Homework 9
Due Fri May 9, 5:00pm

Prof. Amit Chakrabarti
Computer Science Department
Dartmouth College

General Instructions: Same as in Homework 1.

Honor Principle: Please work on Problem 18 entirely on your own. For the other problem, you may discuss with fellow students in the class, as in Homework 1.

18. 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]

19. Assuming one-way functions exist, prove that the above result does not generalize to one-way functions.

[2 points]

Note: These problems are from [Arora-Barak], Chapter 10.