Homework 9
Due Wed May 19, 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.

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 $h_n : \{0,1\}^n \to \{0,1\}^{n^k}$, and prove that your construction works. [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 $1 \le i \le n$) 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: x is fixed, and the probability is only over the choice of r_is. [2 points]

    Hint: Linear algebra over the finite field $\mathbb{F}_2$ works much the same as linear algebra over the reals.