15-424: Foundations of Cyber-Physical Systems

Lecture Notes on Differential Equations & Proofs

André Platzer

Carnegie Mellon University
Lecture 11

1 Introduction

Lecture 5 on Dynamical Systems & Dynamic Axioms gave us a first simple proof principle for differential equations if we find a representable solution of the differential equation. The axiom $[']$ replaces properties of differential equations with suitably quantified properties of solutions, with a universal quantifier over all durations of the solution. Yet, that does not work for all differential equations, because only some of them have explicit closed-form solutions let alone solutions that are simple enough to be quantified over without leaving the decidable parts of the resulting arithmetic.

Lecture 2 on Differential Equations & Domains allows many more differential equations to be part of CPS models than just the ones that happen to have simple solutions. In fact, in a certain sense, most of the interesting differential equations do not possess useful closed-form solutions. Today's lecture reinvestigates the way we prove properties of differential equations from a much more fundamental perspective, which will lead to a way of proving properties of CPS with more general differential equations.

More details can be found in [Pla10a, Pla10b, Chapter 3.5] and also [Pla12b]. Differential invariants were originally conceived in 2008 [Pla10a, Pla08] and later used for an automatic proof procedure for hybrid systems [PC08].

2 Recall

Recall the following results from Lecture 10 on Differential Equations & Differential Invariants:

Definition 1 (Derivation)**.** The operator $(\cdot)'$ that is defined as follows on terms is called *syntactic (total) derivation*:

$$
\begin{aligned}
(r)' &= 0 && \text{for numbers } r \in \mathbb{Q} && \text{(1a)}\\
(x)' &= x' && \text{for variable } x \in \Sigma && \text{(1b)}\\
(a+b)' &= (a)' + (b)' && && \text{(1c)}\\
(a-b)' &= (a)' - (b)' && && \text{(1d)}\\
(a\cdot b)' &= (a)'\cdot b + a\cdot (b)' && && \text{(1e)}\\
(a/b)' &= ((a)'\cdot b - a\cdot (b)')/b^2 && && \text{(1f)}
\end{aligned}
$$

Definition 2 (Differentially augmented state in differential state flow)**.** The value of x' at time $\zeta \in [0,r]$ of a differentiable function $\varphi : [0,r] \to \mathcal{S}$ of some duration $r \in \mathbb{R}$ is defined as:

$$[\![x']\!]_{\varphi(\zeta)} = \frac{\mathsf{d}\varphi(t)(x)}{\mathsf{d}t}(\zeta)$$

Lemma 3 (Derivation lemma)**.** *Let $\varphi : [0,r] \to \mathcal{S}$ be a differentiable function of duration $r > 0$. Then for all terms η that are defined all along φ and all times $\zeta \in [0,r]$:*

$$\frac{\mathsf{d}\,[\![\eta]\!]_{\varphi(t)}}{\mathsf{d}t}(\zeta) = [\![(\eta)']\!]_{\varphi(\zeta)}$$

where differential symbols are interpreted according to Def. 2. In particular, $[\![\eta]\!]_{\varphi(\zeta)}$ is continuously differentiable.

Lemma 4 (Differential substitution property for terms)**.** *If $\varphi : [0,r] \to \mathcal{S}$ solves the differential equation $x' = \theta$, i.e. $\varphi \models x' = \theta$, then $\varphi \models (\eta)' = (\eta)'^{\theta}_{x'}$ for all terms η, i.e.:*

$$[\![(\eta)']\!]_{\varphi(\zeta)} = [\![(\eta)'^{\theta}_{x'}]\!]_{\varphi(\zeta)} \quad \textit{for all } \zeta \in [0,r]$$

3 Differential Invariant Terms

Lecture 10 on Differential Equations & Differential Invariants proved soundness for a proof rule for differential invariant terms, which can be used to prove normalized invariant equations of the form $\eta = 0$.

Lemma 5 (Differential invariant terms)**.** *The following special case of the differential invariants proof rule is sound, i.e. if its premise is valid then so is its conclusion:*

$$(DI_{=0})\ \frac{\vdash {\eta'}^{\theta}_{x'} = 0}{\eta = 0 \vdash [x' = \theta]\eta = 0}$$

4 Proof by Generalization

So far, the argument captured in the differential invariant term proof rule $\mathrm{DI}_{=0}$ works for

$$d^2 + e^2 - r^2 = 0 \to [d' = e, e' = -d]d^2 + e^2 - r^2 = 0 \tag{2}$$

with an equation $d^2 + e^2 - r^2 = 0$ normalized to having 0 on the right-hand side but not for the original formula

$$d^2 + e^2 = r^2 \to [d' = e, e' = -d]d^2 + e^2 = r^2 \tag{3}$$

because its postcondition is not of the form $\eta = 0$. Yet, the postcondition $d^2 + e^2 - r^2 = 0$ of (2) is trivially equivalent to the postcondition $d^2 + e^2 = r^2$ of (3), just by rewriting the polynomials on one side, which is a minor change. That is an indication, that differential invariants can perhaps do more than what proof rule $\mathrm{DI}_{=0}$ already knows about.

But before we pursue our discovery of what else differential invariants can do for us any further, let us first understand a very important proof principle.

Note 6 (Proof by generalization)**.** *If you do not find a proof of a formula, it can sometimes be easier to prove a more general property from which the one you were looking for follows.*

This principle, which may at first appear paradoxical, turns out to be very helpful. In fact, we have made ample use of Note 6 when proving properties of loops by induction. The loop invariant that needs to be proved is usually more general than the particular postcondition one is interested in. The desirable postcondition follows from having proved a more general inductive invariant.

In its purest form, the principle of generalization is captured in the *generalization* rule from Lecture 7 on Control Loops & Invariants. One of the forms of the generalization rule is:

$$([]gen')\ \frac{\Gamma \vdash [\alpha]\phi, \Delta \quad \phi \vdash \psi}{\Gamma \vdash [\alpha]\psi, \Delta}$$

Instead of proving the desirable postcondition ψ of α (conclusion), proof rule $[]gen'$ makes it possible to prove the postcondition ϕ instead (left premise) and prove that ϕ is more general than the desired ψ (right premise). Generalization $[]gen'$ can help us prove the original d$\mathcal{L}$ formula (3) by first turning the postcondition into the form of the (provable) (2) and adapting the precondition using a corresponding *cut* with $d^2+e^2-r^2=0$:

$$\scriptstyle{\to}\text{r}\,\dfrac{[]gen'\,\dfrac{cut,\text{Wl},\text{Wr}\,\dfrac{\mathbb{R}\,\dfrac{*}{d^2+e^2=r^2 \vdash d^2+e^2-r^2=0} \qquad \text{DI}_{=0}\,\dfrac{\dfrac{\mathbb{R}\,\dfrac{*}{\vdash 2de+2e(-d)-0=0}}{\vdash (2dd'+2ee'-2rr'=0)_{d'}^{e}\,{}_{e'}^{-d}\,{}_{r'}^{-0}}}{d^2+e^2-r^2=0 \vdash [d'=e,e'=-d]d^2+e^2-r^2=0}}{d^2+e^2=r^2 \vdash [d'=e,e'=-d]d^2+e^2-r^2=0} \qquad \mathbb{R}\,\dfrac{*}{d^2+e^2-r^2=0 \vdash d^2+e^2=r^2}}{d^2+e^2=r^2 \vdash [d'=e,e'=-d]d^2+e^2=r^2}}{\vdash d^2+e^2=r^2 \to [d'=e,e'=-d]d^2+e^2=r^2}$$

This is a possible way of proving the original (3), but also unnecessarily complicated. Differential invariants can prove (3) directly once we generalize proof rule $\text{DI}_{=0}$ appropriately. For other purposes, however, it is still important to have the principle of generalization Note 6 in our repertoire of proof techniques.

5 Equational Differential Invariants

There are more general logical formulas that we would like to prove to be invariants of differential equations, not just the polynomial equations normalized such that they are single terms equaling 0. Thinking back of the soundness proof for $\text{DI}_{=0}$ in Lecture 10, the argument used involving the value of the left-hand side term $h(t) = [\![\eta]\!]_{\varphi(t)}$ as a function of time t. The same argument can be made by considering the difference $h(t) = [\![\theta - \eta]\!]_{\varphi(t)}$ instead to prove postconditions of the form $\theta = \eta$. How does the inductive step for formula $\theta = \eta$ need to be define to make a corresponding differential invariant proof rule sound? That is, for what premise is the following a sound proof rule?

$$\frac{\vdash ???}{\theta = \eta \vdash [x' = \theta]\theta = \eta}$$

Before you read on, see if you can find the answer for yourself.

Defining the total derivative of an equation $\theta = \eta$ as

$$(\theta = \eta)' \equiv ((\theta)' = (\eta)')$$

results in a sound proof rule by a simple variation of the soundness proof for DI$_{=0}$ as sketched above. The resulting proof rule

$$(\text{DI}_=)\ \frac{\vdash (\kappa' = \eta')_{x'}^{\theta}}{\kappa = \eta \vdash [x' = \theta]\kappa = \eta}$$

for equational differential invariants captures the basic intuition that κ always stays equal to η if it has been initially (antecedent of conclusion) and the derivative of κ is the same as the derivative of η with respect to the differential equation $x' = \theta$. This intuition is made precise by Lemma 3 and Lemma 4. Instead of going through a proper soundness proof for DI$_=$, however, let's directly generalize the proof principles further and see if differential invariants can prove even more formulas for us. We will later prove soundness for the general differential invariant rule, from which DI$_=$ derives as a special case.

Example 6 (Rotational dynamics). The rotational dynamics $d' = e, e' = -d$ is complicated in that the solution involves trigonometric functions, which are generally outside decidable classes of arithmetic. Yet, we can easily prove interesting properties about it using DI and decidable polynomial arithmetic. For instance, DI$_=$ can directly prove formula (3), i.e. that $d^2 + e^2 = r^2$ is a differential invariant of the dynamics, using the following proof:

$$\to\text{r}\ \dfrac{\text{DI}\ \dfrac{\dfrac{\mathbb{R}\ \dfrac{*}{\vdash 2de + 2e(-d) = 0}}{\vdash (2dd' + 2ee' = 0)_{d'}^{e}\,{}_{e'}^{-d}}}{d^2 + e^2 = r^2 \vdash [d' = e, e' = -d]d^2 + e^2 = r^2}}{\vdash d^2 + e^2 = r^2 \to [d' = e, e' = -d]d^2 + e^2 = r^2}$$

This proof is certainly much easier and more direct than the previous proof based on $[]gen'$.

6 Differential Invariant Inequalities

The differential invariant proof rules considered so far give a good (initial) understanding of how to prove equational invariants. What about inequalities? How can they be proved?

Before you read on, see if you can find the answer for yourself.

The primary question is again how to define the total derivative

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

Example 7 (Cubic dynamics). Similarly, differential induction can easily prove that $\frac{1}{3} \leq 5x^2$ is an invariant of the cubic dynamics $x' = x^3$; see the proof in Fig. 7 for the dynamics in Fig. 1. To apply the differential induction rule DI, we again form the total derivative of the differential invariant $F \equiv \frac{1}{3} \leq 5x^2$, which gives the differential expression $F' \equiv (\frac{1}{3} \leq 5x^2)' \equiv 0 \leq 5 \cdot 2xx'$. Now, the differential induction rule DI takes into account that the derivative of state variable x along the dynamics is known. Substituting the differential equation $x' = x^3$ into the inequality yields $F'^{x^3}_{x'} \equiv 0 \leq 5 \cdot 2xx^3$, which is a valid formula and closes by quantifier elimination with $\mathbb{R}$.

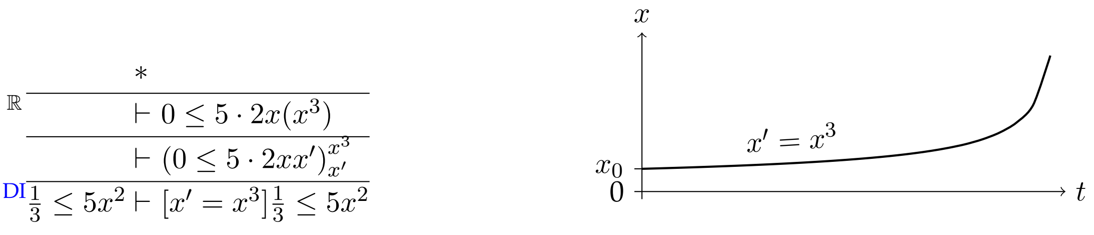
$*$
$\mathbb{R}$
$\vdash 0 \leq 5 \cdot 2x(x^3)$
$\vdash (0 \leq 5 \cdot 2xx')^{x^3}_{x'}$
DI
$\frac{1}{3} \leq 5x^2 \vdash [x' = x^3]\frac{1}{3} \leq 5x^2$
x
$x' = x^3$
x_0
0
t

Figure 1: **a** Cubic dynamics proof 1**b**: Cubic dynamics

Differential invariants that are inequalities are not just a minor variation of equational differential invariants, because they can prove more. That is, it can be shown [Pla12b] that there are valid formulas that can be proved using differential invariant inequalities but cannot be proved just using equations as differential invariants ($\text{DI}_=$). So sometimes, you need to be prepared to look for inequalities that you can use as differential invariants. The converse is not true. Everything that is provable using $\text{DI}_=$ is also provable using differential invariant inequalities [Pla12b], but you should still look for equational differential invariants if they give easier proofs.

Strict inequalities can also be used as differential invariants when defining their total derivatives as:

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

It is easy to see (Exercise 1) that the following slightly relaxed definition would also be sound:

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

Understanding that differential substitution is sound for formulas, i.e. replacing the left-hand side of the differential equation by its right-hand side, requires a few more thoughts now, because the equational differential substitution principle Lemma 4 does not apply directly. The differential substitution principle not only works for terms, however, but also for differential first-order formulas, i.e. first-order formulas in which differential symbols occur:

Lemma 8 (Differential substitution property for differential formulas)**.** *If $\varphi : [0, r] \to \mathcal{S}$ solves the differential equation $x' = \theta$, i.e. $\varphi \models x' = \theta$, then $\varphi \models \mathcal{D} \leftrightarrow \mathcal{D}^{\theta}_{x'}$ for all differential first-order formulas $\mathcal{D}$, i.e. first-order formulas over $\Sigma \cup \Sigma'$.*

Proof. The proof is by using the Substitution Lemma [Pla10b, Lemma 2.2] for first-order logic on the basis of $[\![x']\!]_{\varphi(\zeta)} = [\![\theta]\!]_{\varphi(\zeta)}$ at each time ζ in the domain of φ by Def. 2. □

By Lemma 8, differential equations can always be substituted in along their solutions. Hence, the focus on developing differential invariant proof rules is in defining appropriate total derivatives, since Lemma 8 shows how to handle differential symbols by substitution.

Where do differential first-order formulas come from? They come from the analogue of the total derivation operator on formulas. On formulas, the total derivation operator applies the total derivation operator from Def. 1 to all terms in a first-order formula, yet it also flips disjunctions into conjunctions and existential quantifiers into universal quantifiers.

7 Disequational Differential Invariants

The case that is missing in differential invariant proof rules are for postconditions that are disequalities $\theta \neq \eta$? How can they be proved?

Before you read on, see if you can find the answer for yourself.

By analogy to the previous cases, one might expect the following definition:

$$(\theta \neq \eta)' \overset{?}{\equiv} ((\theta)' \neq (\eta)') \quad ???$$

It is crucial for soundness of differential invariants tha $(\theta \neq \eta)'$ is *not* defined that way! In the following counterexample, variable x can reach $x = 0$ without its derivative ever being 0; again, see Fig. 2 for the dynamics. Of course, just because θ and η start out different, does not mean they would always stay different if they evolve with different derivatives.

$$\lightning\;\dfrac{\dfrac{*\,(\text{unsound})}{\vdash 1 \neq 0}}{x \neq 5 \vdash [x' = 1]x \neq 5}$$

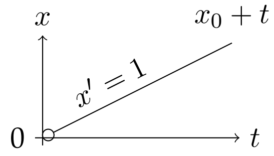

Figure 2: **a** Unsound attempt of using disequalities **2b**: Linear dynamics

Instead, if θ and η start out differently and evolve with the same derivatives, they will always stay different. So the sound definition is slightly unexpected:

$$(\theta \neq \eta)' \equiv ((\theta)' = (\eta)')$$

8 Conjunctive Differential Invariants

The next case to consider is where the invariant that we want to prove is a conjunction $F \wedge G$. Lemma 8 takes care of how to handle differential substitution for the differential equations, if only we define the correct total derivative of $(F \wedge G)'$.

Before you read on, see if you can find the answer for yourself.

To show that a conjunction $F \land G$ is invariant it is perfectly sufficient to prove that both are invariant. This can be justified separately, but is more obvious when recalling the following equivalence from Lecture 7:

$$([]\land)\ [\alpha](\phi \land \psi) \leftrightarrow [\alpha]\phi \land [\alpha]\psi$$

which is valid for all hybrid programs α, also when α is just a differential equation. Consequently, the total derivative of a conjunction is the conjunction of the total derivatives (i.e. $(\cdot)'$ is a homomorphism for $\land$):

$$(F \land G)' \equiv (F)' \land (G)'$$

Again, we will not develop a proper soundness argument, because it will follow from the general differential invariant proof rule.

With a corresponding proof rule that enables us to do the following proof:

$$\text{DI}\,\dfrac{\dfrac{\mathbb{R}\,\dfrac{*}{\vdash 2de + 2e(-d) \leq 0 \land 2de + 2e(-d) \geq 0}}{\vdash (2dd' + 2ee' \leq 0 \land 2dd' + 2ee' \geq 0)_{d'\ e'}^{e\ \ -d}}}{d^2 + e^2 \leq r^2 \land d^2 + e^2 \geq r^2 \vdash [d' = e, e' = -d](d^2 + e^2 \leq r^2 \land d^2 + e^2 \geq r^2)}$$

Since the invariant $d^2 + e^2 \leq r^2 \land d^2 + e^2 \geq r^2$ is easily proved to be equivalent to $d^2 + e^2 = r^2$, the above proof gives yet another proof of (3) when combined with a corresponding use of $[]gen'$.

9 Disjunctive Differential Invariants

The next case to consider is where the invariant that we want to prove is a disjunction $F \lor G$. Lemma 8 takes care of how to handle differential substitution for the differential equations, if only we define the correct total derivative of $(F \lor G)'$. How?

Before you read on, see if you can find the answer for yourself.

The total derivative of a conjunction is the conjunction of the total derivatives. So, by analogy, it might stand to reason to define the total derivative of a disjunction as the disjunction of the total derivatives.

$$(F \lor G)' \overset{?}{\equiv} (F)' \lor (G)' \quad ???$$

Let's try it:

$$\text{↯}\,\dfrac{\dfrac{\mathbb{R}\,\dfrac{\text{unsound}}{\vdash 2de + 2e(-d) = 0 \lor 5d + re \geq 0}}{\vdash (2dd' + 2ee' = 0 \lor r'd + rd' \geq 0)_{d'}^{e}{}_{e'}^{-d}}}{d^2 + e^2 = r^2 \lor rd \geq 0 \vdash [d' = e, e' = -d, r' = 5](d^2 + e^2 = r^2 \lor rd \geq 0)}$$

That would be spectacularly wrong, however, because the formula at the bottom is not actually valid. We have no business of proving formulas that are not valid and if we ever could, we would have found a serious unsoundness in the proof rules.

For soundness of differential induction, it is crucial that Def. 1 defines the total derivative $(F \lor G)'$ of a disjunction conjunctively as $(F)' \land (G)'$ instead of as $(F)' \lor (G)'$. From an initial state ν which satisfies $\nu \models F$, and hence $\nu \models F \lor G$, the formula $F \lor G$ only is sustained differentially if F itself is a differential invariant, not if G is. For instance, $d^2 + e^2 = r^2 \lor rd \geq 0$ is no invariant of the above differential equation, because $rd \geq 0$ will be invalidated if we just follow the circle dynamics long enough. So if the disjunction was true because $rd \geq 0$ was true in the beginning, it does not stay invariant.

In practice, splitting differential induction proofs over disjunctions can be useful if a direct proof with a single differential invariant does not succeed:

$$\rightarrow\!\text{r}\,\dfrac{\lor\text{l}\,\dfrac{[]gen'\,\dfrac{\text{DI}\,\dfrac{\vdash {A'}_{x'}^{\theta}}{A \vdash [x' = \theta]A} \qquad \lor\text{r}\,\dfrac{ax\,\dfrac{*}{A \vdash A, B}}{A \vdash A \lor B}}{A \vdash [x' = \theta](A \lor B)} \qquad []gen'\,\dfrac{\text{DI}\,\dfrac{\vdash {B'}_{x'}^{\theta}}{B \vdash [x' = \theta]B} \qquad \lor\text{r}\,\dfrac{ax\,\dfrac{*}{B \vdash A, B}}{B \vdash A \lor B}}{B \vdash [x' = \theta](A \lor B)}}{A \lor B \vdash [x' = \theta](A \lor B)}}{\vdash A \lor B \to [x' = \theta](A \lor B)}$$

10 Differential Invariants

Differential invariants are a general proof principles for proving invariants of formulas. Summarizing what this lecture has discovered so far leads to a single proof rule for differential invariants. That is why all previous proofs just indicated DI when using the various special cases of the differential invariant proof rule to be developed next.

All previous arguments remain valid when the differential equation has an evolution domain constraint H that it cannot leave by definition. In that case, the inductive proof step can even assume the evolution domain constraint to hold, because the system, by definition, is not allowed to leave it.

Definition 9 (Derivation)**.** The operator $(\cdot)'$ that is defined as follows on first-order real-arithmetic formulas is called *syntactic (total) derivation*:

$$(F \land G)' \equiv (F)' \land (G)' \tag{4a}$$

$$(F \lor G)' \equiv (F)' \land (G)' \tag{4b}$$

$$(\forall x\, F)' \equiv \forall x\, (F)' \tag{4c}$$

$$(\exists x\, F)' \equiv \forall x\, (F)' \tag{4d}$$

$$(a \geq b)' \equiv (a)' \geq (b)' \qquad \text{accordingly for } <, >, \leq, =, \text{but not } \neq \tag{4e}$$

Furthermore, ${F'}^{\theta}_{x'}$ is defined to be the result of substituting θ for x' in F'. The operation mapping F to ${(F)'}^{\theta}_{x'}$ is called *Lie-derivative* of F with respect to $x' = \theta$.

That is, to replace the left-hand side of a differential equation by the right-hand side.

Lemma 10 (Differential invariants)**.** *The differential invariant rule is sound:*

$$\text{(DI)}\ \frac{H \vdash {F'}^{\theta}_{x'}}{F \vdash [x' = \theta \,\&\, H]F} \qquad \text{(DI}')\ \frac{\Gamma \vdash F, \Delta \quad H \vdash {F'}^{\theta}_{x'} \quad F \vdash \psi}{\Gamma \vdash [x' = \theta \,\&\, H]\psi, \Delta}$$

The version DI′ can be derived easily from the more fundamental, essential form DI.

The basic idea behind rule DI is that the premise of DI shows that the total derivative F' holds within evolution domain H when substituting the differential equations $x' = \theta$ into F'. If F holds initially (antecedent of conclusion), then F itself always stays true (succedent of conclusion). Intuitively, the premise gives a condition showing that, within H, the total derivative F' along the differential constraints is pointing inwards or transversally to F but never outwards to $\neg F$; see Fig. 3 for an illustration. Hence, if we start in F and, as indicated by F', the local dynamics never points outside F, then the system always stays in F when following the dynamics. Observe that, unlike F', the premise of DI is a well-formed formula, because all differential expressions are replaced by non-differential terms when forming ${F'}^{\theta}_{x'}$.

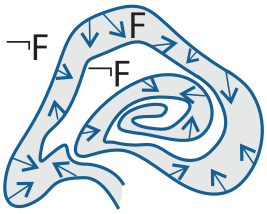

Figure 3: Differential invariant F for safety

Proof. Assume the premise ${F'}^{\theta}_{x'} = 0$ to be valid, i.e. true in all states. In order to prove that the conclusion $F \vdash [x' = \theta]F$ is valid, consider any state ν. Assume that $\nu \models F$, as there is otherwise nothing to show (sequent is trivially *true* since antecedent evaluates to *false*). If $\zeta \in [0,r]$ is any time during any solution $\varphi : [0,r] \to \mathcal{S}$ of any duration $r \in \mathbb{R}$ of $x' = \theta$ beginning in initial state $\varphi(0) = \nu$, then it remains to be shown that $\varphi(r) \models F$. By antecedent, $\nu \models F$, in the initial state $\nu = \varphi(0)$.

If the duration of φ is $r = 0$, we have $\varphi(0) \models F$ immediately, because $\nu \models F$. For duration $r > 0$, we show that F holds all along φ, i.e., $\varphi(\zeta) \models F$ for all $\zeta \in [0,r]$.

We have to show that $\nu \models F \to [x' = \theta \,\&\, H]F$ for all states ν. Let ν satisfy $\nu \models F$ as, otherwise, there is nothing to show. We can assume F to be in disjunctive normal form and consider any disjunct G of F that is true at ν. In order to show that F remains true during the continuous evolution, it is sufficient to show that each conjunct of G is. We can assume these conjuncts to be of the form $\eta \geq 0$ (or $\eta > 0$ where the proof is accordingly). Finally, using vectorial notation, we write $x' = \theta$ for the differential equation system. Now let $\varphi : [0,r] \to (V \to \mathbb{R})$ be any solution of $x' = \theta \,\&\, H$ beginning in $\varphi(0) = \nu$. If the duration of φ is $r = 0$, we have $\varphi(0) \models \eta \geq 0$ immediately, because $\nu \models \eta \geq 0$. For duration $r > 0$, we show that $\eta \geq 0$ holds all along the solution φ, i.e., $\varphi(\zeta) \models \eta \geq 0$ for all $\zeta \in [0,r]$.

Suppose there was a $\zeta \in [0,r]$ with $\varphi(\zeta) \models \eta < 0$, which will lead to a contradiction. The function $h : [0,r] \to \mathbb{R}$ defined as $h(t) = [\![\eta]\!]_{\varphi(\zeta)}$ satisfies the relation $h(0) \geq 0 > h(\zeta)$, because $h(0) = [\![\eta]\!]_{\varphi(0)} = [\![\eta]\!]_{\nu}$ and $\nu \models \eta \geq 0$ by antecedent of the conclusion. By Lemma 3, h is continuous on $[0,r]$ and differentiable at every $\xi \in (0,r)$. By mean value theorem, there is a $\xi \in (0,\zeta)$ such that $\frac{\mathrm{d}h(t)}{\mathrm{d}t}(\xi) \cdot (\zeta - 0) = h(\zeta) - h(0) < 0$. In particular, since $\zeta \geq 0$, we can conclude that $\frac{\mathrm{d}h(t)}{\mathrm{d}t}(\xi) < 0$. Now Lemma 3 implies that $\frac{\mathrm{d}h(t)}{\mathrm{d}t}(\xi) = [\![(\eta)']\!]_{\varphi(\xi)} < 0$. This, however, is a contradiction, because the premise implies that the formula $H \to (\eta \geq 0)'$ is true in all states along φ, including $\varphi(\xi) \models H \to (\eta \geq 0)'$. In particular, as φ is a solution for $x' = \theta \,\&\, H$, we know that $\varphi(\xi) \models H$ holds, and we have $\varphi(\xi) \models (\eta \geq 0)'$, which contradicts $[\![(\eta)']\!] < 0$. □

This proof rule enables us to prove (2) easily in d$\mathcal{L}$'s sequent calculus and all previous proofs as well:

$$\begin{array}{rc}
 & * \\ \cline{2-2}
\mathbb{R} & \vdash 2de + 2e(-d) \leq 0 \\ \cline{2-2}
 & \vdash (2dd' + 2ee' \leq 2rr')_{d'}^{e}{}_{e'}^{-d}{}_{r'}^{-0} \\ \cline{2-2}
\text{DI} & d^2 + e^2 \leq r^2 \vdash [d' = e, e' = -d]d^2 + e^2 \leq r^2 \\ \cline{2-2}
{\to}\text{r} & \vdash d^2 + e^2 \leq r^2 \to [d' = e, e' = -d]d^2 + e^2 \leq r^2
\end{array}$$

11 Example Proofs

Example 11 (Quartic dynamics). The following simple d$\mathcal{L}$ proof uses DI to prove an invariant of a quartic dynamics.

$$\text{DI}\,\dfrac{\dfrac{\mathbb{R}\,\dfrac{*}{a \geq 0 \vdash 3x^2((x-3)^4+a) \geq 0}}{a \geq 0 \vdash (3x^2x' \geq 0)_{x'}^{(x-3)^4+a}}}{x^3 \geq -1 \vdash [x' = (x-3)^4 + a \,\&\, a \geq 0]x^3 \geq -1}$$

Observe that rule DI directly makes the evolution domain constraint $a \geq 0$ available as an assumption in the premise, because the continuous evolution is never allowed to leave it.

Example 12. Consider the dynamics $x' = y, y' = -\omega^2 x - 2d\omega y$ of the damped oscillator with the undamped angular frequency ω and the damping ratio d. See Fig. 4 for one example of an evolution along this continuous dynamics. Figure 4 shows a trajectory in the x, y space on the left, and an evolution of x over time t on the right. General symbolic solutions of symbolic initial-value problems for this differential equation can become surprisingly difficult. Mathematica, for instance, produces a long equation of exponentials that spans 6 lines of terms just for one solution. A differential invariant proof, instead, is very simple:

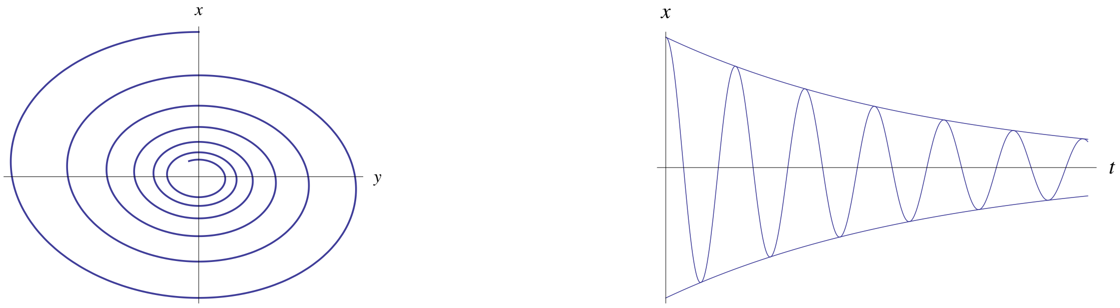

Figure 4: Trajectory and evolution of a damped oscillator

$$\text{DI}\,\dfrac{\dfrac{\mathbb{R}\,\dfrac{*}{\omega \geq 0 \land d \geq 0 \vdash 2\omega^2 xy - 2\omega^2 xy - 4d\omega y^2 \leq 0}}{\omega \geq 0 \land d \geq 0 \vdash (2\omega^2 x x' + 2yy' \leq 0)_{x'\;y'}^{y\;-\omega^2 x - 2d\omega y}}}{\omega^2 x^2 + y^2 \leq c^2 \vdash [x' = y, y' = -\omega^2 x - 2d\omega y \,\&\, (\omega \geq 0 \land d \geq 0)]\,\omega^2 x^2 + y^2 \leq c^2}$$

Observe that rule DI directly makes the evolution domain constraint $\omega \geq 0 \land d \geq 0$ available as an assumption in the premise, because the continuous evolution is never allowed to leave it.

12 Assuming Invariants

Let's make the dynamics more interesting and see what happens. Suppose there is a robot at a point with coordinates (x, y) that is facing in direction (d, e). Suppose the robot moves with constant (linear) velocity into direction (d, e), which is rotating as before. Then the corresponding dynamics is:

$$x' = d, y' = e, d' = e, e' = -d$$

because the derivative of the x coordinate is the component d of the direction and the derivative of the y coordinate is the component e of the direction. If the rotation of the direction (d, e) is faster or slower, the differential equation would be formed correspondingly. Consider the following conjecture:

$$(x-1)^2 + (y-2)^2 \geq p^2 \rightarrow [x' = d, y' = e, d' = e, e' = -d](x-1)^2 + (y-2)^2 \geq p^2 \quad (5)$$

This conjecture expresses that the robot at position (x, y) will always stay at distance p from the point $(1, 2)$ if it started there. Let's try to prove conjecture (5):

$$\text{DI}\,\dfrac{\dfrac{\vdash 2(x-1)d + 2(y-2)e \geq 0}{\vdash (2(x-1)x' + 2(y-2)y' \geq 0)_{x'}^{d}{}_{y'}^{e}}}{(x-1)^2 + (y-2)^2 \geq p^2 \vdash [x' = d, y' = e, d' = e, e' = -d](x-1)^2 + (y-2)^2 \geq p^2}$$

Unfortunately, this differential invariant proof does not work. As a matter of fact, *fortunately* it does not work out, because conjecture (5) is not valid, so we will, fortunately, not be able to prove it with a sound proof technique. Conjecture (5) is too optimistic. Starting from some directions far far away, the robot will most certainly get too close to the point (1,2). Other directions may be fine.

Inspecting the above failed proof attempt, we could prove (5) if we knew something about the directions (d, e) that would make the remaining premise prove. What could that be?

Before you read on, see if you can find the answer for yourself.

Certainly, if we knew $d = e = 0$, the resulting premise would prove. Yet, that case is pretty boring because it corresponds to the point (x, y) being stuck forever. A more interesting case in which the premise would easily prove is if we knew $x - 1 = -e$ and $y - 2 = d$. In what sense could we "know" $x - 1 = -e \land y - 2 = d$? Certainly, we would have to assume this compatibility condition for directions versus position is true in the initial state, otherwise we would not necessarily know the condition holds true where we need it. So let's modify (5) to include this assumption:

$$x - 1 = -e \land y - 2 = d \land (x-1)^2 + (y-2)^2 \geq p^2 \rightarrow \\ [x' = d, y' = e, d' = e, e' = -d](x-1)^2 + (y-2)^2 \geq p^2 \quad (6)$$

Yet, where we need to know $x - 1 = -e \land y - 2 = d$ for the above sequent prove to continue is in the middle of the inductive step. How could we make that happen?

Before you read on, see if you can find the answer for yourself.

One step in the right direction is to convince ourselves that $x - 1 = -e \land y - 2 = d$ is a differential invariant of the dynamics, so it holds always if it held in the beginning:

$$\text{DI}\,\dfrac{\dfrac{\mathbb{R}\,\dfrac{*}{\vdash d = -(-d) \land e = e}}{\vdash (x' = -e' \land y' = d')_{x'}^{d}{}_{y'}^{e}{}_{d'}^{e}{}_{e'}^{-d}}}{x - 1 = -e \land y - 2 = d \vdash [x' = d, y' = e, d' = e, e' = -d](x - 1 = -e \land y - 2 = d)}$$

This proves easily using differential invariants.

Now, how can this freshly proved invariant $x - 1 = -e \land y - 2 = d$ be made available in the previous proof? Perhaps we could consider the conjunction of the invariant we want with the invariant we need:

$$(x-1)^2 + (y-2)^2 \geq p^2 \land x - 1 = -e \land y - 2 = d$$

That does not work (eliding the antecedent in the conclusion just for space reasons)

$$\text{DI}\,\dfrac{\dfrac{\vdash 2(x-1)d + 2(y-2)e \geq 0 \land d = -(-d) \land e = e}{\vdash (2(x-1)x' + 2(y-2)y' \geq 0 \land x' = -e' \land y' = d')_{x'}^{d}{}_{y'}^{e}{}_{d'}^{e}{}_{e'}^{-d}}}{x - 1 = -e \ldots \vdash [x' = d, y' = e, d' = e, e' = -d]((x-1)^2 + (y-2)^2 \geq p^2 \land x - 1 = -e \land y - 2 = d)}$$

because the differential invariant proof rule DI does not make the invariant F available in the antecedent of the premise.

In the case of loops, invariants can be assumed to hold before the loop body in the induction step.

$$(ind)\quad \dfrac{F \vdash [\alpha]F}{F \vdash [\alpha^*]F}$$

By analogy, we could augment the differential invariant proof rule DI similarly to include F in the assumptions. Is that a good idea?

Before you read on, see if you can find the answer for yourself.

It looks tempting to suspect that rule DI could be improved by assuming the differential invariant F in the antecedent of the premise:

$$(DI_{??})\ \frac{H \land F \vdash {F'}_{x'}^{\theta}}{F \vdash [x' = \theta \,\&\, H]F} \quad \text{sound?}$$

After all, we really only care about staying safe when we are still safe. But implicit properties of differential equations are a subtle business. Assuming F like in rule $DI_{??}$ would, in fact, be unsound, as the following simple counterexample shows, which "proves" an invalid property using the unsound proof rule $DI_{??}$:

$$\lightning\ \dfrac{\dfrac{\dfrac{* \text{ (unsound)}}{\vdash -(x-y)^2 \geq 0 \rightarrow -2(x-y)(1-y) \geq 0}}{\vdash -(x-y)^2 \geq 0 \rightarrow (-2(x-y)(x'-y') \geq 0)_{x'}^{1}{}_{y'}^{y}}}{-(x-y)^2 \geq 0 \vdash [x' = 1, y' = y](-(x-y)^2 \geq 0)}$$

Assuming an invariant of a differential equation during its own proof is, thus, incorrect, even though it has been suggested numerous times in the literature. There are some cases for which rule $DI_{??}$ would be sound, but these are nontrivial [Pla10a, Pla12b, Pla12a].

13 Differential Cuts

Instead, there is a complementary proof rule for *differential cuts* [Pla10a, Pla08, Pla12b, Pla12a] that can be used to strengthen assumptions in a sound way:

$$(\text{DC})\ \frac{\Gamma \vdash [x' = \theta \,\&\, H]C, \Delta \qquad \Gamma \vdash [x' = \theta \,\&\, (H \land C)]F, \Delta}{\Gamma \vdash [x' = \theta \,\&\, H]F, \Delta}$$

The differential cut rule works like a cut, but for differential equations. In the right premise, rule DC restricts the system evolution to the subdomain $H \land C$ of H, which changes the system dynamics but is a pseudo-restriction, because the left premise proves that C is an invariant anyhow (e.g. using rule DI). Note that rule DC is special in that it changes the dynamics of the system (it adds a constraint to the system evolution domain region), but it is still sound, because this change does not reduce the reachable set. The benefit of rule DC is that C will (soundly) be available as an extra assumption for all subsequent DI uses on the right premise (see, e.g., the use of the evolution domain constraint in Example 12). In particular, the differential cut rule DC can be used to strengthen the right premise with more and more auxiliary differential invariants C that will be available as extra assumptions on the right premise, once they have been proven to be differential invariants in the left premise.

Proving (6) in a sound way is now easy using a differential cut DC by $x - 1 = -e \land y - 2 = d$:

$$\text{DC}\,\dfrac{\text{DI}\,\dfrac{\dfrac{\mathbb{R}\,\dfrac{*}{\vdash d=-(-d)\land e=e}}{\vdash (x'=-e'\land y'=d')^{d}_{x'}{}^{e}_{y'}{}^{e}_{d'}{}^{-d}_{e'}}}{x{-}1{=}..\vdash [x'=d,\dots](x{-}1{=}{-}e{\land}y{-}2{=}d)} \qquad \text{DI}\,\dfrac{\dfrac{\mathbb{R}\,\dfrac{*}{x{-}1{=}{-}e\land y{-}2{=}d\vdash 2(x-1)d+2(y-2)e\geq 0}}{x{-}1{=}{-}e\land y{-}2{=}d\vdash (2(x-1)x'+2(y-2)y'\geq 0)^{d}_{x'}{}^{e}_{y'}}}{(x{-}1)^2{+}(y{-}2)^2{\geq}p^2\vdash [x'=d,y'=e,d'=e,e'=-d\,\&\,x{-}1{=}{-}e{\land}y{-}2{=}d](x{-}1)^2{+}(y{-}2)^2{\geq}p^2}}{(x{-}1)^2{+}(y{-}2)^2{\geq}p^2{\land}x{-}1{=}{-}e{\land}y{-}2{=}d\vdash [x'=d,y'=e,d'=e,e'=-d](x-1)^2+(y-2)^2\geq p^2}$$

Using this differential cut process repeatedly has turned out to be extremely useful in practice and even simplifies the invariant search, because it leads to several simpler properties to find and prove instead of a single complex property [PC08, PC09, Pla10b].

Proof of Soundness of DC. For simplicity, consider only the case where $H \equiv \mathit{true}$. Rule DC is sound using the fact that the left premise implies that every solution φ that satisfies $x' = \theta$ also satisfies C *all along* the solution. Thus, if solution φ satisfies $x' = \theta$, it also satisfies $x' = \theta \,\&\, C$, so that the right premise entails the conclusion. The proof is accordingly for the case □

14 Differential Weakening

One simple but computable proof rule is *differential weakening*:

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

This rule is obviously sound, because the system $x' = \theta \,\&\, H$, by definition, can never leave H, hence, if H implies F (i.e. the region H is contained in the region F), then F is an invariant, no matter what $x' = \theta$ does. Unfortunately, this simple proof rule cannot prove very interesting properties, because it only works when H is very informative. It can, however, be useful in combination with stronger proof rules (e.g., differential cuts).

15 Summary

This lecture introduced very powerful proof rules for differential invariants, with which you can prove even complicated properties of differential equations in easy ways. Just like in the case of loops, where the search for invariants is nontrivial, differential invariants also require some smarts (or good automatic procedures) to be found. Yet, once a differential invariant has been identified, the proof follows easily.

Note 10 (Proof rules for differential equations)**.**

$$\text{(DI)}\ \frac{H \vdash {F'}^{\theta}_{x'}}{F \vdash [x' = \theta \,\&\, H]F} \qquad \text{(DW)}\ \frac{H \vdash F}{\Gamma \vdash [x' = \theta \,\&\, H]F, \Delta}$$

$$\text{(DC)}\ \frac{\Gamma \vdash [x' = \theta \,\&\, H]C, \Delta \qquad \Gamma \vdash [x' = \theta \,\&\, (H \land C)]F, \Delta}{\Gamma \vdash [x' = \theta \,\&\, H]F, \Delta}$$

Exercises

Exercise 1. We have chosen to define

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

Prove that the following slightly relaxed definition would also give a sound proof rule for differential invariants:

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

Exercise 2. We have defined

$$(\theta \neq \eta)' \equiv ((\theta)' = (\eta)')$$

Suppose you remove this definition 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?

References

[PC08] André Platzer and Edmund M. Clarke. Computing differential invariants of hybrid systems as fixedpoints. In Aarti Gupta and Sharad Malik, editors, *CAV*, volume 5123 of *LNCS*, pages 176–189. Springer, 2008. doi:10.1007/978-3-540-70545-1_17.

[PC09] André Platzer and Edmund M. Clarke. Computing differential invariants of hybrid systems as fixedpoints. *Form. Methods Syst. Des.*, 35(1):98–120, 2009. Special issue for selected papers from CAV'08. doi:10.1007/s10703-009-0079-8.

[Pla08] André Platzer. *Differential Dynamic Logics: Automated Theorem Proving for Hybrid Systems*. PhD thesis, Department of Computing Science, University of Oldenburg, Dec 2008. Appeared with Springer.

[Pla10a] André Platzer. Differential-algebraic dynamic logic for differential-algebraic programs. *J. Log. Comput.*, 20(1):309–352, 2010. doi:10.1093/logcom/exn070.

[Pla10b] André Platzer. *Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics*. Springer, Heidelberg, 2010. doi:10.1007/978-3-642-14509-4.

[Pla12a] André Platzer. A differential operator approach to equational differential invariants. In Lennart Beringer and Amy Felty, editors, *ITP*, volume 7406 of *LNCS*, pages 28–48. Springer, 2012. doi:10.1007/978-3-642-32347-8_3.

[Pla12b] André Platzer. The structure of differential invariants and differential cut elimination. *Logical Methods in Computer Science*, 8(4):1–38, 2012. doi:10.2168/LMCS-8(4:16)2012.