Algorithms – CS-27200/37000 Homework – February 18, 2005

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

TA SCHEDULE: TA sessions are held in Ryerson-255, Tuesday and Thursday 5–6pm, Saturday 11am–noon, and (this is new) **Wednesday after class** 12:30–1:20 or 1:30–2:20 depending on demand. Indicate your interest in the Wednesday session to the instructor immediately after class. (The Wednesday evening sessions are discontinued.)

ADVICE. Take advantage of the TA sessions.

Check the class website, `http://www.classes.cs.uchicago.edu/current/27200-1`.

DATES TO REMEMBER: Mon Feb 21: Quiz 2, Mon Mar 7: Midterm 2, Fri Mar 11: Last class. ATTENDANCE REQUIRED. Fri Mar 18, 10:30–12:30: Final Exam

15.1 (6 points) Let G be an undirected graph (given, as usual, by an array of adjacency lists). Design an algorithm which decides whether or not G contains a cycle and if it does, finds one (outputs the sequence of vertices in the order they occur in the cycle). Your algorithm should run in linear time. Describe it in pseudocode. *Elegance counts.*

15.2 (5 points) Give a simple formula describing a function $f(n)$ of *intermediate growth*: $f(n)$ should grow faster than any polynomial function and slower than any exponential function. Here "exponential function" refers to a function of the form $c^{n^{1/k}}$ for any constants $k, c > 1$. The terms "faster" and "slower" growth refer to the appropriate little-oh relation between functions. State $f(n)$ and prove that it satisfies the required asymptotic relations.

15.3 In this problem, all graphs are *undirected.* Recall that a *clique* in a graph is a subset S of the vertex set such that the members of S are pairwise adjacent. (In other words, a clique is a complete subgraph.) The *size* of this clique is $|S|$. Suppose we have a black box which takes as input a pair (G, k) where G is a graph and k is a positive integer. The black box outputs "yes" if G contains a clique of size $\geq k$; "no" otherwise. In other words, the black box tests membership in the language CLIQUELANG $= \{(G, k) : G$ is a graph, k is an integer, and G contains a clique of size $\geq k\}$. Perform the following *Cook-reductions* to CLIQUELANG.

(a) (4 points) Given a graph $G = (V, E)$, determine the *maximum clique-size* in polynomial time using this black box. You are allowed to make $\leq \lceil \log(|V| + 1) \rceil$ queries to the black box. (The computation time includes the time it takes to write down the questions posed to the black box.) Describe your algorithm in English. Clarity is paramount.

(b) (G only, 5 points) Given a graph $G = (V, E)$, *find a clique of maximum size* in polynomial time using this black box. You are allowed to make a polynomial number of queries to the black box. Describe your algorithm in pseudocode.

15.4 (Due Wednesday, February 23.) The SUBSET-SUM problem is defined as follows: the input is a list of positive integers $a_1, \dots, a_k, b$; the question is to decide whether or not there exists a subset $S \subseteq \{1, \dots, k\}$ such that $\sum_{i \in S} a_i = b$. (Example: for input $31, 41, 28, 17, 19, 77$ the answer is "yes" since 41+17+19=77.)

(a) (5 points) Prove that SUBSET-SUM $\in$ NP. State the (polynomial-time verifiable) witness (of the yes-answers). Indicate why it is verifiable in polynomial time (length of input to verification algorithm, estimated running time of verification).

(b) (Grad only, 7 points) Solve this problem in $O(kb)$ steps (a step is an arithmetic operation or a pointer update). Describe your algorithm in pseudocode. (The output should be "yes" or "no," you don't need to find the subset S.)

15.5 (G only, 8 points. Due Wednesday, Feb 23. Undergrads: review the definition of the language FACTLANG and understand why this is the def.) Prove: if FACTLANG $\in$ NPC then NP = coNP. Here FACTLANG is the decision version of the factoring problem, defined as FACTLANG $= \{(a, x) : (\exists d)((2 \le d \le a) \text{ and } d \mid x)\}$. WARNING: there was a typo in this definition in the version handed out in class.