2 Complexity Theory (ad260)

Let $f : \Sigma^* \to \Sigma^*$ be a function on Σ-strings for some finite alphabet Σ. Say that f is a *pseudo one-way function* if it satisfies the following three conditions:

- There is a constant k such that for every $x \in \Sigma^+$, $|x|^{1/k} \leq |f(x)| \leq |x|^k$. (Here $|x|$ denotes the length of a string x).
- f is computable by a polynomial-time algorithm.
- There is no function g, computable in polynomial time, such that $f(g(y)) = y$ for all strings y in the range (i.e. image) of f.

For a pseudo one-way function f, let $L_f \subseteq \Sigma^* \times \Sigma^*$ be the following set

$$L_f = \{(x, y) \mid \exists z (z \leq_{\text{lex}} x \text{ and } f(z) = y)\}.$$

Here $\leq_{\text{lex}}$ denotes the lexicographic order on strings.

(*a*) How would you modify the definition of a pseudo one-way function to obtain the definition of a *one-way function* in the sense defined by Papadimitriou? [3 marks]

(*b*) Show that for any pseudo one-way function f, the language L_f is in NP. [4 marks]

(*c*) Show that for any pseudo one-way function f, the language L_f is not in P. [4 marks]

In the following, ϕ denotes an arbitrary Boolean formula and T a list assigning a Boolean value to each variable appearing in ϕ. Fix Σ to be a suitable alphabet in which we can write ϕ and T as well as the string "no" and consider the following function defined on all Σ-strings.

$$s(x) = \begin{cases} \phi & \text{if } x = (\phi, T) \text{ and } T \text{ satisfies } \phi \\ \text{``no''}x & \text{otherwise} \end{cases}$$

(*d*) Prove that if P$\neq$NP, then s is a pseudo one-way function. [9 marks]