Algorithms – CS-37000 Homework 10 – March 2, 2006

Instructor: László Babai Ry-164 e-mail: laci@cs.uchicago.edu

ADVICE. Take advantage of the TA's problem sessions. This is the **principal venue to discuss past homework and test problems.** Note that such problems may prop up in future tests.

READING. Review all previous handouts and readings. New reading, due Tuesday, March 7: text 8.1–8.5 (polynomial time reductions, NP, NP-completeness), 8.9 (coNP), 8.10 (hard problems)

Previously assigned , due Tuesday, March 7: text 6.3 (Segmented Least Squares (dynamic programming)); text pp.83–94 (depth-first seach (DFS)); 3.6 topological ordering pp.99-104.

HOMEWORK. Please **print your name on each sheet.** Put each solution on a separate sheet. Please try to make your solutions easily readable.

This homework is due on **Tuesday, March 7**.

10.1 (8 points) Prove: $\mathcal{RE} \cap co\mathcal{RE} = \mathcal{R}$. Here $\mathcal{R}$ is the set of computable sets and $\mathcal{RE}$ is the set of computably enumerable sets.

10.2 (8 points) If we omit the bound on the length of the witness in the formal definition of NP, we get a definition of another complexity class discussed in class. Which one? State the modified definition and prove your answer.

10.3 (5 points) Prove: if $P = NP$ then $NP = coNP$.

10.4 (5+5+5 points)

(a) Give a Karp-reduction from 3-SAT to HALT. (HALT is the language consisting of those C-programs which take no input and eventually terminate.)

(b) Prove that HALT has no Karp-reduction to 3-SAT.

(c) Prove that HALT has no Cook-reduction to 3-SAT.

10.5 (6 points) ILPf (integer linear programming feasibility) belongs to NP, but this fact is far from obvious. What is the problem with this attempted proof: if an ILP has a solution, then the solution itself is a witness.

State a mathematical conjecture we would need to prove to make the above argument complete. (If your answer is right, your conjecture will be true.)

10.6 (8+B10 points) Prove that $FACT \in \text{NP} \cap \text{coNP}$. Here $FACT = \{(m, a) : (\exists d)(2 \le d \le a \text{ and } d \mid m)\}$. (Here m and a are integers.) (a) Prove this result using the AKS theorem (Agrawal-Kayal-Saxena: primality is in P). Clearly state how you are using AKS. (b) (Bonus problem) Do not use AKS.

10.7 (6 points) Reproduce from class the proof that FACT is Cook-equivalent to the problem of factoring integers (INPUT: a positive integer m; output: the list of prime factors of m.)

10.8 (8 points) Assuming that 3-COL is NP-complete, prove that 4-COL is NP-complete. (k-COL is the set of k-colorable graphs.)