Lecturer: Thomas Rothvoss Due date: Friday, Mar 1, 2024, 11pm, on GradeScope

Problem Set 7

CSE 531 - Computational Complexity

Winter 2024

Exercise 7.1 (from the book of Arora and Barak; 10pts)
Show that one can efficiently simulate choosing a uniform random number from 1 to N using coin tosses. That is, show that for every $N \in \mathbb{N}$ and $\delta > 0$ there is a probabilistic algorithm A running in $\text{poly}(\log(N), \log(\frac{1}{\delta}))$ with output in $\{1, \ldots, N, ?\}$ such that

(a) Conditioned on not outputting ?, A's output is uniformly distributed in $\{1, \ldots, N\}$

(b) The probability that A outputs ? is at most δ.

Exercise 7.4 (Error Reduction for RP; from the book of Arora and Barak; 10pts)
Prove that for any polynomial $p(n)$ one has $\mathbf{RP}_{1-\frac{1}{p(n)}} = \mathbf{RP}_{2^{-p(n)}}$.