Problem Set 1 – Due Friday, April 4, 2014

Instructions: *Read the course-information sheet.* Remember to acknowledge anyone with whom you discussed problems. Recall too that homeworks are due at 10:40 am in the turn-in box in 86 Kemper (in the basement) (or can be turned in on the desk in front of the classroom ***before*** lecture begins). Late homeworks are not accepted and the first homework is *obligatory.*

Problem 1 Call a number $x \in \mathbb{N} = \{1, 2, 3, \ldots\}$ a **palindromic number** if, written as a decimal string X without leading zeros, it's a palindrome ($X = X^R$). Write a formula for D_n, the number of n-digit palindromic numbers. By induction, prove your formula correct. What is D_{20}?

Problem 2 Let $(w_1, w_2, w_3, \ldots) = (\varepsilon, 0, 1, 00, 01, 10, 11, 000, \ldots)$ be the enumeration of binary strings in lexicographic order (with $0 < 1$). What is the 1234567'th string, $w_{1234567}$ in the list? To answer this describe a simple and efficient procedure to map the natural number $n \in \mathbb{N}$ to the string w_n.

Problem 3. For each of the following counting problems, give not only your answer, but explain how it is computed, justifying any formulas employed. None of these should be overly tedious or require computer calculation.

(a) Let $L = \{\mathtt{a}, \mathtt{b}, \mathtt{ab}\}$. How many strings of length 10 are in L^*?

(b) Let $L = \{\mathtt{a}, \mathtt{bb}\}$. How many strings of length 10 are in L^*?

Problem 4. Consider the infinite set of numbers $S = \{1, 10, 100, 1000, 10000, \ldots\}$. Prove that there are two numbers in S that differ by a multiple of $N = 314159265359$. *Hint: pigeonhole principle.*

Problem 5 Recall the DIOPHANTINE EQUATION problem: given a multivariate polynomial P with integer coefficients, determine if P has an integer root.

(a) Prof. Rogaway claimed without proof that there is no algorithm to answer this question. But suppose I give you an *oracle* (a "magic box") to answer it. In a single computational step, it says *yes* or *no* according to whether or not P has an integer root. Given such an oracle, describe an algorithm that *finds* an integer root of any multivariate polynomial that has one (and reports *No Root* otherwise).

(b) Let $s(n)$ be the maximum number of computational steps that your algorithm takes to run (on some fixed, oracle-containing computer) when the polynomial P is described by a string of length n. Explain why there is no algorithm to compute $S(n)$ for *any* function S such that $S(n) \geq s(n)$ for all n. (In brief, some functions just grow *too fast* to be computable.)

Problem 6. State whether the following propositions are true or false, carefully explaining each answer.

(a) $\emptyset^*$ is a language.

(b) ε is a language.

(c) Every language is infinite or has an infinite complement.

(d) Some language is infinite and has an infinite complement.

(e) The set of real numbers is a language.

(f) There is a language that is a subset of every language.

(g) The Kleene closure (the star) of a language is always infinite.

(h) The concatenation of an infinite language and a finite language is always infinite.

(i) There is an infinite language L containing the emptystring and such that L^i is a proper subset of L^* for all $i \geq 0$.