$coNL = \{ A : \neg A \in NL \}$

$$NL \stackrel{?}{=} coNL$$

$\neg PATH = \{ (G, s, t) : \exists$ no path in G from s to $t \}$

$\downarrow$

coNL-complete (same reduction used to show PATH ∈ NL-Complete works here)

Thm [Immerman - Szelepscenyi] $\neg PATH \in NL$ $(\Rightarrow NL = coNL)$

Certificate Definition for NL

A language $A \subseteq \Sigma^*$ is in NL if $\exists$ a DTM M with access to an additional read-once input tape and a polynomial $p: \mathbb{N} \to \mathbb{N}$ s.t. $\forall x \in \Sigma^*$

$$x \in A \iff \exists u \in \Sigma^{p(|x|)} \text{ s.t. } M \text{ accepts } (x, u)$$

x: placed on M's i/p tape

u: placed on M's read-once input tape

M runs using $O(\log |x|)$ space

Proof of Immerman-Szelepscenyi Theorem

(G,s,t) : "yes" instance of $\neg$PATH.
We construct a read-once certificate for (G,s,t).

$n = |V(G)|$

R_i : set of vertices reachable from s in $\leq i$ steps

$R_0 = \{s\}$ $\quad$ R_n = set of all vertices reachable from s.

Certificate for $(G,s,t) \in \neg$PATH : $t \notin R_n$.

Proof uses 2 procedures

1. Certifying $v \notin R_i$ given $|R_i|$.
2. Certifying $|R_i| = r$ given $|R_{i-1}|$.

① Certifying $v \notin R_i$ given $|R_i|$

Vertices of G labelled $1, 2, \ldots, n$

$\forall u \in R_i$ C_u: certificate $u \in R_i$

Certificate for $v \notin R_i$: $C_{u_1}, C_{u_2}, \ldots, C_{u_{|R_i|}}$

C_u: a sequence of $\leq i+1$ vertices starting with s & ending with u

$u_1, u_2, \ldots, u_{|R_i|}$: ascending order of their labels

Doable in $\log n$ space.

Read C_{u_i}, verify that it encodes a path of length $\leq i$ from s to u

Verify that $u_i \neq v$

If $v \notin R_i$, then certificate will be accepted.

If $v \in R_i$, then $\nexists$ $|R_i|$ many certificates $C_{u_1}, \ldots, C_{|R_i|}$ s.t. $u_1 < u_2 < \cdots < u_{|R_i|}$ & $v \neq u_i$ $\forall i$.

(2) Certifying $|R_i| = r$ given $|R_{i-1}|$

Certifying $v \notin R_i$ given $|R_{i-1}|$.

Similar to (1).

Certificate : list of $|R_{i-1}|$ certificates for every $u \in R_{i-1}$, in ascending order.

In addition to verifying that $v \notin R_i$, we also need to verify that no neighbors of v has a certificate.

w s.t. $(w, v) \in E(G)$.

For every vertex $v \in V(G)$, if $v \in R_i$, $\exists$ a certificate for this fact; if $v \notin R_i$, given $|R_{i-1}|$, $\exists$ a certificate.

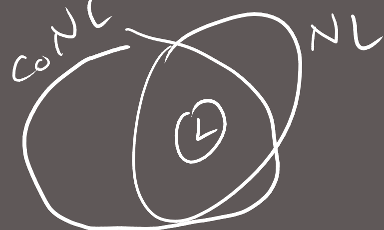
Certificate : $C_1^i, C_2^i, C_3^i, \dots, C_n^i$

$$C_j^i : \begin{cases} \overbrace{\text{certificate that } j \in R_i}^{\text{type (i)}} & \text{if } j \in R_i \\ \underbrace{\text{certificate that } j \notin R_i \text{ given } |R_{i-1}|}_{\text{type (ii)}} & \text{if } j \notin R_i \end{cases}$$

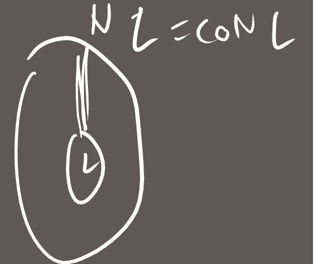
Verification : → each C_j^i is correct &

→ no. of type-(i) certificates $= r$.

Combining (1) & (2)



$R_0 = \{s\}$ $|R_0|, |R_1|, \dots, |R_n|$



Use (1) to certify that $t \notin R_n$.