TU Dresden, Fakultät Informatik
Daniel Borchmann

Summer Term 2016

Advanced Topics in Complexity Theory

Exercise 3: Function Problems

2016-04-19

Exercise 3.1 Show that FSAT is FNP-complete. For this first show that the function problem for

$$\mathsf{A}_{\mathsf{NPTM}} = \{ \langle M, w \rangle \mid M \text{ a polytime NTM accepting } w \}$$

is FNP-complete.

Exercise 3.2 Consider the following function problem: given numbers $a_1, \dots, a_n$ such that $\sum_{i=1}^{n} a_i < 2^n - 1$, find two different subsets $S_1, S_2 \subseteq \{ 1, \dots, n \}$ such that

$$\sum_{i \in S_1} a_i = \sum_{i \in S_2} a_i.$$

Show that this problem is in TFNP.

Exercise 3.3 Let $G = (V, E)$ be an undirected graph with integer weights w on its edges. Think of the nodes as people, and of the edges as an indication of how much two people like each other (or not). A *state* of G is a mapping $S \colon V \to \{ +1, -1 \}$. We say that node i is *happy* in state S if

$$S(i) \cdot \sum_{\{i,j\} \in E} S(j) w(i,j) \geq 0.$$

The HAPPYNET problem is to find for each graph G a state in which each node is happy. Show that HAPPYNET is in TFNP. For this consider the mapping φ defined for states S by

$$\varphi(S) = \sum_{\{i,j\} \in E} S(i) S(j) w(i,j)$$

and suppose that some node i is unhappy. What happens to the value of $\varphi(S)$ if one flips the current state of i?

Exercise 3.4 The goal of this exercise is to show that Primes is in NP (this is Pratt's Theorem). To this end we shall see that we can associate to every prime p a short certificate $C(p)$ that can be checked in polynomial time and that no non-prime number has.

For this we make use of the following characterization of primes, proving which is not part of this exercise: a number $p > 1$ is prime if and only if there is some $1 \leq r < p$ such that $r^{p-1} \equiv 1 \pmod{p}$ and $r^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$ for all prime divisors q of $p - 1$.

From this characterization, let us define the certificate $C(p)$ for a prime p as

$$C(p) = (r, q_1, C(q_1), \dots, q_\ell, C(q_\ell))$$

where $q_1, \dots, q_\ell$ are all prime divisors of $p - 1$.

1. Verify that

$$C(67) = (2, 2, (1), 3, (2, 2, (1)), 11, (8, 2, (1), 5, (3, 2, (1)))).$$

2. Show that the length of $C(p)$ is at most $4(\log p)^2$ (i.e., polynomial in the length of p).

3. Show that $C(p)$ can be checked in polynomial time, i.e., it is checkable in polynomial time that
   a) $r^{p-1} \equiv 1 \pmod{p}$,
   b) $r^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$ for all $q \in \{ q_1, \ldots, q_\ell \}$,
   c) all $q_1, \ldots, q_\ell$ are prime, and
   d) $q_1, \ldots, q_\ell$ are all prime factors of $p - 1$.