Computational Complexity

Mohammad Mahmoody

Session 22
April 2014

Complexity Class **BPP**

Definition 7.3 *(**BPP**, alternative definition)* A language L is in **BPP** if there exists a polynomial-time TM M and a polynomial $p : \mathbb{N} \to \mathbb{N}$ such that for every $x \in \{0,1\}^*$, $\Pr_{r \in_R \{0,1\}^{p(|x|)}}[M(x,r) = L(x)] \geq 2/3$.

Can **BPP** contain **NP** ? Probably not...

$NP \subseteq BPP \Rightarrow PH$ collapses.

$\Sigma_2 = \Pi_2$

Proof: Assuming $NP \subseteq BPP$ (*)

then: by (1) and (*)

$\Rightarrow NP \subseteq P/poly$ (**)

by (**) and (2) $\Rightarrow \Sigma_2 = \Pi_2$

Recall: (1) $BPP \subseteq P/poly$ (2) Karp-Lipton: $NP \subseteq P/poly \Rightarrow \Sigma_2 = \Pi_2$

if $L \in BPP \Rightarrow \exists M$ solves L with err. $< 2^{-n} \Rightarrow$ find r_n s.t.

hardwire r_n + Cook-Levin gives C_n $\Leftarrow \forall |x| = n \; M_{r_n}(x) =$ correct

PH = P

NP = P implies **BPP = P**

Theorem 7.15 *(Sipser-Gács Theorem)*
BPP $\subseteq \Sigma_2^p \cap \Pi_2^p \subseteq$ PH

RP ⊆ NP

Sufficient.. BPP ⊆ Σ2 ⟹ ? BPP ⊆ Π2

coBPP = BPP

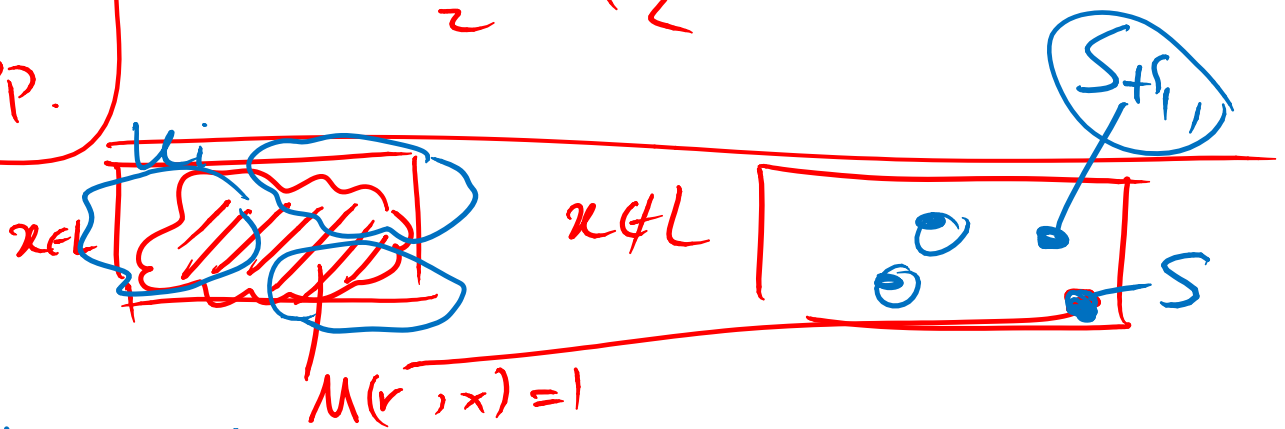
coBPP = BPP ⊆ coΣ2 = Π2

Sketch:

L ∈ BPP ⟹ L ∈ Σ2

idea: first decrease err < 2^{-n}

$x \in L$ iff $\exists u_1 \ldots u_k \; \forall r \; \bigvee_i M(u_i, r, x) = 1$



Hierarchy theorem for **BPP** ?

Open!

$(N)\ DTime(n^2) \subsetneq (N)DTime(n^4)$
(S) (S)

Open: $RTime(n^2) \overset{?}{\subsetneq} RTime(n^4)$

given: randomized $M(\cdot)$

$M(r, x) = \begin{cases} 0 \\ 1 \end{cases}$

huge difference {
- given poly-time det. $M(\cdot)$ it defines language
- given — random. $M(\cdot)$ not clear..

Zero-Error Probabilistic Algorithms

- What if M is randomized and $M(x)$ is correct with prob. 1 ? $\in P$

Given x T_x: random variable; time $M(x)$ ← random.

$\forall x \quad E[T_x] \leq T(n)$

Definition 7.7 The class **ZTIME**$(T(n))$ contains all the languages L for which there is a machine M that runs in an expected-time $O(T(n))$ such that for every input x, whenever M halts on x, the output $M(x)$ it produces is exactly $L(x)$.

We define **ZPP** $= \cup_{c>0}$**ZTIME**(n^c).

$ZPP \subseteq BPP$

$\subseteq RP \subseteq BPP$ ◇

$$\mathbf{ZPP \subseteq RP} \subseteq BPP$$

$$ZPP = coZPP \subseteq coRP$$

$L \in ZPP$: $\exists$ rand $M_r(x)$. runs in time T_n

$E[T_x] < p(x)$ ← Polynomial

$P_r[M_r(x) = \text{correct}] = 1$

Want. $\overline{M}$ that runs in $q(n)$ and gives $P_r[\overline{M}(x) = \text{correct}] \geq \frac{2}{3}$

Conj. $\overline{M}$: run M for $q(n)$ steps and { if M stops: output $M(x)$, oth.. output random.

Try: $q(n) = 3 \cdot p(n)$.

$\Rightarrow$ Claim $P_r[\text{err}] \leq \frac{1}{3}$