Complexity Theory, WS 13/14: Solution Hints 2.

Markus Bläser, Thatchaphol Saranurak

Exercise 2.1 (a.k.a. 3.1) is moved to the next sheet (which will have the number 3 by tradition).

Exercise 2.1 Moved.

Exercise 2.2

a) Let $n = \prod_i {p_i}^{e_i}$ where p_i is the i-th prime. If $l(n) \nmid n$, then there exists an i where $p_i^{e_i+1} \mid l(n)$. Suppose that $l(n) \neq p_i^{e_i+1}$, then $l(n) = p_i^{e_i+1} \cdot k$ where $k > 1$. But then $l(n)/k \nmid n$, which contradicts the minimality of $l(n)$. This proves that $l(n) = p_i^{e_i+1}$. In particular, $l(n)$ is prime power.

b) Observe that for any prime $p < l(n)$, we have $p \mid n$. (Otherwise, we would choose p instead of $l(n)$.) Now by the Prime Number theorem, $\prod_{p<l(n)} p = 2^{\Theta(l(n))}$. So $n > 2^{\Omega(l(n))} \implies l(n) = O(\log n)$.

c) To show that $f(n)$ is a space constructible function, we construct a machine M such that for any input 1^n, it can marks exactly $f(n)$ cells on a work tape using $O(f(n))$ space. (By the compression theorem, it can also use at most $f(n)$ space.)

For any k, we can tests if $k \mid n$ by going left through the input (of size n) by k steps each time. (We uses one counter for counting the steps.) We end up stopping exactly at the end of the input iff $k \mid n$.

We find $l(n)$ by finding the smallest k where $k \nmid n$, starting from $k = 2$. Observe that $f(n) = \lceil \log(l(n) + 1) \rceil$ is a size of bit string representing $l(n)$. Therefore, when we finish, the bit size of k is $f(n)$, and the bit size of the counter is at most $f(n)$ as well.

Exercise 2.3

a) Consider a TM M with a given input 1^n. M wants to mark $s(n)$ cells in the work tape using $O(s(n))$ space.

Since we have only $s(n) = o(\log n)$ space for working, there are $c^{s(n)} < n$ *small* configurations. Hence, while reading n 1's from the input, there exists i, j such that M has the same small configuration when the head of input tape of M is at position i and j.

Therefore, for an input $1^{n'}$ where $n' = n + k \cdot |j - i|$ for any k, M would behave the same way as if M gets the input 1^n. Thus, it must be the case that $s(n') = s(n)$ for infinitely many n'

b) There is no k such that $s(n) \triangleq \lceil \log \log n \rceil = k$ for infinitely many n because $s(n)$ is nondecreasing and unbounded. So $s(n)$ cannot be space constructible.

Exercise 2.4 Let $L \in \mathsf{DSpace}(n^2) \backslash \mathsf{DSpace}(O(n))$ which exists by the space hierarchy theorem. We define $L' = \{x\%^{|x|^2-|x|} \mid x \in L\}$, so that $L' \in \mathsf{DSpace}(n)$.

Suppose for the sake of contradiction that $\mathsf{DSpace}(O(n)) = \mathsf{P}$. Thus, $L' \in \mathsf{P}$, and also $L \leq_p L'$ because there is a reduction which just pads string. Since P is closed under polynomial reduction, $L \in \mathsf{P} = \mathsf{DSpace}(O(n))$, which contradicts the definition of L.