Honors Algorithms CMSC-27230 Second Quiz. February 20, 2020

Instructor: László Babai

NAME (print with LARGE letters) _____

Are you using a cheat sheet? Circle the answer: YES NO
If YES, do not forget to **hand it in** at the end of the test.

Please DO NOT SIT next to anyone (leave an empy seat). Please do not sit near a person to whom you usually sit near in class.

SHOW ALL YOUR WORK. Do NOT use book, notes, or scrap paper. You may use a "cheat sheet": one page of HANDWRITTEN notes in English, written in ink in your handwriting with your name printed in large English letters on the top. NO PHOTOCOPIES! Hand in your cheat sheet with the test.

The use of ELECTRONIC DEVICES is STRICTLY FORBIDDEN.

Write your answers IN THE SPACE PROVIDED. You may **continue on the reverse.** DO NOT USE paper other than the problem sheet provided.

When describing an algorithm in pseudocode, **explain the meaning of your variables** (in English).

This quiz contributes 6% to your course grade.

1. (8 points) Given an n-bit integer $x \geq 2$, we wish to decide whether x is a prime number. We use the following algorithm.

```
0    Initialize: Y := 2
1    while Y^2 ≤ x
2        if Y is a divisor of x
3            then exit while-loop, return "x is composite"
4            else Y := Y + 1
5    end(while)
6    return "x is prime"
```

The time to execute line 2 (decide divisibility) is $O(n^2)$.
Is this a polynomial-time algorithm? Prove your answer.

2. (3+4+6+10 points)

(a) Define the configuration space for an algorithm.

(b) Define the concepts of "predicate" and "transformation" in complete sentences.

(c) Define the concept of a "loop invariant" for a **while**-loop.

(d) Recall the **modular exponentiation** problem:
Calculate $(a^b \bmod m)$ where a, b, m are integers, $a, m \geq 1$, $b \geq 0$.

We solved this problem by the method of **repeated squaring**. Here is the algorithm.

```
0    Initialize: X := 1, B := b, A =: (a mod m)
                 [X is the "accumulator" that collects the partial results]
1    while B ≥ 1 do
2        if B odd then B := B − 1, X := (AX mod m)
3        else B := B/2, A := (A^2 mod m)
4    end(while)
5    return X
```

State and prove the relevant loop invariant for this algorithm and use it to prove the correctness of the algorithm.

3. (12+4+5 points) Let (V, E, s, t, c) be an integral flow network. Here $G = (V, E)$ is a digraph, $s \neq t$ are vertices, and $c : E \to \mathbb{N}^+$ is the assignment of positive integer capacities to the edges.

   (a) Prove: If the maximum $s \to t$ flow is positive then there exists an $s \to \cdots \to t$ directed path in G. (Note: a *path* has no repeated vertices.)

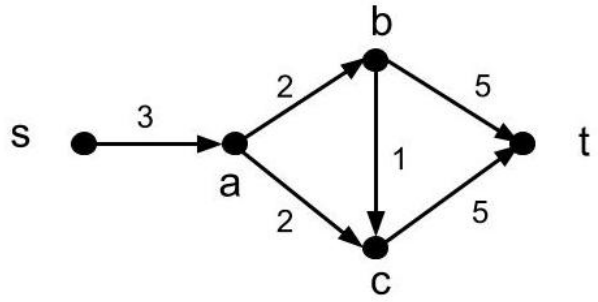
   (b) An edge e is *saturated* by a flow if it is used at full capacity, i.e., if $f_e = c_e$, where c_e is the capacity of edge e and f_e is the amount of flow passing through e.
   TRUE or FALSE: Let $f = (f_e \mid e \in E)$ be a maximum flow. If the value of this flow is positive then there exists an $s \to \cdots \to t$ directed path consisting of saturated edges (all edges of the path are saturated).
   If True, prove. If False, draw the smallest counterexample (minimum number of edges). State the capacities and the flow amounts in your diagram. You don't need to prove that your example is smallest.

   (c) TRUE or FALSE: Let $f = (f_e \mid e \in E)$ be a maximum flow. If the value of this flow is zero then $(\forall e \in E)(f_e = 0)$. (Same rules as for (b).)

4. (8 points) Consider the flow network in the diagram. The capacity of each edge is indicated next to the edge. Consider the following flow f:

   $f(s,a) = 3,\ f(a,b) = 1,\ f(b,t) = 1,\ f(a,c) = 2,\ f(c,t) = 2, f(b,c) = 0$

   Draw in a separate diagram the residual digraph G_f. Indicate on each edge of G_f its orientation and the residual capacity. Make your diagram large and the markings clear.



5. (Bonus, 15 points) Consider an integral flow network (V, E, s, t, c) and a maximum $s \to t$ flow f as in Problem 3. Let G_f denote the residual digraph. Prove: there exists a $t \to \cdots \to s$ directed path in G_f.