Homework 10
Due Fri May 16, 5:00pm

Prof. Amit Chakrabarti
Computer Science Department
Dartmouth College

General Instructions: Same as in Homework 1.

Honor Principle: Same as in Homework 1.

20. Prove that if $g_n : \{0,1\}^n \to \{0,1\}^{m(n)}$ is $(\varepsilon(n), t(n))$-pseudorandom, then it is $(\varepsilon(n), t(n))$-unpredictable. For this problem you may assume that $t(n)$ refers to "running time." [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 $h_n : \{0,1\}^n \to \{0,1\}^{n^k}$. [2 points]

    This is essentially Problem 7 from Chapter 10 of [Arora-Barak].