Introduction to Computational Complexity - Assignment 3

To be submitted by 29/3/2008

1. Prove that if one way-functions exist then there exists one-way functions that are length preserving (i.e., $|f(x)| = |x|$ for every $x \in \{0,1\}^n$).

2. Recall that the definition of one-way functions requires that functions will be hard to invert by polynomial time algorithms, in the following sense: For every probabilistic polynomial time algorithm A, every polynomial p, and all sufficiently large n, it holds that

$$\Pr_{x\in\{0,1\}^n}\left[A\left(f(x),1^n\right)\in f^{-1}\left(f(x)\right)\right]<\frac{1}{p(n)} \tag{1}$$

   One may also require that functions will be hard to invert by polynomial size circuits, in the following sense: For every family of polynomial size circuits $\{C_n\}_n$, every polynomial p, and all sufficiently large n, it holds that

$$\Pr_{x\in\{0,1\}^n}\left[C_n\left(f(x),1^n\right)\in f^{-1}\left(f(x)\right)\right]<\frac{1}{p(n)}$$

   In such case, we say that f is non-uniformly hard to invert.
   Prove that if a function is non-uniformly hard to invert, then it is hard to invert by polynomial time algorithms.

3. Assuming the existence of one-way functions, prove that there exists a weak one-way function that is not strongly one-way.

4. **Bonus exercise (Not obligatory)** Using the notion of a universal machine, present a polynomial-time computable function that is hard to invert (in the first sense of Exercise 2) if and only if there exist one-way functions.

   Guideline Consider the function F that parses its input into a pair (M, x) and emulates $|x|^3$ steps of M on input x. Note that if there exists a one-way function that can be evaluated in cubic time then F is a weak one-way function. Using padding, prove that there exists a one-way function that can be evaluated in cubic time if and only if there exist one-way functions.