Randomized Computation (II)

Guan-Shieng Huang

Dec. 13, 2006

Randomized Complexity Classes

- RP: Randomized Polynomial time
- ZPP: Zero-error Probabilistic Polynomial time
- BPP: Bounded Probabilistic Polynomial time

RP

(Randomized Polynomial time)

Modelled as a non-deterministic Turing machine with

1. each computation on an input of length n terminates at $p(n)$ steps;
2. if $x \in L$, then at least half of the computations halts with "yes";
3. if $x \notin L$, then all computations halts with "no".

Remark Condition 2 can be relaxed to $\Omega(\frac{1}{p(n)})$.
Suppose the probability of false negative is at most $1-\eta$.

- Repeating the RP algorithm k times can reduce the probability $\leq (1-\eta)^k$.
- Let $k = \lceil \log_{(1-\eta)} \frac{1}{2} \rceil = \lceil -\frac{1}{\lg(1-\eta)} \rceil$, which makes $(1-\eta)^k \leq \frac{1}{2}$.
- $\lg(1-\eta) \approx -\frac{\eta}{\ln 2}$,
  $\therefore k \approx -\frac{1}{\lg(1-\eta)} \approx \frac{\ln 2}{\eta} = O(p(n))$ when $\eta = \Omega(\frac{1}{p(n)})$.

ZPP

(Zero-error Probabilistic Polynomial time = RP$\cap$coRP)

It meas that there are two RP algorithms, one for $x \in L$ and the other for $x \in \bar{L}$.

BPP

(Bounded Probabilistic Polynomial time)

$$\begin{cases} \texttt{Prob}[R(x) = \text{``yes''}] \geq \frac{3}{4} & \text{if } x \in L \\ \texttt{Prob}[R(x) = \text{``no''}] \geq \frac{3}{4} & \text{if } x \notin L \end{cases}$$

Remark The condition can be relaxed to

$$\begin{cases} \texttt{Prob}[R(x) = \text{``yes''}] \geq \frac{1}{2} + \epsilon & \text{if } x \in L \\ \texttt{Prob}[R(x) = \text{``no''}] \geq \frac{1}{2} + \epsilon & \text{if } x \notin L \end{cases}$$

where $\epsilon = \Omega(\frac{1}{p(n)})$.

The Chernoff Bound

(Estimate the tail probability of independent Bernoulli trials.)

- $x_1, \ldots, x_n$: independent random variables taking values 1 and 0 with prob. p and $1-p$, respectively.
- $X = \sum_{i=1}^{n} x_i$
- $0 \leq \theta \leq 1$

then $\texttt{Prob}[X \geq (1+\theta)pn] \leq \exp(-\frac{\theta^2}{3}pn)$.

Corollary Let $p = \frac{1}{2} + \epsilon$ for some $\epsilon > 0$.
Then $\texttt{Prob}[\sum_{i=1}^{n} x_i \leq \frac{n}{2}] \leq \exp(-\frac{\epsilon^2 n}{6})$.

Random Sources

Do we have true random sources?

- Pseudo randomness
- Perfect random source
- Slightly random source

Derandomization

Make a randomized algorithm deterministic without losing much efficiency.