 \rightarrow 4$      $5 \rightarrow 1$      $8 \rightarrow 7$   
                         $9 \rightarrow 9$

$$C = \left\{ (c_1, \dots, c_n) \mid c_m + Q(2c_{m-1}) + c_{m-2} + Q(2c_{m-3}) + \dots = 0 \pmod{10} \right\}$$

1-error recognizer (⇒ nu-a găsit o afacere potrivit sau imposibil)

Reacnoare și transpozitia accidentală le-a făcut vecine

→ ISBN-10

$$F = \{0, 1, 2, \dots, 9, \times\}$$

0 - 387 - 96617 - X  
engl.      ↑      ↑      ↑  
lumbe      doar      titlu      cifra  
ed. hura      conțin      de control

$$10z_1 + 9z_2 + \dots + z_{10} = 0 \pmod{11}$$

$Z_{11}$  este cod (nu e prim) ⇒  $i \rightsquigarrow i^2$  este o perm. a modulu

4

 $\rightarrow EAN-13$ 

$$F = \{0, 1, 2, \dots, 9\}, m = 13$$

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

$\| de a merge \Rightarrow$

$z \rightsquigarrow 3z \pmod{10}$  este perm. lui  $F$

Funcția este inj., dom. finit  $\Rightarrow$  funcț. este surj.  $\Rightarrow$  fct. este bij.

3 este inversabil în  $\mathbb{Z}_{10}$

$\rightarrow \underline{\text{def.}}$

Codul este numit perfect  $\Leftrightarrow \exists c \in \mathcal{C} \text{ s.t. } F = \bigcup_{c \in \mathcal{C}} \text{B}_e(c)$

Q) de astăzi în ordine

$\rightarrow \textcircled{T} (\text{Hamming bound})$

$\| pt. toate codurile$

$$|\mathcal{C}| = 2^m, m = \text{lunghimea ev.}, C = \text{cod}, d(C) \geq 2e + 1$$

$$a) 2^m \geq |\mathcal{C}| \sum_{j=0}^e \binom{m}{j} (2^{-1})^j$$

multiplu de tuturor ev.  
peste alfabetul cu 2 lățeu

b)  $C$  perfect  $\Leftrightarrow$  avem egalețatele de a)

Dem: în moduale

$\hookrightarrow$  Ex. de cod perfect Hamming  $\rightarrow$  cod Hamming :

$$(m, |\mathcal{C}|, d) = (4, 2^4, 3)$$

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

care verifică urm. ec.

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

Niciun termen omogen

dim. sp. vectorial =  $f = \text{card base} = \lg(c_1, \dots, c_7)$

$$\dim_{\mathbb{F}_2} \mathbb{F}_2^f = f$$

$$\dim_{\mathbb{F}_2} C = 4 \Rightarrow |C| = 2^4$$

corp  $\mathbb{F}_2$  cu 2 el.

$\mathbb{F}_2^7$  grup abelian  $\Rightarrow$  d. min. le translatii  $\Rightarrow$  dist. minim de la origine

$$d(C) = \min \{d(c, 0) \mid c \in C \setminus \{0\}\}$$

dem. că  $d(C) \geq 3$  și  $d(C) \neq 1$

(1)  $d(C) \geq 3$   $\Rightarrow$  ( $\forall c \in C$  cu cel puțin 3 lățuri)  $\Rightarrow$   
 $\Rightarrow$  fiecare  $c \in C$  conține  $\geq 3$  cifre ≠ 0

PP.  $c_1 = 1 \Rightarrow$  min. unul dintre  $c_4, c_6, c_7 = 1 \Rightarrow$   
 $\Rightarrow$  trei ori cu o cifră logaritmică peste  $2c_2 \cdot 2^{N-3} \Rightarrow$   
 $\Rightarrow$  min. unul dintre  $c_2, c_4, c_5 = 1$

La fel de permanent ca și  $c_i, i > 1$

(2)  $d(C) \leq 3$

Fie  $c = (0, 0, 0, \underbrace{1, 1, 1}_c, 0) \in C$  și  $d(c, 0) = 3$

$c_4, c_5, c_6$

dim(1) și (2)  $\Rightarrow$   $d(C) = 3$

$d(C) \geq 3 = 2 \cdot 1 + 1 \Rightarrow e = 1, t = 2$

Avem adică perfectă: Hamming bound

$$2^t \geq |C| (1+e) = 2^t \cdot (1+t) = 2^4 \cdot 2^3 = 2^7, \text{ deci}$$

$C$  este perfectă  $\square$

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

corpuri finite generale

(nu există coduri perfecte)

$\mathcal{L} = \mathbb{F}^n \Rightarrow$  singurele coduri perfecte sunt

- codurile Hamming  $\left( \frac{\mathbb{F}^{k-1}}{\mathbb{F}^1}, \mathbb{F}^{n-k}, 3 \right)$

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

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

### $\Rightarrow$ (T) Singleton-bound theorem

Dacă  $C$  este un corp de lg.  $n$  cu  $|C| = q$ , și  $d =$  dist. min. atunci  $d \leq n - \log_q |C| + 1$

Dem.:

Fie  $\mathcal{L}: \mathbb{F}^n \rightarrow \mathbb{F}^{n-d+1}$

$$\mathcal{L}(\mu_1, \dots, \mu_n) = (\mu_1, \dots, \mu_{n-d+1})$$

Pt. că  $d = d(C) \Rightarrow \mathcal{L}|_C$  este injectivă

$$\begin{aligned} \mathcal{L}|_C \text{ injectiv} \Rightarrow |C| &= |\mathcal{L}(C)| \leq |\mathbb{F}^{n-d+1}| = q^{n-d+1} \\ \Rightarrow \log_q |C| &\leq \log_q q^{n-d+1} = n-d+1 \end{aligned}$$

$\Rightarrow$  Def:

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

$\Rightarrow$  Coduri:  $(n, N = |C|, d)$

lg. codului coincide cu dist. min.

Coduri limite:  $F = \overline{\mathbb{F}}$  și  $C \subseteq \mathbb{F}^n$  - vectorial pe  $\mathbb{F}$

închiderea cu lexele din  $\mathbb{F}^n$

$$\begin{bmatrix} m, & k, & d \end{bmatrix}$$

$\uparrow$        $\uparrow$   
 $\dim_{\mathbb{F}} C$       dist. limităra

WT = weight = grunță

WT( $h$ ) = m. do. inițială ast. care  $h \neq 0 = d(u, 0)$

$0 \in C$

$$WT(C) = \min_{c \in C} (WT(c)) = d(C)$$

$\Rightarrow$  Sunt suficiente  $k$  avințe pt. o genera toate cele  $2^k$  elemente

$\Rightarrow$  Matrice generatoare

$[m, k]$ -wd  $C$

$G \in M_{k \times n}(\mathbb{F})$  s. m. matrice generatoare a lui  $C$

Fie  $G: \mathbb{F}^k \rightarrow \mathbb{F}^n$ ;  $G(u) = \sum_{i=1}^k u_i G_i$   
vector linie

G are  $k$  linii și  $n$  coloane

$C = G(\mathbb{F}^k) = \text{Im } G$ . Deci linile matricii formează o bază a codului  $\mathbb{F}^k$  linie a lui  $C$  este cunoscătoare?

$\|$  dec. jau un ex. de linie,  $0, 0, 0, 1, 0, \dots, 0 \Rightarrow$  polinomul

$\|$  înmulțit cu  $\mathbb{F} \in \text{Im } G \Rightarrow$  e cunoscătoare

$\| (\mathbb{F})$  linie = bază

de ex. o bază a lui  $C$ , vectorii sunt unul sub altul

$r_K = \dim \text{Im } G \quad \| \text{rank} = \text{rangul mat.-gen.}$

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

$\Rightarrow$  Matrice de control

$C = [m, k]$ -wd

$H \in M_{(n-k) \times n}(\mathbb{F})$  și matrice de control  $\Leftrightarrow$   
 $\Leftrightarrow C = \{u | u \in \mathbb{F}^n, H_u^T = 0\} = \text{Ker } H$   
 vector coloană

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

→ Turs 2 - 02.03.2023

↳ maximum likelihood (Syndrome decoding)

Fie  $\tilde{x} \in K^n$  un cur. reprezentat

Se căuta  $c \in C$  s.t.  $f = \tilde{x} - c$  (\*grădă\*) ;  $f \in \tilde{c} + C$ , weight( $f$ ) minim  
 măsură în care  $\tilde{x} \neq c$

Fie  $H$  matrice de control

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



Def.:  $Hv^T \in \mathbb{F}^{n-k}$  sindrom al lui  $v \Rightarrow \tilde{c} \wedge f$  un vector sindrom  $\Rightarrow f$  se poate recunoaște după sindrom

Se poate face un dicționar al erorilor codabile

Pentru o clăsă de echivalență  $v \in C \subset \mathbb{F}^n$ , găsim un reprezentant  $f_v \in v + C$  astfel încât eroarea să fie minimă

$$\underbrace{\text{wt}}_{\text{weight / pondere}}(f_v) = \min \{ \text{wt}(v + c) | c \in C \}$$

⇒ decodificare :

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

profundă

→ (T) Fie  $C$  un cod de tip  $[n, k]$  pe  $\mathbb{F}$  (nu este) și  $H$  matrice de control  
 Atunci  $d(C) = \text{wt}(C) = \min \{ w | \exists \text{ un nr. } w \text{ de coloane liniori}$   
 dependente în  $H \}$  =  $\max \{ w | \text{t. } w-1 \text{ coloane din } H \text{ sunt liniori}$   
 independenți }

// linear dep.  $\Rightarrow$  primit. code word reads m. de vector

dém:

Die  $h_1, \dots, h_m$  voneinander linear unabh.  
 $\Leftrightarrow$

$C \neq 0 \Rightarrow$  linear dependent

$\Rightarrow$  da es  $\exists w$  minimal s.t.  $h_1, \dots, h_m$  nā s̄ie linear dependent

$\Rightarrow$  da es  $\exists c$  a. r. v.

$$\sum_{j=1}^m c_j h_j = 0, c_j \in K, c_k \neq 0 \Leftrightarrow k \in \{i_1, \dots, i_w\}$$

Die  $c = (c_1, \dots, c_m)$

$Hc^T = 0 \Rightarrow c \in C$  // const. vektor

$$wt(c) = w \Rightarrow \boxed{wt(c) \leq w}$$

Präzumptionsweise  $\exists \tilde{c} \neq 0, \tilde{c} \in C$  en  $wt(\tilde{c}) < w$

$H\tilde{c}^T = 0 \Rightarrow \exists$  un. m.  $< w$  de columnen linear dependent im H

/\*  $\begin{pmatrix} \vdots & \vdots & \vdots \\ \vdots & \ddots & \vdots \\ \vdots & \vdots & \vdots \end{pmatrix} \cdot \begin{pmatrix} \vdots \\ \vdots \\ \vdots \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \end{pmatrix}$

$\Rightarrow$  Hamming codes

Die  $K$  wrg. finit,  $|K| = q$ -erw. vekt.,  $g_i = p^{\alpha_i}$   
 $m p \cdot g_i, p \in \mathbb{P}$

$$F_5 = \mathbb{Z}_5$$

Sp. projektiv der dim  $K^{-1}$



$x, y \in \mathbb{R}, x, y, \text{ vektor } \Rightarrow \exists x^0 + y = x + 3 \in \mathbb{R}^2$

$$x^2 \setminus \{0\} / \sim = P(Q) = P(R)$$

abrupt = projektiv

$$P(\mathbf{z}) = \{\langle u \rangle\}^0 + \mu \tau(u_1, \dots, u_k)^T, \quad u_i \in K$$

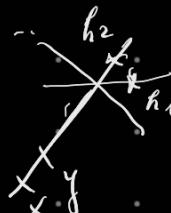
$$\langle u \rangle \Leftrightarrow \exists \lambda \in K^\times, u = \lambda v$$

$$\text{Fie } m = m \text{ d. el. } = |\mathcal{P}^{k-1}(\mathbf{z})| = \frac{2^k - 1}{2 - 1}$$

m. de scoburi multiplicator  $\rightarrow 1$

$$\Rightarrow \underbrace{\mathcal{P}^k(\mathbf{z})}_{\text{m. de scoburi}} = \{\langle h_1 \rangle, \langle h_2 \rangle, \dots, \langle h_m \rangle\}$$

/\* Aleg este un reper referință drept:



/

Fie H matricea  $H = (h_1, \dots, h_m) \in \mathcal{M}_{K \times n}(K)$  //  $\overset{k \text{ linii}}{n \text{ coloane}}$

Def.: codul Hamming este codul corector pe H matrice de control

cls: Fie cel puțin  $n!$  coduri Hamming care diferează

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

multiplică vectorial la linii  $K^n \Rightarrow \text{rg}(H) = k$

rg maxim

demon.:

$$H = \left( \begin{array}{cccc} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{array} \right) \Rightarrow \text{rg}(H) = k$$

linii independ.

Atunci  $\boxed{\dim C = n - k}$  // dim. cod Hamming

→ Dacă 2 coloane din  $H$  sunt linii independenti (din construcție sunt reprez. ai unor duplete independente), iar  $\langle h_1 \rangle, \langle h_2 \rangle, \dots, \langle h_n \rangle$  sunt întreg. linii dependente  $\Rightarrow$   
 $\Rightarrow \text{wt}(c) - d(c) = 3$   
 $\text{dist. min.} = \text{dist. Hamming}$

① de aici în ordine

→ Codul Hamming are par.  $[n, n-k, 3]$  unde  $n = \frac{2^k - 1}{2 - 1}$   
 $\xrightarrow{\text{lungime}}$   $\uparrow$   $\xrightarrow{\text{dimensiune}}$   $\uparrow$   $\xrightarrow{\text{dist. min.}}$

→ Dоказ.

- 1)  $3 \geq 2 \cdot 1 + 1 \Rightarrow$  codul este 1-corrector
- 2) codul este perfect pt. că: imaginea lui Hamming este egală cu  
pt. acest cod

Alegem 2):

$$\left| \bigcup_{c \in C} B_1(c) \right| = |C| \cdot |B_1(0)| \cdot q^{n-k}$$

$\uparrow$  nr. de cuante de  
 $\uparrow$  cod.  $(n-k)$  dim.  
 $\uparrow$  coordonată  
unei linii  
 $\uparrow$  1 pt. cā red  
central

$$= 2^{n-k} \left( 1 + \frac{q^{k-1}}{q-1} (q-1) \right) = 2^n$$

cond. multime de cuv.  $\Rightarrow$

$\Rightarrow$  reunirea disjunctă (bilele nu se intersectează și nu sunt în  
afara unei bili)

→ Not.: Ham<sub>2</sub>(k) = mulțimea codurilor Hamming dif. pe 2<sup>k</sup>, k  
 $\hookrightarrow$  formă de coduri perfecte  
 $\Rightarrow$  nu sunt buse d.p.d.v. proaste

## → Teorema Simplex

// folosim același matrice de la Hamming "pe post" de matrice generatoare  
 // înse. ei sunt aplicație liniară  $\rightarrow$  generația codului simplex  
 $\hookrightarrow$  Def.:  
 Este un cod  $C$ , pe corpul  $K$  care o are pe  $H$  ca matrice generatoare  
 deci,  $C = \{ \underset{\substack{\uparrow \\ \text{vector liniar}}}{\underset{\substack{\uparrow \\ \text{m. de linii ai lui } H}}{\underset{\substack{\uparrow \\ \text{vectorial în } K^n}}{aH \mid a \in K^k}} \} \subseteq K^m$

$\Rightarrow$  (T) (prop.) // între oricare 2 pct. este vecinătate.

de c  $\in C \setminus \{0\} \Rightarrow \text{wt}(c) = 2^{k-1}$   
 există în codul simplex

dimp:

Fie  $z_i$  liniile lui  $H$  și (vectorul)  $c \neq 0$  cu  $c = (c_1, \dots, c_m)$   
 $x = \sum_{i=1}^k x_i z_i = \sum x_i (z_{i,1}, \dots, z_{i,m}) \in C$

$V = \left\{ (h_1, \dots, h_k)^T \mid h_i \in K, \sum_{j=1}^k a_j h_j = 0 \right\} \rightarrow$  sp. de dim.  $k-1 \Rightarrow$   
 $\Rightarrow$  conține  $2^{k-1}$  elemente

Un m. de  $\frac{2^{k-1}}{2-1}$  roboane ale lui  $H$  sunt echivalente cu elemente  $\Rightarrow$

o lini  $h$ .  $\downarrow$  de ce?

o lini construcție  $\Rightarrow$  iau dreptul  $C$  în plan, folig un  
 sprijin pe frâu  $\rightarrow$  construirea  $H \Rightarrow$

$\Rightarrow q-1 \rightarrow$  cord. dreptelor, pt. frâu avem o coloană

$\Rightarrow c_j = 0 \Leftrightarrow \exists v \in V \text{ s.t. } \exists j \text{ a.s. } \langle h_j \rangle = \langle h \rangle$

$$\Rightarrow \text{wt}(c) = m - \underbrace{\frac{2^{k-1}}{2-1}}_{\text{cord. } v=0} = \frac{2^{k-1}}{2-1} - \frac{2^{k-1}}{2-1} = \frac{(2-1)2^{k-1}}{2-1} = 2^{k-1}$$

//  $q \neq 1 \Rightarrow$  pt. că nu lucrăm cu expansiune a unui el.

$$\Rightarrow \left[ \frac{2^{k-1}}{2-1}, \frac{k}{\dim}, \frac{2^{k-1}}{\text{dist. min.}} \right]$$

$\Rightarrow$  Vot: Multimea codurilor simplex date de ecuații perimetru  
 $S_{\text{sim}}_Q(k)$

## → Exercitiu (pag 55)

- 1) Un cod Hamming de nr. [7, 4, 3] are următoarea matrice de control în F<sub>2</sub>  
 $H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$ ;  $\dim(\text{Ker } H) = 7 - \text{rg}(H) = 4$   
 dist. min. Hamming = 3

Găsești matricea generatoare

$$H \vec{x} = \vec{0} \Leftrightarrow \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \text{ cu sistem linear independent.}$$

$$\left\{ \begin{array}{l} x_1 + x_4 + x_5 + x_7 = 0 \\ x_2 + x_4 + x_6 + x_7 = 0 \\ x_3 + x_5 + x_6 + x_7 = 0 \end{array} \right. \Leftrightarrow$$

$$\Rightarrow x_4, x_5, x_6, x_7 \text{ pot fi poz. } (\Rightarrow \dim(\text{Ker } H) = 4 \text{ (1)}) \Rightarrow (x_4, x_5, x_6, x_7) = (a, b, c, d)$$

$$\Leftrightarrow \begin{cases} x_1 = a + b + d \\ x_2 = a + c + d \\ x_3 = b + c + d \end{cases} \Rightarrow \vec{x} = \begin{pmatrix} a + b + d \\ a + c + d \\ b + c + d \\ a \\ b \\ c \\ d \end{pmatrix} \text{ forme generatoare a unui cod. din care codul Hamming} \Rightarrow$$

$$\Rightarrow \vec{x} = a \begin{pmatrix} c_1 \\ 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + b \begin{pmatrix} c_2 \\ 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + c \begin{pmatrix} c_3 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} + d \begin{pmatrix} c_4 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

matricea generatoare este  $(c_1, c_2, c_3, c_4, \text{ devin } l_1, l_2, l_3, l_4)$

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

- 2) Fie  $G = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$  matrice generatoare

matrice unitate  $\Rightarrow \text{rg}_{\min}(G) = 4 \Rightarrow \text{Ker}(G) = 4 \Rightarrow$

$\Rightarrow G$  generă un cod de lungime [7, 4, 3]  $\Rightarrow$  Hamming

T.s.d. mat. de control  $H$

Fie  $H$  matrice de control cu 3 linii (row) și 7 coloane și proprietatea  $H \cdot G^T = 0$

de ce? linile matricei generatoare formează baza vectorială  
0 linie arbitrară a lui  $H$  este  $(a, b, c, d, e, f, g)$

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

Număr par. a, b, c

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

vectorii  $\leftrightarrow$  linii în  $H$

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

3) Să se determine simbolul pt. o greșeală din conținutul  $[7,4,3]$  pt. matricea precedență  $H$ .

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

Hamming este 1-error correcting

$$\text{Fie erorile } f_i = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \\ 0 \end{pmatrix} \rightarrow \text{poziția } i$$

$$\left\{ \begin{array}{lll} Hf_1 = (1, 0, 0) & Hf_4 = (1, 1, 0) & Hf_7 = (1, 1, 1) \\ Hf_2 = (0, 1, 0) & Hf_5 = (1, 0, 1) & \\ Hf_3 = (0, 0, 1) & Hf_6 = (0, 1, 1) & \end{array} \right.$$

dicționarul de simboluri

$Hf_i = \text{coloana } i \text{ corespunzătoare liniei}$

4.) I-a receptionat cuv.  $\tilde{x} = (1, 1, 0, 0, 1, 1, 1)$ . Este  $\tilde{x}$  corect în Hamming  
 $[7, 4, 3]$  dc. H (prudent) este mat. de control? Dc nu, care este  
 originalul?

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

Conform sindromului cdeulot anterior, cel mai probabil Hfr este grecola  $\Rightarrow \tilde{c} - f_t = (1, 1, 0, 0, 1, 1, 0)$  cuv original

→ Term 3 - 09.03.2023

↳ Coduri de evaluare RSC

↳ def.

Die  $K$  auf  $\mathbb{Z}_p$ ,  $|k| = q = p^{\infty}$  s.  $\ell_m$ ,  $1 \leq k \leq m \leq q$ ,  $M = \{m_1, \dots, m_q\} \subseteq K$  (eigentlich identisch)

Für (modul)  $C = \{f(a_1), \dots, f(a_m)\}$  |  $f$  Polynom  $f = k[x]$  si  $\deg f < b\}$

$C$  subsp. rect. in  $K^n$ ;  $C \subseteq K^n$

Cse. num. Reed-Solomon Code (classic)  $\leftrightarrow$  Shamir Secret Sharing

un <sup>↑</sup> cur. do wd est dot

de un polinomio

$$f = \underset{P}{\underbrace{s + t_1 x + \dots + t_{k-1} x^{k-1}}} + \text{terms like}$$

" $x_i$ "  $\leftarrow f(x_i) \Rightarrow (x_i, f(x_i))$   
 (cunoscut  $x_i$ ) identitate

$\Rightarrow$  *recole- secretul 5*

$\Rightarrow$  Característica:  $\left[ \overset{\text{dim}}{n}, \overset{\text{dist. min}}{k}, \overset{\text{dim}}{n-k+1} \right]$

↳ (T) Pers. mentioned must pers. b/w RS Code

### Dem. dist. min

$\hookrightarrow$  (v) we showed our algorithm  $n - (k-1)$  word,  $\neq 0$

cel mult.  $k-1$  nöd. in

arp als pol.  $\Rightarrow$  cel punkt in  $n - (k-1)$  coord.  $\leftrightarrow$

$\Rightarrow (t) \in C$ , not  $(c) \geq n - k_{T_1}$ .

Ex.  $f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_{k-1})$  // pol. de grad max. accepté  $n-k+1$

not.  $c_j = n - k + 1$ .

$$\Rightarrow d(c) = m-k+1$$

→ Alg. Borckamp - Welech

↳ factor commutativus nullig. finit

$$\rightarrow t \geq 1, n = 3t + 1$$

$\rightarrow$  odd  $\rightarrow$  in cars.

$\rightarrow$  (T) : Existe o procedura rapidă (ordine  $O(n^2)$ ) pt. a verifica  $c \leq t$  evenimentelor din C

Dom.

Se consideră polinomul  $Q(x, y) = f_0(x) - f_1(x)y$ .

$f_0, f_1 \in K[t]$ ,  $\deg f_0 \leq 2t$ ,  $\deg f_1 \leq t$  en  $f_1(0) = 1$

$$\left[ 2^{k+1} \right] \quad [7]$$

*neumoscuti*

$\theta_i \rightarrow t$

$\alpha_0 \rightarrow + \Rightarrow t+1 \cos$

der  $f_1(0) = 1$  teimes h. b. einer at

*t* " recompute

Le nuptioeora ( $y_1, \dots, y_n$ ) curant despre cor me cum a e cond  
si a me, des are cel putin o grecolor

$\mathcal{L}_k \rightarrow$  auroscuté / etchelé au core bord  $C \rightarrow$  il n'est pas conservé.

$$\Rightarrow \{Q(x_k, y_k) = 0\} ; k=1, n$$

Sistemul  $2t+1 + t = 3t+1$  nu este corect.

dim resolvente  $\Rightarrow f_1(x) \sim f_0(x)$

To face imponții cu rest în  $K[t]$  }  $\Rightarrow$  astfel  $f(t) = \frac{f_0(t)}{f_1(t)}$   
 pt. că este echivalent cu gr. pd. }

$\mathbb{K}[x] \rightarrow$  inert euclidean

de a - ?

Daca  $P(x) = Q(x, g(x))$ , f este neamănu

Dear, plug  $P(x) \leq 2t$ , one cell pubn m-e no d. (word wrk)

dor  $m - e > m - t > 3t - t = 2t$  are red. mai multe

decor product

deco<sup>r</sup> grooth

$\Rightarrow P \in R \Rightarrow f_0(x) = f(x) \cdot g(x)$  este identitate polinomială

$\Rightarrow c_f = (f(x_1), \dots, f(x_n))$  nu are tot n zero din x

$\rightarrow$  Codul Reed-Muller 1950 pt.  $K = \mathbb{F}_2$

$\hookrightarrow$  generalizare RS Code

$\rightarrow$  Def:

Fie  $\mathbb{F}_2 = [x_1, \dots, x_m]$  cu  $0 \neq f = \sum_{e_1, \dots, e_m} x_1^{e_1} \cdots x_m^{e_m}$

$\deg f = \max \{e_1 + \dots + e_m \mid e_1, \dots, e_m \in \mathbb{F}_2\}$  cu  $\deg 0 = -\infty$

$\mathbb{F}_2^m = \{P_1, \dots, P_m\}$ ,  $m = 2^m$

$f \leftrightarrow c_f = (f(P_1), \dots, f(P_m)) \in K^m$

peste  $\mathbb{F}_2$ , dacă și  $x^2$  se comportă la fel,  $\underbrace{0 \leq e_i \leq 1}_{\text{convenție}}$ ,  $\overbrace{0^0=1}^{\text{convenție}}$  înmulțire

Fie  $\mathbb{W}_r = \{f \in K[x_1, \dots, x_m] \mid \deg f \leq r\}$

$\dim \mathbb{W}_r = \sum_{i=0}^r \binom{m}{i}$ , deoarece  $\dim \mathbb{W}_0 = 1$

d.e.:  $0 \leq r \leq m \Rightarrow RM(r, m) = \{(f(P_1), \dots, f(P_m)) \mid f \in \mathbb{W}_r\}$  codul lui Reed-Muller

$\rightarrow$  (T) corect  $[2^m, \sum_{i=0}^r \binom{m}{i}, 2^{m-r}]$   
lungime dim

$\rightarrow$  Construcția Plotkin pt. codul Reed-Muller

$\hookrightarrow$  Lemă-

Fie  $i = 1, 2$ ,  $c_i$  de par  $[l_i, k_i, d_i]$

$C = C_1 \& C_2 = \{(c_1, c_1 + c_2) \mid c_1 \in C_1, c_2 \in C_2\} \subseteq K^{2m}$  (corect) este un cod  $[2m, k_1 + k_2, \min(l_1, l_2)]$

Denum.:

Fie  $\alpha = c_1 \oplus c_2 \rightarrow C, \alpha(c_1, c_2) = (c_1, c_1 + c_2)$ ;  $\alpha$  inj.  $\Rightarrow$

$\Rightarrow \dim C = k_1 + k_2$

$\text{wt}(c_1) \geq |\text{supp}(c_1) \cap \text{supp}(c_2)|$

//  $\text{supp} = \text{coord. pe care vectorul} - 1$

$\text{wt}(C) = \text{wt}(c_1) + \text{wt}(c_1 + c_2) \geq \text{wt}(c_1) + \text{wt}(c_1) + \text{wt}(c_2) -$

$\geq |\text{supp}(c_1) \cap \text{supp}(c_2)|$

$$\geq \text{wt}(c_2) \geq d_2, d \leq c_2 + r$$

$\delta_C \cdot c_2 = 0 \Rightarrow \text{wt}(c) \leq 2, \text{wt}(c_1) \geq 2d_1$

$\delta_C \cdot c_1 = 0$  și  $(i+j)$  este  $\text{wt}$  (pondere) minimă  $\Rightarrow$  această pondere nu change pt.  $c$   $\square$

$\rightarrow$  Construim  $RM(r, m)$  astfel

$$RM(0, m) = [2^m, 1, 2^m] \text{ cod. de repetitie}$$

$$RM(m, m) = [0, 1]^{2^m} \text{ cod. trivial.}$$

Pentru inducție

$$RM(r, m) = RM(r, m-1) \oplus RM(r-1, m-1)$$

$\hookrightarrow$  dist. min.

$$RM(r, m) : \log 2^m \text{ și } d = \min(2 \cdot 2^{m-1-r}, 2^{m-1-(r-1)}) = 2^{m-r}$$

$\rightarrow$  dimensiune

$$\dim RM(r, m) = \sum_{i=0}^r \binom{m-1}{i} + \sum_{i=0}^{r-1} \binom{m-1}{i} = 1 + \sum_{i=0}^{r-1} \left[ \binom{m-1}{i+1} + \binom{m-1}{i} \right]$$

identitate cunoscută

$$= 1 + \sum_{i=0}^{r-1} \binom{m}{i+1} = \sum_{i=0}^r \binom{m}{i}$$

$\rightarrow$  exemplu

$RM(1, 5)$  este un cod de par {32, 6, 16}  $\rightarrow$  margineră altă dimensiune

cod cu care au reușit să transmită imagini color - negru

$\rightarrow$  Codice Reed-Solomon generalizate

Fie  $K$  corp,  $|K| = q$  cu  $2 \leq d \leq n \leq q$ , fixăm  $a = (a_1, \dots, a_m) \in K^n$ ;  $i \neq j \Rightarrow a_i \neq a_j$  este fixat și  $v = (v_1, \dots, v_n) \in K^n$ , toti  $v_i \neq 0$

$$H \in M_{(d-1) \times n}(K)$$

$$H = \begin{pmatrix} v_1 & v_2 & \dots & v_n \\ a_1 v_1 & a_2 v_2 & \dots & a_n v_n \\ a_1^2 v_1 & a_2^2 v_2 & \dots & a_n^2 v_n \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{d-2} v_1 & a_2^{d-2} v_2 & \dots & a_n^{d-2} v_n \end{pmatrix} \quad \text{matrice de control}$$

$\forall$  minor  $(d-1) \times (d-1)$  al lui  $H$  cu det.  $\neq 0$  pt. că det.  $= v_{i_1} \dots v_{i_{d-1}} \prod (a_{j_i} - a_i)$

$\hookrightarrow$  Def. Generalized Reed-Solomon Code

$\hookrightarrow$  dist. minimă

$$GRS_d(x, v) = \{c \mid c \in K^{n-d}, Hc^T = 0\}$$

$$\boxed{d(GRS_d(x, v)) = d}$$

$$\rightarrow \text{dimensiune } n - rk(H) = n - d + 1$$

$$\{n, n-d+1, d\}$$

$\Rightarrow$  Def:

$K$  este corp finit  $\Rightarrow K^\times$  ciclic și  $\alpha$  este un generator al lui  $K^\times$  și  $v = \alpha = (1, \alpha, \alpha^2, \dots, \alpha^{q-2})$  Reeds-Solomon de dim  $q-d$

$\Rightarrow$  Def:

Un cod  $C$  a numărului ciclic  $\Leftrightarrow \text{pt. } (v) \subseteq C, c = (c_1, \dots, c_n), (c_n, c_1, \dots, c_{n-1}) \in C$

$\Rightarrow$  T:

Oricum cod Reeds-Solomon este ciclic // generat de  $\langle \alpha \rangle$

$\Rightarrow$  Exemplu și exercițiu

$\hookrightarrow$   $\alpha$  de grupuri ciclice  $(\mathbb{Z}_m, +, 0)$ ; "log direct este difiș" numai în grupuri multiplicativi sau în grupuri aditivă peste curbe eliptice

$\hookrightarrow$  Def:  $\alpha$  este generator  $\Leftrightarrow \gcd(\alpha, m) = 1$  // c.m.m.d.c.

Fie  $y \in \mathbb{Z}_m$ ,  $\alpha \in \langle \alpha \rangle = (\mathbb{Z}_m, +, 0)$

Team să calcuțem rea. "  $\alpha^2 = \alpha \cdot \alpha$  ? "

$\gcd(\alpha, m) = 1 \Rightarrow \alpha$  este multiplicativ inversabil

$\underbrace{\exists \alpha^{-1} \text{ mod } m}_{\text{(Euclid extins)}} \text{ s.t. } r = \alpha^{-1}y \text{ mod } m$  "log direct"  
 $O((\log m)^3)$

$\rightarrow$  m.: Parte  $(\mathbb{Z}_m, +, 0, 1)$  opere grupul unităților

$(\mathbb{Z}_m^\times, \cdot, 1) = \{\alpha \mid \gcd(\alpha, m) = 1\} = \text{generatorii lui } (\mathbb{Z}_m, +, 0)$

$\rightarrow$  T  $(\mathbb{Z}_m^\times, \cdot, 1)$  este ciclic  $\Leftrightarrow m \in \{2, 4, p^2, 2p^2\}$  cu  $p$  prim impar

$\rightarrow$  T  $K$  este corp și  $G$  finit  $\leq (K^\times, \cdot, 1)$  atunci  $G$  este ciclic

$\hookrightarrow$  pt.  $\mathbb{R} \rightarrow G = \{1, -1\}$

$\mathbb{C} \Rightarrow G = \left\langle \cos \frac{2\pi i}{n} + i \sin \frac{2\pi i}{n} \right\rangle$  // red. primitive a unității  
 $\hookrightarrow$  or  $n$  elemente  $\sim (G, \circ, 1) \cong (\mathbb{Z}_n, +, 0)$   
isomorf

$K$  corp finit  $\Rightarrow K^*$  ( $K$  multiplicativ) este ciclic

/\*

$\rightarrow \mathbb{F}_{p^2}$  nu este corp divizor  $p^2$  nu este inversabil pt. că  $p \cdot p = 0$  (els)

✓

$\rightarrow$  def:

$\forall \alpha \neq 1$   $K$  corp finit cu  $|K| = p^\ell$  cu  $p$  prim, poate fi în  $\mathbb{F}_{p^\ell}$

$$\ell = 1 \Rightarrow K = \mathbb{F}_p \Rightarrow \mathbb{F}_p = \mathbb{F}_p$$

$$\ell > 1 \Rightarrow \exists \mathbb{F}_{p^\ell}, \text{ dor } \mathbb{F}_{p^\ell} \neq \mathbb{F}_p$$

Se găsește un polinom ireductibil  $f$  din  $\mathbb{F}_p[x]$ ,  $\deg(\mathbb{F}_p) = \ell \wedge$

$$\mathbb{F}_p^\ell = \mathbb{F}_p[x]/(f)$$

ideal gen de pol. în  $\mathbb{F}_p[x]$

"multime" rezervată de produs și închisă la adunare

Fie  $p=2$  și  $\ell=2 \Rightarrow f = x^2 + x + 1$  irred. pe  $\mathbb{F}_2$

Fie  $\omega$  "soluție" a lui  $x^2 + x + 1 = 0 \Rightarrow \omega^2 + \omega + 1 = 0 \Rightarrow$   
nd. formă în  $\mathbb{F}_2: 2=0 \Leftrightarrow 1=-1$

$$\Rightarrow \boxed{\omega^2 = \omega + 1}$$

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

Este  $\mathbb{F}_4$  ciclic?

$$\omega^n: \omega, \omega^2 = \omega + 1, \omega^3 = \omega^2 + \omega = \omega + \omega + 1 = 1 \Rightarrow$$
 toate el.

$\neq 0$  sunt puteri ale lui  $\omega$

$\rightarrow$  In  $\mathbb{F}_7$  este 2 generator? Găsești generatorul/generatorii

$\mathbb{F}_7$ :

$2^n \bmod 7: 2, 4, 1$  generatoare doar 3 el.  $\Rightarrow 2$  nu e generator

$3^n \bmod 7: 3, 2, 6, 4, 5, 1$  toate el  $\Rightarrow$  grup ciclic cu 3 generatori

// e suficient să găsești un generator pt. a dem. că an g.e.c.d.

$$(\mathbb{Z}_7^*, \cdot, 1) \cong (\mathbb{Z}_6, +, 0)$$

generatorii = nr. relativ prime cu 6. = {1, 5}

$$\Rightarrow 1 \cdot k \rightsquigarrow 3^k \Rightarrow$$

$\Rightarrow$  gen. lui  $(\mathbb{Z}_7^*, \cdot, 1)$  sunt 3 și 5

verificare 5: 5, 4, 6, 2, 3, 1

$$\log_5 2 \bmod 7 = 4 \dim 0$$

$$\log_5 6 \bmod 7 = 3 \dim 0$$

$$\Rightarrow \mathbb{Z}_{11}^*: \underbrace{2, 4, 8, 5, 10, 9, 7, 3, 6, 1}_{10 \text{ elemente } \neq 0} \Rightarrow$$

totă el. din  $\mathbb{Z}_{11}^*$   $\Rightarrow$  2 generatori pt.  $(\mathbb{Z}_{11}^*, \cdot, 1)$

$$(\mathbb{Z}_{11}^*, \cdot, 1) \cong (\mathbb{Z}_{10}, +, 0) \Rightarrow 1, 3, 4, 9 \text{ generatoare additive}$$

$$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\} \cong (\mathbb{Z}_4, +, 0)$$

$$\Rightarrow \text{generatorii lui } \mathbb{Z}_{11}^* : 2^1, 2^3, 2^7, 2^9 = 2, 8, 7, 6$$

$$(\mathbb{Z}_{11}^*, \cdot, 1)$$

| dem că  $6^n \bmod 11$  gen.

$\Rightarrow$  Curs 4 - 16.03.2023

$\hookrightarrow$  Rem. prev. courses:

MDS = maximum distance separable (cod.)

// dist. minimă din cod  $\Rightarrow$  max

C cod,  $|F| = 2$ ,  $d = d(C)$

$d \leq n - \log_2 |C| + 1$ ,  $n = \lg \dim C$  // Singleton Bound

$\hookrightarrow$  def:

C este MDS  $\Leftrightarrow d = n - \log_2 |C| + 1$

$\Rightarrow$  dualitate

The K corp (field)  $\forall n \in \mathbb{N}$ ;  $\langle, \rangle : K^n \times K^n \rightarrow K^n$

$\langle u, v \rangle = \sum_{i=1}^m u_i v_i$  // forma biliniara nedegenerata si simetrica

d.c.  $C \subseteq K^m$  (numai multime)  $C^\perp$  ( $C$  ortogonal, complementarea lui  $C$ ) s.i.

 $C^\perp = \{ u \in K^n \mid (\forall) c \in C, \langle u, c \rangle = 0 \}$  // corectul dual al lui  $C$ 

$C$  este auto-dual  $\Leftrightarrow C = C^\perp$  // (f) avand pt.  $c \in C$   $\langle c, c \rangle = 0$   $\Rightarrow$   $\|c\|^2 = 0 \Rightarrow c = 0$

$C$  este auto-ortogonal  $\Leftrightarrow C \subseteq C^\perp$

$\rightarrow (1)$  d.c.  $C$  cod  $[m, k]$  peste  $K$  atunci

- 1)  $H$  este matrice de control pt.  $C \Leftrightarrow H$  este matrice generatoare pt.  $C^\perp$
  - 2)  $(E_k \text{ (matrice unitate)} \mid A)$  este matrice generatoare pt.  $C \Leftrightarrow$   
 $\Leftrightarrow (-A^T \mid E_{m-k})$  matrice generatoare pt.  $C^\perp$
- consecinta: Hamming  $=$  cod Simplex ( $d_{min}(1)$ )

Dem (1)

d.c.  $G$  este generator pt.  $C$  (fiecare element din  $G$  comb. liniera) s.i.  $\Rightarrow G$  matrice  $H(m-k) \times n$  este matrice de control dc.  $HG^T = 0$  si rang  $H = m-k$ .

Dem (2):

$$(-A^T \mid E_{m-k})(E_k \mid A)^T = -A^T + A^T = 0$$

locuri coloane

$\rightarrow$  Exemple

Ex 1 Fie  $GRS_d(\alpha, v)$  si  $K$  corp,  $2 \leq d \leq n \leq 2$  unde  $q = |K|$

$\nearrow$  element vector dim el.  $\in \mathbb{C}^n$

Generalized Reed-Solomon Code

$$\text{Atunci (f) o' (vector) a.i. } GRS_d(\alpha, v)^\perp = GRS_{n-d+2}(\alpha, v')$$

$v'$  este det. prima le (imultitie cu un scalar) de  $\langle v' \rangle = GRS_n(\alpha, v')$   
consecinta

$\Leftrightarrow$  d.c. d.h.  $K = 2$  si  $d \geq \frac{n+2}{2} \Rightarrow (f)v' \in$  a.i.  $GRS_d(\alpha, v)$

$\subseteq GRS_d(\alpha, v)^\perp$  // auto-ortogonal (1)

$\Rightarrow$  dc. (1) + n este par și  $d = \frac{n+2}{2}$  atunci auto-dual

$\rightarrow$  T Fie  $C$  cod,  $\dim C \geq 1$ , atunci  $C$  este MDS  $\Leftrightarrow C^\perp$  este MDS

$$\overline{(C^\perp)}^\perp = C \Rightarrow$$
 este suficient să dim ca "  $\Rightarrow$  " e (A)

Fie  $n = \log_2$  codului și  $k = \log_2 C$ . Fie  $C \neq C^\perp$  atunci  $C^\perp$  are  $\text{wt}(C^\perp) \leq k$ .  $C^\perp$  poate fi sătulă linie în tot generatoare  $G^\perp$  și liniile  $C^\perp$  vor sătă linie cu linie

(A)  $n-k$  coloane în  $G^\perp$  sunt liniar independente

$$\left. \begin{aligned} d(C) = n-k+1 &\Rightarrow \text{ouă } n-k \text{ coloane sunt liniar indep.} \Rightarrow \\ &\Rightarrow d(C^\perp) \geq k+1 \end{aligned} \right\} \Rightarrow$$

$$\Rightarrow \text{contradictie} \Rightarrow d(C^\perp) \leq k+1 \Rightarrow$$

$$\Rightarrow k+1 \leq d(C^\perp) \leq n - (n-k) + 1 = k+1 \Rightarrow \text{Singleton Bound}$$

$\rightarrow$  Def:

Fie  $r \in \mathbb{N}$ ,  $r \geq 1$ , codul  $C$  este  $r$ -divizibil  $\Leftrightarrow$  pt. (4) vector  $c \in C$ , s.t.  $\underbrace{\text{wt}(c)}$  nu de card  $\neq 0$

$\rightarrow$  Lema:

dc.  $C$  este auto-ortogonal peste  $\mathbb{F}_2$  sau  $\mathbb{F}_3 \Rightarrow C$  este 2-divizibil, respectiv 3-divizibil; pe deosebire, dc.  $C/\mathbb{F}_2$  atunci  $(1, 1, \dots, 1) \in C^\perp$

dc. nu în  $C \neq$  pt. că  $C \subseteq C^\perp$

demonstrare:

Fie  $c = (c_1, \dots, c_n) \in C$ ;  $c_i \in \{0, 1\}$  de  $p=2$  respectiv  $c_i \in \{0, 1, -1\}$  dc.  $p=3$

$\sum_i^r$  ambele cazuri; dc.  $c_i \neq 0 \Rightarrow c_i^2 = 1 \Rightarrow 0 = \underbrace{\langle r, c \rangle}_{\text{norma}} = \text{wt}(c) \text{ mod } p$

dc.  $p=2$  atunci  $\langle v, (1, 1, \dots, 1) \rangle = \text{wt}(v) \text{ mod } 2 = 0$

$\rightarrow$  Lema:

dc.  $C$  este binar  $\{0, 1\}$

(1)  $\text{d}_{\mathcal{C}} \cdot \mathcal{C} \subseteq \mathcal{C}^\perp$  și  $\mathcal{C}$  are o bază din vectorii cu wt: 4 și  
 $\Rightarrow \mathcal{C}$  este 4-divizibil

(2)  $\text{d}_{\mathcal{C}} \cdot \mathcal{C}$  este 4-divizibil și  $\mathcal{C}$  este auto-ortogonal

Idee de demis

$$\underbrace{\langle c, c' \rangle}_{\text{prod. scalar}} = |\text{supp}(c) \cap \text{supp}(c')| \bmod 2$$

$$\text{wt}(cc') = \text{wt}(c) + \text{wt}(c') - 2|\text{supp}(c) \cap \text{supp}(c')|$$

II principiu includerii și excluderii

$\Rightarrow$  Codul Golay

$\hookrightarrow$  Def.  $\xrightarrow{\text{cauta in curs}}$  definim extensia lui  $\mathcal{C}$  astfel:  $\hat{\mathcal{C}} = \{(c_1, \dots, c_m, c_{m+1}) \mid (c_1, \dots, c_m) \in \mathcal{C}, \sum_{i=1}^{m+1} c_i = 0\}$

$\hat{\mathcal{C}}$  este un  $\mathbb{F}_{m+1}$ -cod și  $d(\mathcal{C}) \leq d(\hat{\mathcal{C}}) \leq d(\mathcal{C}) + 1$

$\Rightarrow$  def. Codul termal Golay  $\stackrel{\text{not}}{=} \text{Gol}(11)$

$\text{Gol}(11)$  este generat de mat  $G_{11} = \left( \begin{array}{c|c} E_6 & G \end{array} \right)$  cu 6 coloane

$$G \not\in \mathbb{F}_3 \quad \left( \begin{array}{cccccc} 0 & 1 & -1 & -1 & 1 \\ 1 & 0 & 1 & -1 & -1 \\ -1 & 1 & 0 & 1 & -1 \\ -1 & -1 & 1 & 0 & 1 \\ 1 & -1 & -1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 \end{array} \right)$$

Pt.  $\mathcal{C} = \text{Gol}(11)$ ,  $\text{Gol}(12) = \hat{\mathcal{C}}$  (extensia lui  $\mathcal{C}$ )

$\text{Gol}(12)$  este generat de  $G$  la care se adaugă  $\begin{pmatrix} -1 \\ -1 \\ -1 \\ -1 \\ -1 \\ 0 \end{pmatrix}$

$\text{Gol}(12)$  este auto-dual și are par [12, 6, 6]

$$\text{Gol}(12) \subseteq (\text{Gol}(12))^{\perp} \text{ (cu par. } 12-6=6\text{)}$$

// mod. de control  $\Rightarrow$  auto-dul.

$$\stackrel{?}{d}(\text{Gol}(12)) = 6$$

$\Rightarrow \text{Gol}(11)$  nu este auto-dual d<sub>2</sub> este de formă [11, 6, 5] // d=5

$\rightarrow \text{(1)} \text{ Gol}(11) / * [11, 6, 5] * / \text{ este perfect}$

Dom

$d=5 \Rightarrow \text{Gol}(11)$  este e-correctiv pt.  $2e+1 \leq 5 \Rightarrow \boxed{e=2}$

$$3^{11} \geq \left| \bigcup_{c \in \text{Gol}(11)} B_2(c) \right| = |\text{Gol}(11)| \cdot |B_2(0)| = 3^6 \left( 1 + \binom{11}{1} \cdot 2 + \binom{11}{2} \cdot 4 \right)$$

auto-dul  
 pot. le  
 dist. 1  
 dim B<sub>2</sub>(0)

$$= 3^6 \cdot (1 + 22 + 220) = 3^6 \cdot 3^5 = 3^{11} \Rightarrow \text{ineq. egalitate} \Rightarrow$$

somming

$\Rightarrow$  codul este perfect

//  $\rightarrow$  codul minor  $\text{Gol}(23), \text{Gol}(24) \rightarrow$  perfecte

$\rightarrow$  Vomri și caractere

Fie  $K \leq E$  extensie de corpuri finite //  $[F_{p^e} \subseteq F_{p^f} \Leftrightarrow \alpha | \beta]$  cu p prim

/ \* următor:  $\exists \alpha \in F_8 \subseteq F_{16}, F_8 = F_2^3, F_{16} = F_2^4 \Leftrightarrow 3 \nmid 4$  (folos)  $\Rightarrow F_8 \not\subseteq F_{16}$  \*

// caracteristica = nr. prim

Fie  $G$  - grupul Galois al extensiei

//  $G = \{ \varphi : E \rightarrow E \mid \varphi \text{ automorfism de } \underset{n}{\text{ord}}, (\forall i \in K, \varphi(i) = i) \}$

//  $b, c \in E, 0 \neq b, c \rightarrow \text{produs } b \cdot c \text{ - produs, suma } b+c \text{ - suma}$

$\hookrightarrow$  def: Tracse  $\rightarrow T_E$

$\overline{\text{Tr}}_{E/K} : E \rightarrow K$

$$\overline{\text{Tr}}_{E/K}(\alpha) = \sum_{g \in G} g(\alpha)$$

(H)  $\varphi \in G$  (group Galois),  $\varphi$  auto-morfism

$$\varphi(\text{Tr}_{E/K}(a)) = \text{Tr}_{E/K}(\varphi(a)) \Rightarrow \boxed{\text{Tr}_{E/K}(a) \in K}$$

$\varphi$  compus cu tota el. lui  $G$

SDA

lock-free

$\rightarrow$  des

identitate wrt  $\mathbb{Z}_p$

Dacă  $K$  wrt  $p$ ;  $\text{char } K = p \Rightarrow F(x) = x^p$  este automorfism numit Automorfismul lui Frobenius.

$$\mathbb{Z}_p : x^p = x \underbrace{x^{p-1}}_1 = x$$

$$\parallel x \text{ putere și putere} = 1$$

$$\mathbb{F}_4 = \{0, 1, \omega, \omega + 1\} \text{ unde } \omega^2 = \omega + 1 \parallel \text{cc. de definiție}$$

1\*  $\mathbb{F}_2$  inclus pol.  $\mathbb{F}_2[x]$ ,  $x^2 + 1$  ireductibil  $\Rightarrow \nmid (x+1)$  pentru  $x \Rightarrow \omega^2 + \omega + 1 = 0$   
 $x^2 + 1 = -1 \Rightarrow \omega^2 = \omega + 1$

Autom. lui Frobenius  $\Rightarrow$

$$\Rightarrow F(0) = 0, F(1) = 1$$

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

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

$\parallel$  in caracteristica 2  $\parallel$

Automorfism pt. că:

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

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

Automorfism  $\Rightarrow$  inj pt. că ( $\forall$ ) morfism de corpuri este inj. (pt. că  $\ker = 0$ )

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

$\uparrow$  identitate

Automorf. lui Frobenius

$$F^k(x) = ((x^p)^p)^k = \underbrace{x^p}_\text{d.k.m}^k$$

$\Rightarrow$  Ex

Dc.  $|E : K| = n$ ;  $G = \text{grupul automorfismelor} = \langle f \rangle$  generat de Frobenius,  $|K| = 2 \Rightarrow$   
 $\Rightarrow T_{\mathbb{F}_{E/K}}(a) = a + a^2 + a^{2^2} + \dots + a^{2^{n-1}}$

Automorfisme ale lui  $E$  care îl fixează pe  $K$  punct cu punct

$\Rightarrow$  Exercițiu

(1)<sup>5</sup> Fie  $C$  cod.,  $|C|=4$  peste  $\mathbb{F}_2$ . În dem. că  $C$  nu este 1-error-correcting

Răzolvare

Dc. or  $f$  1-error-correcting atunci  $d \geq 3 \quad // d \geq 2e+1$

Ză  $lg = 4$ ,  $d = 4$  imposibil pt. că nu ar avea decât 2 cuv  $\xrightarrow{0,1,\dots,1}$   
 $d=3$  ?

Inug. Hamming  $16 = 2^4 \geq |C| \left( \binom{4}{1}(2-1)^0 + \binom{4}{1}(2-1)^1 \right) = 4(1+4) = 20$   
 cond.  $B_1(C)$  (contradicție)

$\Rightarrow d=3$  imposibil  $\Rightarrow C$  nu poate fi 1-err-correcting

(2)<sup>6</sup> ISBN<sub>10</sub> recunoaște transpozitile de litere nu neapărat alăturate  
 $\downarrow$   
 $(c_1, \dots, c_{10})$  cu  $c_i \in \mathbb{Z}_{11} = \{0, 1, \dots, 9, X\}$

Constr. core def. trans.

$$\sum_{k=1}^{10} k \cdot c_k = 0 \pmod{11} \quad (1)$$

P.p. că avem după o transp.  $(i, j)$

$$\sum_{k=1}^{10} k \cdot c'_k = 0 \pmod{11} \quad (2)$$

$$(1) - (2) \Rightarrow (j-i)(c_i - c_j) = 0 \pmod{11}$$

dor  $j-i \neq 0$  și  $c_i \neq c_j$   $\Rightarrow c_i = c_j \pmod{11}$

$\mathbb{Z}_{11}$  corp (11 nr. prim)

(3) <sup>7</sup> Dem. că  $(\tilde{x})$  este liniștor cu per.  $(7, 8, 5)$   
 Icl.  $\ell$  nu este neap. liniștor.  
 dist. minimă

$$d=2 \text{ distance } 5 \geq 2e+1 \text{ or } e \text{ max} \Rightarrow$$

$$\Rightarrow 2^t = 1 \text{ p. rec. } 1 \geq |C| \cdot B_2 = 8 \cdot \left( 1 + \binom{t}{1} + \binom{t}{2} \right) = 2^3 \left( 1 + t + \frac{t!}{2!5!} \right) = 2^3 \cdot 29$$

↗  
cw. le dist.  
Hamming = 1
      ↗  
cw. le dist.  
Hamming = 2

deci;  $2^7 \geq 2^3 \cdot 29 \Leftrightarrow 2^4 \geq 29 \Leftrightarrow 16 \geq 29$  (Fals)

8  
④ Denumirea (f) urmări binor de firma (90, 2<sup>78</sup>, 5)

$$d=5 \Rightarrow e=2 \stackrel{(\text{veri. ③})}{\Rightarrow} B_2(50) \\ \Rightarrow 2^{50} \geq 2^{78} \cdot \left( \overbrace{1 + \binom{50}{1} + \binom{50}{2}}^{\text{B}_2(50)} \right) \Leftrightarrow$$

$$\Leftrightarrow 2^{12} \geq 1 + 90 + \frac{89 \cdot 90}{2} = 1 + 90 + 89 \cdot 45 = 4096 \Leftrightarrow$$

$$\Leftrightarrow 4096 \geq 4096 \Leftrightarrow$$

$\Rightarrow$  Dc. (3) would transform sing. Homming in egd. tet.

$\Rightarrow$  ac. (7) este perfect

Coolul este binor

$\Rightarrow$  cool Golay and Hamming)

Gol(23), da 23 ≠ 90

$d=5 \Rightarrow$  nu este wod Hamming pt. ca  $d \neq 3$

$\Rightarrow (\mathbb{Z})$  cool binor

⇒ Curs 5 - 23.03.2023

⇒ context (partiel)

A grup abelian

$$\chi : A \rightarrow \mathbb{C}^*, \quad \chi(a+b) = \chi(a) + \chi(b)$$

Caracter de sup

$\chi = 1$  caracter trivial

$\chi$  vector  $\Rightarrow \bar{\chi}$  caracter

$$|\chi(a)| = 1$$

$$\chi(-a) = \frac{1}{\chi(a)} = \bar{\chi}(a)$$

$ch(A)$  - grupul caracterelor  $\cong A$

$$K = \mathbb{F}_2, \quad F = \mathbb{F}_p = \{0, 1, \dots, p-1\}$$

$\epsilon \in \mathbb{C}, \mu \Rightarrow$  rotația complexă a unității

$\mathbb{W}$  - sp. finit dim. peste  $K$

$$\mathbb{W}^* = \text{Hom}_K(\mathbb{W}, K)$$

$$ch(\mathbb{W}) = \{ \chi_f \mid f \in \mathbb{W}^* \}$$

$$\boxed{\chi_f(v) = \sum_{x \in K/F} f(x) \bar{g}(x)}$$

A multime finita,  $\mathbb{C}^A = \{f : A \rightarrow \mathbb{C}\}$

$$\langle f, g \rangle = \frac{1}{|A|} \sum_{x \in A} f(x) \bar{g}(x)$$

A grup abelian

$\chi, \psi$  caractere ale lui  $A$

$ch(A)$  baza ortonormala pt.  $\mathbb{C}^A$

$$\langle \chi, \psi \rangle = \begin{cases} 1, & \text{d.c. } \chi = \psi \\ 0, & \text{altele} \end{cases}$$

→ ⑦ lui McWilliams

Ei  $C$  cod de lungime  $n$

$$A_i = |\{w \in C \mid \text{wt}(w) = i\}| \in \mathbb{N}$$

$$A_C = \sum_{i=0}^n A_i z^i \in \mathbb{Z}[z] \quad \text{polinom cu coef. naturali}$$

polinomul ponderilor weight polynomial

(T) Fie  $C$  cu  $n$  coloane,  $C \subseteq K^n$  ord. peste  $K$ ,  $|C| = 2^k$ ,  $C$  complement ortogonal.  
 $\Leftrightarrow A(z) \in A^\perp(z)$

$$A^\perp(z) = 2^{-k} \cdot (1 + (2^{-1})z)^n A\left(\frac{1-z}{1+(2^{-1})z}\right) \quad \text{if } \omega \in \mathbb{Z}$$

demonstrare:

Fie  $c$  vector nematicial al grupului  $(K, +, \cdot)$

$$\text{pt. } u \in K^n, \quad g_c(z) = \sum_{v \in K^n} \chi(\langle c, v \rangle) z^{\text{wt}(v)} \in \mathbb{Q}[z]$$

$$\begin{aligned} \sum_{c \in C} g_c(z) &= \sum_{c \in C} \sum_{v \in K^n} \chi(\langle c, v \rangle) z^{\text{wt}(v)} = \\ &= \sum_{v \in K^n} f(v) z^{\text{wt}(v)} \quad \text{unde} \quad f(v) = \sum_{c \in C} \chi(\langle c, v \rangle) \end{aligned}$$

$c \rightsquigarrow \chi(\langle c, v \rangle)$  vector  $\chi_v$  al lui  $C$

$\chi_c$  este trivial  $\Leftrightarrow v \in C^\perp$

$$f(v) = \sum_{c \in C} \chi(\langle c, v \rangle) = |C| \langle \chi_v, \chi_C \rangle = \begin{cases} |C|, & \text{d.e. } v \in C^\perp \\ 0, & \text{d.e. } v \notin C^\perp \end{cases}$$

$$\sum_{c \in C} g_c(z) = \underbrace{\sum_{c \in C^\perp} |C|}_{\text{pt. fiecare element din } C^\perp} z^{\text{wt}(c^\perp)} = |C| A^\perp(z) \quad (1)$$

pt. fiecare element din  $C^\perp$   $\rightarrow$  polinomul def. anterior  $A$   
 în adună  $z^{\text{wt}(c^\perp)}$  (produselement)

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

$$\begin{aligned} g_c(z) &= \sum_{v \in K^n} z^{\text{wt}(v)} \chi(\langle c, v \rangle) = \\ &= \sum_{a_1, \dots, a_n \in K} z^{\sum_{i=1}^n \text{wt}(a_i)} \chi\left(\sum_{i=1}^n c_i a_i\right) = \end{aligned}$$

"pondere unui element", d.c.  $i=1 \Rightarrow \text{wt} = 1$ ,  $i=0 \Rightarrow \text{wt} = 0$

$$= \sum_{(a_1, \dots, a_n) \in K^n} \prod_{i=1}^n z^{\sum_{j=1}^m \text{wt}(a_{ij})} \chi(c_i a_{ij}) =$$

$$= \prod_{i=1}^n \sum_{\alpha_i \in K^*} z^{wt(\alpha_i)} \chi(c_i \alpha_i)$$

$$\chi \neq 1 \Rightarrow \sum_{\alpha \in K^*} \chi(\alpha) = -1$$

~~de ce?~~

$$\prod_{\alpha \in \text{prim}(p)} (\alpha^{-1})! \equiv -1 \pmod{p}$$

$K^*$  grup com, de  $\# = p$

de  $\# = p^k \rightarrow -1$  e singurul el. de ad. p dim grup

~~✓~~

$$\sum_{\alpha_i \in K} z^{wt(\alpha_i)} \chi(c_i \alpha_i) = \begin{cases} \sum_{\alpha_i \in K} z^{wt(\alpha_i)} = 1 + (\varphi - 1)z, & \text{de } c_i = 0 \\ 1 + z \sum_{\alpha \in K^*} \chi(\alpha) = 1 - z, & \text{de } c_i \neq 0 \end{cases}$$

$$\Rightarrow g_C(z) = \underbrace{(1-z)^{wt(C)}}_{\textcircled{2}} \underbrace{\left(1 + (\varphi - 1)z\right)^{n-wt(C)}}_{\textcircled{1}}$$

$$\Rightarrow A^L(z) = |C|^{-1} \underbrace{\sum_{c \in C} g_c(z)}_{\dim(C)} = \varphi^{-k} \left(1 + (\varphi - 1)z\right)^n \sum_{c \in C} \left(\frac{1}{1 + (\varphi - 1)z}\right)^{wt(c)} = \\ = \varphi^{-k} \left(1 + (\varphi - 1)z\right)^n A\left(\frac{1-z}{1 + (\varphi - 1)z}\right) \quad \square$$

↳ Exemple

$$\hookrightarrow \text{Sim}_2(k) : A(z) = 1 \cdot z^0 + (\varphi - 1) z^2^{k-1}$$

// codul simplex

→ Exercițiu

(1) pag. 25: - compute the wt pol of  $\text{Hom}_{K-1}$ .

$$\text{Pt. } \mathbb{F}_2, \text{ simplex: } A(x) = 1 + (2^{k-1})x^2$$

$\text{Sim}_2(k)$

$$\text{Hom}_2(K) [2^{k-1}, n-k, 3]$$

$$A^{-1} = \frac{1}{2^k} \left[ (1+x)^m + m(1-x)^{2^{k-1}} (1+x)^{2^{k-1}-1} \right] =$$

$$= \frac{1}{m+1} \left[ (1+x)^m + m(1-x)(1-x^2)^{\frac{m-1}{2}} \right] \Rightarrow$$

$$\Rightarrow A_i^{-1} = \begin{cases} \frac{1}{m+1} \left[ \binom{m}{i} + m(-1)^{\frac{i}{2}} \binom{\frac{m-1}{2}}{\frac{i}{2}} \right] & \text{de } i=2j \\ \frac{1}{m+1} \left[ \binom{m}{i} + m(-1)^{\frac{i+1}{2}} \binom{\frac{m-1}{2}}{\frac{i-1}{2}} \right] & \text{de } i=2j+1 \end{cases}$$

Ex 11

② Fie  $m \geq 1$  și  $C = \{(a_1, \dots, a_m) \in \mathbb{F}_2^m \mid \text{wt}(a_1, \dots, a_m) = 2\}$ , se arată

dem. că  $C$  este liniar și nu generată parțial.

Vector primul din  $C$ , final are 2 poz. de 1

$$\begin{aligned} \text{wt}(v_1) = k_1, \quad \text{nr. poz.} \\ \text{wt}(v_2) = k_2, \quad \text{nr. poz.} \\ s = \text{nr. de 1 suprapuse} \end{aligned} \quad \Rightarrow \begin{aligned} \text{wt}(v_1 + v_2) = (k_1 - s) + (k_2 - s) = \\ = \frac{k_1}{2} + \frac{k_2}{2} - \frac{2s}{2} \xrightarrow[s=2]{C \in \mathbb{F}_2} \end{aligned}$$

$\Rightarrow C$  este liniar (sp)

d.e.  $v = (c_1, \dots, c_m) \in C \Leftrightarrow c_1 + c_2 + \dots + c_m = 0$

$H = (1, 1, \dots, 1)$  // matrice de control

$$(1, 1, \dots, 1) \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix} = 0$$

$d(C) = 2$

Por.  $[n, m-1, 2] \Rightarrow |C| = 2^{m-1} = \text{card sp} \dim \text{sp}$   
m. vectori de  $\text{wt} \geq 2$

Matrice generatoare

element general // contam  $G: \mathbb{F}_2^{m-1} \rightarrow \mathbb{F}_2^n$  îng. liniară,  $C = G(\mathbb{F}_2^{m-1})$

$$\underbrace{(x_1, \dots, x_{m-1})}_{\text{nr. impre}}, x_1 + x_2 + \dots + x_{m-1} = G(x_1, \dots, x_{m-1})$$

$$\begin{array}{l} \text{nr. impre} \Rightarrow \begin{array}{c} 1 \\ \vdots \\ 1 \end{array} \\ \text{nr. poz.} \Rightarrow \begin{array}{c} 1 \\ \vdots \\ 0 \end{array} \end{array}$$

$$\Rightarrow G = \left( \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix} \begin{matrix} 1 \\ \vdots \\ 1 \end{matrix} \right) \text{ are } n \text{ col. și } m-1 \text{ linii}$$

$$(x_1, \dots, x_m) = (x_1, \dots, x_{m-1}) G$$

Ex 12

$$\textcircled{3} C = C_2 = \{(0, \dots, 0), (1, \dots, 1)\} \quad // \text{este } \mathbb{F}_2^n, \text{ de lg } n$$

a) Tăză ne parțială par,

b) Matricea de control  $A'$

c) Matricea generatoare

$$a) [n, d, m], \text{ cond: } 2^{\dim} \rightarrow |C| = 2^{\frac{1}{d}}$$

$$c) G = (1, 1, \dots, 1) \quad // G: \{0,1\} \rightarrow \{0,1\}, G(x) = x \cdot G, G(x) \text{ aplică la mult. gen. } G$$

d) Sist. de ec. pe care îl verifică  $C$

$$\left\{ \begin{array}{l} x_1 = x_m \\ x_2 = x_m \\ \vdots \\ x_{m-1} = x_m \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} x_1 + x_m = 0 \\ x_2 + x_m = 0 \\ \vdots \\ x_{m-1} + x_m = 0 \end{array} \right. \Rightarrow H = \begin{pmatrix} 1 & & & & \\ 1 & 0 & & & \\ \vdots & & 1 & & \\ 0 & & & 1 & \\ & & & & 1 \end{pmatrix} \Rightarrow C_2 = C_1^\perp$$

/\* Se poate aplica (7) lui McW pt. polinom \*/

(4)

$$Ex 19 \quad \text{Ie } U_n \in M_{2^n \times 2^n}(\mathbb{F}_2), \quad U_n = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & 1 & \dots & 1 \end{pmatrix}$$

Def. un sir de matrice

$$H_0 = (0) \in M_{2^0 \times 2^0}(\mathbb{F}_2)$$

$$H_{m+1} = \begin{pmatrix} H_m & H_m \\ H_m & H_m + U_m \end{pmatrix} \in M_{2^{m+1} \times 2^{m+1}}(\mathbb{F}_2)$$

Adem. că limili lui  $H_m = RM(1, m) \neq R_m \Leftrightarrow R_m \text{ nu verifica } \frac{L_1}{L_2} + \frac{L_2}{L_1} = L_1$

$$H_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\mathbb{F}_2 = \left( \begin{array}{|c|c|} \hline 0 & 0 \\ \hline 0 & 1 \\ \hline \hline 0 & 0 \\ \hline 0 & 1 \\ \hline \end{array} \right) \left( \begin{array}{|c|c|} \hline 0 & 0 \\ \hline 0 & 1 \\ \hline \hline 1 & 1 \\ \hline 1 & 0 \\ \hline \end{array} \right) \rightarrow H_1 + U_1$$

Inductie n > m+1 ;  $H_{m+1}$ , linie

$$\text{Caz I : } (x, z) + (y, y) = (x+y, z+y)$$

unde  $x, y$  linii în  $H_{m+1}$  și  $(x+y)(z+y)$  este linie  
din jumătatea I a lui  $H_m$

$$\text{Caz II : } (\vec{x}, \vec{z}) + (\vec{y}, \vec{z} - \vec{y}) = (x+y, z+y)$$

unde  $(x+y)(z+y)$  este linie din jumătatea I a lui  $H_m$   
să  $x, y$  idem ca în caz I

$$\text{Caz III : } (x, z) + (y, z+y) = (x+y, z+y+z)$$

unde  $x, y$  idem ca în caz I și  $(x+y, z+y+z)$  linie din a doua  
jumătate a lui  $H_m$

$\forall o \in H_m$  linie,  $v$  conține un nr. egal de 0 și de 1  $\Leftrightarrow$

$$\Leftrightarrow \text{Sum}_2(n) \Rightarrow \log_2^{n-1}, \dim = n \text{ și } d = 2^{n-1}$$

## → Curs 6 - 30.03.2023 // Quantum comp

↪ Pb. de decizie: Te dă  $n$ , este prim  $\rightarrow \dim 2003 \rightarrow$  mulțimea în timp poli. în lungimea  $(n)$   
alg lui Aronson

PRIME  $\in NP \Leftrightarrow \frac{\text{COMPOSITE} \in NP}{\downarrow}$

un nr. e compus sau nu

→ la RSA:  $d \in \mathbb{Z}^{\times \text{mod}(p-1)(q-1)}$  unde  $N = p \cdot q$ ,  $\lambda$  public,  $p, q$  private

→ Alg. lui Shor

În quantum comp., factorarea este posibilă cu complex. polinomial.

→ NIST: National Institute of Standards & Technology // la concursuri

↪ DES (Horst Feistel + coau.)  $\rightarrow$  criptare bloc 64b

→ AES (Rijmen, Daemen)  $\rightarrow$  criptare bloc 128b

→ turneu 2020 "post quantum security"  $\rightarrow$  încă nu a fost numit un câștigător // cripto. lotică

→ quantum computer

↪ paralel  $\rightarrow$  lent,  $\geq \rightarrow$  liberul arbitru

? determinism

$$\rightarrow \text{def} \quad (\exists) \psi: \mathbb{R}^3 \rightarrow \mathcal{C} \rightarrow \text{probabil. A sa e sa se afle in acel spatiu este} \\ \int_A |\psi(x)|^2 dx \Rightarrow \int_{\substack{\mathbb{R}^3 \\ \text{univers}}} |\psi(x)|^2 dx = 1$$

$\rightarrow$  def:

Sistem probabilistic = multime finita de stari  $x_1, \dots, x_n$  unde  
 $p_i$  = probabilitatea ce sa se afle in starea  $x_i$

Distributia de prob.:

$$p_1[x_1] + p_2[x_2] + \dots + p_n[x_n] \quad \text{cu} \quad p_i \geq 0 \quad \text{si} \quad \sum_{i=1}^n p_i = 1$$

$\rightarrow$   $\Sigma$  cel mai simplu de vis. prob.

moneda  $\rightarrow$  head, tail

$$\text{prob. } \frac{1}{2} h + \frac{1}{2} t$$

$\rightarrow$  Markov  $\rightarrow$  context

Fie  $p_{ij}$  prob. ce sa se traga din  $x_i$  in  $x_j \rightarrow$

$$T_0: \underbrace{x_i}_{\text{stare } x_i} \rightarrow p_{i1}[x_1] + p_{i2}[x_2] + \dots + p_{in}[x_n], \quad p_{ij} \geq 0 \quad \text{si} \quad \sum_{j=1}^n p_{ij} = 1$$

$$\text{la mom. } T_1: p_1(p_{11}[x_1] + p_{12}[x_2] + \dots + p_{1n}[x_n]) + \\ + p_2(p_{21}[x_1] + p_{22}[x_2] + \dots + p_{2n}[x_n]) + \dots$$

$$\Rightarrow \begin{pmatrix} p_1' \\ p_2' \\ \vdots \\ p_n' \end{pmatrix} = \begin{pmatrix} p_{11} & p_{12} & \dots & p_{1n} \\ p_{21} & p_{22} & \dots & p_{2n} \\ \vdots & & & \\ p_{n1} & p_{n2} & \dots & p_{nn} \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{pmatrix} \rightarrow \text{matricea Markov sau stocastica}$$

Nd.  $A \Rightarrow$  d.st.  $\vec{p}$

$\hookrightarrow$  Prop. mat. Markov:  $p_{ij} \geq 0$  si suma pe linie = 1

la mom  $T_2$ : dist. =  $A \vec{p}$

la mom  $T_3$ : dist. =  $A^2 \vec{p}$

$\rightarrow$  Not:

Lantul  $\vec{p}, A\vec{p}, A^2\vec{p}, \dots, A^n$  lant Markov

$\rightarrow$  def: Sistem cuantic

Multime finita de stari  $x_1, x_2, \dots, x_n$  formol, generata sp. Hilbert  $H_n = \mathbb{C}^n$

Fiecărui st. i se poate crea un el. d'unei baze ortonormale  $\{|x_1\rangle, |x_2\rangle, \dots, |x_n\rangle\}$

$\Rightarrow$  Def.:

$$\begin{aligned} |\alpha\rangle \text{ ket } & \Rightarrow \langle \alpha| \text{ bra } \text{ sau } \underline{\text{produs hermitian}} \\ \langle \alpha| \text{ bra } & \quad \langle \alpha| b_i \rangle = \sum_{i=1}^n \alpha_i \overline{b_i} \text{ unde } \overline{x+iy} = x - iy \\ & \quad \downarrow \quad \uparrow \quad \in \mathbb{C} \quad \rightarrow \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} \\ & \quad (0_1, 0_2, \dots, 0_n) \end{aligned}$$

$$\langle \alpha | \quad |b_i\rangle$$

$\Rightarrow$  def.:

O stare a oist. quantice este de forma  $\alpha_1|x_1\rangle + \alpha_2|x_2\rangle + \dots + \alpha_n|x_n\rangle$  unde  $\alpha_i \in \mathbb{C}$  și vector unitar

$$\begin{aligned} \text{i.e. } |\alpha_1|^2 + |\alpha_2|^2 + \dots + |\alpha_n|^2 &= 1 \text{ unde} \\ |\alpha = xy|^2 &= x^2 + y^2; x, y \in \mathbb{R} \end{aligned}$$

Starea = "superpozitie" a stărilor de baza

Prol. stăru  $|x_i\rangle$  este  $|\alpha_i|^2$

$\Psi(x_i) = \alpha_i \rightarrow$  funcție de undă,  $p = |\Psi(x_i)|^2$

Ac. o stare  $|\alpha\rangle = e^{i\theta}|y\rangle \Rightarrow |x\rangle \text{ și } |y\rangle$  sunt echivalente

$\Rightarrow$  CX:

bit = nr. macroscopic cu 2 stări

qubit = nr. cuantic cu 2 stări

stare a unui qubit:  $\alpha_0|0\rangle + \alpha_1|1\rangle$  unde  $\alpha_0, \alpha_1 \in \mathbb{C}$  s.t.

$$|\alpha_0|^2 + |\alpha_1|^2 = 1 \quad \begin{array}{l} \text{// puterea continuu} \\ \text{// norma euclidiană} = 1 \end{array}$$

Evoluția unui nr. cuantic este date de matr. de tranziție:

$$A = \begin{pmatrix} \alpha_1' \\ \alpha_2' \\ \vdots \\ \alpha_n' \end{pmatrix} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix}$$

$$A^* = \bar{A}^T \text{ conjugat în timp} \Rightarrow \boxed{A^* = A^{-1}} \quad \begin{array}{l} \text{// op. unitar} \\ \text{// adjoint al lui } A \end{array}$$

// package C# VS code:  $\mathcal{Q}$

$\rightarrow$  Ulls:

Un circuit boolean  $\rightarrow$  se transformă în circuit boolean reversibil  $\Rightarrow$  circuit quantum  
Dsp. cuantice reversibile  $\Rightarrow$  procese reversibile

$\rightarrow$  Ct.: Dăm cu banul cuantic

Fie b. op. liniară,  $|h\rangle, |t\rangle$  e.i.

$$|h\rangle = \frac{1}{\sqrt{2}}|h\rangle + \frac{1}{\sqrt{2}}|t\rangle$$

$$|t\rangle = \frac{1}{\sqrt{2}}|h\rangle - \frac{1}{\sqrt{2}}|t\rangle$$

$$|\alpha_{\pm}\rangle^2 = \left(\frac{1}{\sqrt{2}}\right)^2 \pm 0 = \frac{1}{2}$$

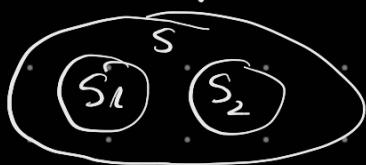
Apli.  $A = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$  cu  $A^T = A$ , dar  $AA = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$  (ident. lini.)  $\Rightarrow$

$$\Rightarrow A^T = A = A^{-1} \Rightarrow A \text{ op. unitar}$$

Fct. s.n. Hadamard Walsh

$\rightarrow$  Ct.:

Fie 2 s.n. cuantice și unul dintre ele are stari cuantice fundamentale  $|\alpha_1\rangle, \dots, |\alpha_n\rangle$   
iar celălalt  $|\gamma_1\rangle, \dots, |\gamma_m\rangle$



$\Rightarrow$  stările fundamentale după reunirene  $(|\alpha_i\rangle, |\gamma_j\rangle) = |\alpha_i \gamma_j\rangle \Rightarrow$

$\Rightarrow H_m \otimes H_m$

produs tensorial de dim.  $m \times m$

$\Rightarrow |\alpha_i\rangle \otimes |\gamma_j\rangle \text{ s.m. } |\alpha_i \gamma_j\rangle \Rightarrow$

$$\Rightarrow \sum_{i=1}^m \alpha_{ij} |\alpha_i \gamma_j\rangle = \left( \sum_{i=1}^m \alpha_i |\alpha_i\rangle \right) \left( \sum_{j=1}^m \gamma_j |\gamma_j\rangle \right)$$

$\rightarrow$  Ulls:

$S_1, S_2$  sunt inolup.  $\Leftrightarrow$  sistemul numit S este produsul superpoz. celor 2 sisteme vizibile separat

$\rightarrow \text{Ex}$

Stare 2 qubits  $Q_1, Q_2$  și  $Q_1 \cup Q_2 = \frac{1}{2} (|100\rangle + |111\rangle + |101\rangle + |110\rangle)$

d.e.s.

$\sum_{\substack{i=1, m \\ j=1, m}} x_{ij} |x_i y_j\rangle = \left( \sum_{i=1}^m x_i |x_i\rangle \right) \left( \sum_{j=1}^m y_j |y_j\rangle \right)$  s.m. stare decompozabilă, iar regele  
este entangled

este stare indecompozabilă

Afirmatie: stare  $Q_1 \cup Q_2$  este decompozabilă

$$Q_1 \cup Q_2 = \underbrace{\frac{1}{\sqrt{2}} (|10\rangle + |11\rangle)}_{\text{f.c. acelor lucru în mod îndep.}} \underbrace{\frac{1}{\sqrt{2}} (|10\rangle + |11\rangle)}_{\text{stările sunt depend.}}$$

f.c. acelor lucru în mod îndep.,  
stările sunt depend.

$\rightarrow \text{Ex: Einstein, Rosen, Podolski "trebuie pe loc anterior"$

$$\rightarrow \frac{1}{\sqrt{2}} (|100\rangle + |111\rangle) \text{ nu stare EPR}$$

// superpos. legată  $\Rightarrow$  sume pot. coef. = 1

// în c.c. acesta, coef. sunt  $\frac{1}{\sqrt{2}}, 10, 0, \frac{1}{\sqrt{2}} \Rightarrow$  suma pot. = 1  $\Rightarrow$

//  $\Rightarrow$  stare EPR este stare legată  
entanglement (!)

$\rightarrow$  exercițiu

① Dem că stare EPR nu este decompozabilă

$$P_E \text{ c.e. } \frac{1}{\sqrt{2}} (|100\rangle + |111\rangle) = (\alpha|10\rangle + \beta|11\rangle)(\delta|10\rangle + \gamma|11\rangle)$$

$$= \alpha\delta|100\rangle + \alpha\gamma|101\rangle + \beta\delta|110\rangle + \beta\gamma|111\rangle$$

$$\alpha, \beta, \delta, \gamma \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = |\delta|^2 + |\gamma|^2 = 1$$

$$\Rightarrow \begin{cases} \alpha\delta = \frac{1}{\sqrt{2}} \\ \alpha\gamma = 0 \\ \beta\delta = 0 \\ \beta\gamma = \frac{1}{\sqrt{2}} \end{cases} \Rightarrow (\alpha=0 \vee \delta=0) \wedge (\beta=0 \vee \gamma=0) \wedge \alpha\neq 0, \beta\neq 0 \text{ nu este soluția în } \mathbb{C} \Rightarrow \text{contradicție}$$

\* back to Teoria Codicilor  $\rightarrow$  exercitiu

\* Recap McWilliams:

$$* \text{ Pol. pendular } A^\perp(z) = 2^{-k} \sum_{m=0}^k (1 + (2-1)z)^m A\left(\frac{1-z}{1+(2-1)z}\right)$$

\* (2) Fie codul  $C = \{(0, \dots, 0), (1, \dots, 1)\} \subseteq \mathbb{F}_2^n$ , iar codul complementar sunt

\* vectorii cu m-poz de 1, adica  $C^\perp = \{\vec{v} \in \mathbb{F}_2^n \mid \text{wt}(\vec{v}) \in 2\mathbb{N}\}$

\*  $A(z) = z^n + 1 \parallel \text{m. de inv. } z$

$$* A^\perp(z) = 2^{-1} ((1+z)^n \cdot \left(1 + \left(\frac{1-z}{1+(2-1)z}\right)^n\right))$$

$$* = \frac{1}{2} \left( (1+z)^n \left(1 + \left(\frac{1-z}{1+z}\right)^n\right) \right) =$$

$$* = \frac{1}{2} \left[ (1+z)^n + (1-z)^n \right] =$$

$$* = \frac{1}{2} (1+z)^n + \frac{1}{2} (1-z)^n =$$

$$* = \frac{1}{2} \sum_{k=0}^n \binom{n}{k} z^k + \frac{1}{2} \sum_{k=0}^n \binom{n}{k} (-1)^k z^k =$$

$$* = \frac{1}{2} \sum_{i \geq 0} \binom{n}{2i} z^{2i} =$$

$$* = \sum_{i \geq 0} \binom{n}{2i} z^{2i}$$

\*  $\Rightarrow$  în codul complementar apoi doar toate comb. wt-pare

\* Expt. (2):

\* (3) Fie  $C = \{(0, 0, 0, 0), (1, 1, 1, 1), (2, 2, 2, 2)\} \subseteq \mathbb{F}_3^4 \Rightarrow$

$$* \Rightarrow A(z) = 1 + 2 \cdot z^4$$

\* Codul complementar?

$$* A^\perp(z) = \frac{1}{3} \cdot (1+2z)^4 \left[ 1 + 2 \left( \frac{1-z}{1+2z} \right)^4 \right] =$$

$$* = \frac{1}{3} \left[ (1+2z)^4 + 2 \cdot (1-z)^4 \right] =$$

$$* = \frac{1}{3} \left[ 1 + 8z + 24z^2 + 32z^3 + 16z^4 + 2 - 8z + (2z^2 - 8z^3 + 2z^4) \right] =$$

\* Imagine: triunghiul lui Pascal.

$$* \begin{array}{c} 1 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 3 & 3 & 1 \end{array} \quad \left| \begin{array}{l} 1 \\ 2 \\ 3 \end{array} \right. \text{ pt. a calcula } (a+b)^n$$

$$\begin{array}{cccc|c} \times & 1 & 4 & 6 & 4 & 1 | 4 \\ \times & & \times & & & \\ \times & & & & & \end{array}$$

$$= \frac{1}{3} (3 + 36z^2 + 24z^3 + 18z^4) =$$

$$= 1 + 12z^2 + 8z^3 + 6z^4$$

$\rightarrow$  McWilliams spune că hiperplanul din  $F_3$  perpendicular pe oblică susțineaza ore 1 vector de pondere 0  
 12 vectori de wt 2  
 8 vectori de wt 3  
 6 vectori de wt 4 }  $\rightarrow$  27 de vectori = cardinalitatea  
 putere a lui  $\frac{3}{7}$   
 $F_3$

$\rightarrow$  McWilliams își poate să nu le excludă

## II. Back to quantum

(4) Te mat. stocastică pt. aruncări cu moneda corectă

$$M = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} \Rightarrow M^2 = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} = M \Rightarrow M^n = M, \forall n$$

nu există efect cumulativ

(5) (4) dor cu moneda incorectă  $\Rightarrow$

$$M = \begin{pmatrix} 1-\epsilon & \epsilon \\ 1-\epsilon & \epsilon \end{pmatrix} \text{ cu } \epsilon \in (0, \frac{1}{2})$$

$$M^2 = \begin{pmatrix} 1-\epsilon & \epsilon \\ 1-\epsilon & \epsilon \end{pmatrix} = M, \forall n$$

nu există efect cumulativ

⑥ Fin M mot stocstrik

$$M = \begin{pmatrix} 1-\epsilon & \epsilon \\ \epsilon & 1-\epsilon \end{pmatrix}; \epsilon \neq \frac{1}{2}, M^2 = M$$

$$\lim_{n \rightarrow \infty} M^n = ?$$

det(1-x-M) ic. karakteristisk

$$(x-1+\epsilon)^2 - \epsilon^2 = 0$$

$$(x-1+2\epsilon)(x-1) = 0$$

$$\lambda_1 = 1, \lambda_2 = 1-2\epsilon$$

$$\begin{pmatrix} 1-\epsilon & \epsilon \\ \epsilon & 1-\epsilon \end{pmatrix} \begin{pmatrix} e \\ u \end{pmatrix} = \begin{pmatrix} 0 \\ u \end{pmatrix} \Rightarrow \begin{pmatrix} e \\ u \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} 1-\epsilon & \epsilon \\ \epsilon & 1-\epsilon \end{pmatrix} \begin{pmatrix} e \\ u \end{pmatrix} = (1-2\epsilon) \begin{pmatrix} e \\ u \end{pmatrix} \Rightarrow \begin{pmatrix} e \\ u \end{pmatrix} = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$\Rightarrow W_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \Rightarrow W_2^{-1} = W_2 \Rightarrow M = W_2 \cdot D \cdot W_2 \text{ under Handermed}$$

Wally

$$D = \text{mot. diagonal a val. prop.} = \begin{pmatrix} 1 & 0 \\ 0 & 1-2\epsilon \end{pmatrix} \Rightarrow$$

$$\Rightarrow M^n = W_2 \cdot D^n \cdot W_2$$

$$\text{dvs. } n \rightarrow \infty \Rightarrow D^n \rightsquigarrow \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \Rightarrow M^n \rightsquigarrow \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

→ Tars 7 - 13.04.2023

↪ Caractere de grup

$(G, +, \circ)$  grup abelian.

caractere:  $\chi : (G, +, \circ) \rightarrow (\mathbb{C}^*, \cdot, 1)$  mărfură

$\chi(\circ) = 1$ .

$|G| = n \Rightarrow \chi(g) \cdot \chi(n \cdot g) = \chi(\circ) = 1 \Rightarrow \chi(g)$  red. a lui 1

$\chi_{1,2}$  caractere  $\rightarrow \chi_1, \chi_2$  caracte

$\widehat{G}$  gr. caractereburi lui  $G$ , în acest sens

$\widehat{\mathbb{Z}_n}$ ;  $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$

$y \in \mathbb{Z}_n$ ,  $\chi_y(x) = e^{\frac{2\pi i xy}{n}}$  caracter al lui  $x$

$\chi_g = \chi_{g+2} \Leftrightarrow g \equiv 2 \pmod{n}$ ;  $\widehat{\mathbb{Z}_n} = \{\chi_x \mid x \in \mathbb{Z}_n\} \cong \mathbb{Z}_n$

(T) Dacă  $G$  gr. abelian finit  $\Rightarrow G$  izomorf cu  $\widehat{G}$  ( $G \cong \widehat{G}$ )

Demis.

Dacă  $G$  gr. ab. finit  $\Rightarrow G$  izomorf cu prod. de gr. ciclice  $\Rightarrow G \cong G_1 \times G_2 \times \dots \times G_m$ ;  $G_i \cong G_i$  și ca  $G_i$  ciclic cu  $j < 1, m$   
 $G \cong G_1 \oplus G_2 \oplus \dots \oplus G_m$ .

\* dif. produs direct VS suma directă \*

// sunt în ceea ce finit

$\forall g \in G$ ,  $g = g_1 + g_2 + \dots + g_m$

în  $\widehat{G}$ ;  $\chi_i \in \widehat{G}_i$  (cor. al lui  $G_i$ ) astfel:  $\chi(g) = \chi_1(g_1) \cdot \dots \cdot \chi_m(g_m)$   
caracter, unic det

□

Ex.: caracterele lui  $\widehat{\mathbb{Z}}_2^n$

$\widehat{\mathbb{Z}}_2^n$ :  $\chi_y(x) = e^{\frac{2\pi i xy}{n}} = (-1)^{xy}$

$\boxed{e^{\frac{\pi i x}{2}}} \text{ Lema lui Euler}$

$$F_2^m : \chi_{\vec{g}}(\vec{x}) = (-1)^{x_1 g_1 + \dots + x_m g_m} = \underbrace{(-1)^{\vec{x} \cdot \vec{g}}}_{\text{prod vector (cont. door paritie)}}$$

$\Rightarrow$  def:

Fie  $G$  gr. al fint;  $G = \{g_1, \dots, g_m\}$

$\mathbb{V} = \{f: G \rightarrow \mathbb{C}\}$  de dimensiune  $= m$   
 sp. vct. vector de lg-n formăt din nr. complexe  
 parte  $\mathbb{C}$

$\ell_i := "e_i(g_i) - \delta_{i,j}" = \begin{cases} 1, & i=j \\ 0, & \text{altfel} \end{cases}$  // baza canonica a lui  $\mathbb{V}$

produsul scalar

$\langle f | h \rangle = \sum_{i=1}^m f^*(g_i) h(g_i)$  // produs Hermitian

$$\|f\| = \sqrt{\langle f | f \rangle}$$

$\Rightarrow$  clu:  $\hat{G} \subseteq \mathbb{V}$

$\Rightarrow$  Th. de Ortogonalitate a coroantei

$$\langle \chi_i | \chi_j \rangle = \begin{cases} 0, & \text{de } i \neq j \\ m, & \text{de } i = j \end{cases}$$

Dem

$$1 = |\chi_{(g)}|^2 \Rightarrow \chi^*(g) = \chi(g)^{-1} \text{ în } \mathbb{C}$$

$$\langle \chi_i | \chi_j \rangle = \sum_{k=1}^m \chi_i^*(g_k) \chi_j(g_k) = \sum_{k=1}^m \chi_i^{-1}(g_k) \chi_j(g_k) = \sum_{k=1}^m (\chi_i^{-1} \chi_j)(g_k)$$

// coroantă trivial?

$$\text{Dc. } i = j \Rightarrow \chi_j^{-1} \chi_i = 1 \text{ cor trivial} \Rightarrow \sum_{k=1}^m (\chi_i^{-1} \chi_j)(g_k) = m$$

$$\text{Dc. } i \neq j \Rightarrow \chi_j^{-1} \chi_i = \chi \text{ cor. netrivial} \Rightarrow (\exists) g \text{ cu } \chi(g) \neq 1$$

Fie  $S = \sum_{k=1}^m \chi(g_k)$  și observăm că  $g_k \leftrightarrow g_k + g$  permutează  $G$

$$\Rightarrow S = \sum_{k=1}^m \chi(g + g_k) = \sum_{k=1}^m \chi(g) \sum_{k=1}^m \chi(g_k) = \chi(g) \cdot S$$

$$\text{Dor. } \chi(g) \neq 1 \text{ și } S = \chi(g)S \Rightarrow S = 0$$

$\Rightarrow$  Corolar

Fct.  $B_n = \frac{1}{\sqrt{n}} \sum_{i=1}^n \chi_i$  formează o bază ortogonală a lui  $\mathbb{V}$

→ Concluzie

cond.  
daca  
de

Fix mod.  $X \in \mathbb{C}^{n \times n}$  cu el. gen.  $X = X_j(g_i) \Rightarrow X^{-1} = \frac{1}{n} X^*$  unde  $X^* = \overline{X^T}$   
 $\frac{1}{\sqrt{n}} X$  este mat. unitara  
 $\Rightarrow X$  poate fi diagonalizat. unde se descompune

→ Transformarea Fourier discretă

Oare set.  $f \in \mathbb{W}$  are o unică reprez. în baza  $B$  carep. lui  $G$   
baza orthonormală  $\frac{1}{\sqrt{n}} K_g$

$$f = \hat{f}_1 B_1 + \dots + \hat{f}_m B_m \text{ unde } \hat{f}_i \in \mathbb{C}$$

↪ def.

Fix  $\hat{f}: G \rightarrow \mathbb{C}$  :  $\hat{f} \in \mathbb{W}$  data de  $\hat{f}(g_i) = \hat{f}_i$ ,  $\hat{f}$  s.m. transformarea Fourier asociată a lui  $f$

↪ ile

$$(1) \langle B_i | f \rangle = \hat{f}_i$$

$$(2) \hat{f}(g_i) = \langle B_i | f \rangle = \frac{1}{\sqrt{n}} \sum_{k=1}^n X_i^*(g_k) f(g_k)$$

→ Ex  $f: \mathbb{Z}_n \rightarrow \mathbb{C}$

$$\hat{f}(x) = \frac{1}{\sqrt{n}} \sum_{y \in \mathbb{Z}_n} e^{\frac{2\pi i x y}{n}} f(y) \quad \text{trans. Fourier a lui } f$$

$\star \rightarrow$  conjugat

→ Ex  $f: \mathbb{F}_2^m \rightarrow \mathbb{C}$

$$\hat{f}(\vec{x}) = \frac{1}{\sqrt{2^m}} \sum_{y \in \mathbb{F}_2^m} (-1)^{\vec{x} \cdot \vec{y}} f(\vec{y})$$

↓

transformata Hadamard-Walsh

$$w_2 \otimes w_2 \otimes \dots \otimes w_2 = \sum_{y \in \mathbb{F}_2^m} (-1)^{\vec{x} \cdot \vec{y}} f(\vec{y})$$

↪ ile

$$\begin{pmatrix} \hat{f}(g_1) \\ \hat{f}(g_2) \\ \vdots \\ \hat{f}(g_n) \end{pmatrix} = \frac{1}{\sqrt{n}} \begin{pmatrix} X_1^*(g_1) & X_1^*(g_2) & \dots & X_1^*(g_n) \\ \vdots & \vdots & \ddots & \vdots \\ X_n^*(g_1) & X_n^*(g_2) & \dots & X_n^*(g_n) \end{pmatrix} \begin{pmatrix} f(g_1) \\ f(g_2) \\ \vdots \\ f(g_n) \end{pmatrix}$$

$\Downarrow$

$X^*$

- ① Transformata Fourier este o ap. liniară (unitară)  
 ② Mat. corespunzătoare este  $\frac{1}{\sqrt{n}} X^*$

$\rightarrow$  trans. Fourier inversă

$$\begin{pmatrix} f(g_1) \\ f(g_2) \\ \vdots \\ f(g_n) \end{pmatrix} = \frac{1}{\sqrt{n}} \begin{pmatrix} \chi_1(g_1) & \dots & \chi_n(g_1) \\ \vdots & \ddots & \vdots \\ \chi_1(g_n) & \dots & \chi_n(g_n) \end{pmatrix} \begin{pmatrix} \hat{f}(g_1) \\ \hat{f}(g_2) \\ \vdots \\ \hat{f}(g_n) \end{pmatrix}$$

care se poate scrie:

$$\boxed{\tilde{f}(g_i) = \frac{1}{\sqrt{n}} \sum_{k=1}^n \chi_k(g_i) \hat{f}(g_k)}$$

$\rightarrow$  Observații:

- (1)  $\tilde{f} = \hat{f} - f$  // jd.  $\hat{f}$  și  $\tilde{f}$  inverse
- (2)  $\|f\| = \|\hat{f}\| = \|\tilde{f}\|$  // identitatea lui Parseval  
demonstrează  $\frac{1}{\sqrt{n}} X$  unitar
- (3) în  $\mathbb{Z}_n$ :  $\chi_x(y) = \chi_y(x)$   $\Rightarrow$  trans. Fourier inversă a  $f$ .  
 $\tilde{f}(x) = \frac{1}{\sqrt{n}} \sum_{y \in \mathbb{Z}_n} e^{\frac{2\pi i xy}{n}} f(y)$  și  $\tilde{f}(\vec{x}) = \frac{1}{\sqrt{2^n}} \sum_{y \in \mathbb{Z}_n^n} (-1)^{\vec{x} \cdot \vec{y}} \tilde{f}(y) = \hat{f}(\vec{x})$

Avem trans. Fourier directă este o involuție

$\rightarrow$  Def:

Fie  $f: G \rightarrow \mathbb{C}$  s. m. periodică  $\Leftrightarrow \exists p \in G, p \neq 0$  s. i.  $(f)(g \in G, f(g+p) = f(g))$   
 periodică

// similar cu  $\sin((x + 2\pi)) = \sin(x)$

//

$$\Rightarrow \hat{f}(g_i) = \frac{1}{\sqrt{n}} \sum_{k=1}^n \chi_i^*(g_k) f(g_k) = \frac{1}{\sqrt{n}} \sum_{k=1}^n \chi_i^*(g_k + p - p) f(g_k + p) =$$

$$= \chi_i^*(-p) \frac{1}{\sqrt{n}} \sum_{k=1}^n \chi_i^*(g_k + p) f(g_k + p) = \chi_i^*(-p) \hat{f}(g_i)$$

(d. c. m.f.)

$$\text{si } \chi_i^*(-p) = \overline{\chi_i(p)}$$

$\Rightarrow$  invers  $\Leftrightarrow -p \sim p$

$\Leftrightarrow$  dacă  $f$  este periodică de perioada  $p$  și  $i \in \sigma(f)$ .  $\underline{\chi_i(p) \neq 1} \Rightarrow \hat{f}(g_i) = 0$

## Transformarea Fourier Cuantică

În  $G$  grup finit și  $H$  sp. Hilbert core să repreze pe  $G$ ,  $H$  este o bază  $\{ |g\rangle \mid g \in G\}$

Convenție:  $|g_i\rangle = (0, 0, 0, \dots, 1, 0, \dots, 0)^T$

Stare:  $c_1|g_1\rangle + \dots + c_n|g_n\rangle$  unde  $\sum |c_i|^2 = 1, c_i \in \mathbb{C}$

adică  $f: G \rightarrow \mathbb{C}$  cu  $f(g_i) = c_i \forall i, \|f\| = 1$   
(quantum Fourier transform)

$$\Rightarrow QFT = \sum_{i=1}^n f(g_i)|g_i\rangle \sim \sum_{i=1}^n \hat{f}(g_i)|g_i\rangle$$

cu mat. unitară  $\frac{1}{\sqrt{n}}X = \frac{1}{\sqrt{n}} \begin{pmatrix} \chi_1^*(g_1) & \dots & \chi_1^*(g_n) \\ \vdots & \ddots & \vdots \\ \chi_n^*(g_1) & \dots & \chi_n^*(g_n) \end{pmatrix}$

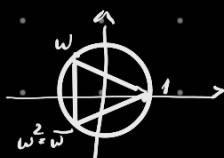
## → App. T. Fourier

### ① Giuseppe Cardano

Fie  $z_1, z_2, z_3 \in \mathbb{C}$  și  $\omega = \exp\left(\frac{2\pi i}{3}\right)$

$z^3 = 1$  are rd. 1,  $\omega, \omega^2$  și  $1 + \omega + \omega^2 = 0$

Cauțăm pol.  $P(z) = \eta_0 + \eta_1 z + \eta_2 z^2$  a.i.  $P(1) = z_0, P(\omega) = z_1, P(\omega^2) = z_2$



$$\begin{cases} z_0 = \eta_0 + \eta_1 + \eta_2 \\ z_1 = \eta_0 + \eta_1 \omega + \eta_2 \omega^2 \\ z_2 = \eta_0 + \eta_1 \omega^2 + \eta_2 \frac{\omega^4}{\omega} \end{cases} \Leftrightarrow \begin{pmatrix} z_0 \\ z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \begin{pmatrix} \eta_0 \\ \eta_1 \\ \eta_2 \end{pmatrix}$$

2?  $\xleftarrow{\text{climatizare}} M \cdot (\bar{M}^*)^T \Rightarrow$   
transpose conjugate

$M$  matrice simetrică  $\Rightarrow M = M^*$  ( $M = M$  conjugat)

$$\Rightarrow \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega^2 & \omega \\ 1 & \omega & \omega^2 \end{pmatrix} = 3 \begin{pmatrix} 1 & p & p \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \Rightarrow$$

$$\Rightarrow S = \frac{1}{\sqrt{m}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \text{ unitar} \Rightarrow S \cdot S^* = I_3$$

Folosind  $M^T \Rightarrow \left\{ \begin{array}{l} 3\eta_0 = z_0 + z_1 + z_2 \\ 3\eta_1 = z_0 + z_1\omega^2 + z_2\omega \\ 3\eta_2 = z_0 + z_1\omega + z_2\omega^2 \end{array} \right.$

$$\left\{ \begin{array}{l} 3\eta_1 = z_0 + z_1\omega^2 + z_2\omega \\ 3\eta_2 = z_0 + z_1\omega + z_2\omega^2 \end{array} \right.$$

Or,  $\eta_0$  este centrul greutății a sistemului  $z_1 z_2 z_3 \Rightarrow$

$\Rightarrow$  după translată ( $\Delta$  adună în 0)  $\Rightarrow \eta_0 = 0$

$$\Rightarrow \begin{cases} z_0 = \eta_1 + \eta_2 \\ z_1 = \eta_1\omega + \eta_2\omega^2 \\ z_2 = \eta_1\omega^2 + \eta_2\omega \end{cases} \Rightarrow 9\eta_1\eta_2 = z_0^2 + z_1^2 + z_2^2 - 2z_0z_1 - z_1z_2 - 2z_2z_0$$

$$\text{de } z_1 + z_2 + z_3 = 0 \Rightarrow z_0^2 + z_1^2 + z_2^2 + 2z_1z_2 + 2z_2z_0 + 2z_1z_3 = 0$$

$$\text{de } \omega^2 + \omega = -1$$

$$\Rightarrow 3\eta_1\eta_2 = -(z_0z_1 + z_1z_2 + z_2z_0)$$

$$z^3 + pz + q = 0 \quad \begin{cases} \text{are coroane soluții reale de var. cu} \\ \text{care } ax^3 + bx^2 + cx + d = 0 \end{cases}$$

$$\text{dim rel. lin. 1. viette} \Rightarrow p = z_1 z_2 + z_0 z_1 + z_1 z_3 \Rightarrow$$

$$\Rightarrow \boxed{3\eta_1 \eta_2 = -P}$$

$$(z-1)(z-\omega)(z-\omega^2) = z^3 - 1 \stackrel{(z \mapsto -z)}{\Rightarrow}$$

$$\Rightarrow (z+1)(z+\omega)(z+\omega^2) = z^3 + 1 \stackrel{(z \mapsto \frac{\eta_1}{\eta_2} + \text{omogn.})}{\Rightarrow}$$

$$\Rightarrow (\eta_1 + \eta_2) \underbrace{(\eta_1 + \omega \eta_2)}_{\omega} \underbrace{(\eta_1 + \omega^2 \eta_2)}_{\omega^2} = \eta_1^3 + \eta_2^3 \Rightarrow$$

$$\Rightarrow \underbrace{(\eta_1 + \eta_2)}_{z_0} \underbrace{(\eta_1 \omega + \omega^2 \eta_2)}_{z_1} \underbrace{(\omega^2 \eta_1 + \eta_2 \omega)}_{z_2} = \eta_1^3 + \eta_2^3$$

$$\Rightarrow \text{dor } z_0 z_1 z_2 = \eta_1^3 + \eta_2^3 = -9 \Rightarrow$$

$$\Rightarrow \begin{cases} \eta_1^3 + \eta_2^3 = -9 \\ \eta_1^3 \eta_2^3 = -\frac{P^3}{27} \end{cases}$$

$\eta_1^3, \eta_2^3$  reaumate + a cuique  $\eta_1^3 + \eta_2^3$  &  $\eta_1^3 \eta_2^3$

$\Rightarrow$  construim ec.  $\Rightarrow$

$$\Rightarrow \text{Resolventa petrolica } x^2 + q x - \frac{P^3}{27} = 0 \Rightarrow$$

$$\Rightarrow \text{pol. } \begin{cases} \eta_1^3 = -\frac{q}{2} + \sqrt{\Delta} \\ \eta_2^3 = -\frac{q}{2} - \sqrt{\Delta} \end{cases} \text{ unde } \boxed{\Delta = \frac{q^2}{4} + \frac{P^3}{27}}$$

det. ec. de gr. = 3

- se calc.  $\eta_1$
- $\eta_1 \eta_2 = -\rho/3 \Rightarrow \eta_2$
- discutie după  $\Delta$  1/pdf