15-819N/18-879L Logical Analysis of Hybrid Systems

Assignment 3 ($\sum 60$) due 03/05/11 in class

André Platzer

Carnegie Mellon University, Computer Science Department, Pittsburgh, PA

Disclaimer: No solution will be accepted that comes without an **explanation**!

Exercise 1 Hybrid Program Image Computation (38p)

1. Formally define a numerical image computation and a numerical bounded model checking procedure for hybrid programs starting from a finite initial set $Y \subseteq \mathbb{Q}^n$. As part of that define the postimage $Post_\alpha(Y)$ of Y under the transitions of a hybrid program α. Give a detailed definition of all cases and discuss the options and assumptions that you make carefully.
2. How do you use this procedure to check validity of formulas of differential dynamic logic? To what extent and for which formulas does this work?
3. Implement your algorithm in a programming language of your choice. Describe how your implementation differs from your answer to question 1.
4. Use your algorithm to model check the following example (if you want to, you can make further simplifying assumptions in the implementation for the purpose of this example). What is the result? What does it mean?

```
(v^2 <= 2*b*(m-z) & b > 0 & A>=0) ->
[(SB:=v^2/(2*b)+(A/b)*(A/2)*ep+(A/b)*ep*v+(A/2)*ep+ep*v;
 ((?m - z <= SB; a:= -b) ++ (?m - z >= SB; a:=A));
 t:=0; {z'=v, v'=a, t'=1, (v >= 0 & t <= ep)}
 )*] (z <= m)
```

Exercise 2 Differential Dynamic Logic (22p)

1. Are the following formulas of differential dynamic logic valid/invalid/satisfiable/unsatisfiable? Explain why.
   a) $x \geq 30 \rightarrow [x := x/2 - 5; x' = 2]x \geq 10$
   b) $x \geq 30 \rightarrow [(x := x/2 - 5; x' = 2)^*]x \geq 10$
   c) $[x' = ax^2]x \leq 100 \rightarrow$
   $\langle y := x; (y := y/4; t := 0; x'' = a, t' = 1, t \leq 2)^*; ?y \leq 25\rangle ax = 0$
   d) $\langle x' = ax\rangle x \geq 100 \rightarrow v^2 \geq (2x-400)a \rightarrow \langle x' = v, v' = a\rangle x = 200 \vee \langle x' = -v, v' = -a\rangle x = 200$
   e) $b \leq 0 \rightarrow \big(\langle (a := b; x' = v, v' = a \,\&\, v \geq 0)^*\rangle (x < y \wedge v > w)$
   $\leftrightarrow \langle z := x; (z' = v, v' = b; ?0 \leq v)^*\rangle (z < y \wedge -v < -w)\big)$
   f) $\forall d \exists a\ \langle x' = ax^3\rangle x = d$

g) $[(SB{:=}v\hat{}2/(2*b)+(A/b)*(A/2)*ep+(A/b)*ep*v+(A/2)*ep+ep*v;$
$((?m-z \leq SB;\ a{:=}-b) \cup (?m-z \geq SB;\ a{:=}A));$
$t{:=}0;\ \{z'{=}v,\ v'{=}a,\ t'{=}1,\ (v \geq 0 \wedge t \leq ep)\}$
$)^*]\ (z \leq m)$
$\leftrightarrow$
$[a{:=}A;(SB{:=}v\hat{}2/(2*b)+(A/b)*(A/2)*ep+(A/b)*ep*v+(A/2)*ep+ep*v;$
$((a{:=}-A;\ ?m-z \geq SB) \cup (a{:=}b;\ ?{-}SB \leq z-m));$
$s{:=}-t;\ t{:=}t+s;\ \{v'{=}-a,\ t'{=}-1,\ z'{=}v,\ (0 \leq ep+t \wedge 0 \leq v)\}$
$)^*]\ !(m{<}z)$

2. Does it make a difference whether division (/) is included in the operators (signature) of differential dynamic logic or not? Please explain why.