Complexity Theory

Georg Moser

Institute of Computer Science @ UIBK

Summer 2008

Outline

- Summary of Last Lecture: Parallel Complexity
- Exercises
- Probabilistic Turing Machines

Theorem

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

Proof $\subseteq$

- $\exists$ a logspace-uniform family of Boolean circuits C_n of polylog depth and polynomial size
- $\exists$ logspace-uniform transducer M
- construct ATM N that simulates the family C_n:
  on input x ($|x| = n$), N runs M to produce C_n and evaluate $C_n(x)$

Proof $\supseteq$

- $\exists$ alternating logspace machine N of required form
- represent the next-configuration relation as Boolean matrix
- represent ATM computation as circuit calculations via Boolean vectors b_i such that $b_i(\alpha) = 1$, if α @ i accepts
- initially b_0 is zero; output $b_{(\log n)^c}(\mathtt{start})$

$\blacksquare$

Homework

- Miscellaneous Exercises 29.
- Homework 6.2.
- Homework 6.3.

Probabilistic Turing Machines

Definition

- a probabilistic Turing machine M is a TM and $\exists$ extra read-only tape containing random bits
- random bits may be consulted to decide on the next step
- outcome $M(x, y)$ for input x and random bits y
- M
  - is $T(n)$ time bounded if $\forall$ input x it runs in $T(n)$ steps
  - is $S(n)$ space bounded if $\forall$ input x it needs $S(n)$ space

  for any random bits y
- probability of accept for $T(n)$ time bounded M:

$$\Pr_y(M(x, y) \text{ accepts}) = \frac{|\{y \in \{0,1\}^k \mid \text{M(x,y) accepts}\}|}{2^k}$$

for $k \geqslant T(|x|)$

Definition — RP

a set A is in RP if $\exists$ probabilitic TM M with polytime bound n^c such that

1. if $x \in A$, then $\Pr_y(M(x, y) \text{ accepts}) \geqslant \frac{3}{4}$
2. if $x \notin A$, then $\Pr_y(M(x, y) \text{ accepts}) = 0$

Fact

$P \subseteq RP \subseteq NP$

Definition — BPP

a set A is in BPP if $\exists$ probabilitic TM M with polytime bound n^c such that

1. if $x \in A$, then $\Pr_y(M(x, y) \text{ accepts}) \geqslant \frac{3}{4}$
2. if $x \notin A$, then $\Pr_y(M(x, y) \text{ accepts}) \leqslant \frac{1}{4}$

Fact

RP $\subseteq$ BPP and BPP is closed under complement

Probabilistic Tests for Polynomials

Example

given a polynomial $p(x_1, \dots, x_n)$ (of low degree) with integer coefficients, verify whether it is identical 0

Restriction

typicall the polynomial is not given in normal form but as a straight-line program

Theorem — Schwartz-Zippel Lemma

- let F be field, let $S \subseteq F$ be arbitrary
- let $p(\overline{x})$ be a nonzero polynomial of n variables over F and total degree d

then the equation $p(\overline{x}) = 0$ has at most $d \cdot |S|^{n-1}$ solutions in S^n

Corollary

- let F be field, let $S \subseteq F$ be arbitrary
- let $p(\overline{x})$ be a nonzero polynomial of n variables over F and total degree d

if p is evaluated on $(s_1, \dots, s_n)$ chosen at random, then

$$\Pr(p(s_1, \dots, s_n) = 0) \leqslant \frac{d}{|S|}$$

Example — perfect matching

a perfect matching in a bipartite graph G in a subset M of the edges such that

1. no two edges in M share a common vertex
2. each vertex is the endpoint of some edge in M

Fact

represent G as a matrix (the Tutte matrix) A, then $\det A$ is a nonzero polynomial of degree n with one monomial for each perfact matching