Homework 8
Due Mon May 17, 5:00pm

Prof. Amit Chakrabarti
Computer Science Department
Dartmouth College

General Instructions: Same as in Homework 1.

Honor Principle: Please work on Problem 19 entirely on your own. For the other problems, you may discuss with fellow students in the class, as in Homework 1.

19. Let $f : \{0,1\}^n \to \{0,1\}^n$ be a function and $k > 0$ be an integer. Define the function $f^{(k)} : \{0,1\}^n \to \{0,1\}^n$ as follows:

$$f^{(k)} = \underbrace{f \circ f \circ \cdots \circ f}_{k\text{times}},$$

where "$\circ$" denotes function composition. Prove that, if f is a one-way permutation, so if $f^{(k)}$. [2 points]

20. Assuming one-way functions exist, prove that the above result does not generalize to one-way functions. Give a specific counterexample. (Obviously, only functions of the form $f : \{0,1\}^n \to \{0,1\}^n$ can be composed with themselves, so your counterexample should have this form.) [2 points]

21. Give formal proofs of the following two statements, which were discussed in class without full formal proofs.

- Every pseudorandom generator is a one-way function. In your proof, make the statement precise, using appropriate $\varepsilon(n)$'s and $s(n)$'s. [1 points]

- If a function is $(\varepsilon(n), s(n))$-pseudorandom (according to Yao's definition), then it is $(\varepsilon(n), s(n))$-unpredictable (according to the Blum–Micali definition). [1 points]

Note: These problems are from [Arora-Barak], Chapter 9.