# Homework 9
## Due Wed May 11, 5:00pm

Prof. Amit Chakrabarti
Computer Science Department
Dartmouth College

**General Instructions:** Same as in Homework 1.

**Honor Principle:** For the first problem, please work entirely on your own. For the others, the principle is the same as in Homework 1.

20. 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.

(Warm-up exercise) Prove that, if $f$ is a one-way permutation and $k$ is a constant, then $f^{(k)}$ is also a one-way permutation.

(The real problem; turn this part in) 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. Suppose the family $g = \{g_n\}_{n\in\mathbb{N}}$, where $g_n : \{0,1\}^n \to \{0,1\}^{n+1}$, is a pseudorandom generator. Suppose $k > 1$ is a constant. Based on $g$, construct a pseudorandom generator $h = \{h_n\}_{n\in\mathbb{N}}$ where $h_n : \{0,1\}^n \to \{0,1\}^{n^k}$, and prove that your construction works. [2 points]