Lecture 8. Randomized Complexity Classes

8.1 A randomized computation model

For studying randomized algorithms, we introduce a randomized Turing machine, which is a standard Turing machine equipped with a *random source tape*. The tape head of this tape can move only to the right reading one bit from the tape. Before the execution, we assume that a random binary sequence (which we call a *random source*) is given on this tape. For each such Turing machine $\mathtt{M}$, we use $r_{\mathtt{M}}(\ell)$ to denote an upper bound of the length of a random source consumed by the machine on length ℓ inputs, which we call a *random source length bound*. Clearly, we have $r_{\mathtt{M}}(\ell) \le \mathrm{time}_{\mathtt{M}}(\ell)$. For any ℓ, any input $x \in \{0,1\}^\ell$, and any $u \in \{0,1\}^{r_{\mathtt{M}}(\ell)}$, let $\mathtt{M}(x;u)$ denote the output of $\mathtt{M}$ when it is executed with x on its input tape and u on its random source tape. We will sometimes use $\mathtt{M}(x;u)$ to mean "the execution of $\mathtt{M}$ on input x and random source u."

We define the probability that the randomized Turing machine $\mathtt{M}$ outputs y on input x (denoted as the left hand side, or, more simply (or more explicitly, $\Pr_{\mathtt{M}}[\,\mathtt{M}(x) = y\,]$) as follows:

$$\Pr_u[\,\mathtt{M}(x;u) = y\,] \;=\; \frac{\left\|\,\left\{\, u \in \{0,1\}^{r_{\mathtt{M}}(\ell)} \mid \mathtt{M}(x;u) = y \,\right\}\right\|}{2^{r_{\mathtt{M}}(\ell)}}.$$

Note that a random binary string u is the source of the randomness used by $\mathtt{M}$; for any event on the execution of M on a given input x, we define its probability in the same way. For example, we can define the *average* running time of $\mathtt{M}$ on a given input x as follows.

$$\mathrm{E}_u[\,\mathrm{time}_{\mathtt{M}}(x)\,] \;=\; \sum_{t \ge 1} t \cdot \Pr_u[\,\mathtt{M}(x;u) \text{ terminates after the } t\text{th move}\,].$$

8.2 Randomized complexity classes

There are several ways to interpret the output of a randomized Turing machine. For any problem L, we consider here the following ways to solve L. (Note that L is a subset of $\{0,1\}^*$; recall that we identify a decision problem with a set of 'yes' instances.)

($\mathtt{M}$ barely solves L)

$$\begin{aligned} x \in L &\;\Rightarrow\; \Pr_{\mathtt{M}}\{\,\mathtt{M}(x) = 1\,\} \;>\; 1/2,\\ x \notin L &\;\Rightarrow\; \Pr_{\mathtt{M}}\{\,\mathtt{M}(x) = 0\,\} \;>\; 1/2. \end{aligned}$$

$$\begin{array}{l}
\text{Bounded error: } (\mathtt{M} \text{ solves } L \text{ in BP-style}) \\
\qquad x \in L \;\Rightarrow\; \Pr_{\mathtt{M}}\{\, \mathtt{M}(x) = 1 \,\} \;\geq\; 2/3, \\
\qquad x \notin L \;\Rightarrow\; \Pr_{\mathtt{M}}\{\, \mathtt{M}(x) = 0 \,\} \;\geq\; 2/3. \\
\text{One sided error: } (\mathtt{M} \text{ solves } L \text{ in R-style}) \\
\qquad x \in L \;\Rightarrow\; \Pr_{\mathtt{M}}\{\, \mathtt{M}(x) = 1 \,\} \;\geq\; 2/3, \\
\qquad x \notin L \;\Rightarrow\; \Pr_{\mathtt{M}}\{\, \mathtt{M}(x) = 0 \,\} \;=\; 1. \\
\text{One sided error: } (\mathtt{M} \text{ solves } L \text{ in coR-style}) \\
\qquad x \in L \;\Rightarrow\; \Pr_{\mathtt{M}}\{\, \mathtt{M}(x) = 1 \,\} \;=\; 1, \\
\qquad x \notin L \;\Rightarrow\; \Pr_{\mathtt{M}}\{\, \mathtt{M}(x) = 0 \,\} \;\geq\; 2/3. \\
\text{Zero error: } (\mathtt{M} \text{ solves } L \text{ in ZP-style}) \\
\qquad x \in L \;\Rightarrow\; \Pr_{\mathtt{M}}\{\, \mathtt{M}(x) = 1, \,\} \;=\; 1, \\
\qquad x \notin L \;\Rightarrow\; \Pr_{\mathtt{M}}\{\, \mathtt{M}(x) = 0 \,\} \;=\; 1.
\end{array}$$

Then define the following "standard" randomized complexity classes[1].

$$\begin{array}{lcl}
\mathrm{BPP} & = & \{\, L \mid \exists \text{ poly. time } \mathtt{M} \text{ solves } L \text{ in BP-style} \,\}, \\
\mathrm{RP} & = & \{\, L \mid \exists \text{ poly. time } \mathtt{M} \text{ solves } L \text{ in RP-style} \,\}, \\
\mathrm{coRP} & = & \{\, L \mid \exists \text{ poly. time } \mathtt{M} \text{ solves } L \text{ in coRP-style} \,\}, \\
\mathrm{ZPP} & = & \{\, L \mid \exists \text{ average poly. time } \mathtt{M} \text{ solves } L \text{ in ZPP-style} \,\}.
\end{array}$$

The following class is a bit different from the above classes because problems in this class may be still much more difficult than P. That is, the PP-style solvability is too weak to guarantee that the polynomial-time (or almost polynomial-time) tractability.

$$\mathrm{PP} \;=\; \{\, L \mid \exists \text{ poly. time } \mathtt{M} \text{ solves } L \text{ in PP-style} \,\}.$$

Note here that the choice of the threshold 2/3 is not so essential w.r.t. the polynomial-time computability. We can increasing correct probability quite easily stated as follows.

Lemma 8.1 (Correct probability amplification lemma)
For any decision problem L, suppose that we have a randomized $\mathtt{M}$ that solves L in BP-style. For any $m \geq 1$ (assuming odd), let $\mathtt{M}^{(m)}$ be a randomized Turing machine that, for a given input x, executes $\mathtt{M}(x)$ for m times independently and outputs the majority of the outputs of $\mathtt{M}(x)$. Then for any input x, we have

$$\Pr_{\mathtt{M}^{(m)}}\left[\, \mathtt{M}^{(m)}(x) \neq L(x) \,\right] \;\leq\; 2^{-m/32}.$$

This can be proved by using the following fact.

Fact (Chernoff bound) Consider independent random variables $X_1, \ldots, X_n$ such that each X_i takes value 1 with probability p and value 0 with probability $1-p$. Let $X = \sum_{i=1}^{n} X_i$ and $\mu = pn$. Then we have the following probability bounds.

$$\begin{array}{rcl}
\Pr[\, X > (1+\varepsilon)\mu \,] & \leq & \exp(-\mu\varepsilon^2/3), \\
\Pr[\, X < (1-\varepsilon)\mu \,] & \leq & \exp(-\mu\varepsilon^2/2)
\end{array}$$

[1]The class ZPP is defined in a different way in the Japanese textbook.

8.3 Complexity analysis of randomized complexity classes

Note that the solvability condition has the following order: ZPP-type $\Rightarrow$ R-type, co-Rtype $\Rightarrow$ BP-type $\Rightarrow$ PP-type, from which the following relations are immediate.

Theorem 8.2

$$\mathrm{P} \subseteq \mathrm{RP},\ \mathrm{coRP} \subseteq \mathrm{BPP} \subseteq \mathrm{PP}.$$

Though not trivial as above, the following relations are also easy.

Theorem 8.3

$$\mathrm{ZPP} = \mathrm{RP} \cap \mathrm{coRP}.$$

Intuitively we think that BPP (and its subclasses) is close to the class P. In fact, we may even conjecture that P = BPP. We show some justification for this conjecture. Recall[2] that PSIZE is the class of problems solvable by polynomial-size circuits. Due to the nonuniformity of our circuit model, we have PSIZE $-$ P $\neq \emptyset$, intuitively, we may think that they are very close complexity classes. By using this class, we can also show that BPP is close to P.

Theorem 8.4

$$\mathrm{BPP} \subseteq \mathrm{PSIZE}.$$

Proof. Consider any problem L in BPP, and let $\mathtt{M}$ be a polynomial-time randomized Turing machine that solves L in BP-style. By the correct probability amplification lemma, we can define $\mathtt{M}_1$ whose error probability is less than $2^{-\ell}$. We may assume that $\mathtt{M}_1$ is still polynomial-time and hence the random source length bound is also polynomial.

Consider any input length ℓ, and let $r = r_{\mathtt{M}_1}(\ell)$ be the length of a random source used by $\mathtt{M}_1$ on any input of length ℓ. (For some input, $\mathtt{M}$ may not use all bits of a given random source.) Then by using the fact that the error probability is less than $2^{-\ell}$ we can show that there exists a random source u_ℓ with which $\mathtt{M}_1$ does not make any error; that is, $\mathtt{M}_1(x; u_\ell) = L(x)$ for all $x \in \{0,1\}^\ell$. We call this u_ℓ a *universal sequence*. Then using this universal sequence, we can define a circuit C_ℓ for the problem L on inputs of length ℓ. A family of circuits are defined by using such C_ℓ's for all $\ell \geq 1$.

Homework exercise from Lecture 8

Homework rule: Choose one of the basic problems or the advanced prolem, and hand your answer in at the next class (for the basic problem) and at the next^2 class (for the advanced problem). (If you cannot attend the next class, you can submit your answer via email <u>before</u> the class.) You do not have to write a long answer. Usually one page would be enough. I will decide OK or NG, and you can get one point (for a basic problem) and two points (for an advanced problem) by each OK answer.

* For writing an answer, you may use Japanese.

[2] I might have forgot to defining this class; if not, then (sorry and) take this as the definition of PSIZE.

Basic problems

1. Prove Lemma 8.1.
2. Prove that ZPP $\subseteq$ RP $\cap$ coRP.
3. Prove that ZPP $\supseteq$ RP $\cap$ coRP.

An Advanced problem

1. In the proof of Theorem 8.4, we can also define $\mathtt{M}_2$ such that the 99% of its random sources are in fact universal sequences. In other words, almost all random sources are universal. Explain how to define $\mathtt{M}_2$ and why.