Homework 2

Due Friday, 09/07/2012

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

This homework assignment is worth more than 100 points. The excess is considered *bonus*.

Problem 2.1 (30 points)**.** Let QuadEq be the language of all satisfiable systems of *quadratic equations* over the field $\mathbb{F}_2$. Show that QuadEq is **NP**-complete. Will this still hold if we allow only *linear equations*?

Also, give a direct reduction from the problem of checking satisfiability of *degree*-4 equations over $\mathbb{F}_2$ to QuadEq.

Problem 2.2 (30 points)**.** Let Q-Sat$_2$ be the set of CNF formulas $\phi(x, y)$ with

$$\exists x \in \{0,1\}^n.\ \forall y \in \{0,1\}^n.\phi(x,y)\,.$$

Prove that if **P** = **NP** then Q-Sat$_2$ $\in$ **P**. In other words, show that a polynomial-time algorithm for Sat also implies a polynomial-time algorithm that given a CNF formula $\phi(x, y)$ decides whether there exists $x \in \{0,1\}^n$ such that for all $y \in \{0,1\}^n$ the formula $\phi(x, y)$ is satisfied.

Remark 2.3. For all $k \in \mathbb{N}$, we can define Q-Sat$_k$ to be the language of satisfiable formulas with k (alternating) quantifiers. These complexity classes corresponding to these problems form the *polynomial hierarchy*. It is conjectured that the polynomial hierarchy does *not collapse*, that is, for all $k \in \mathbb{N}$, the problem Q-Sat$_k$ is strictly harder than the problem Q-Sat$_{k-1}$. You can read more about the polynomial hierarchy in Chapter 5 of the textbook.

Problem 2.4. Let L be a language. Suppose both L and its complement $\overline{L}$ are in **RP** (one-sided bounded probabilistic error in polynomial-time). Show that there exists a probabilistic machine that decides L in *expected* polynomial time (with *zero probabilistic error*).

Remark 2.5. The class of problems that can be decided with **Z**ero **P**robabilistic error in expected **P**olynomial time is called **ZPP**.

Problem 2.6 (20+20 points)**.** Let G be connected, regular graph. We identity G with its normalized adjacency matrix (a symmetric, doubly stochastic matrix). Show that if G is bipartite, then -1 is an eigenvalue of G. (Hint: find a vector v such that $Gv = -v$.) Is the converse also true? If -1 is an eigenvalue of G, does it mean that G is bipartite?