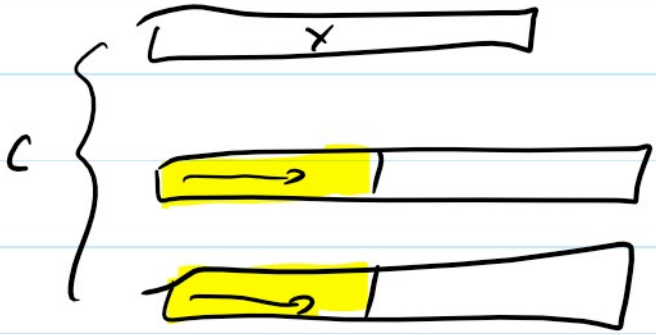
CURS #13

Tuesday, January 17, 2023 1:47 PM

$$PSPACE = \{ A \mid \text{exists a M.T } M \text{ a.i. } L(M) = A \text{ si } \forall x \; space_M(x) = O(|x|^k) \; k > 0 \}$$

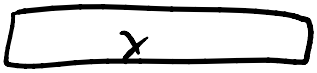


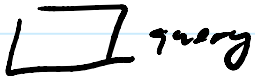
$space_M(C) =$

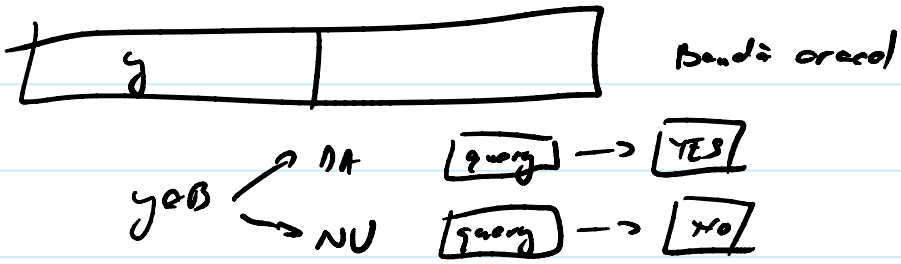
(T) $P \subseteq PSPACE$

$P \subseteq \frac{NP}{co\text{-}NP} \subseteq \Sigma_2^P \cap \Pi_2^P$ $\quad PH \subseteq PSPACE$

$\Sigma_2^P = \{ A \mid$ există o NDTM M și un BCNP a.i. $A = L(M; B) \}$







simulez oracolul on M_1

simulez mașina M on M_2

spațiul$_M(x)$ $\longrightarrow$ spațiul$_{M_1}$

$\longrightarrow$ spațiul$_{M_2}(x)$

PSPACE $\stackrel{?}{=}$ NPSPACE ??

Răspuns NPSPACE = PSPACE

Motiv

Motiv

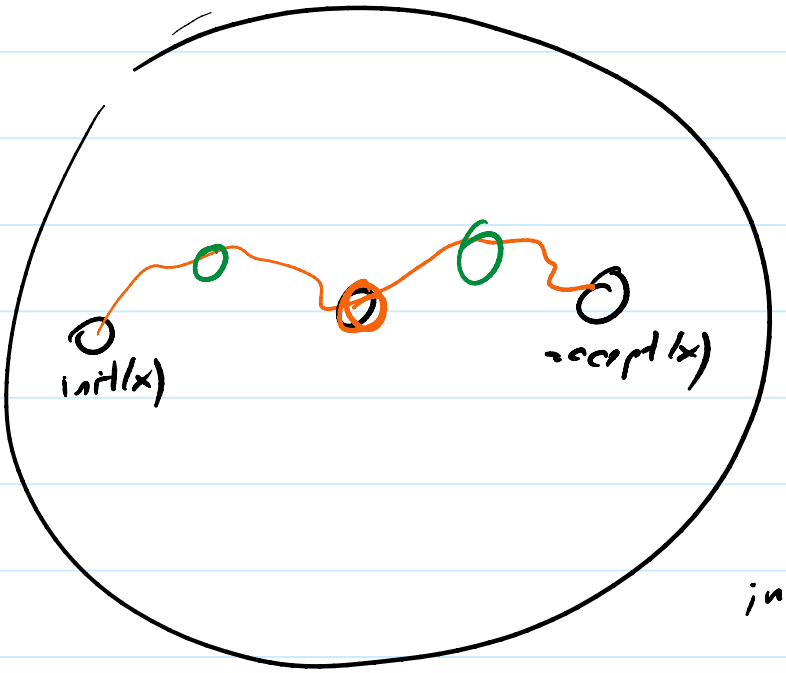
(T) (SAVITCH) Fie A o problemă de decizie care poate fi rez. de o mașină Turing nedet care pe x folosește spațiu $\leq s(|x|)$

$\Downarrow$

există o M.T deterministă M' care decide A și $M'(x)$ folosește spațiu $\leq s^2(|x|)$

IDEE DEM

Graful orientat al config mașinii $M(x)$



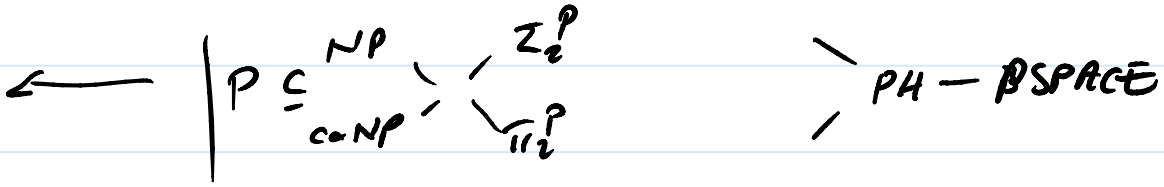
$|V| = O(c^{s(x)})$

$init(x) \to accept(x)$?

$init(x) \to y$

$y \to accept(x)$

Alg are complexitate spațiu $O((s(x))^2)$



$L \subseteq NL$

$\updownarrow$

$LogSpace = \{A \mid \exists$ M.T M a.i. $\forall x$

$space(M(x)) = O(\log |x|)$

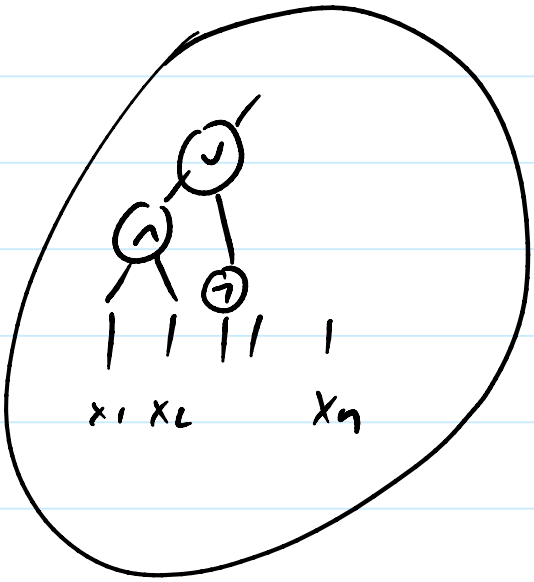
$A \mid \exists$ M.T nondeterministe M a.i. $M = L(A)$

$\forall x \; spatiu_M(x) = O(\log |x|)$

$\underline{S.T\,conn} = \{(G, a, b) \mid$ există un drum p în G de la a la $b\}$

a ␣ b

Circuite booleene



Nu se cunoaște o funcție booleană $f_n : \{0,1\}^n \to \{0,1\}$ care să se necesite un circuit boolean cu $\geq n^2$ porți

$\underbrace{\quad}_{5n}$

$$PARITY_n(x_1 \dots x_n) = \begin{cases} 1 & x_1 \oplus x_2 \dots \oplus x_n = 1 \\ 0 & x_1 \oplus \dots \oplus x_n = 0 \end{cases}$$

(T) Nu putem calcula $PARITY_n$ cu circuite booleene cu:

- adâncimea unui circuit $\in k$
- # porți $\in poly(n)$
- chiar dacă dăm voie $\wedge$, $\vee$ de orice aritate.

k ⟺

$+ MOD_6$

$$MOD(x_1 \dots x_n) = \begin{cases} 1 & \sum x_i \equiv 0 \pmod 6 \\ 0 & altfel \end{cases}$$

$maj(x_1, \ldots x_n) = \begin{cases} 1 & \text{dacă} \\ 0 & \text{altfel} \end{cases}$

↓

Nu știm că astfel de circuite booleene nu pot calcula QDF

Unde se aplică complexitatea?

(1) Criptografie