6.842 Randomness and Computation October 4, 2017

Homework 4

Lecturer: Ronitt Rubinfeld *Due Date: October 11, 2017*

Homework guidelines: As in previous homeworks.

The following problems are not for turning in.

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. 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.

The following problem is to be turned in.

1. 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 $\binom{n}{4}2^{-5}$.