Assignment 4: Differential Invariants and Nondeterministic Assignment
15-424/15-624 Foundations of Cyber-Physical Systems
Course TA: Sarah Loos (sloos+fcps@cs.cmu.edu)

Due: **Beginning of recitation**, Friday 10/25/13
Total Points: 60

1. **Differential invariants and differential cuts.** Prove the following theorems using the sequent proof rules you learned in class. You **must** apply a differential invariant rule (DI or DI') and you may **not** use the solution of the differential equation. You may find the differential cut (DC) and differential weakening (DW) rules helpful for some problems. Be **very careful** with the real arithmetic on these problems; it is easy to make a mistake. Also, recall that context does not stick around when using Differential Invariant rules.

   (a) $\vdash x \geq 10 \rightarrow [x' = x^8]x \geq 0$

   (b) $\vdash x \geq 0 \rightarrow [x' = x^2]x^3 \geq 0$

   (c) $\vdash x \neq y \rightarrow [x' = x, y' = x]x \neq y$

   (d) $\vdash (x \geq 0 \wedge y \geq 0 \wedge z \geq 0) \rightarrow [x' = y, y' = z, z' = x^2]x \geq 0$

   (e) $\vdash (x \geq 0 \wedge x \leq y) \rightarrow [x' = 5y^4 + x, y' = 5x^4 - y]x \leq y + 1$

2. **Syntactic derivatives.** In lecture 11, the *syntactic derivative* is introduced for terms in Definition 1. Later in the lecture notes, we define the syntactic derivative for formulas as follows:

$$(\theta \leq \eta)' \equiv ((\theta)' \leq (\eta)') \tag{1}$$
$$(\theta < \eta)' \equiv ((\theta)' < (\eta)') \tag{2}$$
$$(\theta \neq \eta)' \equiv ((\theta)' = (\eta)') \tag{3}$$

   (a) Prove that the following slightly relaxed definition for the syntactic derivative of a strict inequality (2) would also give a sound proof rule for differential invariants (you may assume all other definitions remain the same).

$$(\theta < \eta)' \equiv ((\theta)' \leq (\eta)')$$

   (b) Suppose you remove definition (3) so that you can no longer use the differential invariant proof rule for formulas involving $\neq$. Can you derive a proof rule to prove such differential invariants regardless? If so, how? If not, why not?

3. **Valid, satisfiable, or unsatisfiable.** For each of the following, determine whether the statement is valid, satisfiable, or unsatisfiable.

   (a) $[a := *]a = x$

   (b) $\langle a := *\rangle a = x$

   (c) $\langle (a := *)^* \rangle (a = x \wedge a = y)$

   (d) $([a := *; ?(L \leq a \leq U)](ax + by \geq 0)) \leftrightarrow (\forall a \ ((L \leq a \leq U) \rightarrow ax + by \geq 0))$

4. **Hybrid programs and nondeterministic assignment.** For each of the following, write the appropriate hybrid program.

   (a) Write a hybrid program using nondeterministic assignment which assigns any real values to x and y, and ensures that y is double the value of x.

   (b) Write a hybrid program using nondeterministic assignment which assigns x to be any real number in the range $[0, A]$.

   (c) Write a hybrid program equivalent to $(x := *)$ which does **not** use nondeterministic assignment.

5. **Lab1 revisited.** In lab1, question 3, you wrote a hybrid program in which a robot accelerates along a straight line for a non-zero duration less than or equal to T, and then decelerates to stop on a charging station. We will now revisit this problem using non-deterministic assignment.

   (a) Rewrite this hybrid program using guarded nondeterministic assignment for the first choice of acceleration. Your guards should allow *all* safe choices of acceleration, thus defining a safety envelope within which all control choices are safe.

   (b) What are the pros and cons of changing the hybrid program from lab1 to use guarded non-deterministic assignment?

   (c) *Suppose* you were to prove the safety and efficiency properties from lab1 for this new hybrid program. Is this new theorem stronger than the one you proved in lab1 (in other words, would this theorem imply the original)? Or is the old theorem stronger? Or neither? Explain.