Problem Set 1 – Due Friday, April 5, 2013

Instructions: *Read the course-information sheet.* Remember to acknowledge anyone with whom you discussed problems. Recall too that homeworks are due at 10:30 am in the turn-in box in Kemper 2131, or on the desk in front of the class ***before*** lecture begins. Late homeworks are not accepted and the first two homeworks are *obligatory.*

Problem 1 Let $G = (V, E)$ be a (finite, simple) graph with maximal vertex degree Δ. (The degree of a vertex is the number of vertices to which it is adjacent.) Prove, inductively, that the vertices of G can be colored using $\Delta + 1$ colors. (Saying that a graph $G = (V, E)$ can be colored with k colors means that exists a mapping $c\colon V \to \{1, \ldots, k\}$ such that $c(v) \neq c(w)$ for all $\{v, w\} \in E$.)

Problem 2

(a) If L and L' are (finite) lists of strings and x is a string, let $L \parallel L'$ be the list of elements in L followed by the list of elements in L'; let L^{flip} be the list L in reverse order; and let xL be the list of strings in L with each one preceded by x. Consider the sequence of lists $L_0 = (\varepsilon)$ and $L_n = 0L_{n-1} \parallel 1L_{n-1}^{\text{flip}}$ for $n \geq 1$. Enumerate the elements of L_4.

(b) The Hamming distance between equal-length strings x and y is the number of positions on which they disagree (that is, $x[i] \neq y[i]$). Prove that for every number n there is an ordering of the points in $\{0, 1\}^n$ such that successive points have Hamming distance one.

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 12 are in L^*?

(b) Let $L = \{\mathtt{a}, \mathtt{bb}\}$. How many strings of length 12 are in L^*?

Problem 4 Recall the DIOPHANTINE EQUATION problem: given a multivariate polynomial P with integer coefficients, determine if P has an integer root.

(a) In lecture 1, Prof. Rogaway claimed without proof that there is no algorithm to answer this question. But suppose I provide you with an *oracle* (a "magic box") that did answer the question. 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 5. 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 $i \geq 0$.

Problem 6. Draw DFAs for the following languages. Assume an alphabet that includes all and only the mentioned symbols. Each of your DFAs should use a minimum number of states.

(a) The set of all strings that have `abba` as a substring.

(b) The set of all strings that do not have `abba` as a substring.

(c) The complement of $\{0, 01\}^*$.

(d) The set of all strings that have an even number of 0's and an even number of 1's.

(e) The binary encodings of numbers divisible by 5. Allow leading zeros.