6.842 Randomness and Computation February 17, 2022

Lectures on Derandomization

Lecturer: Ronitt Rubinfield *Scribe: Yuchong Pan*

1 Randomized Complexity Class

Definition 1. A *language* is a subset of $\{0,1\}^*$.

Definition 2. P is a complexity class that consists of all languages L with a polynomial time deterministic algorithm A.

Definition 3. RP is a complexity class that consists of all languages L with a polynomial time probabilistic algorithm A such that

$$\begin{aligned}
&\mathbb{P}[A \text{ accepts } x] \geq 1/2, && \text{if } x \in L,\\
&\mathbb{P}[A \text{ rejects } x] = 1, && \text{if } x \notin L,
\end{aligned}$$

This is called 1-*sided error*.

Definition 4. BPP is a complexity class that consists of all languages L with a polynomial time probabilistic algorithm A such that

$$\begin{aligned}
&\mathbb{P}[A \text{ accepts } x] \geq 2/3, && \text{if } x \in L,\\
&\mathbb{P}[A \text{ rejects } x] \geq 2/3, && \text{if } x \notin L,
\end{aligned}$$

This is called 2-*sided error*.

2 Derandomization via Enumeration

Consider a problem L in BPP. Given a randomized algorithm A that decides L with running time $t(n)$ and $r(n) \leq t(n)$ random bits, we can define a deterministic algorithm in Algorithm 1 that decides L. By the definition of BPP, the majority answer is the correct answer. The running time of Algorithm 1 is $2^{r(n)} \cdot t(n)$.

```
1 run A on every possible random string of length r(n)
2 output the majority answer
```

Algorithm 1: A deterministic algorithm that derandomizes a randomized algorithm A with running time $t(n)$ and $r(n) \leq t(n)$ random bits.

Definition 5. $\text{EXP} = \bigcup_c \text{EXP}(2^{n^c})$.

Corollary 6. BPP $\subseteq$ EXP.