Complexity Theory

Georg Moser

Institute of Computer Science @ UIBK

Summer 2008

Outline

- Summary of Last Lecture: Probabilistic Turing Machines
- Project Assignment
- Probabilistic Turing Machines (Proof)

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

$\mathrm{P} \subseteq \mathrm{RP} \subseteq \mathrm{NP}$

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

$\mathrm{RP} \subseteq \mathrm{BPP}$ and BPP is closed under complement

Homework

- Project assignment: Find references to Csanky's algorithm and show that this algorithm is in NC.

Amplification

Lemma — Amplification Lemma

if $A \in \text{RP}$, then $\forall$ polynomials n^d
$\exists$ probabilistic polytime TM M such that on input x ($n = |x|$):

1. if $x \in A$, then $\Pr_y(M(x,y) \text{ accepts}) \geqslant 1 - 2^{-n^d}$
2. if $x \notin A$, then $\Pr_y(M(x,y) \text{ accepts}) = 0$

Lemma

if $A \in \text{BPP}$, then $\forall$ polynomials n^d
$\exists$ probabilistic polytime TM M such that on input x ($n = |x|$):

1. if $x \in A$, then $\Pr_y(M(x,y) \text{ accepts}) \geqslant 1 - 2^{-n^d}$
2. if $x \notin A$, then $\Pr_y(M(x,y) \text{ accepts}) \leqslant 2^{-n^d}$

Theorem

$\text{BPP} \subseteq \Sigma_2^p \cap \Pi_2^p$

$\text{BPP} \subseteq \Sigma_2^p \cap \Pi_2^p$

Corollary

let $A \in \text{BPP}$
- $\exists$ probabilistic polytime TM M running in time n^c such that
- $\forall$ inputs x
  - if $x \in A$, then $\Pr_y(M(x,y) \text{ accepts}) \geqslant 1 - 2^{-n}$
  - if $x \notin A$, then $\Pr_y(M(x,y) \text{ accepts}) \leqslant 2^{-n}$

Definition

fix input x and let $m = n^c$

$$A_x = \{y \in \{0,1\}^m \mid M(x,y) \text{ accepts}\}$$
$$R_x = \{y \in \{0,1\}^m \mid M(x,y) \text{ rejects}\} = \{0,1\}^m - A_x$$

Fact

for $x \in A$

$$|A_x| \geqslant 2^m - 2^{m-n} \quad \text{and} \quad |R_x| \leqslant 2^{m-n}$$

for $x \notin A$

$$|R_x| \geqslant 2^m - 2^{m-n} \quad \text{and} \quad |A_x| \leqslant 2^{m-n}$$

Claim

$x \in A$ if and only if $\exists\, z_1, \dots, z_m$ ($|z_i| = m$) such that

$$\{y \oplus z_j \mid 1 \leqslant j \leqslant m, y \in A_x\} = \{0,1\}^m$$

($\oplus$ is bitwise sum mod 2)

Proof (of $\text{BPP} \subseteq \Sigma_2^p \cap \Pi_2^p$)

we only need to show $\text{BPP} \subseteq \Sigma_2^p$ as $\text{coBPP} = \text{BPP}$
let $A \in \text{BPP}$, we show $A \in \Sigma_2^p$:

1. guess $z_1, \dots, z_m$
2. generate all w of length m
3. check

   $$w \in \{y \oplus z_j \mid 1 \leqslant j \leqslant m, y \in A_x\}$$

   for that

   - test $\{w \oplus z_j \mid 1 \leqslant j \leqslant m\} \cap A_x \neq \varnothing$
   - by running $M(x, w \oplus z_j)$ for all j

∎