Assignment 5: Differential Auxiliaries, dTL and Quantifier Elimination
15-424/15-624 Foundations of Cyber-Physical Systems
Course TA: Sarah Loos (sloos+fcps@cs.cmu.edu)

Due: **Beginning of recitation**, Friday 11/8/13
Total Points: 60

1. **Differential Auxiliaries.** Prove the following properties using the sequent rules presented in class. You must use the differential auxiliary rule in each (DA).
   (a) $x \geq 0 \rightarrow [\{x' = x\}]x \geq 0$
   (b) $x > 10 \rightarrow [\{x' = 10 - x\}]x > 10$
2. **Valid, Satisfiable, or Unsatisfiable.** Determine whether each of the following *differential temporal dynamic logic* (dTL) formulas is valid, satisfiable, or unsatisfiable.
   (a) $(v \geq 0 \land a > 0 \land T > 0) \rightarrow [t := 0; \{x' = v, v' = a, t' = 1\}; ?t = T]\Box v > 0$
   (b) $\big([v := a; v := a + d; \{x' = v\}]\ x \leq b\big) \leftrightarrow \big([v := a; v := a + d; \{x' = v\}]\Box\ x \leq b\big)$
   (c) $\big([v := a; v := a + d; \{x' = v\}]\ v \leq b\big) \leftrightarrow \big([v := a; v := a + d; \{x' = v\}]\Box\ v \leq b\big)$
   (d) $\big([\{x' = v, v' = a \ \&\ v \geq 0\}]\Box\ x \geq 0\big) \leftrightarrow \big([\{x' = v, v' = a\}; ?v \geq 0]\ x \geq 0\big)$
3. **d$\mathcal{L}$ vs. dTL.** Consider the formula $F \equiv [\alpha]\phi \leftrightarrow [\alpha]\Box\phi$.
   (a) Assign a (non-trivial) HP to α and formula to ϕ such that F is valid.
   (b) Describe a general set of restrictions on α and ϕ that ensure F is valid.
4. **Quantifier Elimination.** Apply quantifier elimination to eliminate the quantified variables in each of the following formulas.
   (a) $\exists x\ (y = x^4 \land x^2 = 3)$
   (b) $\exists x\ (a = b + x^2)$
   (c) $\exists y\ (y = x^2 \land x - y \geq 0)$
5. **Convergence and Divergence.** Consider the infinite summation over function $f(i)$:

$$\sum_{i=0}^{\infty} f(i)$$

   (a) Write a theorem in d$\mathcal{L}$ which, if proved true, would guarantee the sum converges.
   (b) Write a theorem in d$\mathcal{L}$ which, if proved true, would guarantee the sum diverges.

6. **Creative Invariants.** Derive two distinct (i.e. not equivalent) loop invariants that could be used to prove the following property.

$$(c1 = -2 \wedge c2 = 0 \wedge r = 0 \wedge c1 = c2 - (2 - r))$$
$$\rightarrow$$
$$[(if(r < 2)\ then$$
$$\quad s := 2$$
$$else$$
$$\quad s := 1$$
$$fi;$$
$$if(c1 \geq 7)\ then$$
$$\quad c1 := 0$$
$$fi;$$
$$if(c2 \geq 7)\ then$$
$$\quad c2 := 0$$
$$fi;$$
$$\{c1' = s, c2' = 2 - s, r' = 2 * s - 2\ \&\ c1 \leq 7 \wedge c2 \leq 7 \wedge r \leq 2\})^*]$$
$$(c1 - c2 \leq 2 \wedge c2 - c1 \leq 2)$$