Algorithms CMSC-37000 Final Exam. March 15, 2007

Instructor: László Babai

Show all your work. **Do not use text, notes, or scrap paper.** When describing an algorithm in pseudocode, **explain the meaning of your variables** (in English). This exam contributes 30% to your course grade. **Take this problem sheet home** for your amusement.

1. (15 points) Let $L \in \mathrm{NP}$. Prove that L is recursive (computable). Estimate the time it takes to decide membership in L for a string of length n.

2. (20 points; lose 8 points for each mistake) Consider the following three statements: (A) Hamiltonicity of graphs can be decided in polynomial time. (B) RSA can be broken in polynomial time. (C) Integers can be factored into their prime factors in polynomial time.

   Which of the six implications is known (circle all that apply): (A) $\Rightarrow$ (B); (B) $\Rightarrow$ (A); (A) $\Rightarrow$ (C); (C) $\Rightarrow$ (A); (B) $\Rightarrow$ (C); (C) $\Rightarrow$ (B).

   Do not prove.

3. (25 points) (k-way merge) Given k sorted lists of reals, merge them into a single sorted list in $O(n \log k)$ where n is the total number of items. Describe your algorithm in high level pseudocode. You may refer to a known data structure.

4. (15+10+8)

   (a) Describe the "update" subroutines for Dijsktra's algorithm and for Jarník's (a.k.a. Prim's) algorithm.

   (b) Give an accurate definition of the problems solved by each of these algorithms (input, including the assumptions on the input, and an exact description of the output; make a clear distinction between directed and undirected graphs).

   (c) Name the three abstract data structure operations required to implement each of these algorithms.

5. (30 points) A divide-and-conquer algorithm reduces a problem instance of size n to two instances of size $n/2$ each. The overhead (cost of the reduction) is $O(\sqrt{n})$. State the recurrence for the complexity $T(n)$. Prove: $T(n) = O(n)$.

6. (25 points) Find three languages L_1, L_2, L_3 over the same alphabet such that $L_1 \subset L_2 \subset L_3$ and $L_2 \in \mathrm{P}$ while L_1 and L_3 are undecidable.

7. (25 points) Recall that the integer g is a *primitive root modulo the prime* p if $g^{p-1} \equiv 1 \pmod{p}$ but $g^k \not\equiv 1 \pmod{p}$ for any k in the interval $1 \leq k \leq p-2$. Let ROOT $= \{(p, g) : p$ is a prime and g is a primitive root modulo $p\}$. Prove: ROOT $\in \mathrm{NP} \cap \mathrm{coNP}$. Use the result that PRIMES $\in$ NP (Pratt, 1976), but do not use the theorem that PRIMES $\in$ P (AKS, 2002).

8. (30 points) The "weighted interval scheduling" problem takes as input a list of n intervals $(s(i), t(i))$ and corresponding weights $w_i > 0$ and asks to find a set of disjoint intervals among these of maximum total weight. Solve this problem in $O(n)$ plus sorting whatever needs to be sorted. Hint: dynamic programming. Half the credit goes for a clear definition of the array of problems to be solved (the "brain" of the algorithm).

9. (12 points) On an $n \times n$ matrix, Gaussian elimination takes $O(n^3)$ arithmetic operations. Why is it not evident then that solving a system of linear equations using Gaussian elimination is polynomial time? (Assume we have n linearly independent equations in n unknowns, so the solution is unique.)

10. (25 points) (a) Batcher's odd-even merging network has depth (parallel time) $M(n)$. Write a recurrence for $M(n)$. Evaluate $M(n)$ for $n = 2^k$. (b) Batcher's sorting network has depth $S(n)$. Write a recurrence for $S(n)$. Evaluate $S(n)$ (exactly) for $n = 2^k$.

11. (12 points) What is the (a) minimum (b) maximum number of keys stored in a 3-4-5-6-tree (B-tree with parameter $t = 3$) of height h? Give simple closed-form expressions. Prove.

12. (20 points) As part of a divorce settlement, Alice wants to send a digitally signed note to Bob ("the pet is yours") using a public key cryptosystem (not necessarily RSA). Describe how this is done; indicate who needs to have a public key (Alice or Bob). In case Alice wants to keep the pet, indicate how Bob can prove to a judge that the note came from Alice, and why should the judge believe.

13. (18+20B points) (a) Given a list of reals, $a_1, \ldots, a_n$ and an odd positive integer k, let b_i denote the median of the sublist $\{a_i, a_{i+1}, \ldots, a_{i+k-1}\}$.

Determine $b_1, \ldots, b_{n-k+1}$ in $O(n \log k)$. (b) (Bonus problem) Let $c_i = \min\{a_i, a_{i+1}, \ldots, a_{i+k-1}\}$. Determine $c_1, \ldots, c_{n-k+1}$ in $O(n)$.

14. (10+15B points) (a) Given k, prove that F_k (the k-th Fibonacci number) cannot be computed in polynomial time. (b) Given k and m, compute $F_k \pmod m$ in polynomial time. Assuming m and k are both n–bit integers, estimate the time; state the exponent of n.