COS 522 Homework 4: Due Nov. 30 in class

1. Let $f : \{0,1\}^n \to \{0,1\}$ be any function such that for every size S circuit C:

   $$\Pr_{x \in \{0,1\}^n}[C(x) = f(x)] \leq 1 - \delta.$$

   Let $f^{\otimes k} : \{0,1\}^{nk} \to \{0,1\}$ be defined as

   $$f^{\otimes k}(x_1, x_2, \ldots, x_k) = (f(x_1), f(x_2), \ldots, f(x_k)).$$

   Then show that for all circuits of size ϵS,

   $$\Pr_{x_1,x_2,\ldots,x_k}[C(x_1, \ldots, x_k) = f^{\otimes k}(x_1, x_2, \ldots, x_k)] \leq O(\epsilon \log(\frac{1}{\epsilon})).$$

2. (*Robust interpolation*) We saw that a univariate degree d polynomial can be interpolated from any $d+1$ values. Here we consider a *robust* version of this fact, whereby we wish to recover the polynomial from $4d$ values of which d are faulty.

   Let $(a_1, b_1), (a_2, b_2), \ldots, (a_{2d}, b_{4d})$ be a sequence of (point, value) pairs, and such that there exists a degree d polynomial $g(x)$ such that

   $$g(a_i) = b_i \qquad \text{for at least } 3d \text{ values of } i. \tag{1}$$

   Our goal is to construct g.

   (a) Show that if the polynomial g exists then there is a degree $2d$ polynomial $c(x)$ and a degree $d-1$ polynomial $e(x)$ such that

   $$c(a_i) = b_i e(a_i) \qquad \text{for all } i. \tag{2}$$

   (b) Show how to find c, e. (Hint: think of the coefficients of c, e as "unknowns" and solve the linear system.)

   (c) Show that if c, e are any polynomials satisfying (2) then e divides c and that in fact $c(x) = g(x)e(x)$.

3. Solve problems 1, 2, 3, 8 from Chapter 18.

4. A *vertex cover* in graph $G = (V, E)$ is a set of vertices that is incident to every edge. Show that for every $\epsilon > 0$, approximating the size of the minimum vertex cover within a factor $17/16 - \epsilon$ is NP-hard. (Hint: Reduce from instances of MAX-3SAT obtained from Hastad's 3-bit PCP Theorem.)