

Undergraduate Complexity Theory

Lecture 22: BPP

Marcythm

July 24, 2022

1 Lecture Notes

Definition 1.1. BPP, bounded probability of error probability computation (two sided-error prob poly time), $L \in \text{BPP}$ if \exists PTM N s.t.

$$\begin{aligned}x \in L &\implies \Pr[N(x) \text{ accept}] \geq 2/3 \\x \notin L &\implies \Pr[N(x) \text{ accept}] \leq 1/3\end{aligned}$$

current hierarchy: $P \subseteq ZPP \subseteq RP, \text{coRP} \subseteq RP \cup \text{coRP} \subseteq \text{BPP}$, all these are believed to be equal!
Alternative View: DTM $M(x, r)$ with input x and a random tape input r .

Lemma 1.2. $\text{BPP} \subseteq \text{EXP}$.

Corollary 1.3. $\text{BPP} \subseteq \text{PSPACE}$.

$\text{BPP} \subseteq \text{NP}$? not known. Even cannot separate BPP from NEXP.

Theorem 1.4. $P = \text{NP} \implies P = \text{BPP}$ (*contra*: $P \neq \text{BPP} \implies P \neq \text{NP}$).

Definition 1.5. P/poly is the class of languages with a circuit family of poly size deciding it.

Theorem 1.6. $\text{BPP} \subseteq P/\text{poly}$.

Proof. $L \in \text{BPP}$, \exists DTM M , $M(x, r)$ acc with $p \geq 1 - 2^{-2^{|x|}}$ if $x \in L$, acc with $p \leq 2^{-2^{|x|}}$ if $x \notin L$ in poly time. M can be translated into poly size circuit C_M , which has two kinds of inputs, x and r . The r input is what we should get rid of.

For each fixed $x \in \{0, 1\}^n$, all but $1/4^n$ of random coins r yield correct answer. Since only 2^n possible x and $1/4^n$ bad r for each, there are at most $1/2^n$ r s are bad for some x , i.e. most of r s are simultaneously good for all x , so find them and hardwire them into circuit. \square

Derandomization:

Theorem 1.7 ('98). *If 3SAT requires circuit family of size $2^{\delta n}$ for some $\delta > 0$, then $P = \text{BPP}$.*

two major steps: (worst-case hardness) to (strong average-case hardness) to (PRNG)

2 Reading

2.1 sipser 10.2 (Probabilistic Algorithms)

2.1.1 Read-Once Branching Programs

proof of $EQ_{\text{ROBQ}} \in \text{BPP}$: construct polynomial, randomly select an element in finite field.