Last time:
- finish PSPACE-completeness of QSAT
- PSPACE & 2-player games
- Generalized Geography is PSPACE-complete

Today:
- Last part of space unit:

  Immerman-Szelepcsényi thm: nondet space is closed under complement

  ↳ NL = co-NL

  AB 4.3.2, Sipser 8.6, Papad. 7.3, Cai 3.3

- Start randomized computation unit   Cai: 5.1

  ~~(probability basics)~~

  ↳ read ; ↳ tail bounds, poly. id. testing

Questions?

Recall: • det class $\mathcal{C}$ (P, L, EXP) closed under compl: $\mathcal{C} = \text{co-}\mathcal{C}$

• we don't think, in general, time classes are : we expect $NP \neq \text{co-}NP$, etc.

☆ Nondet space classes are closed under compl.!

Thm: (Immerman-Szelepcsényi '87, '88)

Let $f(n) \geq \log n$ be a p.c.f.

Then $NSPACE(f(n)) = \text{co-}NSPACE(f(n))$.

(Cor: $NL = \text{co-}NL$.)

Pf: Fix $L \in NSPACE(f(n))$.

Let M be $f(n)$-space NTM deciding L.

We'll design a NTM, N, running in $O(f(n))$ space, s.t. $\forall x$, N acc. x (on some path) iff M rej x (on every path). (so N acc $\bar{L}$).

→ So N should acc x iff $G_{M,x}$ is a NO inst. of REACH.

Setup: (So M's runtime on x is $\leq m$.)

Fix $|x| = n$.

\# configs of M on x is at most $m := c^{f(n)}$.

Let s = init config of M on x,

" t = ! final " " " " ".

→ Let $\ell :=$ \# configs in $G_{M,x}$ that are reachable from s.

First: describe how an NTM that's given ℓ as input can correctly determine whether M rej. x on every path.

Like this:

- set $r = 0$ (counter of \# nodes reachable from s)

- For every config c of M on x <u>besides t</u>:
    - guess whether $\exists$ comput. path (length $\leq m$) in $G_{M,x}$ from s to c; if guess Y, guess + verify the path.
    - if succ. confirmed c reachable from s: increm. r. ($r \leftarrow r+1$)
- If $r = \ell$ accept, o/w reject.

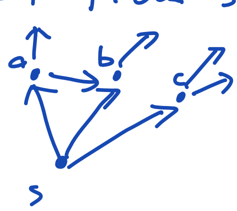
$O(f(n))$ space.

Machine acc. iff its guesses proved that there are ℓ (non-t) reachable nodes; all other nodes, incl. t, are non-reachable. So this nondet alg has an accept path iff t not reachable from s.

? our machine will have some branch giving right value for ℓ; all other branches will reject. :)

Remains to show how to nondet. compute ℓ.
"Inductive counting" (ℓ = # configs in $G_{M,x}$ that are reachable from s.)

For $i = [m]$, let A_i = set of all configs at dist. $\leq i$ from s in $G_{M,x}$. So $A_0 = \{s\}$,



$A_1 = \{s, a, b, c\}$, etc.

Have $A_0 \subseteq A_1 \subseteq A_2 \subseteq \dots$

+ A_m = all configs reachable from s; $|A_m| = \ell$.
$|A_0| = 1$:)

Here's nondet procedure to compute $|A_{i+1}|$ given $|A_i|$
(some path gets it right, all others reject):

similar to before

<u>Outer loop:</u>

- Go over all configs c, for each one decide if in A_{i+1}, keep count of # that are in A_{i+1}.

Here's how we decide, for a given config c, if it's in A_{i+1}:

<u>Inner loop:</u>

- Loop over all config. c'.

For each c', guess whether $c' \in A_i$; if guess Y, guess s-to-c' path of length $\leq i$; if confirmed succ. that c' is in A_i, check (det) that $c' \to c$ edge is in $G_{M,x}$; if Y, know (decide) c is in A_{i+1}.

While doing this, keep count of # config c' that we verified to be in A_i.

At end of inner loop: if # configs that

were verified as being in A_i is $\neq$ (must be $<$) actual $|A_i|$, we missed some elt of A_i + reject on this path.

If # config we is $= |A_i|$ + c wasn't found to be reachable from any $c' \in A_i$, then decide c not in A_{i+1}. (end of inner loop)

That's it !!

End of space unit!

New unit: Randomness in Computing

Rand. comput: alg can make rand. choices. Like nondet, but realistic b/c of diff. crit. for success:

NTM acc. if ANY path accepts;

rand. TM " " most "s accept.

Why is rand. useful? Confer unpredictability. Can view alg. design as adversarial scenario:

given a fixed alg, may be some adversarial alg.

A randomized alg: there is no fixed alg; can potentially help thwart adversarial inputs.

We'll assume knowledge of basics of probability:

- Sample space S, probabilistic experiment
- dist $\mathcal{D}$ over S. $\Pr[s]$ $\Pr_{\mathcal{D}}[s]$
- Events. $A \subseteq S$ $\bar{A}$ = complem. of A
- Compound events: $A \wedge B$
- $\Pr[A \wedge B] = \Pr[A] \cdot \underbrace{\Pr[B|A]}_{\text{condit. prob.}}$
- $\Pr[A] \leq \Pr[B] + \Pr[A|\bar{B}]$
- Independence:

$$\Pr[A \wedge B] = \Pr[A] \cdot \Pr[B]$$

- Random variables $X: S \to \mathbb{R}$
- Expectation $\mathbb{E}[X] = \sum_{s \in S} X(s)\,\mathcal{D}(s)$

$$= \sum_a a \cdot \Pr[X=a]$$

- Linearity of expectation:

  for any random vars X_1, X_2 (not necc. indep.!),

  $\mathbb{E}[X_1 + X_2] = \mathbb{E}[X_1] + \mathbb{E}[X_2]$.

Ex: $S = \{0,1\}^n$

$\mathcal{D} = $ unif over $\{0,1\}^n$

$X(s) = $ # 1's in s

$$\mathbb{E}[X] = \sum_{i=0}^{n} i \cdot Pr[i] = \sum_{i=0}^{n} i \cdot \frac{\binom{n}{i}}{2^n}$$

$X = X_1 + \dots + X_n$, $X_i = \begin{cases} 1 & \text{if } i^{th} \text{ bit} = 1 \\ 0 & \text{"} \quad = 0 \end{cases}$

$$\mathbb{E}[X] = \underbrace{\mathbb{E}[X_1] + \dots + \mathbb{E}[X_n]}_{} = \frac{1}{2} \cdot n .$$

Next time:
- tail bds
- rand algs.
