Randomized Complexity Classes

TECHNISCHE UNIVERSITÄT DARMSTADT

Las Vegas algorithms:	**Monte Carlo** algorithms:
always correct result,	always polynomial time,
expected time polynomial	results expected correct

Def: $L \in \mathbf{RP}$ if there is a polytime NTM which

- on inputs $\underline{x} \notin L$ has only rejecting computations
- on inputs $\underline{x} \in L$ has $\geq 50\%$ accepting computations.

$\mathbf{P} \subseteq \mathbf{RP} \subseteq \mathbf{NP}$ $\mathbf{RP} \subseteq \mathbf{BPP}$

∃strong pseudo-random number generators?

Example: MaMu $\in$ **coRP**.

Open Question: **P** versus **RP** versus **NP** versus **BPP**

Def: $L \in \mathbf{BPP}$ if there is a polytime NTM which

- on inputs $\underline{x} \notin L$ has $\geq 75\%$ rejecting computations
- on inputs $\underline{x} \in L$ has $\geq 75\%$ accepting computations.

Randomized Complexity Classes

Def: $L\in$ **PP** if there is a polytime NTM which

- on inputs $\underline{x}\notin L$ has $\geq$50% rejecting computations
- on inputs $\underline{x}\in L$ has >50% accepting computations.

Lemma: $L\in$ **BPP** if there is polyn. p and NTM which

- on all inputs $\underline{x}\in\Sigma^n$ makes exactly $p(n)$ steps
- on $\underline{x}\notin L$ has $\geq(1\text{-}2^{-n})\cdot 2^{p(n)}$ rejecting computations
- on $\underline{x}\in L$ has $\geq(1\text{-}2^{-n})\cdot 2^{p(n)}$ accepting computations.

Proof: Repeat O(n) times and report the majority vote

Def: $L\in$ **BPP** if there is a polytime NTM which
- on inputs $\underline{x}\notin L$ has $\geq$75% rejecting computations
- on inputs $\underline{x}\in L$ has $\geq$75% accepting computations.

Relativized Complexity Classes

Reminder: Turing reduction, oracle-TM $M^?$ has state $q_?$ and query tape: for $O \subseteq \Sigma^*$, $q_? \to q_1$ if contents $\in O$, else $\to q_0$

Theorem (Baker, Gill, Solovay 1975):
There exist $A,B \subseteq \Sigma^*$ such that $\mathbf{P}^A = \mathbf{NP}^A$ and $\mathbf{P}^B \neq \mathbf{NP}^B$

Definition: Fix some class $\mathbf{C}$ of languages.

$\mathbf{P}^{\mathbf{C}}$:= { $L \subseteq \Sigma^*$ decided by polytime ODTM M^O, $O \in \mathbf{C}$}

$\mathbf{NP}^{\mathbf{C}}$:= { $L \subseteq \Sigma^*$ decided by polytime O**N**TM M^O, $O \in \mathbf{C}$}

Examples:

a) $\mathrm{MinCircuit} \in \mathbf{coNP}^{\mathrm{SAT}} = \mathbf{coNP}^{\mathbf{NP}} \subseteq \mathbf{P}^{\mathbf{NP}^{\mathbf{NP}}}$ (Exercise)

b) $\mathbf{P}^{\mathbf{P}} = \mathbf{P}$, $\mathbf{NP}^{\mathbf{P}} = \mathbf{NP}$, $\mathbf{PSPACE}^{\mathbf{PSPACE}} = \mathbf{PSPACE}$

c) $\mathbf{NP} \cup \mathbf{coNP} \subseteq \mathbf{P}^{\mathbf{NP}}$; „$\neq$“ unless $\mathbf{NP} = \mathbf{coNP}$ (Exercise)