Complexity Theory

Georg Moser

Institute of Computer Science @ UIBK

Summer 2008

Outline

- Summary of Last Lecture: The Polynomial-Time Hierarchy
- Exercises
- Nick's Class
- Relation to Time-Space Classes

Theorem

consider

$$\mathrm{NP} \subseteq \mathrm{NP}^{\mathrm{NP}} \subseteq \mathrm{NP}^{\mathrm{NP}^{\mathrm{NP}}} \ldots$$

i.e., $\mathrm{NP}_1 := \mathrm{NP}$ and $\mathrm{NP}_{k+1} := \mathrm{NP}^{\mathrm{NP}_k}$, then $\forall k \geqslant 1$: $\mathrm{NP}_k = \Sigma_k^{\mathrm{p}}$

Theorem

a language A is in Σ_k^{p} iff there is a deterministic polytime computable $(k+1)$-ary predicate R and a constant c such that

$$A = \{x \mid \exists^{|x|^c} y_1 \forall^{|x|^c} y_2 \exists^{|x|^c} y_3 \ldots \mathrm{Q}^{|x|^c} y_k R(x, y_1, \ldots, y_k)$$

$(\mathrm{Q} \in \{\exists, \forall\})$

Definition

- a set A is recursive enumerable in B if $A = \mathrm{L}(M^B)$ for some oracle TM M^B
- A is recursive in B if $A = \mathrm{L}(M^B)$ and M^B is a total oracle TM
- $A \leqslant_T B$, if A recursive in B — Turing reducibility
- $A \leqslant_m B$, if A many-one reduces to B — many-one reducibility

Definition — Arithmetical Hierarchy

we fix a binary alphabet $\Sigma = \{0, 1\}$

$\Sigma_1^0 := \{\text{r.e. sets}\}$ $\quad$ $\Sigma_{n+1}^0 := \{\mathrm{L}(M^B) \mid B \in \Sigma_n^0\}$

$\Delta_1^0 := \{\text{recursive sets}\}$ $\quad$ $\Delta_{n+1}^0 := \{\mathrm{L}(M^B) \mid B \in \Sigma_n^0, M^B \text{ total}\}$

$\Pi_n^0 := \{\sim L \mid L \in \Sigma_n^0\}$

Theorem

- a set A is in Σ_n^0 iff $\exists$ a decidable $(n+1)$-ary predicate R such that
$$A = \{x \mid \exists y_1 \forall y_2 \dots \mathrm{Q} y_n R(x, y_1, \dots, y_n)\}$$
($\mathrm{Q} \in \{\exists, \forall\}$)
- a set A is in Π_n^0 iff $\exists$ a decidable $(n+1)$-ary predicate R such that
$$A = \{x \mid \forall y_1 \exists y_2 \dots \mathrm{Q} y_n R(x, y_1, \dots, y_n)\}$$
($\mathrm{Q} \in \{\exists, \forall\}$)

Example

- HP is $\leqslant_m$-complete for Σ_1^0
- MP is $\leqslant_m$-complete for Σ_1^0
- $\mathrm{FIN} = \{M \mid \mathrm{L}(M)$ is finite$\}$ is $\leqslant_m$-complete for Σ_2^0

Homework

1. Miscellaneous Exercises 27
2. Miscellaneous Exercises 32
3. Miscellaneous Exercises 34
4. Miscellaneous Exercises 35
5. Miscellaneous Exercises 128

Definition

a family of Boolean circuits $C_0, C_1, C_2, \ldots$ is a logspace-uniform family of Boolean circuits of polylog depth and polynomial size if

1. C_n has n inputs and is composed of $\wedge$, $\vee$ and $\neg$-gates
2. C_n is of depth at most $(\log n)^{\mathrm{O}(1)}$

   depth is the length of the longest path from input to output
3. C_n has no more than $n^{\mathrm{O}(1)}$ gates
4. the $(C_i)_{i \in \mathbb{N}}$ is logspace-uniform:
   $\exists$ a logspace transducer that produces the circuits C_n on input 0^n

Definition — NC

a set $A \subseteq \{0,1\}^*$ is in NC if $\exists$ a logspace-uniform family of Boolean circuits of polylog depth and polynomial size, where each C_n has one output and $\forall\ x \in \{0,1\}^*$

$$x \in A \Leftrightarrow C_{|x|}(x) = 1$$

Definition — STA

the class STA$(S(n), T(n), A(n))$ is the class of sets accepted by ATMs that

1. are $S(n)$-space bounded,
2. $T(n)$-time bounded, and
3. consist of at most $A(n)$ alternating sections

Example

$$\begin{aligned}
\mathrm{LOGSPACE} &= \mathrm{STA}(\log n, *, 0) \\
\mathrm{NLOGSPACE} &= \mathrm{STA}(\log n, *, \Sigma 1) \\
\mathrm{P} &= \mathrm{STA}(\log n, *, *) = \mathrm{STA}(*, n^{\mathrm{O}(1)}, 0) \\
\mathrm{NP} &= \mathrm{STA}(*, n^{\mathrm{O}(1)}, \Sigma 1) \\
\Sigma^{\mathrm{p}}_k &= \mathrm{STA}(*, n^{\mathrm{O}(1)}, \Sigma k) \\
\Pi^{\mathrm{p}}_k &= \mathrm{STA}(*, n^{\mathrm{O}(1)}, \Pi k) \\
\mathrm{PSPACE} &= \mathrm{STA}(*, n^{\mathrm{O}(1)}, *) = \mathrm{STA}(n^{\mathrm{O}(1)}, *, 0)
\end{aligned}$$

Theorem

$\mathrm{NC} = \mathrm{STA}(\log n, *, (\log n)^{\mathrm{O}(1)})$