Algorithms – CMSC-27200/37000 Homework – January 7, 2004
Instructor: László Babai Ry-164 e-mail: `laci@cs.uchicago.edu`
Text: *"Introduction to Algorithms,"* by Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Cliff Stein, published by MIT Press and McGraw-Hill. Available in the Seminary Bookstore (University Ave at 58th St).

In all assignements, the term "grad students" will refer to those seeking 37000 credit, regardless of actual graduate or undergraduate status, similarly, "undergraduates" refers to those seeking 27200 credit. **G** and **U**, respectively, will abbreviate these terms.

READING (due next class) Review the elements of Number Theory (especially, congruences and Euclid's algorithm) from Discrete Mathematics (CMSC-17400) Review asymptotic notation. Study the PSEUDOCODE conventions.

HOMEWORK. Please print your name and U/G status on each sheet. Please try to make your solutions readable. Unless expressly stated otherwise, all solutions are due at the **beginning of next class.**

1.1 (U,G) (8 points) Suppose we are given a sorted list $A[1..n]$ (as an array), of n real numbers: $A[1] \leq A[2] \leq \ldots \leq A[n]$. Given a real number x, decide whether x is in the array, using **binary search**: compare with the middle, eliminate half the elements, etc. Write a short and elegant pseudocode for this algorithm. State the exact number of comparisons your algorithm will make in case x is not in the array. Do NOT write a recursive algorithm.

1.2 (U,G) (Due Monday, 10 points) Recall the communication complexity problem discussed in class: Two processors, Alice and Bob, each possess a string of 10^{15} binary digits (bits); Alice's string is X, Bob's string is Y. The problem is to determine whether or not $X = Y$ with minimum number of bits communicated between Alice and Bob. The Yao–Rabin–Simon protocol solved this problem using the following steps:

1. Alice generates a 300-bit prime, chosen uniformly at random from among all 300-bit prime numbers (each 100-bit prime has the same probability to be selected).
2. Alice calculates the quantity $(X \bmod p)$, the remainder of the division of X (a 10^{15}-bit integer) by p. Note that this remainder has at most 300 binary digits.

3. Alice sends p and $(X \bmod p)$ to Bob.
4. Bob calculates $(Y \bmod p)$.
5. If $(X \bmod p) \neq (Y \bmod p)$ then Bob outputs "NO." Else, Bob outputs "YES."

The cost of this protocol is at most 600 bits of communication (step 3); the cost of local computation by either Alice or Bob is ignored in the "communication complexity" model.

We proved in class that no matter what the input strings X, Y, the probability that the output is in error is less than 2^{-72}.

Extend the protocol to solve the following problem: if $X \neq Y$, *find the location of a digit* where X and Y differ. Accomplish this with less than 20,000 bits of communication. The probability of error should be exactly the same as the probability that the Yao–Rabin–Simon protocol errs. (*Hint.* Start with applying the Yao-Rabin-Simon protocol. If the output produced is "NO," proceed deterministically (no more random numbers generated) to find a location where X and Y differ.) **Grad students (2 extra points)** use less than 13,000 bits of communication.

3 (U, G) (Due Monday) For (a), (b), (c) below, answer: true or false? (Clearly state your answer and **prove it.** Use, without proof, the fact that $(\forall c > 0)(\log n = o(n^c)$ (little-oh). Indicate where and how this fact helps you.)

(a) (2 points) $n^2 = O(n^2 - 100n^{3/2} \log n)$.

(b) (2 points) $n = O((n - \sqrt{n})/2)$.

(c) (2 points) $2^n = O(2^{n/2})$.

(d) **(Grad only)** (2 points) Find two sequences a_n and b_n of integers such that $\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n = \infty$ and neither $a_n = O(b_n)$ nor $b_n = O(a_n)$ holds.

4 (U, G) (Due Monday) CLR, Problem 3.2, Page 58

5 (U, G) (Due Monday) CLR, Problem 3.3, Page 58