Computability and Complexity Theory

Instructor: Alexander Razborov, University of Chicago
razborov@cs.uchicago.edu
Course Homepage: www.cs.uchicago.edu/~razborov/teaching/winter12.html

Winter Quarter, 2012

`You are encouraged to work together on solving homework problems, but please put their names clearly at the top of the assignment. Everyone must turn in their own independently written solutions. Homework is due at the beginning of class.`

Homework 2, due February 24

1. Show that multiplication is definable in the language $L = \langle 0, S, +, x^3 \rangle$, that is there exists a first-order formula $M(x, y, z)$ in that language such that for arbitrary non-negative integers $\mathbf{m}, \mathbf{n}$ and $\mathbf{k}$, $\mathbf{m} \cdot \mathbf{n} = \mathbf{k}$ if and only if $M(\mathbf{m}, \mathbf{n}, \mathbf{k})$ is true on the set $\mathbb{N}$ of all non-negative integers.

2. (a) Prove that for any first-order formula A in the first-order language $\langle 0, S, \leq \rangle$ (possibly with free variables) there exists another **open** formula B such that the equivalence $A \equiv B$ is true on the set of all non-negative integer numbers.

   (b) Does a similar statement hold for the language $\langle 0, \leq \rangle$ (explain why)?

3. Let $D_{\mathbb{Z}}$ be the language consisting of all (encodings of) systems

$$p_1(x_1, \ldots, x_n) = 0, \ldots, p_m(x_1, \ldots, x_n) = 0$$

   of diophantine equations with integer coefficients that have at least one integer solution. Let $D_{\mathbb{Q}}$ be defined likewise for the field of rational numbers.

   Give a direct (i.e., not referring to Matiyasevich's theorem) proof that $D_{\mathbb{Q}}$ is many-one reducible to $D_{\mathbb{Z}}$.

`Hint.` I think that for this exercise you may find *Lagrange's four-square theorem* somewhat useful.

4. Prove that for any three random variables X, Y, Z on the same sample space we have:

$$2H(X,Y,Z) \leq H(X,Y) + H(Y,Z) + H(X,Z).$$

5. Let $\omega = \omega_1\omega_2 \ldots ...\omega_n \ldots$ be an infinite random sequence (w.r.t. the uniform measure). Prove that the sequence $(\omega_1 \oplus \omega_2)(\omega_2 \oplus \omega_3) \ldots (\omega_n \oplus \omega_{n+1}) \ldots$ is also random ($\oplus$ is addition mod 2).