12/10/21

$$NPSPACE = coNPSPACE$$

$$NL = NSPACE(\log n)$$

$$coNL = \{ L \mid \bar{L} \in NL \}$$

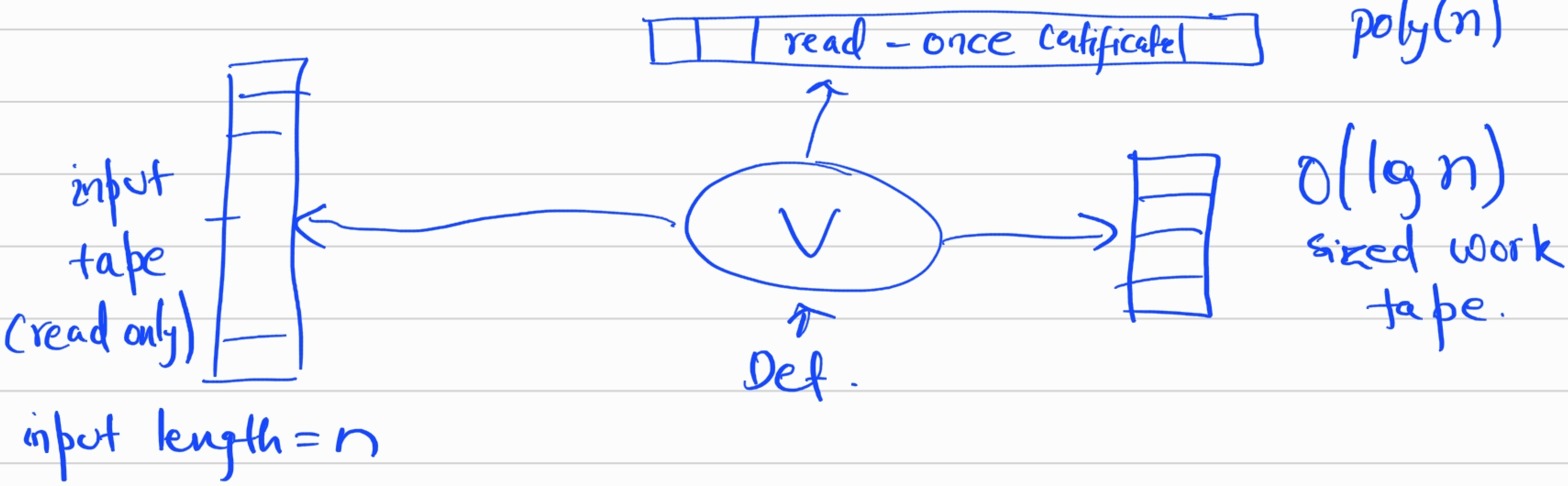
"Scaled down" $NL = coNL$?

Thm: [Immerman – Szelepcsényi] (1988) $NL = coNL$.

$REACH := \{ \langle G, s, t \rangle \mid$ if $\exists$ a path from s to t in G $\}$

Thm: REACH is NL-complete.

Defn:- (Alternative defn of NL):



Implication of $NL = coNL$

$REACH \in coNL \Rightarrow \overline{REACH} \in NL$

$\overline{REACH} := \{ \langle G, s, t \rangle \mid \nexists$ a path from s to t in digraph G $\}$

Thm: $\overline{REACH} \in NL$.

Proof:- $R_k := \{ v \in G \mid v$ is reachable from s in at most k steps$\}$

$0 \le k \le n$

Define : $|R_k| := r_k$

$|R_0| = 1$; $R_0 = \{s\}$

overview of the certificate. $n \times n^4 + n^3 \le O(n^5)$

Cert. for r_1	Cert. for r_2	- - - -	Cert. for r_n	Cert. for $t \notin R_n$

Case 1: Suppose the verifier knows r_n. then let us build a certificate for $t \notin R_n$

Cert. that $s \rightsquigarrow \#1$	Cert. that $s \rightsquigarrow \#3$	-	- . .	. .	Cert. that $s \rightsquigarrow \#n-1$

Cert for $s \rightsquigarrow \#L$

Verifier Checks

(1) individual certificates are valid.
(2) that it has got r_n certificates
(3) $t \notin$ this list of r_n vertices

$\Big\}$ $O(\lg n)$ space.

(4) certificates are ordered. w.r.t vertices$\}$ $O(\log n)$

$\{1, 3, 7, 10\}$

$\underline{1}, \underline{3}, \underline{7}, \underline{10},$

$r_n \le n$

$|\text{path}| \le n$

each path requires $\le n^2$

Case 2:- Suppose the verifier knows r_i then build a certificate for r_{i+1}

$\boxed{\text{Certify that } \#1 \in R_{i+1}}$ $\boxed{\text{Certify } \#2 \notin R_{i+1}}$ $\boxed{\text{Certify } \#3 \in R_{i+1}}$

↑easy ↑easy

- - - - - $\boxed{\text{certify } \#n \notin R_{i+1}}$

$n \times \max\{n^2, n^3\} \leq n^4$

$\#1 \in R_{i+1} \rightarrow$ give a path of length at most $i+1$ from s.

$\#2 \notin R_{i+1}$: certify all r_i vertices in R_i

$\boxed{\text{Certify } s \rightsquigarrow \#3 \text{ in } i \text{ steps}}$ · $\boxed{\text{Certify } \#5 \in R_i}$ · · · · · · $\boxed{\text{Certify } \#n\text{-}2 \in R_i}$

↑ ↑ ↑

$r_i \times n^2 \leq n^3$

Verifier Checks:

(1) validity of each certificate

(2) Keep a count of the no. of certificates

(3) Certificates are in increasing order w.r.t. vertices

(4) #2 doesn't belong to the given list.

and no neighbor of #2 is in the list

Check that no vertex in the list has an edge to #2.

Overall keep a count of vertices that belong to R_{i+1}

$\boxtimes$

"Inductive counting"

This Shows $\overline{REACH} \in NL$

$\Rightarrow NL = co\text{-}NL$

"Scale up"

$\hookrightarrow \quad NSPACE(f(n)) = co\text{-}NSPACE(f(n))$

for all $f(n) \geq \log n$

$$NPSPACE = co\text{-}NPSPACE.$$

$$L \subseteq NL \subseteq P \subseteq NP \subseteq PSPACE = NPSPACE \subseteq EXP$$

$$EXP = \bigcup_{k \geq 0} 2^{O(n^k)}$$

$P \subsetneq EXP$

$L \subsetneq PSPACE$

$\rightarrow$ POLYNOMIAL HIERARCHY

$QBF := \exists x_1 \forall x_2 \exists x_3 \cdots \forall x_n \, \varphi(x_1, \ldots, x_n)$

# of quantifier alternations is polynomial in n.

NP := $L \in NP$ if $\exists$ a det. TM V and a polynomial p s.t. for all $x \in \{0,1\}^*$

$$x \in L \iff \exists\, u \in \{0,1\}^{p(|x|)} \text{ s.t. } V(x,u) = 1$$

$$coNP := \{ L \mid \overline{L} \in NP \}$$

$$y \in \overline{L} \iff \exists\, u \in \{0,1\}^{p(|y|)} \text{ s.t. } V(y,u) = 1$$

$$y \in L \iff \forall\, u \in \{0,1\}^{p(|y|)}\ V(y,u) = 0$$

Clique $:= \{ \langle G, k \rangle \mid G$ has a clique of size $\geq k \}$

Tautology $:= \{ \langle \varphi \rangle \mid \varphi$ is tautology$\}$

Clique $\in$ NP & Tautology $\in$ coNP

EXACT-CLIQUE $:= \{ \langle G, k \rangle \mid$ size of the largest Clique in $G = k \}$

Exact-Clique $\in NP$? Exact-Clique $\in$ Co-NP?

Minimum-Ckt-Size $:= \{ \langle C \rangle \mid C$ is the smallest ckt representing the function f computed by $C \}$

Min-Ckt-Size $\in NP$? Min-Ckt-Size $\in$ Co-NP?

Exact-Clique : $\exists\, S \subseteq V$ s.t. $|S| = k$

$\forall\, S' \subseteq V$ s.t. $|S'| \geq k+1$

S is a clique and

S' is not a clique.

Min-Ckt-Size : $\forall\, C'$ s.t. $\text{size}(C') < \text{size}(C)$

$\exists\, x$ s.t. $C'(x) \neq C(x)$.

Defn:- (Σ_2^P / Σ_2) $L \subseteq \{0,1\}^*$

$L \in \Sigma_2$ if $\exists$ a poly-time verifier V and a polynomial $p(\cdot)$ s.t. $\forall x \in \{0,1\}^*$

$$x \in L \iff \exists\, u_1 \in \{0,1\}^{p(|x|)} \ \forall\, u_2 \in \{0,1\}^{p(|x|)}$$

$$V(x, u_1, u_2) = 1$$

Defn. (Π_2^p / Π_2) $\forall \ \exists$