Final Exam **Due: December 15** **CAS705 Fall 2011**

strict deadline

You are encouraged to typeset your exam, preferably in LaTeX.

1. In Cook's seminal 1975 paper *Feasible constructive proofs*, where he introduces the now classical theory PV, he uses a nice result of Cobham characterizing polytime functions.

   The *dyadic* notation for the natural number n is the unique string $d_k d_{k-1} \dots d_0$ over the alphabet $\{1, 2\}$ such that $\sum_{i=0}^{k} d_i 2^i = n$. In particular, the dyadic notation for 0 is the empty string. The dyadic successor functions s_i, $i = 1, 2$ are defined as: $s_i(x) = 2x + i$, and correspond to concatenating the digits 1 and 2, respectively, on the right end of the dyadic notation of x. We shall thus abbreviate $s_i(x)$ by xi.

   A function f comes from functions $g_1, \dots, g_m$ by the operation of *substitution* iff some equation of the form $f(x_1, \dots, x_n) = t$ holds for all $x_1, \dots, x_n$, where t is a term over $\{s, 0, +, \cdot\}$, where 0 is zero, and $s00000$ is the numeral for 5, the variables $x_1, \dots, x_n$, and the function symbols $g_1, \dots, g_m$. For example, $f(x_1, x_2) = g_1((s000)x_1 + x_2 \cdot g_2(x_2))$.

   The function f comes from functions g, h_1, h_2, k_1, k_2 by the operation of *limited recursion on dyadic notation* iff

   $$\begin{aligned} &f(0, \vec{y}) = g(\vec{y}) \\ &f(xi, \vec{y}) = h_i(x, \vec{y}, f(x, \vec{y})) \qquad i = 1, 2 \\ &f(x, \vec{y}) \leq k_i(x, \vec{y}) \qquad i = 1, 2 \end{aligned}$$

   for all natural number values of the variables, where $\vec{y} = (y_1, \dots, y_k)$. We allow the case $k = 0$, in which g is a constant.

   Finally, the dyadic notation for $*(x, y)$ is the dyadic notation for x concatenated with itself $|y|$ times.

   Let $\mathscr{P}$ be the smallest class of functions which includes the initial functions s_1, s_2 and $*$, and which is closed under the operations of substitution and limited recursion on dyadic notation.

   Show that $\mathscr{P}$ is precisely the class of polytime functions.

2. Let #Matchings($\langle G \rangle$) be the number of matchings of a bipartite graph G. A matching is any set of edges of G such that no two edges in the set share a common vertex. Let #Mon2Sat(α) be the number of satisfying assignments of a monotone 2CNF formula α. (A propositional formula is monotone if it is constructed from $\wedge, \vee, 0, 1$, i.e., no negations.) Use the fact that #Matchings is #**P** complete to show that #Mon2Sat is #**P** complete.

3. The following text has been encrypted with a Vignère cipher. Your task is to decode it. Hint: use the *Krasiski method*.

```
Eget Aboxzhyfe, bsghfogw, vprvyj, trq rcua, avtb s vszfijmeoly zhqr
ahv aecps vbwcomammbn, mwxqrd ng nrvty khqr oz lai oeml uprsmagkf oz
wqmftyfvi; nnx zth yipww rraldr xjehlr-sae swtvf ih lai joldw avtb
nxvl lclmpr ti vbwgrykl se vyp aie.  Sbw pef tbw rshnawlx bf nzx xjo
xsnkutyjl ss a gglx nfzwvxvohsmi, vnxmekrnn xtxuel; sgh uax, ag
gbnmwjyrnww hj uel kbwgel'k feercszi, oeyf fmftlwlw bf bal lbumw yvbm
u nxvl eujec celahh. Uel ehxuel zth qiyv msb lifz eto zgk lrr ng aeie
ggki ghuf tr vnxalxvnwl kizegtkeacy gy lrr wskifsyk; trq hyj ipncy zth
oeyf lycpfaxh oy uf xbpefdxrg wietr ns agoienykl, auo bsw jnlfwg
pvtndx wuoll hj n milaie ih syjrcnahr.
```