LECTURE 10

Note Title 3/12/2007

TODAY : RANDOMIZED COMPUTATION

- COMPLEXITY CLASSES:

  ZPP, RP, co-RP, BPP

- BASIC PROPERTIES

———— x ————

Some Intriguing Problems

1. Given n-bit integer N find prime $p \in [N+1, 2N]$.

Dirichlet's theorem $\Rightarrow$ such p exists.

Prime # theorem $\Rightarrow$ $\Omega\left(\frac{1}{n}\right)$ fraction of numbers in interval are prime.

Yields simple randomized algorithm.

Deterministically ?

2. Given n bit integers a, p (p prime) find square root α of $a \pmod p$.
(i.e. $\alpha^2 = a \pmod p$)

randomized algorithm due to [Berlekamp] [Adleman-Manders-Miller] ...

Deterministic ?

3. Given k matrices $M_1 \ldots M_k$ with $M_i \in \mathbb{Z}^{n \times n}$, find integers $r_1 \ldots r_k$ s.t.

$$\det\left(\sum r_i M_i\right) \neq 0$$

randomized algorithm: Pick $r_1 \ldots r_k \in_U [1 \ldots 2n]$
[Schwartz-Zippel ...] $\Rightarrow$ if $\exists\, x_1 \ldots x_k$ s.t. $\det(\sum x_i M_i) \neq 0$ then $\det(\sum r_i M_i) \neq 0$ w.p. $\geq \frac{1}{2}$.

4. Given algebraic circuits C_1, C_2 over $\mathbb{Z}$, [gates add / multiply / subtract]; decide if

$C_1 \equiv C_2$.

Analogous Boolean problem NP-complete.

Modelling Randomized Computation:

Can augment Turing Machine (as usual) ...
Or use two-input model. We'll do the latter.

Consider deterministic poly time machine $M(x, y)$

x = real input

y = randomness

We say M decides L "probabilistically" if usually $M(x,y) = 1 \iff x \in L$.

Formalizing: When can M err? 4 options

1. When $x \in L$ $\longrightarrow$ RP
2. When $x \notin L$ $\longrightarrow$ coRP
3. Both of the above $\longrightarrow$ BPP
4. None of the above! $\longrightarrow$ ZPP

Defn: $L \in RP$ if $\exists\ M(\cdot,\cdot)$ running in expected poly($|x|$) time for every $x \in \{0,1\}^n$

s.t. Completeness: $x \in L \Rightarrow \Pr_y[M(x,y)=1] \geq 2/3$.

Soundness: $x \notin L \Rightarrow \Pr_y[M(x,y)=1] = 0$.

Defn: $L \in \text{coRP}$ if $\exists\, M(\cdot,\cdot)$ running in expected $\text{poly}(|x|)$ time for every $x \in \{0,1\}^n$

s.t. **Completeness**: $x \in L \Rightarrow \Pr_y[M(x,y)=1] = 1$.

Soundness: $x \notin L \Rightarrow \Pr_y[M(x,y)=1] \leq \frac{1}{3}$.

Defn: $L \in \text{BPP}$ if $\exists\, M(\cdot,\cdot)$ running in expected $\text{poly}(|x|)$ time for every $x \in \{0,1\}^n$

s.t. **Completeness**: $x \in L \Rightarrow \Pr_y[M(x,y)=1] \geq \frac{2}{3}$.

Soundness: $x \notin L \Rightarrow \Pr_y[M(x,y)=1] \leq \frac{1}{3}$.

Defn: $L \in \text{ZPP}$ if $\exists\, M(\cdot,\cdot)$ running in expected $\text{poly}(|x|)$ time for every $x \in \{0,1\}^n$

s.t. **Completeness**: $x \in L \Rightarrow \Pr_y[M(x,y)=1] = 1$.

Soundness: $x \notin L \Rightarrow \Pr_y[M(x,y)=1] = 0$.

Clarifying Terminology

- RP : Randomized Polytime.
- Co-RP : Complement - Randomized Polytime.
- BPP : Bounded-error Probabilistic Polytime.
- ZPP : Zero-error " " .

Basic Properties

- ZPP Example :

$$L_{\sqrt{\ } \text{ mod prime}} = \{ (p, a, b, c) \mid p = \text{prime}, \; 0 \le a, b, c < p, \; \& \; \exists \; b \le \alpha \le c \text{ s.t. } \alpha^2 = a \bmod p \}$$

if $a^{\frac{p-1}{2}} \neq 1 \pmod{p}$ say NO.

else find α, $p-\alpha$ such that

$$\alpha^2 \equiv a \pmod p$$

& say YES iff $b \le \alpha \le c$

or $b \le p-\alpha \le c$.

- ZPP = RP $\cap$ coRP

  $\subseteq$ obvious by definition.

  $\supseteq$ run both RP & coRP algorithms;
  accept if RP accepts
  reject if coRP rejects.

- For RP, coRP, BPP:

  Can replace "expected polytime" by "polytime":

  (Exercise)

Amplification

> Lipton '2007 : " Central phenomenon in scientific progress "

Meta Theorem : Thresholds $\frac{1}{3}$, $\frac{2}{3}$ arbitrary.

Parametrized RP :

For $c : \mathbb{Z} \to \mathbb{R}$, $L \in RP_c$, if $\exists$ polytime machine $M(x,y)$ s.t.

$\forall \; x \in \{0,1\}^n$

- $x \in L \Rightarrow \Pr_y [M(x,y) = 1] \geq c(n)$.
- $x \notin L \Rightarrow$ " $= 0$.

Amplification Theorem for RP :

For any pair of polynomials $p(n)$ & $q(n)$

$$RP_{p(n)} \equiv RP_{1-2^{-q(n)}} .$$

Proof : $\left(\supseteq \quad \text{trivial} \right)$

- Fix $L \in RP_{p(n)}$ & let M be $\underset{\wedge}{}$ RP m/c accepting L.

- Consider M' which does the following
  - Given $x \in \{0,1\}^n$ & $\bar{z} = (y_1 .. y_t) \in \{0,1\}^{n \cdot p(n) q(n)}$
  - if $M(x, y_i) = 1$ for some i, accept.

    else reject

$y_i \in \{0,1\}^n$; $t = \Theta(p(n) \cdot q(n))$

Claim: M' places $L \in RP_{1-2^{-q(n)}}$.

Proof: $x \notin L \Rightarrow \Pr[M' \text{ accepts } x] = 0$

$x \in L \Rightarrow \Pr[M' \text{ rejects } x]$

$$= \left(1 - \frac{1}{p(n)}\right)^{p(n)\cdot q(n)}$$

$$\leq \left(\frac{1}{e}\right)^{q(n)} \leq 2^{-q(n)}$$ $\boxtimes$

Parametrized BPP

- $L \in BPP_{c,s}$ $\quad (c, s : \mathbb{Z} \to \mathbb{R})$

  if $\exists\, M$ s.t. $\forall\, x \in \{0,1\}^n$

  $x \in L \Rightarrow \Pr[M \text{ accepts}] \geq c(n)$

  $x \notin L \Rightarrow$ " $\leq s(n)$

BPP Amplification Theorem

For polytime computable $s(n)$ & polynomials $p(n), q(n)$ it is the case that

$$BPP_{s(n)+\frac{1}{p(n)},\, s(n)} \equiv BPP_{1-2^{-q(n)},\, 2^{-q(n)}}.$$

Proof: Chernoff Bounds; Majority voting.