CS 221 Lecture 8

2/15/2018

Today: Randomized Computation

- Complexity Classes:

  ZPP, RP, coRP, BPP

- Basic Properties

Problems solvable in Randomized Poly Time but not known to be in Det. Poly Time

(1) Find n-bit Prime: $2^{n-1} \leq P \leq 2^n$

(2) Square roots mod Prime P: Given a find b s.t. $a = b^2 \bmod P$.

(3) Given k matrices $M_1 \dots M_k \in \mathbb{Z}^{n \times n}$ find integers $r_1 \dots r_k$ s.t. $\det(\sum r_i M_i \neq 0)$ (if such $r_1 \dots r_k$ exist).

(4) Given arithmetic circuit C over $\mathbb{Z}$, $\exists X_1 \dots X_n$ s.t. $C(X_1 \dots X_n) \neq 0$. [logical version $\equiv$ SAT $\equiv$ NP-Complete]

Modelling Randomized Computation

[Will restrict (*) to decision problems]

Approach 1: • Augment algorithm with "Pick $b \in \{0,1\}$ randomly"
• Expect alg. output to be correct whp.

Approach 2: (Equivalent but crisper math notation)
• Use 2-input model $M(x,y)$ & take majority vote over y.

We'll follow latter approach

• Randomized poly time algorithm for "$X \in L$?" is of the form $M(x,y)$: M poly($|x|$) time; y random

& usually $M(x,y) =$ "$X \in L$"
wrong for y if $M(x,y) \neq$ "$X \in L$".

When can we make errors? →

(*) • Even though all problems on page (1) were search problems.

• Even though search $\not\equiv$ decision for randomized computation
↑ not known [See Prof

Errors allowed?

$x \notin L$ \ $x \in L$	Y	N
Y	BPP	coRP
N	RP	ZPP

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

s.t.

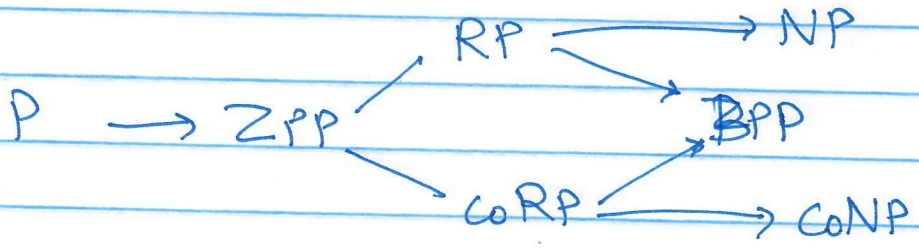
Completeness $x \in L \Rightarrow \Pr_y [M(x,y)=1] \geq 2/3$

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

coRP: completeness 1 ; soundness $1/3$

BPP: " $2/3$ "

ZPP : completeness 1 ; soundness 0 .



Claim: $ZPP = RP \cap coRP$

Proof: $\subseteq$ obvious ; $\supseteq$ → Run RP & coRP alg in parallel.

Accept if RP accepts

Reject if coRP rejects

repeat.

~~Can do~~

Amplification: "Thresholds $\frac{2}{3}, \frac{1}{3}$ arbitrary".

Given $1 \geq c > s \geq 0$ can define

$$RP_c, \quad coRP_s, \quad BPP_{c,s}$$

Lemma 1: $RP_{1/poly(n)} = RP_{1-\exp(-n^c)}$ $\forall$ poly, c.

Lemma 2: $BPP_{s+\frac{1}{poly(n)},\, s} = BPP_{1-\exp(-n^c),\, \exp(-n^c)}$

Proof of Lemma 1: Suppose $L \in RP_{1/poly(n)}$

$\Rightarrow \exists M$ s.t. $\forall x$ if $x \in L$ $\Pr_y[M(x,y)=1] \geq \frac{1}{poly(n)}$

M'

- $k \triangleq poly(n) \cdot n^c$
- Pick $y_1 \ldots y_k$ independently
- if $\exists i\, M(x, y_i) = 1$ output 1
- if $\forall i$ $M(x, y_i) = 0$ output 0

$x \in L \Rightarrow \Pr[M' \text{ outputs } 1] \geq 1 - \left(1 - \frac{1}{poly(n)}\right)^k = 1 - \exp(-n^c)$

BPP Amplification [Lemma 2].

Ingredient: "Chernoff Bounds"

- Thm ["Chernoff Bound"]: if $X_1 \dots X_n$ are independent random variables, identically distributed with $X_i \in \{0,1\}$ & $\mathbb{E}[X_i] = \mu$.

Then $\forall k$

$$\Pr\left[\left|\sum X_i - n\mu\right| \geq k \cdot \sqrt{n}\right] \leq e^{-k^2/2}$$

Proof of Lemma 2: Let $M \in BPP_{c,s}$ with $c > s$ & $M(\cdot,\cdot)$ verifies this.

M'

Given x

- Pick $y_1 \dots y_k$ ind. $\quad k = n^c \cdot \frac{1}{(c-s)^2}$
- Let $Z_i = M(x, y_i)$
- if $\sum Z_i > \left(\frac{c+s}{2}\right) \cdot k$ output 1

else output 0.

if $x \in L$

Analysis: $\mathbb{E}[Z_i] = c$

$Z_i \in \{0,1\}$; $Z_1 \dots Z_k$ independent.

By "C.B."

$$\Pr\left[\left|\sum Z_i - c\cdot k\right| \geq \lambda\cdot\sqrt{k}\right] \leq e^{-\lambda^2/2}$$

$$\Rightarrow \Pr\left[\sum Z_i - ck \leq -\lambda\sqrt{k}\right] \leq e^{-\lambda^2/2}$$

$$\Rightarrow \Pr\left[\sum Z_i \leq ck - \lambda\sqrt{k}\right] \leq e^{-\lambda^2/2}$$

Set $\lambda\sqrt{k}$ so that $\left(\frac{c+s}{2}\right)k \leq ck - \lambda\sqrt{k}$

$$\Leftrightarrow \left(\frac{c-s}{2}\right)k \geq \lambda\sqrt{k}$$

$$\Leftrightarrow x \leq \left(\frac{c-s}{2}\right)\sqrt{k}$$

$$e^{-\lambda^2/2} = e^{-\left(\frac{c-s}{2}\right)^2 \cdot k} = e^{-n^c}$$

$$\Rightarrow \Pr\left[\text{'}M\text{'} \text{ outputs wrong answer if } x \in L\right] \leq e^{-n^c}$$

$x \notin L$ similar (symmetric)

$\boxtimes$

Thanks to Shafi Goldwasser for this page

RP

- Search Problems

Goal: is to find x s.t. $V(x) = 1$

$\therefore$ V given by poly size circuit $V: \{0,1\}^m \to \{0,1\}$

Search-V Problem $\in$ Randomized Polytime

if $\exists$ eff. alg whose outputs satisfies V.

Promise RP- Search:

Input = (C, V) circuits

Promise = $\Pr_{z}[V(C(z)) = 1] \geq 2/3$

Task: Output x s.t. $V(x) = 1$.

Promise - BPP - Search ?

Input = circuits C, V

Promise: $\Pr_{z}\left[\Pr_{y}[V(C(z), y) = 1] \geq 2/3\right] \geq 2/3$

Task: Output x s.t. $\Pr_{y}[V(x, y) = 1] \geq 2/3$.