

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

**Honor Principle:** Please work on Problem 20 entirely on your own. For the other problem, you may discuss with fellow students in the class, as in Homework 1.

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

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

where “ $\circ$ ” denotes function composition. Prove that, if  $f$  is a one-way permutation, so is  $f^{(k)}$ .

[2 points]

21. Assuming one-way functions exist, prove that the above result does not generalize to one-way functions. (Obviously, only functions of the form  $f : \{0, 1\}^n \rightarrow \{0, 1\}^n$  can be composed with themselves.)

[2 points]

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