CS151
Complexity Theory

Lecture 13

May 11, 2004

Outline

- Natural complete problems for PH and PSPACE
- proof systems
- interactive proofs and their power

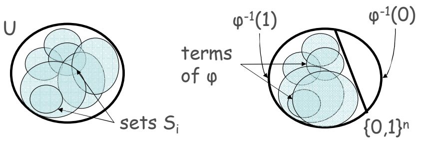
Simpler version of MIN DNF

<u>Theorem</u> (U): MIN DNF is $\mathbf{\Sigma_2}$-complete.

- we'll consider a simpler variant:
  - IRREDUNDANT: given DNF φ, integer k; is there a DNF φ' consisting of at most k terms of φ computing same function φ does?

Simpler version of MIN DNF

- analogy with an **NP**-complete problem:
  - SET COVER: given subsets $S_1, S_2, \ldots, S_m \subset U$, integer k, is there a collection of at most k sets that cover U.



SSC is $\mathbf{\Sigma_2}$-complete

- "sets" in IRREDUNDANT lie in an exponentially larger universe; they are represented succinctly by terms of φ
- helpful intermediate problem:
  - SUCCINCT SET COVER (SSC): given 3-DNFs $S = \{\varphi_1, \varphi_2, \varphi_3, \ldots, \varphi_m\}$ on n variables, integer k; is there a collection $S' \subset S$ of size at most k for which $\vee_{\varphi \in S'} \equiv 1$ (S' is a cover)?

SSC is $\mathbf{\Sigma_2}$-complete

<u>Theorem</u>: SSC is $\mathbf{\Sigma_2}$-complete.

- Proof:
  - in $\mathbf{\Sigma_2}$ (why?)

    "$\exists\ S' \subset S \quad \forall\ x \quad [\vee_{\varphi \in S'}(x) = 1]$"
  - reduce from $QSAT_2$
  - instance: $\exists A \forall B\ \varphi(A, B) = 1$
  - assume $|A| = |B| = n$

SSC is Σ_2-complete

$\exists A \forall B\ \varphi(A, B) = 1$

- Proof (continued):
  - 2 new sets of variables S, T
  - $|S| = |T| = n$
  - Define: wt(S, T) = # of 1s in S and T together
  - "(S,T) encodes A" means $\forall i\ (s_i = a_i) \wedge (t_i = \neg a_i)$

SSC is Σ_2-complete

- From $\varphi(A, B)$ we define function f(S, T, B):
  - 0 if wt(S, T) < n
  - 0 if wt(S, T) = n and (S,T) does not encode any A
  - **0 if wt(S, T) = n and (S,T) encodes A for which $\varphi(A, B) = 0$**
  - **1 if wt(S, T) = n and (S,T) encodes A for which $\varphi(A, B) = 1$**
  - 1 if wt(S, T) > n
- verify: poly(n) size circuit C computes f
- verify: f is monotone in S and T

SSC is Σ_2-complete

0 if wt(S, T) < n
0 if wt(S, T) = n and (S,T) does not encode any A
0 if wt(S, T) = n and (S,T) encodes A : $\varphi(A,B) = 0$
1 if wt(S, T) = n and (S,T) encodes A : $\varphi(A,B) = 1$
1 if wt(S, T) > n

- Proof (continued):
  - produce an instance of SSC:
    - # of sets m = 2n + 1
    - $\varphi_i = (\neg s_i)$ $\varphi_{i+n} = (\neg t_i)$
    - from C get a 3-DNF $\varphi_m(S,T,B,W)$:

      $f(S,T,B) = 1 \Leftrightarrow \forall W\ \varphi_m(S,T,B,W) = 1$

SSC is Σ_2-complete

0 if wt(S, T) < n
0 if wt(S, T) = n and (S,T) does not encode any A
0 if wt(S, T) = n and (S,T) encodes A : $\varphi(A,B) = 0$
1 if wt(S, T) = n and (S,T) encodes A : $\varphi(A,B) = 1$
1 if wt(S, T) > n

$=(\neg s_i)$

$=(\neg t_i)$

Claim: $\exists A \forall B\ \varphi(A, B) = 1$ implies

$S' = \{\varphi_i \mid a_i = 1\} \cup \{\varphi_{i+n} \mid a_i = 0\} \cup \{\varphi_m\}$

is a cover of size n+1.

Proof: consider each fixed point (S,T,B,W)

- if there exists (S',T') that encodes A and we have $(S',T') \preceq (S,T)$ then $\varphi_m(S,T,B,W) = 1$
- else, $\exists i$ ($a_i = 1$ and $s_i = 0$) or ($a_i = 0$ and $t_i = 0$)

SSC is Σ_2-complete

Claim: cover S' of size n+1 implies

$\exists A \forall B\ \varphi(A, B) = 1$

Proof:

- S' must contain φ_m; otherwise it fails to cover the all-ones point
- consider the pair (S*, T*) for which:
  - $s_i = 1$ if $\varphi_i \in S'$ and 0 otherwise
  - $t_i = 1$ if $\varphi_{i+n} \in S'$ and 0 otherwise
- must have: $\forall B \forall W\ \varphi_m(S^*, T^*, B, W) = 1$
- implies: $\forall B\ f(S^*, T^*, B) = 1$

SSC is Σ_2-complete

0 if wt(S, T) = n and (S,T) does not encode any A
0 if wt(S, T) = n and (S,T) encodes A : $\varphi(A,B) = 0$
1 if wt(S, T) = n and (S,T) encodes A : $\varphi(A,B) = 1$

- defined the pair (S*, T*) as follows:
  - $s_i = 1$ if $\varphi_i \in S'$ and 0 otherwise
  - $t_i = 1$ if $\varphi_{i+n} \in S'$ and 0 otherwise
- concluded: $\forall B\ f(S^*, T^*, B) = 1$
- Note: $wt(S^*, T^*) = n$
- (S*,T*) must encode A s.t. $\forall B\ \varphi(A, B) = 1$
- Conclude: $\exists A \forall B\ \varphi(A, B) = 1$

IRR is $\mathbf{\Sigma_2}$-complete

- Recall:

  IRREDUNDANT: given DNF φ, integer k; is there a DNF φ' consisting of at most k terms of φ computing same function φ does?

Theorem: IRR is $\mathbf{\Sigma_2}$-complete.

- Proof:
  - in $\mathbf{\Sigma_2}$: "$\exists\ \varphi'\ \forall\ x\ [\varphi'(x) = \varphi(x)]$"

IRR is $\mathbf{\Sigma_2}$-complete

- reduce from SSC
- instance: $S = \{\varphi_1, \varphi_2, \varphi_3, \ldots, \varphi_m\}$
- may assume
  - $\varphi_1, \varphi_2, \ldots, \varphi_{m-1}$ single literals
  - φ_m necessary in any cover
  - S is a cover
- write out terms: $\varphi_m = t_1 \vee t_2 \vee t_3 \vee \ldots \vee t_n$
- produce an instance of IRR:

$\varphi = \vee_{i=1\ldots n}\ (z_1\ldots z_{i-1}\, z_{i+1}\ldots z_n\, t_i) \vee \vee_{j=1\ldots m-1}\ (z_1\ldots z_n \varphi_j)$

IRR is $\mathbf{\Sigma_2}$-complete

$S = \{\varphi_1, \varphi_2, \varphi_3, \ldots, \varphi_m = t_1 \vee \ldots \vee t_n\}$

$\varphi = \vee_{i=1\ldots n}\ (z_1\ldots z_{i-1}\, z_{i+1}\ldots z_n\, t_i) \vee \vee_{j=1\ldots m-1}\ (z_1\ldots z_n \varphi_j)$

- Proof (continued):

  Claim: if $S' \subset S$ is a cover of size k then

  $\varphi' = \vee_{i=1\ldots n}\ (z_1\ldots z_{i-1}\, z_{i+1}\ldots z_n\, t_i) \vee \vee_{j<m,\ \varphi_j \in S'}\ (z_1 z_2\ldots z_n\, \varphi_j)$

  is equivalent to φ and has k+n-1 terms.

  Proof: by cases

IRR is $\mathbf{\Sigma_2}$-complete

$S = \{\varphi_1, \varphi_2, \varphi_3, \ldots, \varphi_m = t_1 \vee \ldots \vee t_n\};\ \ S' \subset S$

$\varphi = \vee_{i=1\ldots n}\ (z_1\ldots z_{i-1}\, z_{i+1}\ldots z_n\, t_i) \vee \vee_{j=1\ldots m-1}\ (z_1\ldots z_n \varphi_j)$

$\varphi' = \vee_{i=1\ldots n}\ (z_1\ldots z_{i-1}\, z_{i+1}\ldots z_n\, t_i) \vee \vee_{j<m,\ \varphi_j \in S'}\ (z_1 z_2\ldots z_n \varphi_j)$

- more than one z variable 0: both φ', φ are 0
- z_i 0, other z's 1: φ', φ equivalent to t_i
- all z's 1:
  - φ' equivalent to $\vee_{\varphi_j \in S'}\ (z_1 z_2\ldots z_n \varphi_j)$
  - φ' equivalent to $\vee_{\varphi_j \in S}\ (z_1\ldots z_n \varphi_j)$
  - S' is a **cover** implies both equivalent to 1

IRR is $\mathbf{\Sigma_2}$-complete

$S = \{\varphi_1, \varphi_2, \varphi_3, \ldots, \varphi_m = t_1 \vee \ldots \vee t_n\}$

$\varphi = \vee_{i=1\ldots n}\ (z_1\ldots z_{i-1}\, z_{i+1}\ldots z_n\, t_i) \vee \vee_{j=1\ldots m-1}\ (z_1\ldots z_n \varphi_j)$

- Proof (continued):

  Claim: if $\varphi' \equiv \varphi$ uses k+n-1 terms of φ, then there exists a cover S' of size k

  Proof:

  - each "t_i term" of φ must be present

IRR is $\mathbf{\Sigma_2}$-complete

$S = \{\varphi_1, \varphi_2, \varphi_3, \ldots, \varphi_m = t_1 \vee \ldots \vee t_n\}$

$\varphi = \vee_{i=1\ldots n}\ (z_1\ldots z_{i-1}\, z_{i+1}\ldots z_n\, t_i) \vee \vee_{j=1\ldots m-1}\ (z_1\ldots z_n \varphi_j)$

$\varphi' = \vee_{i=1\ldots n}\ (z_1\ldots z_{i-1}\, z_{i+1}\ldots z_n\, t_i) \vee ???$ (k+n-1 terms total)

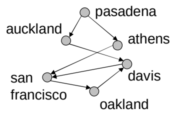
- other k-1 terms all involve some φ_j
- let S' be these φ_j together with φ_m

$(\vee_{\varphi_j \in S'} \varphi_j) \equiv \varphi'_{z \leftarrow 11\ldots 1} \equiv \varphi_{z \leftarrow 11\ldots 1} \equiv (\vee_{\varphi_j \in S} \varphi_j) \equiv 1$

- conclude S' is a cover of size k

PSPACE

- General phenomenon: many 2-player games are PSPACE-complete.
  - – 2 players I, II
  - – alternate picking edges
  - – lose when no unvisited choice



- GEOGRAPHY = {(G, s) : G is a directed graph and player I can win from node s}

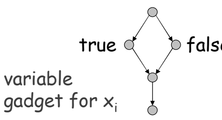
PSPACE

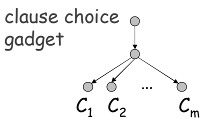
Theorem: GEOGRAPHY is PSPACE-complete.

Proof:
- – in PSPACE
  - easily expressed with alternating quantifiers
- – PSPACE-hard
  - reduction from QSAT

PSPACE

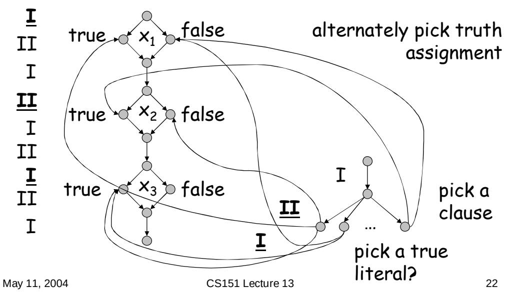
$\exists x_1 \forall x_2 \exists x_3 \ldots \forall x_n\ \varphi(x_1, x_2, \ldots, x_n)$?





PSPACE

$\exists x_1 \forall x_2 \exists x_3 \ldots (\neg x_1 \vee x_2 \vee \neg x_3) \wedge (\neg x_3 \vee x_1) \wedge \ldots \wedge (x_1 \vee \neg x_2)$



Proof systems

L = { (A, 1^k) : A is a true mathematical assertion with a proof of length k}

- New topic:

What is a "proof"?

complexity insight: meaningless unless can be **efficiently** verified

Proof systems

- given language L, goal is to prove $x \in L$
- **proof system** for L is a verification algorithm V
  - – completeness: $x \in L \Rightarrow \exists$ proof, V accepts (x, proof)

    "true assertions have proofs"
  - – soundness: $x \notin L \Rightarrow \forall$ proof*, V rejects (x, proof*)

    "false assertions have no proofs"
  - – efficiency: $\forall$ x, proof, V(x, proof) runs in polynomial time in |x|

Classical Proofs

- previous definition:

  "classical" proof system
- recall:

  $L \in$ **NP** iff expressible as

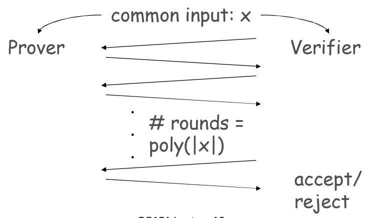
  $L = \{ x \mid \exists\, y, |y| < |x|^k, (x, y) \in R \}$ and $R \in$ **P**.
- **NP** is the set of languages with classical proof systems (R is the verifier)

Interactive Proofs

- Two new ingredients:
  - **randomness**: verifier tosses coins, errs with some small probability
  - **interaction**: rather than "reading" proof, verifier **interacts** with computationally unbounded **prover**
- **NP** proof systems lie in this framework: prover sends proof, verifier does not use randomness

Interactive Proofs

- **interactive proof system** for L is an interactive protocol (P, V)



Interactive Proofs

- **interactive proof system** for L is an interactive protocol (P, V)
  - completeness: $x \in L \Rightarrow$

    $\Pr[V$ accepts in $(P, V)(x)] \geq 2/3$
  - soundness: $x \notin L \Rightarrow \forall P^*$

    $\Pr[V$ accepts in $(P^*, V)(x)] \leq 1/3$
  - efficiency: V is p.p.t. machine
- repetition: can reduce error to any ε

Interactive Proofs

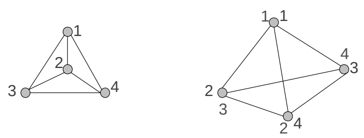
IP = {L : L has an interactive proof system}

- Observations/questions:
  - philosophically interesting: captures more broadly what it means to be convinced a statement is true
  - clearly **NP** $\subset$ **IP.** Potentially larger. How much larger?
  - if larger, randomness is essential (why?)

Graph Isomorphism

- graphs $G_0 = (V, E_0)$ and $G_1 = (V, E_1)$ are isomorphic ($G_0 \cong G_1$) if exists a permutation $\pi: V \rightarrow V$ for which

  $(x, y) \in E_0 \Leftrightarrow (\pi(x), \pi(y)) \in E_1$



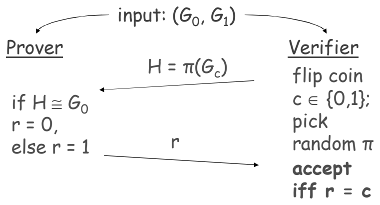
Graph Isomorphism

- GI = $\{(G_0, G_1) : G_0 \cong G_1\}$
  – in **NP**
  – not known to be in **P**, or **NP**-complete
- GNI = complement of GI
  – not known to be in **NP**

<u>Theorem</u> (GMW): GNI $\in$ **IP**
  – indication **IP** may be more powerful than **NP**

GNI in **IP**

- interactive proof system for GNI:



GNI in **IP**

- completeness:
  – if G_0 not isomorphic to G_1 then H is isomorphic to exactly one of (G_0, G_1)
  – prover will choose correct r
- soundness:
  – if $G_0 \cong G_1$ then prover sees same distribution on H for c = 0, c = 1
  – no information on c $\Rightarrow$ *any* prover P* can succeed with probability at most 1/2