# Consultatii sesiune 2

Saturday, June 5, 2021 8:00 AM

Viewing A.M. N.'s applicatio...

## Ordine de mărime

$g: \mathbb{N} \to \mathbb{R}_+$

$O(g) = \{ f: \mathbb{N} \to \mathbb{R}_+ \mid \exists c > 0, \exists n_0 \in \mathbb{N}, \forall n \geq n_0 : f(n) \leq c \cdot g(n) \}$

$\Omega(g) = \{ f: \mathbb{N} \to \mathbb{R}_+ \mid \exists c > 0, \exists n_0 \in \mathbb{N}, \forall n \geq n_0 : f(n) \geq c \cdot g(n) \}$

$\Theta(g) = \{ f: \mathbb{N} \to \mathbb{R}_+ \mid \exists c_1, c_2 > 0, \exists n_0 \in \mathbb{N}, \forall n \geq n_0 : c_1 g(n) \leq f(n) \leq c_2 g(n) \}$

$o(g) = \{ f: \mathbb{N} \to \mathbb{R}_+ \mid \forall c > 0, \exists n_0 \in \mathbb{N}, \forall n \geq n_0 : f(n) < c \cdot g(n) \}$

**Ex 5** Dem. că

Dacă $f(n) = O(h_1(n))$ și $g(n) = O(h_2(n))$ atunci $f(n) + g(n) = O(\max\{h_1(n), h_2(n)\})$

$\exists c > 0, \exists n_0 \in \mathbb{N}, \forall n \geq n_0 : f(n) + g(n) \leq c \cdot \max\{h_1(n), h_2(n)\}$

$c = ?$

$f(n) = O(h_1(n)) \Rightarrow \exists c_1 > 0, \exists n_0' \in \mathbb{N}, \forall n \geq n_0' : f(n) \leq c_1 \cdot h_1(n)$

$g(n) = O(h_2(n)) \Rightarrow \exists c_2 > 0, \exists n_0'' \in \mathbb{N}, \forall n \geq n_0'' : g(n) \leq c_2 \cdot h_2(n)$

$f(n) + g(n) \leq c_1 \cdot h_1(n) + c_2 \cdot h_2(n) \leq c_1 \cdot \max\{h_1(n), h_2(n)\} + c_2 \cdot \{h_1(n), h_2(n)\}$

$\leq (c_1 + c_2) \cdot \max\{h_1(n), h_2(n)\}$

---

[Thm. Euler] $n \geq 1, \forall a \in \mathbb{Z}_n^*, \quad a^{\phi(n)} \equiv 1 \bmod n$ $\quad \phi(n) = |\mathbb{Z}_n^*|$

[Consl. Fermat] $p \geq 2, p$ prim, $p \nmid a, \quad a^{p-1} \equiv 1 \bmod p$ $\quad p^1 p^0 = p - 1$, $\phi(p^e) = p^e - p^{e-1}$

[Criteriul lui Euler] $a \in QR_p \iff a^{\frac{p-1}{2}} = 1 \bmod p$ $\quad a \equiv x^2 \bmod p$

$a \in QNR_p \iff a^{\frac{p-1}{2}} \equiv -1 \bmod p$ $\quad a \in QR_p$

[Thm. Wilson] $p$ prim $\iff (p-1)! \equiv -1 \bmod p$ $\quad QR_p = \{1^2, 2^2, (3^2)_p, (4^2)_p, (5^2)_p, (6^2)_p\}$

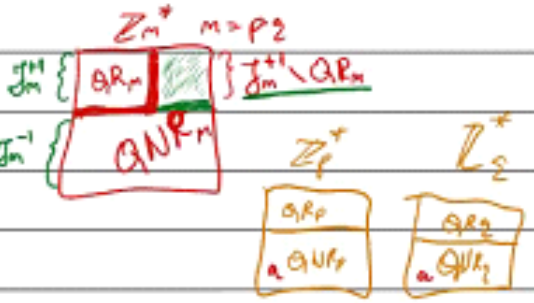
**Simbolul Legendre** $\left(\frac{a}{p}\right) = \begin{cases} 0, & p \mid a \\ 1, & p \nmid a \text{ și } a \in QR_p \\ -1, & p \nmid a \text{ și } a \in QNR_p \end{cases}$ $a \in \mathbb{Z}_p - \mathbb{Z}_p^*$, $a \in \mathbb{Z}_p^*$

**Reguli de calcul pentru simb. Legendre**

1. $a \equiv b \bmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ — $\left(\frac{5}{3}\right) = \left(\frac{2}{3}\right)$, $5 \bmod 3 = 2$, $5 \equiv 2 \bmod 3$
2. $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
3. $\left(\frac{1}{p}\right) = 1$
4. $\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \bmod 4 \\ -1, & p \equiv 3 \bmod 4 \end{cases}$
5. $\left(\frac{2}{p}\right) = \begin{cases} 1, & p \equiv \pm 1 \bmod 8 \\ -1, & p \equiv \pm 3 \bmod 8 \end{cases}$

$1 \mid 7$

$3 \mid 5$




**Simbolul Jacobi** $\left(\frac{a}{m}\right) = \begin{cases} 1, & m = 1 \\ \left(\frac{a}{p_1}\right)^{e_1} \cdots \left(\frac{a}{p_k}\right)^{e_k}, & \text{altfel} \end{cases}$

$1 \Rightarrow QR_m$

$-1 \Rightarrow QNR_m$ ✓

unde $m = p_1^{e_1} \cdots p_k^{e_k}$, $p_i \neq p_j$, prime

$\left(\frac{a}{m}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a}{q}\right) = (-1)(-1) = 1$

$m = p \cdot q$, $p, q$ prime dist.

$a \in J_m^{t+1} \setminus QR_m$

**Ecuația** $ax^2 + bx + c \equiv 0 \bmod p$ are
- 2 rădăcini în $\mathbb{Z}_p$, dacă $\Delta \equiv y^2 \bmod p$, $y \in \mathbb{Z}$, $p \nmid y$
- 1 rădăcină în $\mathbb{Z}_p$, dacă $\Delta \equiv 0 \bmod p$
- 0 rădăcini altfel

$\Delta = b^2 - 4ac$

$x = \frac{-b \pm \sqrt{\Delta}}{2a}$

$x^2 \equiv 1 \bmod p$ < sol. 1, sol. $p-1$

$x^2 \equiv 1 \bmod p_1 \cdots p_k \Rightarrow 2^k$ sol. în $\mathbb{Z}_{p_1 \cdots p_k}$

Ex2 Calculați cardinalul mulțimilor $Z_{324}^*$ și $Z_{539}^*$.

$324 = 2^2 \cdot 3^4$

$\phi(324) = \phi(2^2 \cdot 3^4) = \phi(2^2) \cdot \phi(3^4) = (2^2 - 2^1)(3^4 - 3^3) = 2 \cdot 54 = 108$

$539 = 7^2 \cdot 11$

$\phi(539) = \phi(7^2 \cdot 11) = 420 = \phi(7^2) \cdot \phi(11) = (49 - 7)(11 - 1) = 42 \cdot 10$

$\phi(p) = p - 1$

$\phi(p^k) = p^k - p^{k-1}$

$\phi(n) = \phi(p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}) = \phi(p_1^{e_1}) \cdot \ldots \cdot \phi(p_k^{e_k}) = (p_1^{e_1} - p_1^{e_1 - 1}) \cdots (p_k^{e_k} - p_k^{e_k - 1})$

$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$

$(a, b) = 1$

Reguli de calcul pentru simb. Legendre

1. $a \equiv b \bmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
2. $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
3. $\left(\frac{1}{p}\right) = 1$
4. $\left(\frac{-1}{p}\right) \overset{a,b}{=} \begin{cases} 1, & p \equiv 1 \bmod 4 \\ -1, & p \equiv 3 \bmod 4 \end{cases}$
5. $\left(\frac{2}{p}\right) \overset{a,b}{=} \begin{cases} 1, & p \equiv \pm 1 \bmod 8 \\ -1, & p \equiv \pm 3 \bmod 8 \end{cases}$
6. $\left(\frac{q}{p}\right) \overset{a,b}{=} \begin{cases} -\left(\frac{p}{q}\right), & p \equiv_4 q \equiv_4 3 \\ \left(\frac{p}{q}\right), & p \equiv_4 1 \text{ sau } q \equiv_4 1 \end{cases}$

Ex3. Calculați simbolurile:

a) $\left(\frac{82}{17}\right) =$

b) $\left(\frac{111}{991}\right) \overset{6a}{=} -\left(\frac{991}{111}\right) \overset{1}{=} -\left(\frac{991 \bmod 111}{111}\right) \overset{1}{=} -\left(\frac{103}{111}\right) = -\left(\frac{-8}{111}\right) = -\left(\frac{2^3}{111}\right)\left(\frac{-1}{111}\right) \overset{6b}{=}$

$\overset{2.}{=} -\left(\frac{2^2}{111}\right)\left(\frac{2}{111}\right)\left(\frac{-1}{111}\right) \overset{4b}{=} -(-1)(-1) = -1$

(1 — nu 6b — 4b)

c) $\left(\frac{41}{163}\right) =$

$991 \bmod 4 = 3$

$111 \bmod 4 = 3$

$\left(\frac{a}{111}\right) = 0^2$

$x^2 \equiv a \bmod 111$

Ex3. Calculați simbolurile:

a) $\left(\frac{82}{17}\right) \overset{2}{=} \left(\frac{41}{17}\right) \cdot \left(\frac{2}{17}\right) \overset{5a}{=} 1 \cdot \left(\frac{7}{17}\right) \overset{6b}{=} \left(\frac{17}{7}\right) \overset{1}{=} \left(\frac{3}{7}\right) \overset{6a}{=} -\left(\frac{7}{3}\right) \overset{1}{=} -\left(\frac{1}{3}\right) \overset{3}{=} -1$

$(17)_8 = 1$; $(17)_4 = 1$

b) $\left(\frac{111}{991}\right) =$

$-\left(\frac{-1}{p}\right) \overset{4b}{=} -(-1) = 1$

c) $\left(\frac{41}{163}\right) =$

$\overset{4a}{=} -(1) = -1$

Legea reciprocității

Legea reciprocității

Ex1 $(S)\begin{cases} x \equiv b_1 \bmod m_1 \\ x \equiv b_2 \bmod m_2 \end{cases}$

a) Demonstrați că sistemul (S) are soluție dacă și numai dacă $b_1 \equiv b_2 \bmod (m_1, m_2)$, unde $(m_1, m_2) \neq 1$.

b) Dacă are soluție, atunci ea este unică modulo $[m_1, m_2]$

c) Rezolvați următorul sistem utilizând demonstrațiile anterioare

$\begin{cases} x \equiv 31 \bmod 50 \\ x \equiv 16 \bmod 35 \end{cases}$ $\quad 50 \mid (x-31) \Rightarrow x - 31 = 50y \Rightarrow \boxed{x = 50y + 31}$

$50y + 31 \equiv 16 \bmod 35 \iff$

$50y \equiv 16 - 31 \equiv 20 \bmod 35$

$50y - 35z = 20$ $\quad V_{50} = (1,0) \quad V_{-35} = (0,1)$

$50 = -35 \cdot (-1) + 15$ $\quad V_{15} = V_{50} - (-1) V_{-35} = (1,0) - (-1)(0,1) = (1,0) - (0,-1) = (1,1)$

$-35 = 15 \cdot (-3) + 10$ $\quad V_{10} = V_{-35} - (-3) V_{15} = (0,1) - (-3)(1,1) = (0,1) - (-3,-3) = (3,4)$

$15 = 10 \cdot 1 + \boxed{5}$ $\quad V_5 = V_{15} - V_{10} = (1,1) - (3,4) = (-2,-3)$

$10 = 5 \cdot 2 + 0$ $\quad V_f : (-2) \cdot 50 + (-3)(-35) = \underbrace{-100}_{\alpha} + \underbrace{105}_{\beta} = 5$ ✓

$y = \alpha \cdot \frac{c}{d} = (-2) \cdot \frac{20}{5} = (-2) \cdot 4 = -8 \bmod 35 = 27$

$x = 50 \cdot 27 + 31 =$

## Monoizi de cuvinte

monoid → comutativ; → asociativ

**Def.** cuvânt de lungime $k \geq 1$ peste $\Sigma$ este o funcție $w : \{1, \dots, k\} \to \Sigma$

$w = w(1) \dots w(k)$, dacă $k \geq 1$, atunci $|w| = k$

$\lambda$ - cuvântul nul

**Notații** $\Sigma^0 = \{\lambda\}$

$\Sigma^+ = \bigcup_{k \geq 1} \Sigma^k$, $k \geq 1$

$\Sigma^* = \bigcup_{k \geq 0} \Sigma^k = \Sigma^+ \cup \{\lambda\}$

2 cuv. sunt egale $u, v \in \Sigma^k \iff |u| = |v|$ și $u(i) = v(i)$, $\forall i = \overline{1,k}$

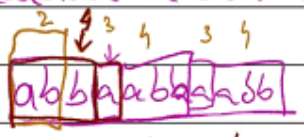
**Thm. Levi** $x, y, u, v$ cuvinte, a.î. $xy = uv$; $|x| < |u|$, at. $\exists! z \in \Sigma^+$, a.î. $u = xz$

$|x| = |u| \Rightarrow x = u$; $y = v$

$|x| > |u|$, $\exists! z$ $\quad x = uz$

Def $C$ cod, $C \subseteq \Sigma^+$ $\Leftrightarrow \forall w \in C^+$, $w = u_1 \cdots u_m = v_1 \cdots v_n$, $u_i, v_j \in C \Rightarrow$

$\Rightarrow (m = n) \wedge (u_i = v_i, \forall i)$ → o concatenare de cuvinte din $C$

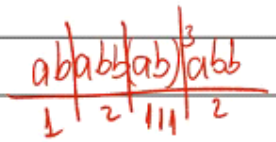
$w =$ 


$w = 2\ 1\ 3\ 4\ 3\ 4 = 434134$

$ab|b|a|abb|a|abb = ab^2|a|ab^2|a|ab^2 \Rightarrow$ C nu e cod

~~$\exists$~~ dacă C e cod!

w 



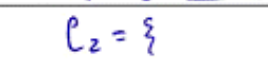

$C_2 = \{ab, abb\}$ este cod

$(ab)^2 = abab$

$C_1 = \{b, ab, a, abb\}$ (1, 2, 3, 4)

$abbab = \begin{cases} 42 = abb|ab \\ 212 = ab|b|ab \end{cases}$

**Ex1** Produsul a 2 coduri nu este întotdeauna cod.

$C_1 = \{$  $\}$  $= w_1 w_2 w_2 w_1$ → scriere unică ($C_1$ - cod)

$C_2 = \{$ $\}$

$C_1C_2 = \{$  $\}$ → $\forall w_i \in C_1$ și $\forall u_j \in C_2$

$C_2C_1 = \{$  $\}$

$C_1 = \{a, ab\}$

$C_2 = \{bab, b\}$

$C_1C_2 = \{abab, ab, abbab, abb\}$ (1, 2, 3, 4)

$abab \begin{cases} 1 \\ 22 \end{cases}$

Improbabil să fie la examen

**Ex 2** Fie $C$ cod, $k \geq 2$, dem. că $C^k$ este cod; $C^k = \{w_1 \cdots w_k \mid \forall w_i \in C\}$ $\in C^k$

$\forall a_i = a_{i_1} a_{i_2} \cdots a_{i_k}$

Pres că $C^k$ nu e cod, ab. $\Rightarrow \exists x \in (C^k)^+$ x se scrie în 2 moduri:

$x = a_1 a_2 \cdots a_m = b_1 b_2 \cdots b_n \Rightarrow a_i \in C^k \Rightarrow a_i = a_{i_1} a_{i_2} \cdots a_{i_k}$ concatenare de $k$ cuvinte din $C$; $a_i, \forall i$, are scriere (descompunere) unică în cuvinte din $C$

Similar pt $b_i$

$x = \underbrace{a_1 a_{1_2} \cdots a_{1_k}}_{a_{1_j} \in C} \underbrace{a_{2_1} \cdots a_{2_k}} \cdots \underbrace{a_{m_1} \cdots a_{m_k}} = \underbrace{b_{1_1} \cdots b_{1_k}} \underbrace{b_{2_1} \cdots b_{2_k}} \cdots \underbrace{b_{n_1} \cdots b_{n_k}}_{\forall b_{i_j} \in C}$

$C$ cod $\Rightarrow a_{i_j} = b_{i_j}, \forall i,j \Rightarrow m = n \Rightarrow C^k$ cod $\Rightarrow$ contradicție!

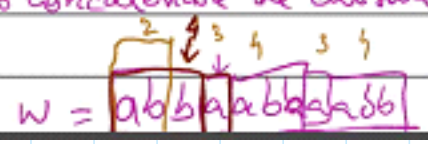
$a_i = b_i, \forall i$

Scriere (descr.) e unică.

---

**Def.** $C$ cod, $C \subseteq \Sigma^+$ $\Leftrightarrow \forall w \in C^+$, $w = u_1 \cdots u_m = v_1 \cdots v_n$, $u_i, v_i \in C \Rightarrow$

$\Rightarrow (m = n) \wedge (u_i = v_i, \forall i)$ → o concatenare de cuvinte din $C$




---

Alg. Sardinas-Patterson $C = \{$  ,  ,  $\}$ ? $C$ este cod?

$C_1 = \{x \in \Sigma^+ \mid \exists c \in C, cx \in C\}$

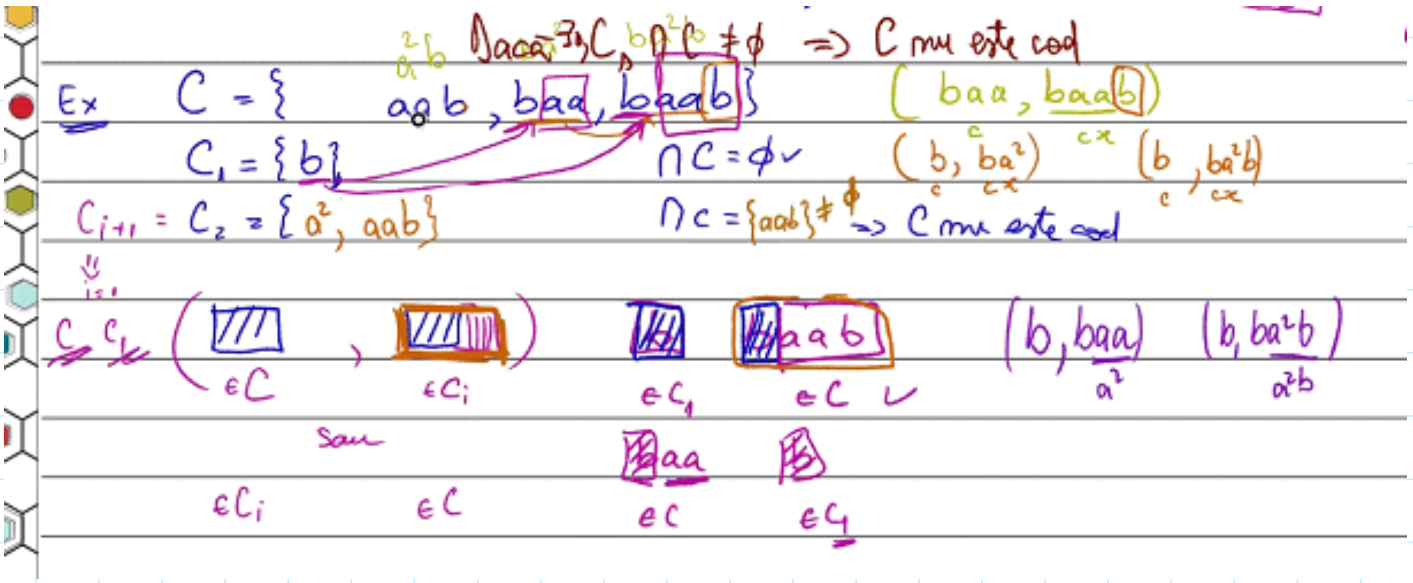
$\overset{cd}{=}$ sufixal → ab → abcd

$C_{i+1} = \{x \in \Sigma^+ \mid (\exists c \in C, cx \in C_i) \vee (\exists c \in C_i, cx \in C)\}$ $C_i = \{a, \ldots$

$C_t = C_j$, $j < t$ → oprire

Dacă $C_i \cap C = \emptyset$, $\forall i \Rightarrow C$ cod

Dacă $\exists i, C_i \cap C \neq \emptyset \Rightarrow C$ nu este cod




**Ex3** a) $C = \{ab, ab^2, b^3a\}$

b) $C = \{aba^2, ba^2, (ab)^2, aba^2bab\}$

c) $C = \{ab, ab^m, b^ma\}$ $m, m \geq 1$

a) $C_1 = \{b\} \cap C = \phi$ $(ab, ab^2)$

$C_2 = \{b^2a\} \cap C = \phi$ $(b, b^3a)$

$C_3 = \phi$ ; $C_4 = \phi = C_3$ => C cod

$m - m + 1 \stackrel{?}{=} m$

b) $C_1 = \{bab\} \cap C = \phi$ $(aba^2, aba^2bab)$

$C_2 = \phi = C_3$ => C cod

$m = 1$

$C_1 = \{b^{m-1}\}$

$C_2 = \{b^{m-m+1}a\} \cap C_1$

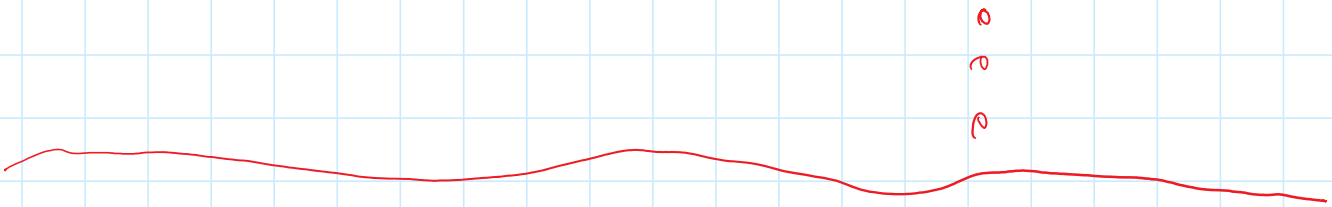
$C_3 = \phi = C_4$ => C cod

c) caz 1: $m > 1$ $C_1 = \{b^{m-1}\}$

$m > m$

caz 1: $m-1 < m$

$m-1 > m$



# Codificarea Huffman clasic

Sursa de informatie $(is) = (A, \Pi)$ A - alfabet $\Pi$ - probabilitatea de aparitie

| | | | | |
|---|---|---|---|---|
| A | $a_1$ | .... | $a_{m-1}$ | $a_m$ |
| $\Pi$ | $\Pi_1$ | .. | $\Pi_{n-1}$ | $\Pi_m$ |

$h$ $\quad \Pi_1 + \dots \Pi_{m-1} + \Pi_m = 1 \qquad \Pi_1 \geq \dots \geq \Pi_m$

$$L_h(is) = \sum_{i=1}^{m} (\Pi_i \cdot |h(a_i)|) = \sum_{a \in A} (\Pi(a) \cdot |h(a)|)$$ lungimea medie a lui $h$

**Ex** anaaremere $\quad IS = (A, \Pi)$ $\quad$ * codificarea H.b.

00 10 00 00 10 01 111 01 10 01

a n a a r e ...

IS: *

| A | a | e | r | n | m |
|---|---|---|---|---|---|
| $\Pi$ | $\frac{3}{10}$ | $\frac{3}{10}$ | $\frac{2}{10}$ | $\frac{1}{10}$ | $\frac{1}{10}$ |

0 / 1 *

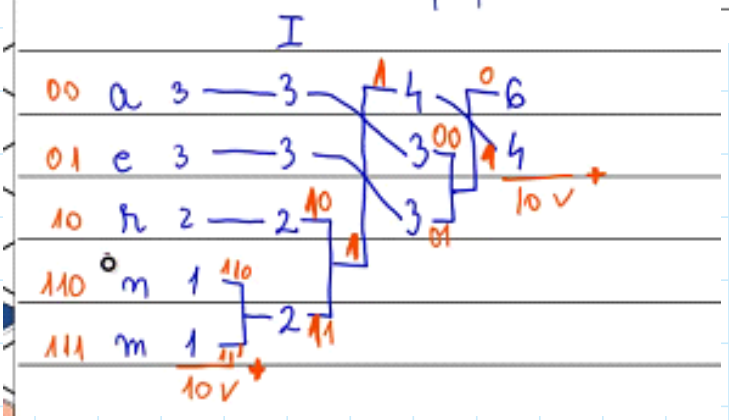
→ ord. alf. * → ord. aparitiei caracterelor in text → 0 1 ; → 0

nr. de biti ai codificării caracterului / frecvența caracterului

$$L_h(is) = 2 \cdot \frac{3}{10} + 2 \cdot \frac{3}{10} + 2 \cdot \frac{2}{10} + 3 \cdot \frac{1}{10} + 3 \cdot \frac{1}{10}$$

a e r n m

$$L_h(is) = \frac{22}{10} = 2{,}2$$



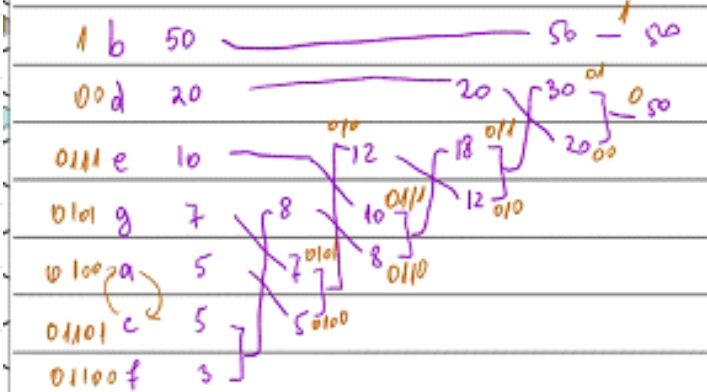
# Shannon - Fano

| | | | | | |
|---|---|---|---|---|---|
| 00 | a | 3 | 0 | 0 | |
| 01 | e | 3 | | 1 | |
| 10 | r | 2 | 1 | 0 | |
| 110 | m | 1 | | 0 | |
| 111 | m | 1 | | 1 | |

$$L_h(is) = \frac{\overset{a}{2}\cdot 3 + \overset{e}{2}\cdot 3 + \overset{n}{2}\cdot 2 + \overset{m}{3} + 3}{10} = 2{,}2$$

**Ex3** Specificați care dintre coduri este cHb (codificare H. binară)?

| is: A | a | b | c | d | e | f | g |
|---|---|---|---|---|---|---|---|
| $\Pi$ | 0,05 | 0,5 | 0,05 | 0,2 | 0,1 | 0,03 | 0,07 |
| $h_1$ | 0100 | 1 | 0101 | 00 | 0111 | 0100 | 0101 |
| $h_2$ | 1101 | 0 | 1110 | 100 | 101 | 1111 | 1100 |




1 / 0

$L_h(is) = \boxed{2{,}18} = L_{h_1}(is) \Rightarrow$

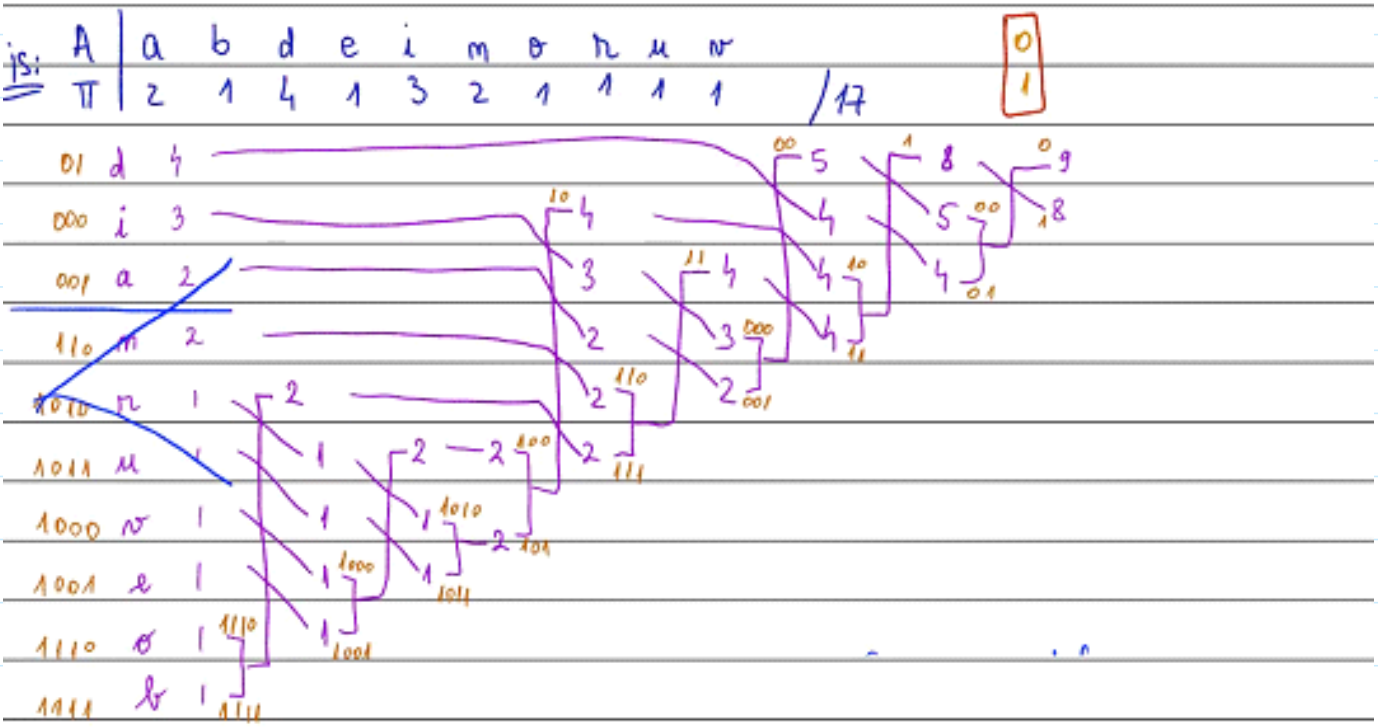
$h_1$ poate fi codif. Hb.

S-P pe $h_1$

$C_1 = \phi$

$C_2 = \phi \Rightarrow h_1$ este cod

Ex2 Decodificați 01001101010110001100111000100100001111010111001101000




## Huffman adaptiv

- ~~o singură parcurgere pt. codificare~~
- un caracter poate fi codificat diferit

~~Observații:~~
- numărul arborelui == conținutul rădăcinii
- frunzele conțin numărul de apariții al caracterului reprezentat / esc
- ~~nodurile intermediare conțin suma fiilor~~

Citirea unui caracre nou:
- ~~pe poziția lui esc va apărea un nod intermediar~~
- esc devine fiul său sâng
- caracterul nou devine fiul său drept

Citirea unui caracter deja întâlnit:
- se incrementează conținutul frunzei corespunzătoare

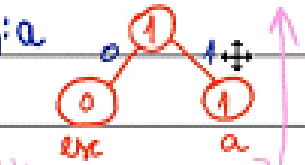
Verificarea proprietății de **sibling**:
- citit de jos în sus și de la stânga la dreapta conținutul nodurilor trebuie să fie ordonat crescător (în cazu
- ~~Numai după ce proprietatea de sibling este asigurată~~, **etichetăm**.

cazurile de felul 2211 regula este să interschimbăm cel mai din stânga subarbore cu cel mai din dreapta)

w = a a b b c a a c b b

H. ad. cu secv. esc.

$A_0$: 0 (esc)  $A_1$: a

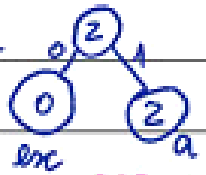



0 / 1

Sibling → 0 1 1 ✓

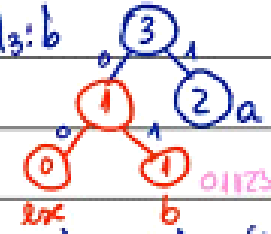
Cod: a

$A_2$: a




022 ✓

$A_3$: b

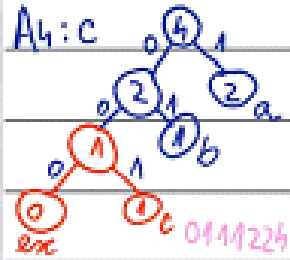



01123 ✓

cod += 1

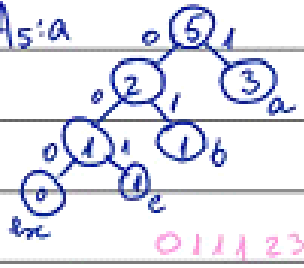
cod += cod esc (A2) 0 b

$A_4$: c




01112240 ✓

$A_5$: a

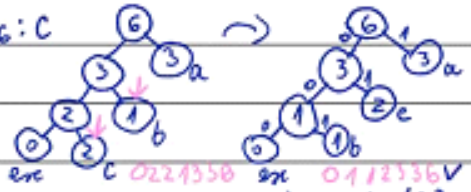



01112350 ✓

cod += cod esc (A3) 00 c

cod += cod a (A4) 1

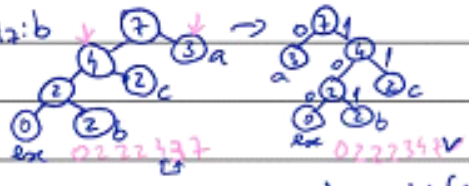
$A_6$: c




02213500 → 01123360 ✓

cod += cod c (A5) 001

$A_7$: b




02223370 → 02223470 ✓

cod += cod b (A6)

| | cod ASCII a | A1 a | A2 esc | cod ASCII b | A3 esc | cod ASCII c | A4 a | A5 c | A6 b | A7 b |
|---|---|---|---|---|---|---|---|---|---|---|
| COD: | 01100001 | 1 | 0 | 01100010 | 00 | 01100011 | 1 | 001 | 001 | 101 |
| | a A1 | a A2 | | b A3 | | c A4 | a A5 | c A6 | b A7 | b |

La ce frunză mă duce codul pe care îl citesc acum?

COD:

- când apare primul ch din cuv: cod ASCII
- " " un ch nou: cod esc din arb. anterior + cod ASCII al ch nou
- " " " " vechi: codul ch din arb. anterior → de la rădăcină până la frunza corespunzătoare ch, o singură

DECODIFICAREA:

- prima dată citim un cod ASCII

COD:

- când apare primul ch din cuv: cod ASCII
- " " un ch nou: cod esc din arb. anterior + cod ASCII al ch nou
- " " " " vechi: codul ch din arb. anterior → de la rădăcină până la frunza corespunzătoare ch, o singură dată

DECODIFICAREA:

- prima dată citim un cod ASCII
- fie dăm peste codul lui esc din arb. curent → citim încă 8 biți (cod ASCII)
- " " " " unui alt ch " "

# Grupuri

Noțiuni: - grup
- grup ciclic
- $\phi(m)$
- ordinul unui el. într-un grup ciclic
- propr. ord. unui el. în cazul $\mathbb{Z}_m^*$
- rădăcini primitive

$\mathbb{Z}_6 = \{0,1,2,3,4,5\}$ $\mathbb{Z}_8^* = \{1,3,5,7\}$ $\phi(8) = \phi(2^3) = 2^3 - 2^2 = 8-4 = 4$

(1,8)=1, (3,8)=1, (5,8)=1, (7,8)=1

$\mathbb{Z}_m = \{0, 1, \dots, m-1\}$ $\mathbb{Z}_6^* = \{1,5\}$

$\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid (a,m)=1\}$ $\phi(6) = \phi(2)\cdot\phi(3) = (2-1)(3-1) = 1 \cdot 2 = 2$

$(\mathbb{Z}_m^*, \cdot, ^{-1}, 1)$ grup abelian ← op. asoc. și comut. / elementele inversabile / element neutru

$\phi(535) = \phi(7^2 \cdot 11) = \phi(7^2)\cdot\phi(11) = (7^2-7)(11-1) = 420$ $\phi(143) = \phi(11\cdot 13) = \phi(11)\cdot\phi(13) = (11-1)(13-1) = 10\cdot 12 = 120$

- $\text{ord}_{\mathbb{Z}_m^*}(a) = \text{ord}_m(a) = \min\{k \mid a^k \equiv 1 \bmod m,\ k \geq 1\}$
- Funcția lui Euler $\phi(m) = |\mathbb{Z}_m^*|$
  - câte numere $< m$ sunt coprime cu $m$
  - $\phi(m)$ reprezintă ordinul grupului $\mathbb{Z}_m^*$

1) $\phi(1) = 1$
2) $\phi(p) = p-1$, $p$ prim
3) $\phi(a\cdot b) = \phi(a)\cdot\phi(b)$, $(a,b)=1$
4) $\phi(p^e) = p^e - p^{e-1}$, $p$ prim — $\phi(7^3) = 7^3 - 7^2 = 294$ ✓
5) $\phi(n) = (p_1^{e_1} - p_1^{e_1-1}) \cdot \dots \cdot (p_k^{e_k} - p_k^{e_k-1})$, unde $n = p_1^{e_1} \cdot \dots \cdot p_k^{e_k}$

Dacă $ord_m(a) = t$, atunci $ord_m(a^k) = t$ ddacă $(k,t) = 1$

Prop. 6 $ord_m(a^k) = \frac{ord_m(a)}{(k, ord_m(a))}$

* Ordinul unui element divide ordinul grupului

$\forall a \in \mathbb{Z}_m^*$, $ord_m(a) \mid \phi(m)$

- Rădăcini primitive

Dacă $ord_m(a) = \phi(m)$, atunci a este rād. primitivă mod m

Câte rād. primitive există în $\mathbb{Z}_m^*$? $\phi(\phi(m))$

$\mathbb{Z}_7^* = \{1,2,3,4,5,6\}$ $a \cdot a^{-1} \equiv 1 \bmod m$ $\forall a \in \mathbb{Z}_m^*, (a,m)=1$

ordinul grupului = # de el. din grup = $|\mathbb{Z}_m^*| = \phi(m)$

$\phi(7) = 7-1 = 6$

ordinul unui el. din grup = # de el. distincte pe care le gen. (din $\mathbb{Z}_m^*$)

| | | | | | | |
|---|---|---|---|---|---|---|
| $1^1 \bmod 7 = 1$ | $2^1 \bmod 7 = 2$ | $3^1 = 3$ | $4^1 = 4$ | $5^1 = 5$ | $6^1 = 6$ | 1 |
| $1^2$ " $= 1$ | $2^2$ " $= 4$ | $3^2 = (9)_7 = 2$ | $4^2 \equiv_7 2$ | $(5^2)_7 = 4$ | $6^2 \equiv_7 1$ | 2 |
| . | $(2^3)_7 = (8)_7 = 1$ | $3^3 = (27)_7 = 6$ | $4^3 \equiv_7 1$ | $(5^3)_7 = 6$ | $6^3 \equiv_7 6$ | 3 |
| . | $2^4 = (16)_7 = 2$ | $3^4 \equiv_7 4$ | $4^4 \equiv_7 4$ | $(5^4)_7 = 2$ | $6^4 \equiv_7 1$ | . |
| . | $2^5 = (64)_7 = 4$ | $3^5 \equiv_7 5$ | $4^5 \equiv_7 2$ | $(5^5)_7 = 3$ | $6^5 \equiv_7 6$ | . |
| $1^6 \bmod 7 = 1$ | $2^6 \equiv_7 1$ | $3^6 \equiv_7 1$ | $4^6 \equiv_7 1$ | $(5^6)_7 = 1$ | $6^6 \equiv_7 1$ | $\phi(m)$ |
| $ord_7(1) = 1$ | $ord_7(2) = 3$ | $ord_7(3) = 6$ | $ord_7(4) = 3$ | $ord_7(5) = 6$ | $ord_7(6) = 2$ | div $\mid \phi(m)$ |

* $\forall a \in \mathbb{Z}_m^*$, $a^{\phi(m)} \equiv_m 1$

1, 2, 3, 6 | 6 = ord. grupului = $\phi(m) = \phi(7)$

3 și 5 au generat toate el. grupului $\mathbb{Z}_7^*$ $\Rightarrow$ „generator" = „rădăcini primitive"

$m = 1, 2, 4, p^k, 2p^k$, p prim $\geq 3$

* ord. unui el. din gr., vom verifica dacă $x^{\text{divizorii ord. gr.}} \equiv_m 1$, ordinul = c.m.m.d.c. puteri

$\mathbb{Z}_7^*$, gen 3; $1 \equiv_7 3^6$ $2 \equiv_7 3^2$ $3 \equiv_7 3^1$ $4 \equiv_7 3^4$ $5 \equiv_7 3^5$ $6 \equiv_7 3^3$

3 ogn. $\mathbb{Z}_7^*$

$\phi(7) = ord_7(3)$

↓ nr. de el. din grup

↳ este el. dist. gen. 3 în $\mathbb{Z}_7^*$

$$ord_G(a^t) = \frac{ord_G(a)}{(t, ord_G(a))}$$

$$ord_7(3^t) = \frac{ord_7(3)}{(t, ord_7(3))} = \frac{\phi(7)}{(t,6)} = \frac{6}{1} = 6$$

# total de el. din grup.

$t = \{1, 5\}$

$\phi(6) = \phi(2) \cdot \phi(3) = (2-1)(3-1) = 1 \cdot 2 = 2$

$ord_7(3^1) = 6 \qquad ord_7(3^5) = 6$