Assignment 4.

Post date: Oct. 13, 2014.
Due date: Oct. 20, 2014 (Monday) by noon. Hand in printed paper at assignment box at 4th floor of MC across from the tutorial centre.

Marking TA: Chuan Guo

Mandatory requirement for assignment being accepted:

The answers need to be typed up with a computer and printed on letter size paper. Only minor corrections can be made with handwriting. The first page of the submission must be a cover page that contains your name, student id, and course number (CS466 or CS666) and assignment number.

Question 1. (10 marks)

Generating random numbers is not a trivial task. One may have to rely on physical devices to produce "true" random numbers. Assume you have such a physical device that can reliably produce a random bit in constant time upon each request. The bit is 1 with probability p and 0 with probability q. Here p and q are two positive numbers that add up to 1. The results for different requests are independent to each other. When $p \neq q$, how can you utilize this device to obtain a random bit that is uniform (with probability 0.5 to be 0 and 0.5 to be 1). You are allowed to use a "Las Vegas" algorithm. More accurately, the algorithm can return the desired bit in expected constant time. However, when it returns, the bit must be a uniform random bit. Describe the algorithm, and prove the correctness and running time.

Question 2. (10 marks)

Now suppose you have access to a true random number generator that can give you a uniform bit (with probability 0.5 to be either 0 or 1) upon each request. Please design an algorithm to generate a random integer between 1 to N. Here N may not be a power of 2. Similar to Question 1, here you are also allowed to use a "Las Vegas" algorithm. Describe the algorithm, and prove the correctness and running time.

Question 3. (10 marks)

Suppose you have a polynomial time Las Vegas algorithm for a problem. Prove that there is also a polynomial time Monte Carlo algorithm with one-sided error for the same problem.