Homework 9
Due Wed May 20, 5:00pm

Prof. Amit Chakrabarti
Computer Science Department
Dartmouth College

General Instructions: Same as in Homework 1.

Honor Principle: Same as in Homework 1.

22. 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]

23. Suppose $x \in \{0,1\}^n$ is an unknown n-bit string. A helper reveals to us the bits $x \odot r_i$ (for $1 \leq i \leq n$) where the the strings $r_1, \ldots, r_n \in_R \{0,1\}^n$ are chosen uniformly at random, and independently. Describe a deterministic algorithm that successfully reconstructs x from this information, with probability at least $1/4$. Note: the probability is only over the choice of r_is.

    These are essentially Problems 7 and 5 from Chapter 10 of [Arora-Barak].