15-819/18-879 Hybrid Systems Analysis & Theorem Proving

Assignment 3 due by Thu 4/9/2009 hand in WEH 7120/7109

André Platzer

Carnegie Mellon University, Computer Science Department, Pittsburgh, PA aplatzer@cs.cmu.edu

Disclaimer: No solution will be accepted that comes without an **explanation**! Exercises 2–3 are meant as alternative exercises to choose from. By solving both Exercises 2 and 3, you can get extra credit or catch up on missing points for previous exercises.

Exercise 1 Hybrid Systems Verification (8p)

KeYmaera[1] is a verification tool for hybrid systems presented in the lecture. Turn the option **Differential Saturation** in the *Hybrid Strategy* tab to **off**. Then prove the following example in KeYmaera, send in the saved proof file and give a hand-written/LaTeX-version of a proof in the calculus of differential dynamic logic. Please describe/mark all steps in the proof that you did interactively.

```
\functions {
  R ep;
  R b;
  R A;
}

\problem {
  \[ R x, s, a, v, t, e; \] (
    ( 2*b*(e-x) - v^2 >= 0 & A >= 0 & b>0 )
  ->
    \[(   /* loop */
    (    /* choice */
      (a:= -b)
      ++ (?e >= x + (v^2)/(2*b) + ((A/b) + 1)*((A/2)*ep^2 + ep*v);
            a:=A)
    );
    t:=0;
    {x'=v, v' = a, t'=1, (v >= 0 & t <= ep)}
    )*
    \] (x <= e)
  )
}
```

[1] http://symbolaris.com/info/KeYmaera.html

*** Exercise 2 Hybrid Systems Modeling and Verification (42p)

TCAS (Traffic Collision and Avoidance System) is an onboard unit installed on aircraft. It is responsible for detecting upcoming possible collisions and for giving resolution advisories (RA) to prevent them. Possible RA consist of either climbing or descending actions.

1. Develop a hybrid program modeling (simplified) TCAS.
2. Specify desirable properties of the TCAS system in differential dynamic logic.
3. Prove an interesting safety property (e.g., collision freedom) of simplified TCAS in KeYmaera. Identify and explain constraints that ensure safety with respect to the property (equivalent characterizations are not necessary but reasonable overapproximations are accepted). Please describe/mark all steps in the proof that you did interactively.
   Hint: At all times are you allowed to simplify TCAS whenever you explain why your simplification is actually necessary and helpful provided that you argue why/under what circumstances your simplifications are adequate. For instance, simplify TCAS by assuming that the continuous flows of the system are linear functions. You can further work with a series of increasingly more complicated models starting from a simple one.

*** Exercise 3 Hybrid Systems Modeling and Verification (42p)

Consider a robot that moves on planar ground. Suppose the floor has a (small and constant) number of dangerous areas that can be described in terms of simple shapes like rectangles, circles and/or ellipses. Devise a controller that allows the robot to move around freely according to some planning objective but always avoids the dangerous areas.

1. Considering the plan and how to achieve it as a set-value input for the controller develop a hybrid program modeling the robot system.
2. Specify desirable properties of the robot system in differential dynamic logic.
3. Prove an interesting safety property (including avoidance of dangerous areas) of the robot system. Identify and explain constraints that ensure safety with respect to the property (equivalent characterizations are not necessary but reasonable overapproximations are accepted). Please describe/mark all steps in the proof that you did interactively.
4. How could you incorporate the planning objectives into the system and its proofs?
   Hint: At all times are you allowed to simplify the robot system whenever you explain why your simplification is actually necessary and helpful provided that you argue why/under what circumstances your simplifications are adequate.