15-424/15-624 Recitation 6: Differential Invariants
15-424/15-624 Foundations of Cyber-Physical Systems

Notes: Khalil Ghorbal(kghorbal@cs.cmu.edu)

Recall: Three main proof rules: Differential Invariant, Differential Cut, Differential Weakening
The Cut rule "cuts" $A \to B$ into $A \to C \wedge C \to B$ (if such a C exists). The same intuition can be used in the differential context:

$$(DC)\frac{F \vdash [x' = \theta \& H]C \quad F \vdash [x' = \theta \& H \wedge C]F}{F \vdash [x' = \theta \& H]F}$$

The differential invariant rule is essentially used to lift a property about the differential terms to a property about their derivatives.In conjunction with the D operator, the property is rewritten using the θ (right-hand side of the differential equation), which we can deal with as a first-order logic formula.

$$(DI)\frac{H \vdash {F'}^{\theta}_{x'}}{F \vdash [x' = \theta \& H]F}$$

The differential weakening rule is trivial (the invariant is enforced by design) and essentially used to close the proof after a DC.

$$(DW)\frac{H \vdash F}{F \vdash [x' = \theta \& H]F}$$

The D operator on first-order real-arithmetic: what intuitions to keep in mind

To prove that a differentiable real function: $f : \mathbb{R}_+ \to \mathbb{R}; t \mapsto f(t)$ has a constant sign ($f(t) \leq 0$, say), it is sufficient to prove that $f(0) \leq 0$ and its derivative w.r.t. to the variable t is also non-positive: $f'(t) \leq 0$

$$f(0) \leq 0 \wedge f'(t) \leq 0 \to f(t) \leq 0, \forall t \geq 0$$

Following the same reasoning, given two functions f and g, one has:

$$f(0) \leq 0 \wedge g(0) \leq 0 \wedge f'(t) \leq 0 \wedge g'(t) \leq 0 \to f(t) \leq 0 \wedge g(t) \leq 0, \forall t \geq 0$$

which also implies that $f(t) \leq 0$ or $g(t) \leq 0$, $\forall t \geq 0$. This should give an intuition about why we need to switch from $\vee$ to $\wedge$ for the D operator to be sound. Observe that all of these transformations are sufficient conditions. This means, that the differential invariant rule is sound but, alone, is not complete directly.

Case Study: 3D Lotka-Volterra

The following predator/pray model describes the behavior of the biomasses x, y and z of three distinct species. We want to prove that none of the three involved species will disappear: that is we reach an equilibrium cycle.

```
\programVariables {
   R x,y,z;
}

\problem{
  x != 0 & y != 0 & z !=0
    ->
    \[
    {x'=x*(y-z),y'=y*(z-x),z'=z*(x-y)}
  \] (x != 0 & y!=0 & z!=0)
}
```

1. Apply a DI first (with the postcondition as differential invariant). Observe that the proof does not close because the condition asks about separate properties for x, y and z.

2. Apply a DC with $xyz \neq 0$ (which is equivalent to the post-condition, but links explicitly the involved variables).

3. Close the proof by a DI and DW.

Quiz

1. Can you prove that $y > 0 \wedge x < 0 \rightarrow [x' = x, y' = y]x \neq y$? Explain why or why not.

2. Can you prove $x < x_o \rightarrow [a := \frac{v^2}{2(x-x_o)}; \{x' = v, v' = a, v \geq 0\}]x \leq x_o$ using DI instead of ODE (solving the differential equation) ? Write down your DI.