

Algorithms CMSC-37000 Midterm Exam. February 23, 2006
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 midterm contributes 12% to your course grade. **TAKE THIS PROBLEM SHEET HOME** and work on it.

1. (7+4+3)
 - (a) Describe the “update” subroutine for Dijkstra’s algorithm and for Prim’s algorithm. (Prim’s was the second algorithm we studied for the min cost spanning tree problem).
 - (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).
 - (c) Name the three abstract data structure operations required to implement each of these algorithms.
2. (15 points) Describe in pseudocode an algorithm that finds the convex hull of n points in the plane in $O(n \log n)$ steps. Do not analyze.
3. (4+9 points) A “divide and conquer” algorithm reduces an instance (input) of size n to an instance of size $\lfloor n/2 \rfloor$ and two instances of size $\lfloor n/5 \rfloor$ each. The cost of the reduction is $O(n)$. (a) State the recurrence satisfied by $T(n)$. (b) Prove: $T(n) = O(n)$.
4. (4 points) Name two significant computational tasks, discussed in class, each of which led to the recursive inequality $T(n) \leq 2T(n/2) + O(n)$.
5. (6+6 points) Consider the implementation, discussed in class, for the UNION-FIND data structure, which builds a directed tree in every “country,” directed toward the “capital.” We discussed two UNION strategies: (a) bigger wins; (b) deeper wins. Prove that under each of these strategies, the depth of each tree remains $\leq \log n$ where n is the number of “cities.”

6. (a) (4 points) Define the concept of a “loop invariant.” Be as formal as reasonable. Make sure you give a clear definition of what kind of statement can be a candidate loop invariant. Include the definition of the domain and range of the predicates and transformations (functions) involved.
- (b) (3+3+3 points) Decide which of the following statements are loop-invariants for Dijkstra’s algorithm. Reason your answers. (b1) All black vertices are accessible. (b2) All accessible vertices are black. (b3) All accessible vertices will eventually become black.
7. (4+5+3+10 points)
- (a) Alice wants to receive RSA-encrypted messages. State (i) her public key (ii) her private key.
- (b) Given Alice’s two prime numbers p, q and her choice of a public exponent e , name the computational task she needs to perform to create her private exponent f . Name this task in general terms, without reference to the RSA context. Indicate what algorithm she needs to use to compute f in polynomial time. Do not code or analyse.
- (c) Bob wants to send Alice a message using Alice’s public RSA-key. State Bob’s main computational task (in general terms, without reference to the RSA context).
- (d) Solve Bob’s task in polynomial time. Describe the required algorithm in pseudocode. Your algorithm should make no recursive calls. - Do not analyse the algorithm.
8. (5 points) Suppose algorithm \mathcal{A} takes as input an array of n real numbers, arranged in a heap (in accordance with the array implementation of heaps discussed in class). \mathcal{A} sorts such an input using $\leq T(n)$ comparisons. Prove: $T(n) \gtrsim n \log n$.

Note: this is *not* a question about the Heapsort algorithm. \mathcal{A} can take advantage of its random access to the array and make whatever comparisons it wishes to; it is by no means bound by the heap structure. If it wishes, it can take advantage of the comparisons implicit in the heap structure. You are asked you to prove that this advantage is insignificant.