Homework 1

Due Friday, 08/31/2012

You may use any result discussed in class. Unless explicitly stated otherwise, you should not use other sources. Whenever you do use other source, you need to reference them.

For this homework assignment, you may assume that all sets and probability spaces are finite.

Problem 1.1 (10 points)**.** Please send me (through piazza) by **next Tuesday, August 28** some information about you, e.g., research interests and related courses. See the post titled "Student Info" on piazza for details.

Problem 1.2 (Bonferroni inequality, 30 points)**.** Lookup the definitions of probability spaces and events. Prove that events $A_1, \ldots, A_m$ over a probability space Ω satisfy

$$\mathbb{P}[\cup_{i \in [m]} A_i] \geqslant \sum_{i \in [m]} \mathbb{P}[A_i] - \sum_{i < j \in [m]} \mathbb{P}[A_i \cap A_j]\,.$$

Problem 1.3 (Independent random variables, 30 points)**.** Look up the definition of random variables and what it means for them to be independent. Prove that any two independent random variables X, Y satisfy

$$\mathbb{E}\, XY = (\mathbb{E}\, X)(\mathbb{E}\, Y) \quad \text{and} \quad \operatorname{Var}(X + Y) = \operatorname{Var}(X) + \operatorname{Var}(Y)\,.$$

Problem 1.4 (Jensen's inequality, 30 points)**.** Look up what it means for a function $f \colon \mathbb{R} \to \mathbb{R}$ to be convex. Prove that for every convex function f, a random variable X satisfies

$$\mathbb{E}[f(X)] \geqslant f(\mathbb{E}[X]).$$

Problem 1.5 (Average-case hard functions, 20 points)**.** We showed in class that there exist functions that cannot be computed even by very large circuits. **(a)** Look up Chernoff bounds. **(b)** Show that there are functions that cannot even be *approximated* by large circuits: that is, show that for any sufficiently large n, there exists a function $f : \{0,1\}^n \to \{0,1\}$ such that for every circuit C of size at most $2^{n/10}$, $f(x) \neq C(x)$ for at least a 0.49 fraction of the inputs x in $\{0,1\}^n$. **(c)** Show that for every function $f : \{0,1\}^n \to \{0,1\}$, there exists a circuit C of size at most $10n$ such that $C(x) = f(x)$ for at least a $1/2$ fraction of the inputs x in $\{0,1\}^n$.