CSCI 1590
Intro to Computational Complexity
PSPACE-Complete Languages

John E. Savage

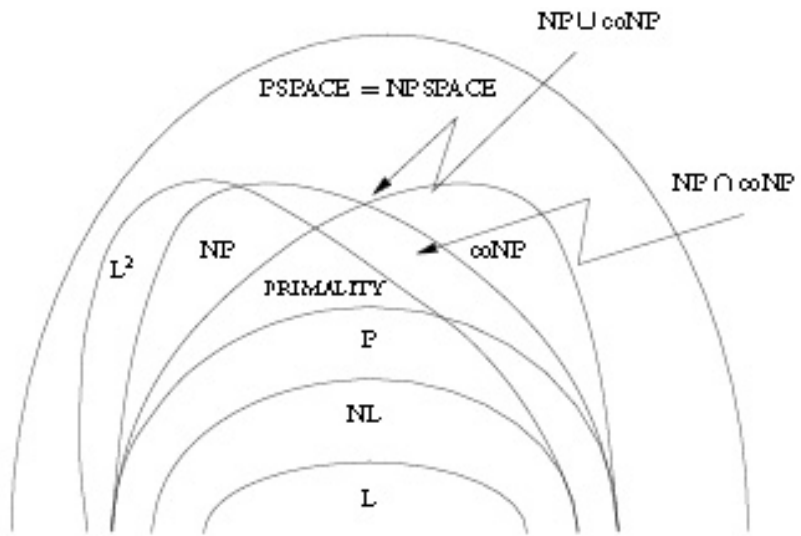
Brown University

February 20, 2008

Summary

Complexity Classes from Last Lecture

- **P**, co**NP**,
- Π_i^p and Σ_i^p
- **PH**
- **PSPACE**



Polynomial Time Hierarchy

- A language is in **NP**(co**NP**) if and only if it can be reduced in polynomial time to a statement of the form $\exists \mathbf{x}\ b(\mathbf{x})$ ($\forall \mathbf{x}\ b(\mathbf{x})$)
- By adding additional levels of quantification, as shown below, potentially new complexity classes are added.
  - $\forall \mathbf{x}_1\ \exists \mathbf{x}_2\ b(\mathbf{x}_1, \mathbf{x}_2)$
  - $\exists \mathbf{x}_1\ \forall \mathbf{x}_2\ b(\mathbf{x}_1, \mathbf{x}_2)$
- The sets of languages PTIME reducible to statements of this form are denoted Π_i^p and Σ_i^p respectively, when there are i alternations of existential and universal quantifiers and the outermost quantifier is $\forall$ and $\exists$, respectively.

Definition

The Polynomial Hierarchy (**PH**) is defined as

$$\mathbf{PH} = \bigcup_i \Sigma_i^p$$

PH and PSPACE

Definition

A language L is **PH-complete** if a) $L \in$ **PH** and b) all languages in **PH** are PTIME reducible to L.

- It is not hard to see that **PH** $\in$ **PSPACE**.
- If a **PH**-complete language exists, the polynomial hierarchy collapses. (See last lecture.)

Definition

TQBF denotes the family of quantified boolean formulas Ψ with an unbounded number of alternations that evaluate to True.

$$\Psi = Q_1 x_1 Q_2 x_2 \ldots Q_n x_n \; \phi(x_1, x_2, \ldots, x_n)$$

Here Q_j denotes either universal ($\forall$) or existential ($\exists$) quantification.

TQBF is an example of a **PSPACE**-complete language.

Games and TQBF

- Languages in **NP** are analogous to puzzles where we ask, "Is there a solution?".
- By contrast, TQBF allows us to ask a seemingly harder question, "Is there a winning strategy?". Player 1 can win if there is a choice for its variable such that for all choices by Player 2 there is a choice by Player 1, etc.
- In a game one player tries to account for all possible decisions that an opponent can make. Each level of alternation is like a single turn of the game.
- Unlike problems in **NP**, it does not appear that a certificate suffices to demonstrate membership in the class. Instead it seems necessary to provide the full set of alternatives implied by alternation of quantifiers.

Outline of Proof that TQBF is **PSPACE**-Complete

Definition

TQBF is **PSPACE**-complete if it is in **PSPACE** and every language $L \in$ **PSPACE** can be reduced to TQBF in polynomial time.

To show the second result, we use the following lemma on directed graphs.

Lemma

For $G = (V, E)$ directed, let $PATH_G(a, b, k)$ have value 1 (0) if $\exists$ ($\neg\exists$) path from vertex a to vertex b in G of length $\leq 2^k$. (Used in Savitch's Theorem.) It can be described by a TQBF *of length $O(k\mu + |PATH_G(a, b, 0))|)$ where μ and $|PATH_G(a, b, 0)|$ are lengths of $v \in V$ and formula that determines if b is reachable from a in one step.*

The following expansion of $\text{PATH}_G(a, b, 2^k)$ is from Savitch's Theorem.

$$\text{PATH}_G(a, b, k) = \exists z\ \text{PATH}_G(a, z, k-1) \wedge \text{PATH}_G(z, b, k-1)$$

Expanding this gives length-$O(2^k|\text{PATH}_G(a, b, 0)|)$ instance of TQBF.

Reducing PATH Predicate to TQBF Efficiently

To avoid expanding both $\text{PATH}_G(a, z, k-1)$ and $\text{PATH}_G(z, b, k-1)$, restate the expansion of $\text{PATH}_G(a, b, k)$ as shown below where $p(u, v, a, z, b) \equiv (((u = a) \wedge (v = z)) \vee ((u = z) \wedge (v = b)))$.

$$\text{PATH}_G(a, b, k) \equiv \exists z \forall (u, v)\ p(u, v, a, z, b) \Rightarrow \text{PATH}_G(u, v, k-1)$$

Equality $(u = v)$ and implication $(u \Rightarrow v)$ can be expressed as the Boolean formulas $(u \wedge v) \vee (\bar{u} \wedge \bar{v})$ and $(\bar{u} \vee v)$, respectively, giving

$$\text{PATH}_G(a, b, k) \equiv \exists z \forall (u, v)\ (\bar{p}(u, v, a, z, b) \vee \text{PATH}_G(u, v, k-1))$$

Notice that $\bar{p}(u, v, a, z, b)$ has 16μ literals where μ is the number of Boolean variables used to represent of each of u, v, a, z, b as a binary tuple.

Applying the expansion to $\text{PATH}_G(u, v, k-1))$ introduces two more quantifiers, increases the number of literals by 16μ, and expresses the result in terms of $\text{PATH}_G(u, v, k-2))$. The hypothesis follows.

TQBF is **PSPACE**-Complete

Theorem

TQBF *is* **PSPACE**-*Complete*

Proof

We show that TQBF is in **PSPACE**

$$\Psi = Q_1 x_1 Q_2 x_2 \ldots Q_n x_n \; \phi(x_1, x_2, \ldots, x_n)$$

To show this, note that Ψ is the OR of $\Psi\,|_{x_1=1}$ and $\Psi\,|_{x_1=0}$ when $Q_1 = \exists$ whereas it is the AND when $Q_1 = \forall$. Systematically run through all assignments to variables. For each assignment, evaluate a copy of the original $\phi(x_1, x_2, \ldots, x_n)$. If $\phi(x_1, x_2, \ldots, x_n)$ uses space m, this execution consumes space $O(n + m)$.

TQBF is **PSPACE**-Complete

Proof (cont.)

As shown in the Lemma, an instance of $\text{PATH}_G(a, b, k)$ can be translated into an instance of TQBF of length $O(k + |\text{PATH}_G(a, b, 0))|$.

As in Savitch's Theorem, we now show that any language $L \in$ **PSPACE** recognized by M can be reduced in PTIME to an instance of $\text{PATH}_G(a, b, k)$ such that k and $|\text{PATH}_G(a, b, 0))|$ are polynomial in the input **x**. This provides a PTIME reduction from L to TQBF.

Let G be config. graph G of M on input **x** with start and accept configs. C_{start} and C_{accept} (to ensure C_{accept} is unique, modify M so it erases its tape after accepting). **x** is in $L \Leftrightarrow C_{accept}$ is reachable from C_{start}.

$k = O(S(n))$ because there are $O(c^{S(n)})$ configs. in G, c a constant. $|\text{PATH}_G(a, b, 0))|$ is polynomial in $S(n)$ because there is a DTM that can recognise the language $\text{PATH}_G(a, b, 0))$. Since it is in **P**, it can be reduced to an instance of SAT of polynomial length in $S(n)$.