

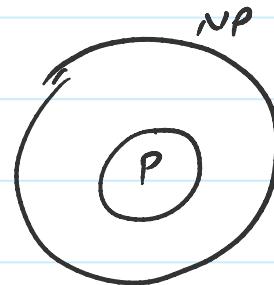
# CURS #7

Tuesday, November 15, 2022 1:48 PM

Google classroom: jyc6xvl

$$\overline{P \neq NP}$$

$\{A \mid A \in \bigcup_{k \geq 1} \text{TIME}(n^k) : n > 0\}$



$\approx^{NP}$  nondeterministic polynomial time

Def  $A \in NP \Leftrightarrow \exists f(\cdot, \cdot)$  calculable in time polynomial

a.i.

$$x \in A \Leftrightarrow \exists y \in \{0,1\}^{P(|x|)} \text{ a.i. } f(x, y) = 1$$

↓  
mostar  
pt x

Ex. (1) Sudoku  $x = \text{table partial/complete}$   
 $y = \text{table complete}$

(2) SAT  $x = \text{Formula logic} \Phi / x_1 \dots x_n$   
 $y = y_1 \dots y_n \in \{0,1\}^n$

(3) TSP

(4) Cobraco habi graf

$$x = (G, k)$$

$$y \in \{1, \dots, k\}^n$$

(5) Composites =  $\{ x \in \{0,1\}^n \mid \exists y, z \neq 1$   
a.t.  $x = y \cdot z \}$

$\leq_{NP}$

nondeterministic

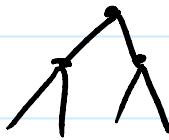
Def Magine Turing nondeterministic

$$|\delta(s,a)| \geq 2$$

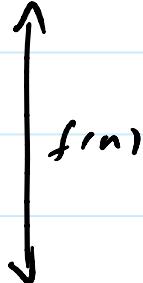
DET



NDET



$\wedge \wedge \wedge \wedge$

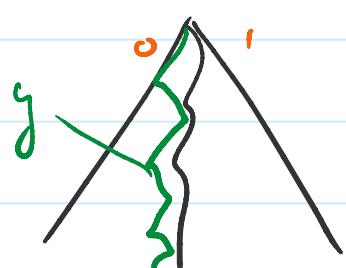


$A \in \text{NTIME}(f(n)) \Leftrightarrow$  exists a m.t. nondeterministic M  
 $M(x)$  free  $O(f(|x|))$  per

$f(x)$  für alle  $x \in \mathbb{N}$

a.i.  $M = L(M)$

⑦  $NP = \bigcup_{k \geq 1} \text{NTIME } S_n^k$



Dann

gr. de algorithme déterministe  
||  
certificat



So oracle

$P \neq NP$  (1 million de \$, premier Clay)

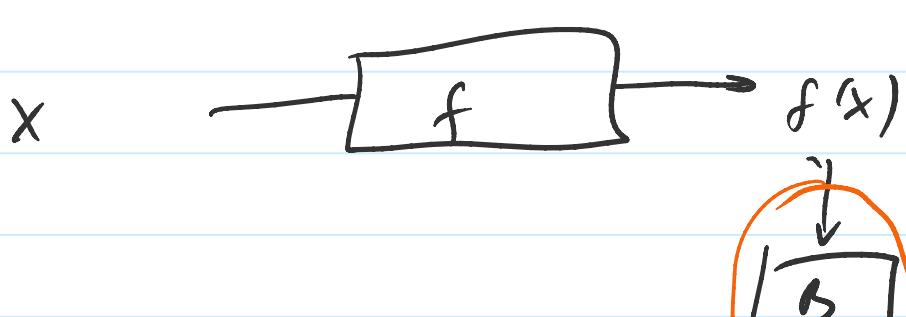
Def  $A \leq_m^P B$

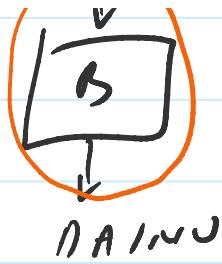
$\exists f: \Sigma^* \rightarrow \Sigma^*$

calculable in temp polynomial

a.i.  $\forall x \in \Sigma^*$

$x \in A \Leftrightarrow f(x) \in B$





Ex. Card. grafurilor  $\leq_m^P$  SAT

$$(G, k) \longrightarrow \phi_{G, k}$$

$$X_{v,i} = \begin{cases} \text{TRUE} & c(v)=i \\ \text{FALSE} & \text{if } v \neq i \end{cases}$$

$$\phi_{G, k}: X_{v, 1} \vee X_{v, 2} \vee \dots \vee X_{v, c} \\ (\forall v \in V)$$

$$\bar{X}_{v, i} \vee \bar{X}_{v, j} \quad \begin{matrix} \neq v \in V \\ \forall 1 \leq i < j \leq c \end{matrix}$$

$$r = (v, w) \in E \quad \bar{X}_{v, 1} \vee \bar{X}_{w, 1}$$

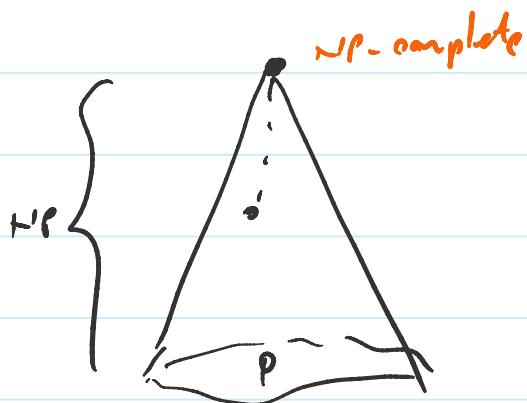
$$\vdots \\ \bar{X}_{v, k} \vee \bar{X}_{w, k}$$

Def A este numită NP-hard

$$\forall B \in NP \quad B \leq_m^P A$$

A se numește NP-complete

A ∈ NP și ∃ B ∈ NP  $B \leq_m^P A$



(T) SAT este NP-completă

(Cook - Levin)

TORONTO

ROGERS  
UNIV.

Consecință  $P = NP \Leftrightarrow$  SAT are algoritmuri polinomiale

Soluție  
de demonstrare

Fie M o mașină Turing nedet. care pe intrarea x face  $\leq p(|x|)$  pasi

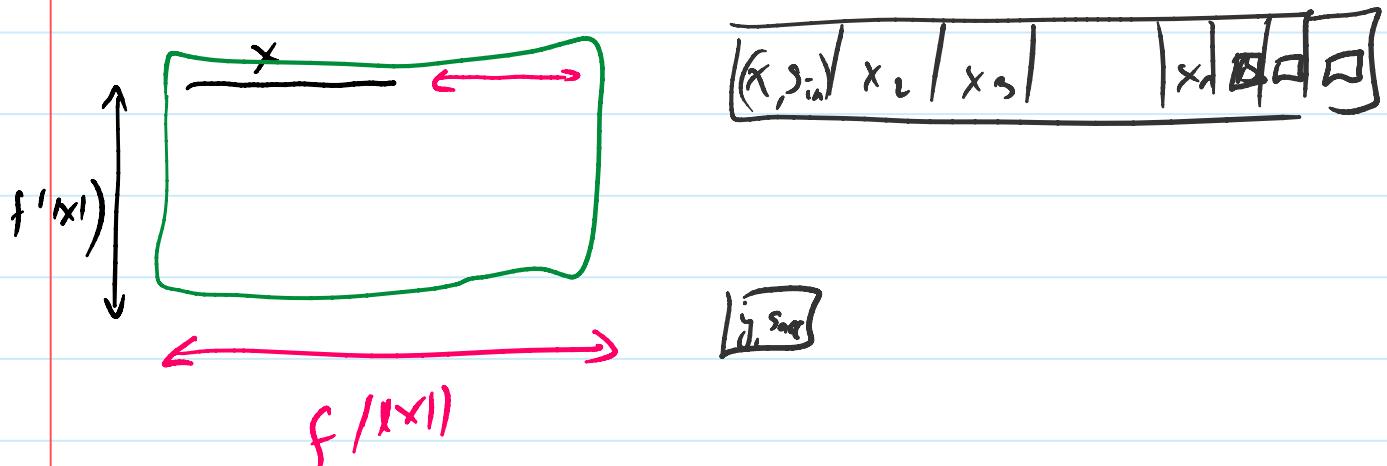
$f(x) \in P^1 / X_1$  posă

Vream

$L(M) \leq_m^P \text{SAT}$

$x \in \Sigma^*$   $\xrightarrow{\text{a.i.}} \phi_{f(x)}$  formulă logică

$m(x)$  acceptă  $\Leftrightarrow \phi_{f(x)}$  satisfăcătoare



Pp M dacă acceptă atunci copia ei e pe prima poziție

$x \in L(M) \Leftrightarrow \exists T_x$  a.i.

(1)  $T$  pe prima linie codifică  $M(x)$  în starean initială

(2)  $T$  pe ultima linie codifică  $M(x)$  acceptat

(3)  $T$  pe linii consecutive codifică o mișcare

legată a lui M

conform lui  $\delta_M$

Vream forma logică  $\Phi_{f(x)}$   
care trăduce existența lui  $T_x$   
în logică

$$\Phi_{f(x)} = \underbrace{\Phi_{f(x)}^{(1)}}_{\text{}} \wedge \underbrace{\Phi_{f(x)}^{(2)}}_{\text{}} \wedge \underbrace{\Phi_{f(x)}^{(3)}}_{\text{}}$$

$$\Phi'_{f(x)} = \bigwedge \underbrace{\Phi_{f(x),i}}_{\text{variable separate}} \rightarrow \text{cu } \underline{\text{variable}} \underline{\text{separate}}$$

↓  
casuți de pe linie.

$\leq 2^k$

$$\Phi_{f(x),i} (y_1, y_2, \dots, y_k)$$

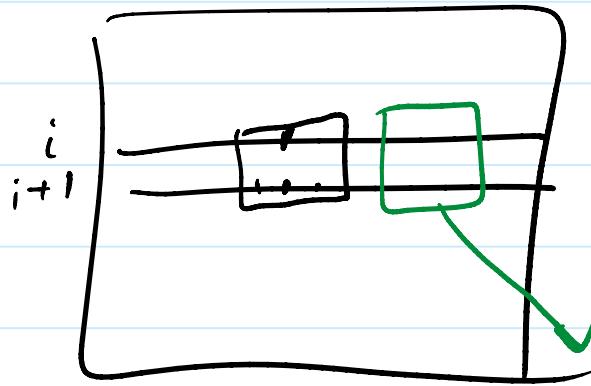
b. tri codificare

$$\Phi_{f(x),i} \quad \boxed{x_1 \\ \text{simt}}$$

$$\{ \overline{y}_1, \overline{y}_2, \dots, \overline{y}_k \}$$

0..0

$$\Phi_{g(x)}^3 = \bigwedge \underbrace{\Phi_{g(x),i}^{(3)}}_{\text{casuți}}$$



$$\psi_i: C_i \xrightarrow{\delta} C_{i+1}$$



$$\underline{\underline{C}} = C$$

$$\left( \begin{array}{c} \nearrow \\ \dots \end{array} \right) = \phi_{f(x)}^{(2)}$$