CS670 Final Exam - Prof. Ming-Deh Huang

Dec 17, 2012

Duration: 2 hour. Be concise and accurate. Calculators are allowed.

1. Give an $O(n \log n + m)$-time algorithm that on input a weighted connected and undirected graph $G = (V, E)$ with n vertices and m edges and an edge $e \in E$, constructs a spanning tree of G with minimum possible weight that contains e. Argue that your algorithm works and analyze its time complexity. (20%)

2. Let $G = (V, E)$ be a weighted directed graph with n vertices and m edges where the weight $w(e)$ for all $e \in E$ is non-negative. Construct an $O(n \log n + m)$ time algorithm that given $s, t \in V$, find all vertices $v \in V$ such that v lies on some shortest path from s to t. (20%)

3. Suppose we are given a flow network N with a source and a terminal and a flow f of N. (a) Show that it can be checked in linear time whether the flow is a maximum flow. (b) Let N_f denote the residual network of N induced by f. Show that a flow g of N_f is maximum if and only if $f + g$ is a maximum flow of N. (20%)

4. Let p be an odd prime. A number $a \in \mathbb{Z}_p^*$ is called a quadratic residue if the equation $x^2 = a \pmod p$ has a solution for the unknown x. Define the Legendre symbol $(\frac{a}{p})$, for $a \in \mathbb{Z}_p^*$, to be 1 if a is a quadratic residue modulo p and -1 otherwise. Let $n = pq$ where p and q are distinct odd primes. For $a \in \mathbb{Z}_n^*$ define $(\frac{a}{n}) = (\frac{a}{p})(\frac{a}{q})$. (i) Let $a \in \mathbb{Z}_n^*$ such that $a \equiv 1 \pmod p$ and $(\frac{a}{q}) = -1$. Show that $(\frac{a}{n}) = -1$, and that $a^{\frac{n-1}{2}} \not\equiv (\frac{a}{n}) \pmod n$. (ii) Use (i) to design an algorithm that on input a positive integer n outputs 1 if n is prime and outputs 0 with probability at laest 1/2 if n is the product of two distinct odd primes. (20%)

5. A hamiltonian cycle of an undirected graph $G = (V, E)$ is a simple cycle that contain every vertex in V. The hamiltonian cycle problem is: given an undirected graph G does G have a hamiltonian cycle? The problem is known to be NP-complete. Consider the following problem: given an undirected graph G and a positive integer k, does G have a simple cycle of length k? Give a polynomial time transformation from the hamiltonian cycle problem to this problem and show that the problem is NP-complete. Then show that if the problem is decidable in polynomial time then the following problem can also be solved in polynomial time: given an undirected graph G to find a simple cycle on G of maximum length. (20%)