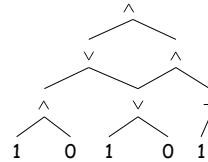


CS151 Complexity Theory

Lecture 3
April 7, 2009

Time and Space

- Can we evaluate an n node Boolean **circuit** using $O(\log n)$ space?



April 7, 2009

2

Relationships between classes

- So far:
 - $L \subseteq P \subseteq PSPACE \subseteq EXP$
- believe all containments strict
- know $L \subsetneq PSPACE$, $P \subsetneq EXP$
- even before any mention of NP, two **major** unsolved problems:

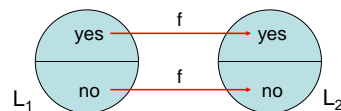
$$L \stackrel{?}{=} P \quad P \stackrel{?}{=} PSPACE$$

April 7, 2009

3

A P-complete problem

- We don't know how to prove $L \neq P$
- But, can identify problems in P **least likely** to be in L using P -completeness.
- need stronger notion of reduction (why?)



April 7, 2009

4

A P-complete problem

- logspace reduction**: f computable by TM that uses $O(\log n)$ space
 - denoted " $L_1 \leq_L L_2$ "
- If L_2 is P -complete, then $L_2 \in L$ implies $L = P$ (homework problem)

April 7, 2009

5

A P-complete problem

- Circuit Value (CVAL)**: given a variable-free Boolean circuit (gates $\wedge, \vee, \neg, 0, 1$), does it output 1?

Theorem: CVAL is P -complete.

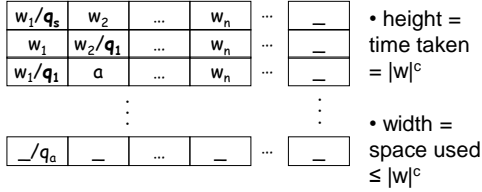
- Proof:
 - already argued in P
 - L arbitrary language in P , TM M decides L in n^c steps

April 7, 2009

6

A P-complete problem

- **Tableau** (configurations written in an array) for machine M on input w:

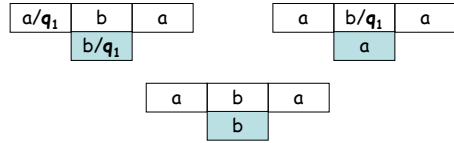


April 7, 2009

7

A P-complete problem

- Important observation: contents of cell in tableau determined by 3 others above it:

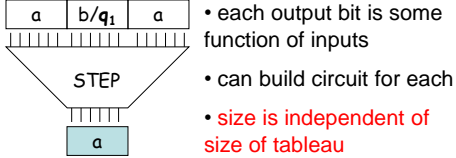


April 7, 2009

8

A P-complete problem

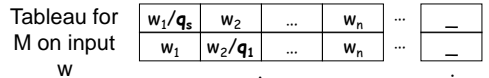
- Can build Boolean circuit STEP
 - input (binary encoding of) 3 cells
 - output (binary encoding of) 1 cell



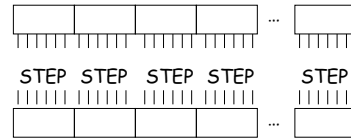
April 7, 2009

9

A P-complete problem



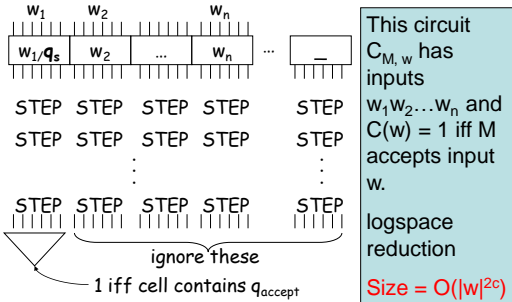
- $|w|^c$ copies of STEP compute row i from i-1



April 7, 2009

10

A P-complete problem



April 7, 2009

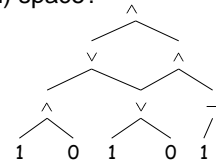
11

Answer to question

- Can we evaluate an n node Boolean circuit using $O(\log n)$ space?

- **NO!** (probably)

- CVAL in L if and only if $L = P$



April 7, 2009

12

Padding and succinctness

Two consequences of measuring running time as function of input length:

- “padding”
 - suppose $L \in \mathbf{EXP}$, and define

$$\text{PAD}_L = \{ x\#^N : x \in L, N = 2^{|x|^k} \}$$
 - TM that decides PAD_L : ensure suffix of N #s, ignore #s, then simulate TM that decides L
 - running time now polynomial !

April 7, 2009

13

Padding and succinctness

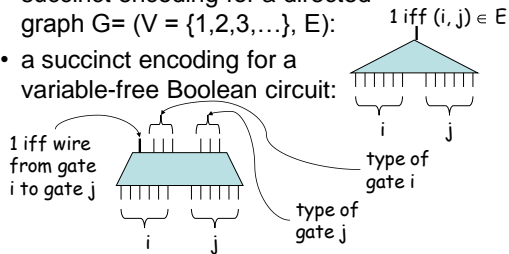
- converse (intuition only): “succinctness”
 - suppose L is **P-complete**
 - intuitively, some inputs are “hard” -- require full power of **P**
 - **SUCCINCT_L** has inputs encoded in different form than L , some exponentially shorter
 - if “hard” inputs are exponentially shorter, then candidate to be **EXP-complete**

April 7, 2009

14

Succinct encodings

- succinct encoding for a directed graph $G = (V = \{1, 2, 3, \dots\}, E)$:
 - 1 iff $(i, j) \in E$
- a succinct encoding for a variable-free Boolean circuit:



April 7, 2009

15

An EXP-complete problem

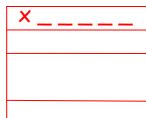
- **Succinct Circuit Value**: given a **succinctly encoded** variable-free Boolean circuit (gates $\wedge, \vee, \neg, 0, 1$), does it output 1?
- Theorem**: Succinct Circuit Value is **EXP-complete**.
- Proof:
 - in **EXP** (why?)
 - L arbitrary language in **EXP**, TM M decides L in 2^{n^k} steps

April 7, 2009

16

An EXP-complete problem

- **tableau** for input $x = x_1x_2x_3\dots x_n$:



height,
width 2^{n^k}

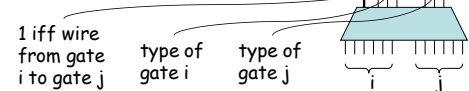
- Circuit C from CVAL reduction has size $O(2^{2^{n^k}})$.
- TM M accepts input x iff circuit outputs 1

April 7, 2009

17

An EXP-complete problem

- Can encode C succinctly:



- if i, j within single STEP circuit, easy to compute output
- if i, j between two STEP circuits, easy to compute output
- if one of i, j refers to input gates, consult x to compute output

April 7, 2009

18

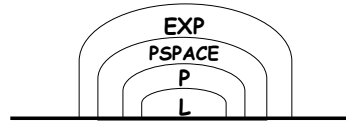
Summary

- Remaining TM details: big-oh necessary.
- First complexity classes:
 $L, P, PSPACE, EXP$
- First separations (via simulation and diagonalization):
 $P \neq EXP, L \neq PSPACE$
- First major open questions:
 $L \stackrel{?}{=} P \quad P \stackrel{?}{=} PSPACE$
- First complete problems:
 - CVAL is P-complete
 - Succinct CVAL is EXP-complete

April 7, 2009

19

Summary



April 7, 2009

20

Nondeterminism: introduction

A motivating question:

- Can computers replace mathematicians?

$L = \{ (x, 1^k) : \text{statement } x \text{ has a proof of length at most } k \}$

April 7, 2009

21

Nondeterminism: introduction

- Outline:
 - nondeterminism
 - nondeterministic time classes
 - NP, NP-completeness, P vs. NP
 - coNP
 - NTIME Hierarchy
 - Ladner's Theorem

April 7, 2009

22

Nondeterminism

- Recall deterministic TM
 - Q finite set of states
 - Σ alphabet including blank: “_”
 - $q_{\text{start}}, q_{\text{accept}}, q_{\text{reject}}$ in Q
 - transition function:
 $\delta : Q \times \Sigma \rightarrow Q \times \Sigma \times \{L, R, -\}$

April 7, 2009

23

Nondeterminism

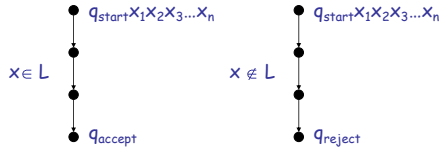
- **nondeterministic** Turing Machine:
 - Q finite set of states
 - Σ alphabet including blank: “_”
 - $q_{\text{start}}, q_{\text{accept}}, q_{\text{reject}}$ in Q
 - **transition relation**
 $\Delta \subset (Q \times \Sigma) \times (Q \times \Sigma \times \{L, R, -\})$
 - given current state and symbol scanned, several choices of what to do next.

April 7, 2009

24

Nondeterminism

- deterministic TM: given current configuration, unique next configuration

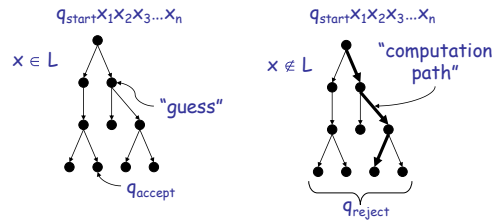


- nondeterministic TM: given current configuration, several possible next configurations

April 7, 2009

25

Nondeterminism



- asymmetric accept/reject criterion

April 7, 2009

26

Nondeterminism

- all paths terminate
- time used**: maximum length of paths from root
- space used**: maximum # of work tape squares touched on any path from root

April 7, 2009

27

Nondeterminism

- NTIME(f(n))** = languages decidable by a multi-tape NTM that runs for at most f(n) steps *on any computation path*, where n is the input length, and $f : \mathbf{N} \rightarrow \mathbf{N}$
- NSPACE(f(n))** = languages decidable by a multi-tape NTM that touches at most f(n) squares of its work tapes *along any computation path*, where n is the input length, and $f : \mathbf{N} \rightarrow \mathbf{N}$

April 7, 2009

28

Nondeterminism

- Focus on time classes first:

$$\mathbf{NP} = \cup_k \mathbf{NTIME}(n^k)$$

$$\mathbf{NEXP} = \cup_k \mathbf{NTIME}(2^{n^k})$$

April 7, 2009

29

Poly-time verifiers

Very useful alternative to NP: "witness" or "certificate"

Theorem: language L is in NP iff it is efficiently verifiable

$$L = \{ x \mid \exists y, |y| \leq |x|^k, (x, y) \in R \}$$

where R is a language in P.

- poly-time TM M_R deciding R is a "verifier"

April 7, 2009

30

Poly-time verifiers

- Example: 3SAT expressible as
 $3SAT = \{\varphi : \varphi \text{ is a 3-CNF formula for which } \exists \text{ assignment } A \text{ for which } (\varphi, A) \in R\}$
 $R = \{(\varphi, A) : A \text{ is a sat. assign. for } \varphi\}$
 - satisfying assignment A is a “witness” of the satisfiability of φ (it “certifies” satisfiability of φ)
 - R is decidable in poly-time

April 7, 2009

31

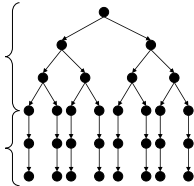
Poly-time verifiers

$$L = \{x \mid \exists y, |y| \leq |x|^k, (x, y) \in R\}$$

Proof: (\Leftarrow) give poly-time NTM deciding L

phase 1: “guess” y with $|x|^k$ nondeterministic steps

phase 2: decide if $(x, y) \in R$



April 7, 2009

32

Poly-time verifiers

Proof: (\Rightarrow) given $L \in NP$, describe L as:

$$L = \{x \mid \exists y, |y| \leq |x|^k, (x, y) \in R\}$$

- L is decided by NTM M running in time n^k
- define the language
 $R = \{(x, y) : y \text{ is an accepting computation history of } M \text{ on input } x\}$
 - check: accepting history has length $\leq |x|^k$
 - check: R is decidable in polynomial time
 - check: M accepts x iff $\exists y, |y| \leq |x|^k, (x, y) \in R$

April 7, 2009

33

Why NP?

problem requirements

stochastic model of

object we are seeking

- but, captures important computational feature of many problems:

exhaustive search works

- contains **huge** number of natural problems

efficient test: does y meet requirements?

- many problems have form:

$$L = \{x \mid \exists y \text{ s.t. } (x, y) \in R\}$$

April 7, 2009

34

Why NP?

- Why not **EXP**?
 - too strong!
 - important problems not complete.

April 7, 2009

35

Relationships between classes

- Easy: $P \subset NP$, $EXP \subset NEXP$
 - TM special case of NTM
- Recall: $L \in NP$ iff expressible as
 $L = \{x \mid \exists y, |y| \leq |x|^k, (x, y) \in R\}$
- $NP \subset PSPACE$ (try all possible y)
- The central question:

$$P \stackrel{?}{=} NP$$

finding a solution vs. recognizing a solution

April 7, 2009

36

NP-completeness

- **Circuit SAT**: given a Boolean circuit (gates \wedge, \vee, \neg), with variables y_1, y_2, \dots, y_m is there some assignment that makes it output 1?

Theorem: Circuit SAT is **NP**-complete.

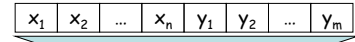
- Proof:
 - clearly in **NP**

April 7, 2009

37

NP-completeness

- Given $L \in \mathbf{NP}$ of form
 $L = \{ x \mid y \text{ s.t. } (x, y) \in R \}$



1 iff $(x, y) \in R$ CVAL reduction for R

- hardwire input x ; leave y as variables

April 7, 2009

38

NEXP-completeness

- **Succinct Circuit SAT**: given a **succinctly encoded** Boolean circuit (gates \wedge, \vee, \neg), with variables y_1, y_2, \dots, y_m is there some assignment that makes it output 1?

Theorem: Succinct Circuit SAT is **NEXP**-complete.

- Proof:
 - same trick as for Succinct CVAL **EXP**-complete.

April 7, 2009

39

Complement classes

- In general, if **C** is a complexity class
- **co-C** is the complement class, containing all **complements** of languages in **C**
 - $L \in \mathbf{C}$ implies $(\Sigma^* - L) \in \mathbf{co-C}$
 - $(\Sigma^* - L) \in \mathbf{C}$ implies $L \in \mathbf{co-C}$
- Some classes closed under complement:
 - e.g. $\mathbf{co-P} = \mathbf{P}$

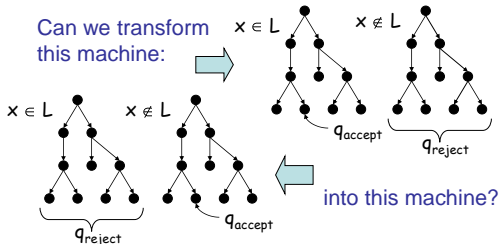
April 7, 2009

40

coNP

- Is NP closed under complement?

Can we transform this machine:



into this machine?

April 7, 2009

41

coNP

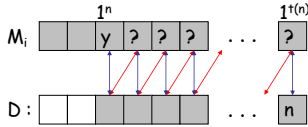
- “proof system” interpretation:
- Recall: $L \in \mathbf{NP}$ iff expressible as
 $L = \{ x \mid y, |y| \leq |x|^k, (x, y) \in R \}$
 - “proof” (pointing to y)
 - “proof verifier” (pointing to R)
- languages in **NP** have “short proofs”
- **coNP** captures (in its complete problems) problems **least likely** to have “short proofs”.
 - e.g., UNSAT is **coNP**-complete

April 7, 2009

42

NTIME Hierarchy Theorem

- Did we diagonalize against M_i ?
 - if $L(M_i) = L(D)$ then:



- equality along all arrows.
- contradiction.

April 7, 2009

49

NTIME Hierarchy Theorem

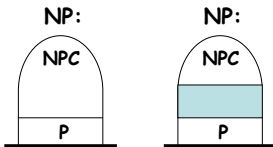
- General scheme:
 - interval $[1 \dots t(1)]$ kills M_1
 - interval $[t(1) \dots t(t(1))]$ kills M_2
 - interval $[t^{i-1}(1) \dots t^i(1)]$ kills M_i
- Running time of D on 1^n : $f(n+1) +$ time to compute interval containing n
- conclude D in **NTIME(g(n))** ($g(n) = \omega(f(n+1))$)

April 7, 2009

50

Ladner's Theorem

- Assuming $P \neq NP$, what does the world (inside NP) look like?



April 7, 2009

51