DD2445 COMPLEXITY THEORY: LECTURE 7

LAST WEEK

- Space complexity (measure work space only – input on read-only tape)
- TQBF true quantified Boolean formulas PSPACE-complete
- PSPACE = NPSPACE
- Can simulate nondeterminism with quadratic blow-up in space
- Very important concept CONFIGURATION GRAPH $G_{M,x}$
- Logarithmic space: L and NL
- PATH = $\{ \langle G, s, t \rangle \mid \exists$ path $s \rightsquigarrow t$ in digraph $G \}$ NL-complete. Don't know if PATH $\in$ L
- Some care needed with logarithmic space
  - Reductions computed bit by bit (must <u>not</u> be stronger than cplx class reduced to)
  - In verifier-style definition of NL, witness is only <u>read-once</u> (why didn't we worry about this for NP?)
- End of last lecture: NL = co-NL plus sketch of proof

Prove $NL = coNL$ by showing $\overline{PATH} \in NL$ IS I

Construct readonce certificate (or show how NL-machine can guess successfully

Yes-instance

$\langle G, s, t \rangle \qquad s \not\rightsquigarrow t \qquad n = |V(G)|$

Reminder

$\boxed{R(i)}$ = { vertices reachable from s in $\leq i$ steps }

$$s \not\rightsquigarrow t \iff t \notin R(\infty) \iff t \notin R(n)$$

Idea

Compute $R(0) = \{s\}, R(1), R(2), \ldots, R(n-1), R(n)$

Show $t \notin R(n)$

Problem

We cannot remember $R(i)$ in log space

Only $|R(i)|$

Solution

Amazingly, this is enough!

Three subcertificates (that will be combined)

$\boxed{\text{IsMember}(v, i)}$ = "$v \in R(i)$"

Just list path of length $i' \leq i$

$\boxed{\text{MembershipExpansion}(i, r, r')}$ = "$|R(i-1)| = r \Rightarrow |R(i)| = r'$"

$\boxed{\text{ListMembers}(i, r)}$ = List of r elements in $R(i)$ in increasing order, each with IsMember certificate

Full certificate:

$$\boxed{\begin{array}{l}
\text{MembershipExpansion}(1, 1, r_1) \\
\text{MembershipExpansion}(2, r_1, r_2) \\
\text{MembershipExpansion}(3, r_2, r_3) \\
\quad\vdots \\
\text{MembershipExpansion}(n, r_{n-1}, r_n) \\
\text{ListMembers}(n, r_n)
\end{array}}$$

Verification

Check that r_i is correct, keeping r_{i-1} in memory ($\log n$ space for counters) for $i = 1, 2, \ldots, n$

Finally check that t is not listed in ListMembers(n, r_n)

Done!

ISMEMBER and LISTMEMBER are clear.

MEMBERSHIPEXPANSION (i, r, r')

We already know $|R(i-1)| = r$ (by assumption)

Give subcertificates for all vertices $j = 1, 2, \ldots, n$ in increasing order

(a) $j \in R(i)$

$\boxed{j : \text{ISMEMBER}(j, i)}$ proves this

increment r' by one.

(b) $j \notin R(i)$

$\boxed{j : \text{LISTMEMBERS}(i-1, r)}$

Go over list

For every member u, check

(i) $u \neq j$

(ii) u does not have edge to j

Check that list contained r distinct elements *

After having verified all subcertificates, we know $r = |R(i)|$.

But note that for every single $j \in R(i)$, the same long certificate LISTMEMBERS$(i-1, r')$ is repeated over and over again...

Extremely wasteful.

---

* How? Can't remember the list! No, but

a) we can count #elements seen / know

b) if in increasing order, then all different.

Summing up:

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

Some inclusions <u>must</u> be strict

[since $L \subsetneq PSPACE$ (space hierarchy theorem)

$P \subsetneq EXP$ (time hierarchy theorem)]

But we don't know which

Probably most of them, or maybe even all...

What lies between P and PSPACE? | PH I

Next we will explore
- natural complete problems (seemingly) in between
- stronger version of $P \neq NP$ hypothesis

Let F CNF formula; α assignment

<u>CNF EVAL</u> $= \{ \langle F, \alpha \rangle \mid F(\alpha) = 1 \}$

In P

<u>CNF SAT</u> $= \{ F \mid \exists \alpha \text{ s.t. } F(\alpha) = 1 \}$

NP-complete

<u>MIN CNF SIZE</u> $= \{ (F, S) \mid \exists$ CNF formula F' of size $\leq S$ s.t. $F' \equiv F \}$

$F' \equiv F$ equivalence: same value for all α

Two quantifiers
1) $\exists$ CNF formula F'
2) $\forall$ assignments α $F'(\alpha) = F(\alpha)$

Could MIN CNF SIZE be in NP?

To verify yes-instance, would need to check $F' \equiv F$

How to do this efficiently?

For no-instance of $F' \equiv F'$
$\exists$ concise, easily verifiable witness:

Assignment α s.t. $F'(\alpha) \neq F(\alpha)$

I.e., coNP-problem

Can solve MinCNFSize decision problem by

a) Guessing formula F' NP-problem
b) Checking if $F' \equiv F$ coNP-problem

<u>DEF</u> $\boxed{\Sigma_2^P}$ set of all languages L for which exists poly-time TM M and polynomial q such that

$$x \in L$$
$$\Updownarrow$$
$$\exists u \in \{0,1\}^{q(|x|)} \; \forall v \in \{0,1\}^{q(|x|)} \quad M(x,u,v) = 1$$

(As before, don't need to insist on strings of <u>exactly</u> length $q(|x|)$)

Observe: Σ_2^P contains both

- NP (use u, ignore v)
- coNP (ignore u, use v)

Can go further and define the POLYNOMIAL HIERARCHY

DEF Fix $i \in \mathbb{N}^+$

A language L is in $\boxed{\Sigma_i^P}$ if
$\exists$ deterministic poly-time TM M
$\exists$ polynomial q
such that

$$x \in L$$
$$\Updownarrow$$
$$\exists u_1 \forall u_2 \exists u_3 \cdots Q_i u_i \quad M(x, u_1, u_2, u_3, \ldots, u_i) = 1$$

where all $u_i \in \{0,1\}^{q(|x|)}$
$Q_i = \exists$ for i odd, $\forall$ for i even

Polynomial hierarchy

$$\boxed{PH} = \bigcup_{i=1}^{\infty} \Sigma_i^P$$

$$\Pi_i^P = co\Sigma_i^P = \{ L \mid \overline{L} \in \Sigma_i^P \}$$

Some observations:

- $\Sigma_i^P \subseteq \Pi_{i+1}^P \subseteq \Sigma_{i+2}^P \subseteq \ldots$
- Hence $PH = \bigcup_{i=1}^{\infty} \Pi_i^P$
- $\Sigma_1^P = NP \qquad \Pi_1^P = coNP$

Many natural problems at 2nd level of hierarchy (Σ_i^2 & Π_i^2) PH IV

Higher up it gets a bit sparser

Survey "Completeness in the Polynomial-Time Hierarchy – A Compendium" by Schaefer & Umans

Complete problems do exist, though

Σ_i SAT $\exists u_1 \forall u_2 \exists u_3 \cdots Q_i u_i \; \varphi(u_1, u_2, u_3, \ldots, u_i)$

Π_i SAT $\forall u_1 \exists u_2 \forall u_3 \cdots Q_i u_i \; \varphi(u_1, u_2, u_3, \ldots, u_i)$

u_i vectors/sets of variables

φ Boolean formula

Say
φ CNF if innermost $Q = \exists$
φ DNF if innermost $Q = \forall$

(Why?) Will get back to formal definition

Common belief (& kind of assumption for this course):

$P \neq NP$ $\qquad$ $NP \neq coNP$

But we can go further

Is it true that
$$\Sigma_1^P \subsetneq \Sigma_2^P \subsetneq \Sigma_3^P \subsetneq \Sigma_4^P \subsetneq \cdots \ ?$$

Is it true that "the polynomial hierarchy doesn't collapse"?

Don't know, but widely believed
Standard assumption in complexity theory

THM

1. For every $i \in \mathbb{N}^+$ it holds that if $\Sigma_i^P = \Pi_i^P$, then $PH = \Sigma_i^P$ ("the polynomial hierarchy collapses to the ith level")

2. If $P = NP$, then $PH = P$ ("the polynomial hierarchy collapses to P")

Many complexity theory results have form:

Unless <statement we believe to be true> holds, then PH collapses to the ith level

Smaller $i \Longrightarrow$ stronger result

WILL SOON SEE (WHEN TALKING ABOUT CIRCUITS)

Ex NP has poly-size circuits $\Longrightarrow$ PH collapses to 2nd level

(so we don't believe $NP \subseteq P/poly$)

Proof

1. Might end up on a problem set near you

2. Prove by induction:

If $P = NP$, then $\Sigma_i^P = \Pi_i^P = P$

Base case ($i=1$): Nothing to prove

By assumption $P = NP$

$coNP = coP = P$ (P closed under complement)

Induction step Suppose $\Sigma_{i-1}^P = P = \Pi_{i-1}^P$

By definition $\Pi_{i-1}^P \subseteq \Sigma_i^P$ so $P \subseteq \Sigma_i^P$

Enough to prove $\Sigma_i^P \subseteq P$. Then $P = \Sigma_i^P$ and we can take complements to get $P = \Pi_i^P$.

Consider $L \in \Sigma_i^P$. Want to show $L \in P$

By def, $\exists$ poly-time TM M and poly q such that

$x \in L \iff \exists u_1 \forall u_2 \cdots Q_i u_i \; M(x, u_1, \dots, u_i) = 1$

for $u_i \in \{0,1\}^{q(|x|)}$

Define L' by

$\langle x, u_1 \rangle \in L' \iff \forall u_2 \exists u_3 \cdots Q_i u_i \; \{M(x, u_1, u_2, \dots, u_i)$

By syntactic pattern matching $L' \in \Pi_{i-1}^P$

By inductive hypothesis $\Pi_{i-1}^P = P$

I.e., $\exists$ poly-time TM M' deciding L'

That is,

$$(x, u_1) \in L' \iff M'(x, u_1) = 1$$

But then

$$x \in L \iff \exists u_1 \; M'(x, u_1) = 1$$

so $L \in NP$

By induction hypothesis, $L \in NP = P$.
Since $L \in \Sigma_i^P$ was arbitrary, $\Sigma_i^P \subseteq P$, QED $\blacksquare$

DEF Language $L \subseteq \{0,1\}^*$ is Σ_i^P-complete if

- $L \in \Sigma_i^P$
- $\forall L' \in \Sigma_i^P$ it holds that $L' \leq_p L$

Π_i^P-complete languages and PH-complete languages defined analogously.

But: We believe PH is a class without complete languages

LEMMA PH does not have complete languages unless the hierarchy collapses

Proof Suppose $\exists$ PH-complete language L.
$PH = \bigcup_{i \in \mathbb{N}^+} \Sigma_i^P$, so $\exists i^*$ s.t. $L \in \Sigma_{i^*}^P$

But then every language in PH can be reduced to $L \in \Sigma_i^P$ $\blacksquare$

COROLLARY PH $\subseteq$ PSPACE but PH $\neq$ PSPACE unless the polynomial hierarchy collapses.

Proof If $L \in$ PH, then there exists a poly-time TM M s.t. $x \in L$ iff

$$\exists u_1 \forall u_2 \exists u_3 \dots Q_i u_i \; M(x, u_1, u_2, \dots, u_i)$$

Do Cook-Levin-style reduction for M
Obtain QBF. Verifiable in PSPACE
(Or argue from first principles)

PSPACE has complete problems (TQBF, for instance). So if PSPACE = PH, PH has complete problems and the hierarchy collapses.

Complete problems for Σ_i^P

$$\Sigma_i \text{SAT} = \{ \psi \mid \psi = \exists u_1 \forall u_2 \exists u_3 \dots Q_i u_i \; \varphi(u_1, \dots, u_i) \}$$

where φ propositional formula

For Σ_{2i+1}SAT can let φ be CNF formula.

For Σ_{2i} SAT not (why? Good exercise.)

Π_iSAT defined similarly

(and φ can be CNF for i even)

Can choose to define
Innermost quantifier $\exists$ – φ CNF $\quad \forall$ – φ DNF