Martin Ziegler
MiJin Kim

Issued on Nov.24, 2015
Solutions due: Dec.8, 2015

CS422

Fall 2015, Assignment #4

PROBLEM 10 (2+2+2+2+2+2+2+2+2P)**:**
Formalize the following decision problems as subsets of $\mathbb{N}$.
Which ones are in $\mathcal{NP}$, which are (provably/probably) not — and why?

a) Given a `WHILE+` program with quadratic runtime; does there exist an input x it accepts?

b) Given a finite automaton; does there exist an input $\vec{x}$ it accepts?

c) Given a multivariate integer polynomial; does it have an integer root?

d) Given a multivariate integer polynomial; does it have a real root?

e) Given two Boolean expressions; are they equivalent?

f) Given a Boolean expression; does there exist a shorter, equivalent one?

g) Given a configuration of a game of Go (Baduk, Weiqi); does black have a winning strategy?

h) Given two graphs G and H; are they isomorphic?

j) Given a graph G; can it be drawn on the plane without edges crossing?

PROBLEM 11 (2+1+~~2~~+5+2P)**:**

a) Devise a polynomial-time reduction from SubsetSum to ILP as defined in the lecture.

b) Let $G = (V, E)$ denote a (directed or undirected) graph and $s, t \in V$. Prove that there exists a path in G from s to t of length at most 2^k iff there exists a vertex $r \in V$ and paths from s to r as well as from r to t of length at most 2^{k-1} each.

~~c) Devise a recursive algorithm that, given a graph $G = (V, E)$ and vertices $s, t \in V$, decides whether there exists a path in G from s to t using only $\mathcal{O}(\log^2 n)$ bits of memory/space.~~

d) Devise a parallel algorithm/circuit that solves the problem from c) in time $\mathcal{O}(\log^2 n)$ using poly(n) processors/gates. Hint: repeatedly square the Boolean adjacency matrix.

e) Prove that there exists a $L \subseteq \mathbb{N}$ which can be decided in space $\mathcal{O}(n^4)$ but not in space $\mathcal{O}(n^2)$.

PROBLEM 12 (2+3P)**:**

a) Install the public-key system `pgp` on your computer; free versions are available from GNU for LINUX, WINDOWS, and MACOS X. Become familiar with the software (RTFM). Create a key pair! Deliberate on where to store the private and how to distribute the public part.

b) Print, and submit on Dec.8, 25 ‘tickets’ showing your name and public key’s fingerprint. Send me your solutions of Problems #10+#11 (scan/readable photo/PDF) by 2pm of Dec.8, signed with your private key and encrypted with my public one: available for instance from `http://pgp.mit.edu/pks/lookup?op=get&search=0x227F4D274A4BE6FE` with fingerprint `AF37 ECD4 AEBE 3D4E 76EB 4445 227F 4D27 4A4B E6FE`.