6.842 Randomness and Computation February 26, 2014

Homework 4

Lecturer: Ronitt Rubinfeld *Due Date: March 5, 2014*

Homework guidelines: You may work with other students, as long as (1) they have not yet solved the problem, (2) you write down the names of all other students with which you discussed the problem, and (3) you write up the solution on your own. No points will be deducted, no matter how many people you talk to, as long as you are honest. If you already knew the answer to one of the problems (call these "famous" problems), then let me know that in your solution writeup – it will not affect your score, but will help me in the future. It's ok to look up famous sums and inequalities that help you to solve the problem, but don't look up an entire solution.

The following problems are to be turned in. You should upload your solution to Stellar as a pdf file.

1. **(Quadratic non-residuosity)** Let Z_n^* be the group of integers that are relatively prime with n. An element $s \in Z_n^*$ is said to be a *quadratic residue* modulo n if there exists $r \in Z_n^*$ s.t. $s \equiv r^2 \bmod n$. Give a private-coin interactive proof system for the language of pairs (s, n) such that s is *not* a quadratic residue modulo n.

2. Give a *deterministic* poly(n)-time algorithm that, given n, finds a coloring of the edges of the complete graph K_n by two colors such that the total number of monochromatic copies of K_4 is at most $\binom{n}{4}2^{-5}$.

3. Let $A_1, \ldots, A_n \subseteq \{1, \ldots, m\}$ with $\sum_{i=1}^{n} 2^{1-|A_i|} < 1$. Prove that there exists a two-coloring $\chi : \{1, \ldots, m\} \to \{0, 1\}$ with no A_i being monochromatic. For the case where $m = n$, give a deterministic algorithm to find such a χ in polynomial time.

4. You are given a 2-SAT formula $\phi(x_1, \ldots, x_n)$. Consider the following algorithm for finding a satisfying assignment:

   - Start with an arbitrary assignment. If it's satisfying, output it and halt.
   - Do s times:
     - Pick an arbitrary unsatisfied clause
     - Pick one of the two literals in it uniformly at random
     - Complement the setting of the chosen literal
     - If the new assignment satisfies ϕ, output the assignment and halt.

   Show that if you pick s to be $O(n^2)$, and ϕ is satisfiable, you will output a satisfying assignment with probability at least $3/4$.