Exercises – set 2
DESIGN METHODS
Shenggen Zheng, March 7, 2013, 8:30–9:30 B411

1. Suppose you are given a coin for which the probability of "heads", say ρ, is unknown. How can you use this coin to generate unbiased coin-flips? Give a scheme for which the expected number of flips of the biased coin for extracting one unbiased coin-flip is no more that $\frac{1}{\rho(1-\rho)}$.

2. Any Las Vegas algorithm A_1 can be converted to a Las Vegas algorithm A_2 that solves the same problem and never produces ??. Construction of A_2 is simple. Each time A_1 is to produce the output ??, what can be done only with bounded probability, a new run of A_1 is initialized with the same input. If A_1 accepts $x \in L$ with probability $\frac{1}{p(|x|)}$, A_1 rejects $x \notin L$ with probability $\frac{1}{q(|x|)}$. Let $T(|x|)$ be the running time of A_1 on input x.
   (a) If $\frac{1}{p(|x|)} = \frac{1}{q(|x|)} = \frac{1}{3}$, what is the expected running time of A_2?
   (b) Prove that the expected running time of A_2 on input x is $\mathbf{O}(\max\{p(|x|), q(|x|)\} \cdot T(|x|))$.

3. Let A be a algorithm for a language L such that
   (a) for $x \in L$, A accepts x with probability ε_x, where ε_x depends on $|x|$;
   (b) for $x \notin L$, A rejects x for sure.

   How many repetitions $k = k(|x|)$ of the work of A on x are necessary to achieve that A accepts x with probability $1 - \delta$ for any $x \in L$, if
   (i) $\varepsilon_x = \frac{1}{|x|}$,
   (ii) $\varepsilon_x = \frac{1}{2^{|x|}}$?

   If the number of times we repeat the algorithm A must not depend on the length of input x (i.e. a constant), we can design a new algorithm A' base on A as follows:

   Repeat the following ad infinitum:
   (1). run algorithm A on input x on;
   (2). if A accepts x, A' accepts x and halts;
   (3). if A rejects x, A' rejects x with probability $p(|x|)$ and halts.

   How large of $p(|x|)$ in order to achieve that A accepts x with probability $1 - \delta$ for any $x \in L$, if
   (i) $\varepsilon_x = \frac{1}{|x|}$,
   (ii) $\varepsilon_x = \frac{1}{2^{|x|}}$?

   What is the expected number of repetitions of A during execution of A'? (**Hint**: $p(|x|)$ is relative to $k(|x|)$.)